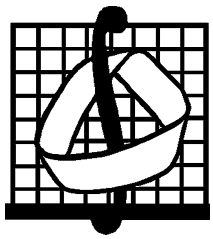
МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М. В. ЛОМОНОСОВА



МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

МАТЕРИАЛЫ

XI Международного семинара

«ДИСКРЕТНАЯ МАТЕМАТИКА И ЕЕ ПРИЛОЖЕНИЯ»,

посвященного 80-летию со дня рождения академика О. Б. ЛУПАНОВА

(Москва, 18–23 июня 2012 г.)

Издательство механико-математического факультета МГУ

Москва 2012

М34
УДК 519.7

Издание осуществлено при поддержке Российского фонда фундаментальных исследований по проекту 12–01–06040

М34 Материалы XI Международного семинара «Дискретная математика и ее приложения», посвященного 80-летию со дня рождения академика О. Б. Лупанова (Москва, МГУ, 18–23 июня 2012 г.) / Под редакцией О. М. Касим-Заде. — М.: Изд-во механико-математического факультета МГУ, 2012. — 453 с.

Сборник содержит материалы XI Международного семинара «Дискретная математика и ее приложения», посвященного 80-летию со дня рождения академика О. Б. Лупанова, проходившего на механико-математическом факультете МГУ имени М. В. Ломоносова с 18 по 23 февраля 2012 г. при поддержке Российского фонда фундаментальных исследований (проект 12–01–06040). Для студентов, аспирантов и научных работников в области дискретной математики и математической кибернетики.

Научное издание

МАТЕРИАЛЫ
XI МЕЖДУНАРОДНОГО СЕМИНАРА
«ДИСКРЕТНАЯ МАТЕМАТИКА И ЕЕ ПРИЛОЖЕНИЯ»,
посвященного 80-летию со дня рождения академика О. Б. Лупанова
(Москва, МГУ, 18–23 июня 2012 г.)

Под общей редакцией О. М. КАСИМ-ЗАДЕ

Редакционная группа:
О. С. Дудакова, К. А. Зыков, Р. М. Колпаков, В. В. Кочергин, А. В. Чашкин

Ответственный за выпуск *В. В. Кочергин*

Н/К
ИД № 04059 от 20.02.2001 Подписано к печати 02.08.2012. Формат 60 × 90/16.
Бумага типогр. № 1. Печ. л. 28,5. Тираж 200 экз.
Издательство механико-математического факультета МГУ. 119991, Москва, Ленинские горы, МГУ.
Отпечатано с оригинал-макета в типографии «11-й ФОРМАТ», Москва

ПРЕДИСЛОВИЕ

XI Международный семинар «Дискретная математика и ее приложения», посвященный 80-летию со дня рождения академика О. Б. Лупанова, проходил на механико-математическом факультете МГУ имени М. В. Ломоносова с 18 по 23 июня 2012 г. при поддержке Российского фонда фундаментальных исследований (проект 12–01–06040–г).

Оргкомитетом семинара до начала его работы были разосланы информационные письма в ведущие научные центры и университеты стран СНГ, отобраны наиболее интересные доклады и сообщения для заслушивания на пленарных и секционных заседаниях.

Семинар собрал более 200 участников (в том числе более 50 докторов наук) из 40 научных центров России, Беларуси, Украины и Молдовы.

Работа семинара проходила в семи секциях:

— синтез, сложность и надежность управляющих систем,

— теория функциональных систем,

— комбинаторный анализ,

— теория графов,

— математическая теория интеллектуальных систем,

— дискретная геометрия,

— теория кодирования и математические вопросы теории защиты информации.

Всего было заслушано 15 пленарных и 165 секционных докладов; содержание большинства из них отражено в настоящем сборнике.

Тексты публикуются в авторской редакции (исправлены замеченные опечатки).

ПЛЕНАРНЫЕ ДОКЛАДЫ

О НОВЫХ ПРИМЕНЕНИЯХ АРИФМЕТИКИ В КРИПТОГРАФИИ

М. П. Минеев, В. Н. Чубариков (Москва)

Светлой памяти
дорогого Олега Борисовича Лупанова

Введение. В последние полвека криптография пережила период своего существенного обновления, связанного, в первую очередь, со следующими факторами.

Во-первых, бурное развитие в начале 60-х годов прошлого века *электронной вычислительной техники* и ее широкое использование привело к постановке задачи *защиты компьютерной информации*.

Во-вторых, задача защиты переписки от несанкционированного доступа стала *массовой*, что потребовало разработки новых методов защиты информации.

Шифрование информации решает одну из основных задач криптографии: *обеспечение конфиденциальности данных при передаче информации*.

В основе шифрования лежат *криптографические алгоритмы*. Приведем основные их типы.

бесключевые	одноключевые	двухключевые
	алгоритмы симметричного шифрования	алгоритмы асимметричного шифрования
хэш-функция	хэш-функция	алгоритмы электронной подписи
генераторы случайных чисел	генераторы псевдослучайных чисел	
	алгоритмы аутентификации	алгоритмы аутентификации

Напомним, что *ключом криптографического алгоритма* называется конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования, обеспечивающее выбор

одного преобразования из совокупности возможных преобразований для данного алгоритма. Ключи бывают двух типов: секретные, известные только законным пользователям, и открытые, обычно публикуемые в соответствующих справочниках и известные любому пользователю. Также и каналы связи могут быть секретными и открытыми.

Далее, *хэш-функцией* называют выполнение "свертки" данных переменной длины в последовательность знаков фиксированного размера.

В современной "гражданской" криптографии различают две ветви развития: классическую традиционную криптографию, связанную с "симметричным" шифрованием и "асимметричную" криптографию. Понятие симметрии и асимметрии связано с использованием *ключей* при шифровании и дешифровании информации.

1. Шифры классической криптографии. Как известно, "работа симметричных шифров включает в себя два преобразования: $c = E_k(m)$ и $m = D_k(c)$, где m — открытый текст, E — шифрующая функция, D — расшифровывающая функция, k — секретный ключ, c — шифртекст".

Тип преобразования $E_k(m)$ открытого текста используется в качестве первичного признака, по которому производится классификация шифров. Имеются следующие три класса шифров:

- шифры замены;
- шифры перестановки;
- композиционные шифры.

1.1. Постановка задачи искажения частот в шифре простой замены. Большое распространение получили поточные шифры простой замены. Эти шифры можно рассматривать как подстановку, в которой верхняя строка является множеством значений шифрвеличины, а нижняя — множеством шифробозначений. Это означает, что для дешифрования текста следует знать эту подстановку. При этом предполагается, что происходит взаимно однозначное отображение алфавита $\mathcal{A}$ открытого текста в алфавит $\mathcal{B}$ зашифрованного текста.

Задача состоит в том, *как не зная подстановки, по шифртексту восстановить открытый текст?* Уже в 1-м тысячелетии нашей эры арабы заметили, что для одного и того же языка частота встречаемости букв в различных текстах будет примерно одна и та же. Тогда решение задачи может быть сформулировано в следующем виде.

Если в шифртексте некоторый знак Δ появляется с той же частотой, как и буква a открытого текста, то это означает, что буква a открытого текста зашифрована знаком Δ.

Согласно закону больших чисел частота появления любой буквы в достаточно длинном тексте некоторой спецификации при дополнительной гипотезе о независимости появления каждой буквы является устойчивой характеристикой. Опыт показывает, что с определенной точностью этот закон справедлив для реальных открытых текстов (например, текстов литературных произведений прозы). Поэтому составлены таблицы частот появления букв в текстах для разных языков мира.

Как было отмечено ранее, более существенно то, что в шифре простой замены частотные характеристики появления букв первоначального текста совпадают с частотными характеристиками зашифрованного текста. Это обстоятельство позволяет производить их расшифровку без знания ключа.

Первое, дошедшее до нас, описание подобного частотного метода криптоанализа относится к IX веку [27, с. 30–32]. Оно принадлежит известному "философу арабского мира" Абу Юсуф Якуб ибн Исхак ибн ас-Сабах ибн Умран ибн Исмаил аль-Кинди. Его знаменитый трактат "Рукопись по дешифрованию криптографических сообщений" был открыт в 1987 г. в Стамбуле в оттоманском архиве Сулайманийа.

Еще на одно обстоятельство обращено внимание в учебнике [2, с. 106], что для открытых текстов с "почти равномерным" распределением частот появления знаков, зашифрованных с помощью шифра простой замены, задача об их расшифровке становится практически не решаемой. Там же указано, что методы "рандомизации" и "сжатия" открытых текстов позволяют значительно усложнить задачу вскрытия шифра простой замены.

Тем самым, там сформулирована задача *о преобразовании текстов, зашифрованных с помощью шифра простой замены, так, чтобы изменилась частота появления букв в зашифрованном тексте.*

1.2. Метод искажения знаков в шифре простой замены с помощью возведения в квадрат. Далее излагается подход, предложенный авторами этого сообщения [18]. Пусть задан открытый текст T_o русским алфавитом $\mathcal{A}_{31}$, состоящем из 31 буквы. Обозначим буквой σ шифрующую подстановку, переводящую текст T_o в зашифрованный текст $T_{\text{Ш}}$.

Далее буквы русского алфавита заменяются натуральными числами от 0 до 30 по следующему правилу. Эти числа рассматриваем как вычеты по модулю 31 и распределяем их в два класса. В первый класс $K_{\text{Н}}$ относим квадратичные невычеты по модулю 31, а во второй класс $K_{\text{В}}$ — квадратичные вычеты и нуль.

Затем располагаем буквы алфавита $\mathcal{A}$ в порядке убывания час-

тот их появления в тексте. Первым 15 буквам присваиваем значения квадратичных невычетов из $K_{\text{Н}}$, а остальным 16 буквам — значения квадратичных вычетов и нуля из $K_{\text{В}}$. Записываем текст T_o с помощью замены русского алфавита на указанные выше числа. Получим шифртекст $T_{\text{Ш}}$.

Для расшифрования нам понадобится двоичное число m, которое составляется следующим образом. В тексте $T_{\text{Ш}}$ на месте квадратичного невычета ставим цифру 1, а на остальных местах — цифру 0.

Наконец, каждый квадратичный невычет а $T_{\text{Ш}}$ заменяем квадратом по модулю 31 из промежутка от нуля до 30. Таким образом получен новый шифртекст $T'_{\text{Ш}}$, алфавит которого состоит из 16 букв. Это значит, что статистика частот появления символов изменена. Найденный шифртекст $T'_{\text{Ш}}$ и число m передаются абоненту, причем для передачи числа m по открытому каналу связи можно, например, использовать алгоритм Шамира.

Для расшифровки текста $T'_{\text{Ш}}$ и получения текста $T_{\text{Ш}}$ на местах в числе m, отмеченных 1, соответствующий квадратичный вычет извлечением квадратного корня заменяем квадратичным невычетом по модулю 31.

Так как простое число 31 сравнимо с 3 по модулю 4, то при извлечении квадратного корня получим два решения: одно будет квадратичным невычетом по модулю 31, а другое квадратичным вычетом. Решения сравнения $x^2 \equiv t \pmod{31}$ будут иметь вид $x \equiv \pm t^8 \pmod{31}$, а невычет определяется с помощью критерия Эйлера $\left(\frac{x}{31}\right) \equiv x^{15} \pmod{31}$.

2. Асимметричные шифры. При симметричном шифровании абоненты при переписке должны иметь копию общего секретного ключа. При открытом асимметричном шифровании используются два ключа. Один из которых является открытым, а второй — секретным ключом. Открытый ключ абонента A может быть опубликован и всякий, кто хочет послать секретное сообщение абоненту A может зашифровать его с помощью опубликованного ключа, в то время, как прочитать его может только абонент A с помощью секретного ключа, известного только ему. Первое сообщение о шифровании с открытым ключом появилось в 1976 г. в работе Диффи и Хеллмана “Новые направления в криптографии”.

Идея криптографии с открытым ключом тесно связана с понятием однонаправленной (односторонней) функции. Строго однонаправленной функцией называют взаимно-однозначное отображение $f : X \to Y$ с условием, что существует “эффективный” метод вычисления значения $f(x)$ для всех $x \in X$, но не существует “эффек-

тивного" метода для нахождения x из соотношения $y = f(x)$ для любого $y \in f(X)$.

Отметим, что первая и наиболее успешная криптосистема с открытым ключом — RSA, появилась в 1977 г.

Основные преимущества асимметричного шифрования состоят в том, что его можно использовать для большого числа абонентов (банковские и финансовые поручения, цифровые подписи и заказы), для решения проблемы распределения ключей. Н. Смарт [28] отмечает также, что в основе алгоритмов шифрования с открытым ключом лежит на удивление мало идей. Малое количество идей связано с трудностью построения односторонней функции. К таким функциям относятся те, которые возникают в задачах о разложении натуральных чисел на простые сомножители, о вычислении дискретного логарифма (индекса вычета по некоторому модулю) и нахождение корней квадратных по составным модулям.

На наш взгляд о месте асимметричного шифрования достаточно определенно сказано в следующей цитате: "Асимметричные системы шифрования обеспечивают значительно меньшие скорости шифрования, нежели симметричные, в силу чего они обычно используются не столько для шифрования сообщений, сколько для шифрования пересылаемых между корреспондентами ключей, которые затем используются в симметричных системах" [2].

2.1. Разложение на простые сомножители. Задача о разложении на простые сомножители натурального числа доставляет достаточно сложную одностороннюю функцию.

В криптографии используются, например, натуральные числа, имеющие всего два различных простых сомножителя. Наиболее известными способами разложения таких чисел на простые сомножители являются следующие.

Пробное деление, решето Эратосфена. Проверяется для всех простых p, не превосходящих корня квадратного разлагаемого на простые сомножители числа N, что N/p является целым числом.

Метод эллиптической кривой. Эффективен для сильно отличающихся друг от друга простых сомножителей.

2.2. Квадратичные вычеты по составному модулю. RSA. Дискретный логарифм. С задачей о разложении $N = pq$, где p и q — простые числа тесно связаны следующие задачи.

Задача RSA. Даны числа N, C, E, где $(E, \varphi(N)) = 1$, $E < \varphi(N)$, $C < N$, причем неизвестно разложение числа N на простые сомножители. Найти натуральное число $m < N$ такое, что $m^E \equiv C \pmod{N}$.

Проверка числа на квадратичный вычет. Пусть неизвестно разложение числа N на простые сомножители. Проверить, будет ли дан-

ное число A квадратичным вычетом по модулю N. В случае положительного ответа решить квадратное сравнение $x^2 \equiv A \pmod N$.

Можно показать, что задача RSA не сложнее задачи разложения числа на простые сомножители. Предполагают, что последняя задача на самом деле сложнее.

Ограничимся только постановкой задач.

Пусть G — мультипликативная группа поля или эллиптическая кривая над конечным полем. Тогда задача дискретного логарифмирования состоит в том, чтобы для любого y из G найти натуральное число x такое, что $g^x = y$, где g — образующая группы G.

Близкой к ней и не более сложной является задача Диффи – Хеллмана, которая состоит в том, чтобы по заданным элементам $A, B = A^x, C = A^y$ из G найти $D = A^{xy}$ из G.

2.3. Вычислительно-сложные задачи теории чисел в криптографии. К сожалению, на сегодняшний день строгого математического доказательства "сложности" той или иной теоретико-числовой задачи не найдено. Тем не менее, существуют несколько утверждений, сравнивающих их сложность между собой, т. е. утверждения типа, что одна задача сложнее другой.

Здесь мы не будем обсуждать проблему сложности задачи, но только приведем список "сложных" задач в виде таблицы.

	Задача	Дано	Найти
1	Разл.на мн.	натур.число n	$\prod\limits_{p\mid n} p^\alpha = n$
2	RSA	$n(=pq), c \in \mathbf{N}$, $e : (e, \varphi(n)) = 1$	$m : m^e \equiv c \pmod n$
3	кв.выч.	$a : \left(\frac{a}{n}\right) = 1$	$a -$ кв.выч. $\pmod n$
4	кв.корень	$a -$ кв.выч. $\pmod n$	$x : x^2 \equiv a \pmod n$
5	дискр.лог.	$g -$ перв.кор.p, a	$x : g^x \equiv a \pmod p$
6	гр.диск.лог.	$G -$ кон.цикл.гр.	$x : g^x = a$
7	Диффи-Хеллман	$A \equiv g^a \pmod p$, $B \equiv g^b \pmod p$	$C : C \equiv g^{ab} \pmod p$
8	Диффи-Хеллман	$G -$ цикл.гр., $A = g^a, B = g^b$	$C : C = g^{ab}$
9	Диффи-Хеллман	$A \equiv g^a, B \equiv g^b \pmod p$ $C \equiv g^c \pmod p$	$g^{ab} \equiv C \pmod p$
10	О рюкзаке	$a_1, \ldots, a_n \in \mathbf{N}$	$\sum a_{k_l} = n$

3. Об одном применении китайской теоремы об остатках к шифру Виженера. Здесь дан арифметический подход к констру-

ированию известного многоалфавитного шифра Виженера, который можно рассматривать как обобщение одноалфавитного шифра простой замены или как шифр гаммирования с периодической гаммой (см., например, [5, с. 151–152]).

Пусть количество символов алфавита равно составному числу n. Каждому символу $\alpha_r, r = 1, \ldots, n$, алфавита присваивается некоторый вычет a_r по модулю n, причем различным символам отвечают различные вычеты. Пусть, также, число n представимо в виде $n = dq, (d, q) = 1, d > 1, q > 1$. Например, $n = 35 = dq = 5 \cdot 7$ или $n = 36 = 4 \cdot 9$.

Тогда можно предложить следующий способ шифрования.

3.1. Предварительные преобразования. Представим каждое число $1 \leq a \leq n$ в виде

$$a \equiv qb + dc \pmod{n}, \tag{1}$$

где $1 \leq b \leq d, 1 \leq c \leq q$. Тогда по китайской теореме об остатках вычет a по модулю n однозначно определяет вычеты b по модулю d и c по модулю q и наоборот.

Составим две таблицы Виженера, отвечающие вычетам b и c. Пусть $b_1, \ldots, b_d$ — полная система вычетов по модулю d, например, $1, 2, \ldots, d$, и $c_1, \ldots, c_q$ — полная система вычетов по модулю q.

Для каждой из этих таблиц Виженера при некоторых натуральных числах s, t с условиями $1 \leq s \leq d, 1 \leq t \leq q$, возьмем свой ключ $k = (b_{k_1}, b_{k_2}, \ldots, b_{k_s})$ для первой таблицы и соответственно $p = (c_{p_1}, c_{p_2}, \ldots, c_{p_t})$ для второй таблицы. Над каждым вычетом первой строки первой таблицы выписываем в строку символы ключа k следующим образом

$$b_{k_1}, b_{k_2}, \ldots b_{k_s}, b_{k_1}, b_{k_2}, \ldots .$$

Аналогично выписываем ключ p над второй таблицей.

3.2. Процедура шифрования открытого текста. Пусть задан открытый текст $a_{h_1} a_{h_2} \ldots a_{h_u}$. По формуле (1) преобразуем его в два текста. Имеем

$$b_{h_1} b_{h_2} \ldots b_{h_u}; \quad c_{h_1} c_{h_2} \ldots c_{h_u}.$$

На пересечении h_1-го столбца и k_1-й строки в первой таблице находим символ x_1, а на пересечении h_1-го столбца и p_1-й строки второй таблицы находим символ y_1. Повторим эту процедуру для следующего символа a_{h_2} и т. д. Получим шифрованный текст

$$x_1 y_1 x_2 y_2 \ldots x_u y_u$$

или два шифрованных текста $x_1x_2\dots x_u$ и $y_1y_2\dots y_u$, или $z_1z_2\dots z_u$, где $z_t = qx_t + dy_t, 1 \le t \le u$.

3.3. Процедура расшифрования. По ключам k и p в первой и второй таблицах Виженера находим строки с номерами k_1 и p_1 соответственно. На этих строках находим элементы x_1 в первой таблице и y_1 во второй таблице, а затем по этим элементам находим, отвечающие им столбцы, и получаем элементы b_{h_1} и c_{h_1}. По тому же правилу восстанавливаются элементы b_{h_2} и c_{h_2} и т. д.

Далее, используя формулу (1), по паре символов (b_{q_t}, c_{q_t}) находим символ a_{q_t}, $t = 1, \dots, u$. Процедура расшифрования завершена.

Наконец, дадим обобщение предыдущей процедуры шифрования. Пусть алфавит состоит из m символов, причем имеет место представление $m = m_1 \dots m_r$ с попарно простыми множителями $m_1, m_2, \dots, m_r$, превосходящими единицу. Определим числа M_s и M'_s следующими условиями

$$m_1m_2\dots m_r = M_sm_s, \quad M_sM'_s \equiv 1 \pmod{m_s}, s = 1, 2, \dots, r.$$

Положим

$$a = M_1M'_1b_1 + M_2M'_2b_2 + \dots + M_rM'_rb_r. \tag{2}$$

И пусть $b_1, b_2, \dots, b_r$ независимо друг от друга пробегают полные системы по модулям $m_1, m_2, \dots, m_r$ соответственно. Тогда a пробегает полную систему вычетов по модулю $m_1m_2\dots m_r$ (см., например, [10, гл. IV, § 3]).

Пусть, например, $m = 30, m = m_1m_2m_3 = 2 \cdot 3 \cdot 5 = 2 \cdot 15 = 3 \cdot 10 = 5 \cdot 6$. Тогда $M_1M'_1 \equiv 15 \cdot 1 \equiv 1 \pmod 2, M_2M'_2 \equiv 10 \cdot 1 \equiv 1 \pmod 3, M_3M'_3 \equiv 6 \cdot 1 \equiv 1 \pmod 5$.

Поэтому имеем $a \equiv 15b_1 + 10b_2 + 6b_3 \pmod{30}$.

Пусть, теперь, $b_{1,s}, b_{2,s}, \dots, b_{m_s,s}$ — полная система вычетов по модулю m_s, например, $1, 2, \dots, m_s, 1 \le s \le r$. Составим r таблиц Виженера для каждого из алфавитов $b_{1,s}, b_{2,s}, \dots, b_{m_s,s}, 1 \le s \le r$.

Для каждой из приведенных выше таблиц Виженера при некотором натуральном числе t_s с условиями $1 \le t_s \le m_s$, задаем ключ $k_s = (b_{k_1,s}, b_{k_2,s}, \dots, b_{k_{t_s},s}), 1 \le s \le r$.

Пусть, далее, задан открытый текст $a_{h_1}a_{h_2}\dots a_{h_u}$. По формуле (2) преобразуем его в r текстов. Имеем

$$b_{h_1,s}b_{h_2,s}\dots b_{h_u,s}, s = 1, 2, \dots, r.$$

Аналогично вышеприведенному с помощью таблицы Виженера с номером s и ключа k_s шифруем текст $b_{h_1,s}b_{h_2,s}\dots b_{h_u,s}, s = 1, 2, \dots, r$. Расшифрование проводится также аналогично вышеизложенному.

4. Об одной цифровой подписи и новом блочном шифре. Здесь мы даем приложение p-адического анализа к построению цифровой подписи и блочного шифра (см. также [2, 22, 25, 26]).

Собственноручная подпись каждого человека на бумажном носителе свидетельствует о принадлежности ее данному лицу, о невозможности отказа этого лица от своей подписи и о подтверждении данным лицом некоторого текста или сообщения.

Цифровая подпись для сообщения представляет собой некоторое число, допускающее проверку с помощью открытого ключа того факта, что оно отвечает данному сообщению и некоторому секретному ключу, известному только владельцу подписи, причем она дает возможность решить те же задачи, что и собственноручная подпись человека.

Отметим, что цифровая подпись зависит от конкретного подписанного сообщения и от секретного ключа, верна для любой копии данного сообщения, требует наличия определенных вычислительных средств, быть может электронных, для ее создания и проверки, а также сертификации открытых ключей. Более того, проверку цифровой подписи можно осуществить третьей стороне без доступа к секретному ключу, но получить саму подпись без секретного ключа не представляется возможным.

Нами обобщается цифровая подпись М. О. Рабина [25] (см. также [22]). Цифровая подпись, построенная здесь, связана с рассмотрением чисел по модулю, равному степени простого числа.

Пусть абонент $\mathcal{A}$ создает цифровую подпись и передает ее по открытому каналу связи абоненту $\mathcal{B}$. В качестве секретного ключа абонент $\mathcal{A}$ выбирает большие нечетные простые числа p и q, сравнимые с 3 по модулю 4 и два натуральных числа a и b. Открытый ключ состоит из двух чисел $n = p^a$ и $r = p^b$. Секретный ключ известен только абоненту $\mathcal{A}$.

Далее абоненту $\mathcal{A}$ присваивается некоторая метка Q — натуральное число. Затем выбирается часть L передаваемого сообщения m. Числа L и Q обязаны удовлетворять следующим условиям

$$(L,p)=1, 0<L<n, \left(\frac{L}{p}\right)=1, (Q,q)=1, 0<Q<r, \left(\frac{Q}{q}\right)=1.$$

Если для чисел L или Q не выполняется хотя бы одно из этих условий, то абонент $\mathcal{A}$ заменяет в случае необходимости число L на $L\pm 1$ и метку Q на $Q\pm 1$. Он повторяет эту процедуру до тех пор, пока не найдет числа L и Q, удовлетворяющие приведенным выше условиям.

Абонент $\mathcal{A}$ образует новое сообщение C_1, C_2, где $0<C_1<n, 0<$

$C_2 < r$, вида

$$L \equiv C_1^2 \pmod{n}, Q \equiv C_2^2 \pmod{r},$$

и передает числа C_1, C_2 и L, Q, а также те величины, на которые изменились числа L и Q, по открытому каналу связи абоненту $\mathcal{B}$. Эти четыре числа C_1, C_2, L, Q и образуют цифровую подпись.

Решения C_1, C_2 строятся абонентом $\mathcal{A}$, обладающим секретными ключами p, q и a, b. Сравнения $L \equiv C_1^2 \pmod{n}$ и $Q \equiv C_2^2 \pmod{r}$ решаются единым алгоритмом. Поэтому рассмотрим сравнение $H \equiv x^2 \pmod{p^s}$, где заданы натуральные числа H, s, простое число p, и величина x является неизвестной. Представим переменную x в виде $x \equiv u_\nu \pmod{p^{\nu+1}}$, где $u_\nu = u_{\nu-1} + x_\nu p^\nu, \nu \geq 1, u_0 = x_0$, и координаты $x_0, x_1, \ldots, x_{s-1}$ изменяются в пределах от 0 до $p-1$.

Решим сначала сравнение

$$H \equiv x_0^2 \pmod{p}.$$

Все его решения суть: $x_0 \equiv \pm H^{(p+1)/4} \pmod{p}$. Из двух найденных значений величины x_0 возьмем то, которое является квадратичным вычетом по модулю p, и обозначим его y_0, причем $0 < y_0 < p$. Далее, предположим, что найдено $u_{\nu-1}$ при $\nu \geq 1$, причем $u_0 = y_0$. Найдем значение u_ν при $\nu \geq 1$. Имеем цепочку сравнений

$$H \equiv (u_{\nu-1} + p^\nu x_\nu)^2 \pmod{p^{\nu+1}}, H \equiv u_{\nu-1}^2 + 2p^\nu u_{\nu-1} x_\nu \pmod{p^{\nu+1}},$$

$$x_\nu \equiv (H - u_{\nu-1}^2)(2u_{\nu-1})^{-1} \pmod{p},$$

поскольку $H \equiv x_0^2 \pmod{p}$, $H \equiv u_{\nu-1}^2 \pmod{p^\nu}$ и $2u_{\nu-1} \equiv 2x_0 \pmod{p}$, $2x_0 \not\equiv 0 \pmod{p}$.

Абонент $\mathcal{B}$ и представитель третьей стороны могут проверить подлинность подписи с помощью открытого ключа n. Для этого вычисляются значения $L' \equiv C_1^2 \pmod{n}$ и $Q' \equiv C_2^2 \pmod{r}$. Достаточно установить, что $L' = L, Q' = Q$.

Перейдем теперь к построению блочного шифра.

Пусть задан открытый текст, представленный в цифровом виде числом m, имеющим в двоичной записи k цифр. Возьмем любое натуральное число r, удовлетворяющее условиям $1 \leq r \leq k/2$. Разобьем число m на блоки, представив его в виде

$$m = m_1 + m_2 2^r + \cdots + m_n 2^{(n-1)r},$$

где $0 \le m_1, \ldots, m_n < 2^r$ и $(n-1)r \le k < nr$.

Расположим числа $m_1, \ldots, m_n$ в порядке возрастания, при этом отметим места, где встречаются равные числа m_s и числа m_s, равные нулю. Далее, выбросим все m_s, равные нулю и оставим по одному экземпляру из ненулевых равных чисел. Получим $0 < \tilde{m}_1 < \cdots < \tilde{m}_d < 2^r$.

Затем найдем сумму $\tilde{m}_1 + \cdots + \tilde{m}_d = N_1$. Очевидно, имеем $d(d+1)/2 \le N_1 < d2^r$. Выберем простое число p, находящееся в промежутке $N_1 \le p < 2N_1$. Предположим, что $\tilde{m}_s \not\equiv \tilde{m}_t \pmod{p}$ для всех $s \ne t, 1 \le s, t \le d$. Наконец, найдем суммы вторых, ..., d-х степеней чисел $\tilde{m}_1, \ldots, \tilde{m}_d$. Получим

$$\begin{cases} \tilde{m}_1 + \cdots + \tilde{m}_d = N_1, \\ \tilde{m}_1^2 + \cdots + \tilde{m}_d^2 = N_2, \\ \ldots \qquad \ldots \qquad \ldots \\ \tilde{m}_1^d + \cdots + \tilde{m}_d^d = N_d. \end{cases} \tag{1}$$

Заметим, что $p \ge N_1 \ge \tilde{m}_d > \cdots > \tilde{m}_1$.

Числа $N_1, \ldots, N_d$ составят часть шифртекста.

Покажем, как по этим числам можно восстановить числа $\tilde{m}_1, \ldots, \tilde{m}_d$. Рассмотрим систему сравнений

$$\begin{cases} x_1 + \cdots + x_d \equiv N_1 \pmod{p}, \\ x_1^2 + \cdots + x_d^2 \equiv N_2 \pmod{p}, \\ \ldots \qquad \ldots \qquad \ldots \\ x_1^d + \cdots + x_d^d \equiv N_d \pmod{p}. \end{cases} \tag{2}$$

Эта система сравнений имеет единственное решение $0 < \nu_{1,0} < \cdots < \nu_{d,0} \le p$, причем $\nu_{1,0} \equiv \tilde{m}_1 \pmod{p}, \ldots, \nu_{d,0} \equiv \tilde{m}_d \pmod{p}$.

Действительно, пусть при $1 \le s \le d$ символ $\sigma_s = \sigma_s(x_1, \ldots, x_d)$ обозначает s-ю элементарную симметрическую функцию. Тогда при $p > d$ из формул Ньютона—Варинга (см., например, [9, с. 60–61])

$$N_s - N_{s-1}\sigma_1 + \cdots + (-1)^s s\sigma_s \equiv 0 \pmod{p},$$

функции $\sigma_1, \ldots, \sigma_d$ однозначно выражаются через суммы степеней $N_1, \ldots, N_d$. С другой стороны, в поле из p элементов многочлен $f(z) = z^d - \sigma_1 z^{d-1} + \cdots + (-1)d\sigma_d$ однозначно разлагается на линейные множители $f(z) = (z - x_1) \ldots (z - x_d)$. Тем самым, с точностью до перестановки находятся корни $\nu_{1,0}, \ldots, \nu_{d,0}$ предыдущей системы сравнений.

Пусть при $1 \le s \le d$ найдены решения $u_{1,s-1}, \dots, u_{d,s-1}$ системы сравнений

$$\begin{cases} u_{1,s-1} + \dots + u_{d,s-1} \equiv N_1 \pmod{p^{s-1}}, \\ u_{1,s-1}^2 + \dots + u_{d,s-1}^2 \equiv N_2 \pmod{p^{s-1}}, \\ \dots \quad \dots \quad \dots \\ u_{1,s-1}^d + \dots + u_{d,s-1}^d \equiv N_d \pmod{p^{s-1}}. \end{cases}$$

Далее будем искать решение $u_{1,s}, \dots, u_{d,s}$ системы сравнений по модулю p^s. При $1 \le t, s \le d$ положим $u_{t,s} = u_{t,s-1} + p^{s-1} x_{t,s}$. Имеем систему сравнений

$$\begin{cases} u_{1,s} + \dots + u_{d,s} \equiv N_1 \pmod{p^s}, \\ u_{1,s}^2 + \dots + u_{d,s}^2 \equiv N_2 \pmod{p^s}, \\ \dots \quad \dots \quad \dots \\ u_{1,s}^d + \dots + u_{d,s}^d \equiv N_d \pmod{p^s}. \end{cases} \tag{3}$$

Эта система сравнений эквивалентна следующей линейной относительно неизвестных $x_{1,s}, \dots, x_{d,s}$ системе сравнений вида

$$\begin{cases} x_{1,s} + \dots + x_{d,s} \equiv N_1' \pmod{p}, \\ u_{1,s-1} x_{1,s} + \dots + u_{d,s-1} x_{d,s} \equiv N_2' \pmod{p}, \\ \dots \quad \dots \quad \dots \\ u_{1,s-1}^{d-1} x_{1,s} + \dots + u_{d,s-1}^{d-1} x_{d,s} \equiv N_d' \pmod{p}, \end{cases} \tag{4}$$

где $p^{s-1} N_l' \equiv N_l - u_{1,s-1}^l - \dots - u_{d,s-1}^l \pmod{p^s}$ при $1 \le l \le d$.

Поскольку для всех $t = 1, \dots, d$ имеем $u_{t,s-1} \equiv \nu_{t,0} \pmod{p}$, определитель системы сравнений является определителем Вандермонда с элементами $\nu_{1,0}, \dots, \nu_{d,0}$, не сравнимыми между собой по модулю p, т. е. этот определитель отличен нуля. Следовательно, предыдущая система сравнений имеет единственное решение $x_{1,s} \equiv \nu_{1,s} \pmod{p}, \dots, x_{d,s} \equiv \nu_{d,s} \pmod{p}$.

Таким образом, при $s = d$ из предыдущей системы сравнений получим ее единственное решение вида

$$u_{t,d} = \nu_{t,0} + p\nu_{t,1} + \dots + p^{d-1}\nu_{t,d} \equiv \tilde{m}_t \pmod{p^d},\ 1 \le t \le d.$$

Кроме того, так как $0 \le u_{t,d} < p^d$ и $0 < \tilde{m}_t < N_1 \le p^d$, то $u_{t,d} = \tilde{m}_t$ при всех $t = 1, \dots, d$.

Тем самым, доказано, что по числам $N_1, \ldots, N_d$ однозначно восстанавливаются числа $\tilde{m}_1, \ldots, \tilde{m}_d$.

Таким образом, весь шифрованный текст будет состоять из натуральных чисел $N_1, \ldots, N_d$, указания мест расположения нулевых чисел m_s, т. е. указания индексов s для нулевых m_s, далее указания индексов чисел m_t в порядке возрастания $\tilde{m}_s, 1 \leq s \leq d$ и простого числа p.

Восстановление открытого текста по приведенному шифртексту проведем по следующим шагам.

1. Вычислим $\sigma_d = \sigma_d(N_1, \ldots, N_d)$, где $\sigma_d = \tilde{m}_1 \ldots \tilde{m}_d$.

2. Найдем $\tilde{\sigma}_d \equiv \sigma_d \pmod{p}$. Поскольку при всех $t = 1, \ldots, d$ справедливы сравнения $\tilde{m}_t \equiv \nu_{t,0} \pmod{p}$, имеем $\tilde{\sigma}_d \equiv \tilde{m}_1 \ldots \tilde{m}_d \pmod{p}$. Последнее обстоятельство упрощает перебор наборов при поиске решения системы сравнений (2) по модулю p.

3. При $s = 1, \ldots, d$ находим решение $u_{1,s}, \ldots, u_{d,s}$ системы сравнений (3), решая линейную систему сравнений (4). Тем самым будут найдены $\tilde{m}_1, \ldots, \tilde{m}_d$.

4. Так как имеется взаимно однозначное соответствие между набором $\tilde{m}_1, \ldots, \tilde{m}_d$ и набором $m_1, \ldots, m_n$, то открытый текст будет восстановлен.

Заметим, что избавиться от условия, что числа $\tilde{m}_t, 1 \leq t \leq d$, не сравнимы между собой по модулю p, можно добавлением к каждому из этих чисел натуральных слагаемых, не превосходящих d.

5. Деревья Хуа Ло-кена в теории сравнений. Для полноты изложения приведем полезную для дальнейших приложений в дискретной математике связь теории p-адических чисел с теорией графов.

Отметим, что на одном из заседаний семинара по дискретной математике и математической кибернетике О. Б. Лупанов обратил внимание одного из авторов настоящей статьи на перспективность рассмотрения взаимосвязи между разрешимостью сравнений по модулю, равному степени простого числа, и теорией графов. На этом заседании обсуждалась теорема Хуа Ло-кена о построении p-адического решения уравнения $f(x) = 0$ для произвольного многочлена с целыми рациональными коэффициентами, лежащая в основе вывода оценки полной рациональной тригонометрической суммы [29, с. 17–18].

Первые утверждения о разрешимости полиномиальных уравнений в целых p-адических числах сводились к нахождению условий, при которых решение соответствующего решения сравнения по некоторому модулю, равному степени простого числа p, возможно было “поднять” до решения соответствующего уравнения в целых p-

адических числах. Как правило, таким способом удавалось получать обобщения утверждений для однократных корней сравнений и уравнений.

В основу своей схемы Хуа Ло-кен положил утверждение о взаимосвязи кратностей корней соответствующих p-адических сравнений по простому модулю (теорема Д). В частности, в случае многочленов от одной переменной он показал, что все решения сравнения можно интерпретировать как некоторое дерево.

5.1. Критерий, теорема Гензеля и ее следствия для разрешимости уравнения в целых p-адических числах. Взаимосвязь теории сравнений по модулям, равным степеням фиксированного простого числа с теорией p-адических чисел содержится в следующем простом критерии [8].

Теорема А. *Для многочлена $F(x_1, \ldots, x_r)$, $r \geq 1$ с целыми рациональными коэффициентами разрешимость уравнения*

$$F(x_1, \ldots, x_r) = 0$$

в целых p-адических числах эквивалентна разрешимости при любом натуральном числе k сравнения

$$F(x_1, \ldots, x_r) \equiv 0 \pmod{p^k}.$$

Первый результат о "подъеме" решения сравнения до решения соответствующего уравнения в p-адических числах известен как лемма Гензеля [30].

Теорема Б. *Пусть $f(x)$ многочлен с целыми коэффициентами и*

$$f(x) \equiv g_0(x)h_0(x) \pmod{p},$$

где $g_0(x)$ и $h_0(x)$ взаимно простые многочлены, тогда существуют два многочлена $g(x)$, $h(x)$ с целыми p-адическими коэффициентами, такие, что

$$f(x) = g(x)h(x).$$

Весьма простое достаточное условие для p-адической разрешимости полиномиального уравнения в случае однократного корня с использованием всего лишь конечного числа сравнений дает следующее утверждение, основанное по существу на методе касательных Ньютона для приближенного решения уравнения в действительных числах [8].

Теорема В. *Пусть* $F(x_1, \ldots, x_r)$ — *многочлен с целыми* p-*адическими коэффициентами,* δ — *неотрицательное целое рациональное число и пусть существует набор целых* p-*адических чисел* $(\gamma_1, \ldots, \gamma_r)$ *таких, что при некотором* s, $1 \leq s \leq r$, *справедливы соотношения*

$$F(\gamma_1, \ldots, \gamma_r) \equiv 0 \pmod{p^{2\delta+1}},$$

$$\frac{\partial F(\gamma_1, \ldots, \gamma_r)}{\partial x_s} \equiv 0 \pmod{p^{\delta}},$$

$$\frac{\partial F(\gamma_1, \ldots, \gamma_r)}{\partial x_s} \not\equiv 0 \pmod{p^{\delta+1}}.$$

Тогда существует набор целых p-*адических чисел* $(\theta_1, \ldots, \theta_r)$ *такой, что*

$$F(\theta_1, \ldots, \theta_r) = 0,$$

$$\theta_1 \equiv \gamma_1 \pmod{p^{\delta_1}}, \ldots, \theta_r \equiv \gamma_r \pmod{p^{\delta_r}}.$$

Следующий критерий p-адической разрешимости диофантовых уравнений нашли Б. Д. Бёрч и К. Мак Кэнн [7]. Они определили эффективно вычислимое число $D_n(F)$, названное ими "дискриминантом" многочлена $F = F(x_1, \ldots, x_r)$ с целыми рациональными коэффициентами. Это число $D_n(F)$ находится из самого многочлена F и всех его формальных частных производных. Далее, определим наивысшую степень R числа p, входящую в $D_n(F)$.

Теорема Г. *Пусть* $F(x_1, \ldots, x_r)$ — *многочлен с целыми рациональными коэффициентами,* R — *неотрицательное целое рациональное число, определенное выше, и пусть существует набор целых рациональных чисел* $(\gamma_1, \ldots, \gamma_r)$ *таких, что справедливо сравнение*

$$F(\gamma_1, \ldots, \gamma_r) \equiv 0 \pmod{p^R}.$$

Тогда существует набор целых p-*адических чисел* $(\theta_1, \ldots, \theta_r)$ *такой, что*

$$F(\theta_1, \ldots, \theta_r) = 0,$$

$$\theta_1 \equiv \gamma_1 \pmod{p^R}, \ldots, \theta_r \equiv \gamma_r \pmod{p^R}.$$

Последняя теорема является многомерным обобщением леммы Гензеля – Рычлика, описанном в [1].

5.2. Деревья Хуа Ло-кена для полиномиальных сравнений от одной переменной по модулю, равному степени простого числа. Необходимость разработки другого подхода к понятию

разрешимости полиномиальных сравнений возникла в связи нахождением оценок полных рациональных тригонометрических сумм Хуа Ло-кена [29] при нахождении точного значения показателя сходимости особого ряда в проблеме Терри.

Пусть p — фиксированное простое число и $l \geq 1$ — фиксированное натуральное число. Пусть $f_1(x) = f(x)$ — многочлен степени n с коэффициентами из кольца вычетов по модулю p^l. Пусть $\tau_0 \geq 0$ — наибольшее целое число такое, что p^{τ_0} делит все коэффициенты многочлена $f_1(x)$. Пусть x_1 — решение сравнения

$$p^{-\tau_0} f_1(x) \equiv 0 \pmod{p}, \quad 0 \leq x_1 < p.$$

Положим

$$f_2(x) = p^{\tau_0} f_1(px + x_1).$$

Рассмотрим $f_2(x)$ вместо $f_1(x)$ и модуль $p^{l-\tau_0}$ вместо модуля p^l. Тогда определим наивысшую степень τ_1 числа p такую, что p^{τ_1} делит все коэффициенты многочлена $f_2(x)$. Имеем $\tau_1 \geq 1$. Пусть, теперь, x_2 — решение сравнения

$$p^{-\tau_1} f_2(x) \equiv 0 \pmod{p}, \quad 0 \leq x_2 < p.$$

Аналогично строится многочлен $f_3(x)$ и модуль $p^{l-\tau_0-\tau_1}$ и т. д.

После s шагов получим $\tau_0 + \cdots + \tau_{s-1} \geq l$, но $\tau_0 + \cdots + \tau_{s-2} < l$, и все коэффициенты $g_l(x)$ делятся на $p^{l-(\tau_0+\cdots+\tau_{s-2})}$.

Символически рассмотренное решение сравнения $f(x) \equiv 0 \pmod{p^l}$ обозначим через

$$x_1 + px_2 + \cdots + p^{s-1}x_s. \tag{1}$$

Пусть, теперь, k, $1 \leq k \leq s$ и $g(x) = f_k(x)$. Тогда справедливо следующее утверждение.

Теорема Д. *Пусть $g(x)$ — многочлен с целыми рациональными коэффициентами и a — корень кратности m сравнения*

$$g(x) \equiv 0 \pmod{p}.$$

Пусть, далее, u — наивысшая степень числа p, делящая все коэффициенты многочлена $h(x) = g(px + a)$. Тогда число корней (с учетом их кратности) сравнения

$$p^{-u} h(x) \equiv 0 \pmod{p},$$

не превосходит m.

Заметим, что величина показателя степени u не превосходит m.

Множество решений (1) сравнения $f(x) \equiv 0 \pmod{p^l}$ по теореме Д будет представлять совокупность деревьев в количестве, не превосходящем степени n многочлена $f(x) = f_1(x)$. Пусть количество деревьев равно $n_1 \le n$. Их вершины $a_{1,u},\ 1 \le u \le n_1$, отвечают решениям $x_1 = x_{1,u}$ кратности m_u сравнения $f_1(x) \equiv 0 \pmod{p}$. Для того, чтобы рассматривать одно дерево введем вершину a_0. Проведем из нее n_1 ребер к вершинам $a_{1,u},\ 1 \le u \le n_1$. Далее из каждой вершины $a_{1,u},\ 1 \le u \le n_1$, проведем не более m_u, которые отвечают решениям $x_1 + px_2 = x_{1,u} + px_{2,u,v},\ 1 \le u \le n_1,\ 1 \le v \le m_u$, кратности $m_{u,v} \le m_u$.

Таким образом для каждого корня (1) сравнения $f(x) \equiv 0 \pmod{p^l}$ однозначно определяется ветвь построенного дерева некоторой длины s. Количество корней (1) не превосходит n.

Свяжем описанную схему построения решения сравнения по модулю, равному степени простого числа, с оценкой модуля тригонометрической суммы.

Пусть $(a_n, \dots, a_1, p) = 1$ и $g(x) = a_n x^n + \cdots + a_1 x + a_0$ — многочлен с целыми рациональными коэффициентами.

Рассмотрим, следуя Хуа Ло-кену, решение $x_0 + px + \cdots + p^r x_r$ сравнения $g'(x) \equiv 0 \pmod{p^l}$. Определим последовательность многочленов $g_1(x), \dots, g_r(x)$ и набор показателей $u_1, \dots, u_r$ из следующих соотношений

$$p^{u_1} g_1(x) = g(x_0 + px) - g(x_0),$$

где коэффициенты многочлена $g_1(x)$ в совокупности взаимно просты с p.

Аналогично определяются многочлены $g_s(x),\ s = 2, \dots, r$,

$$p^{u_s} g_s(x) = g_{s-1}(x_{s-1} + px) - g_{s-1}(x_{s-1}) =$$

$$= p^{-u_1 - \cdots - u_{s-1}} \left(g(x_0 + px_1 + \cdots + p^{s-1} x_{s-1} + p^s x^s) - \right.$$

$$\left. - g(x_0 + px_1 + \cdots + p^{s-1} x_{s-1}) \right).$$

Заметим, что показатели $u_s,\ s = 1, \dots, r$ удовлетворяют условиям

$$n \ge u_1 \ge u_2 \ge \cdots \ge u_r \ge 2,$$

и количество многочленов с данным набором показателей не превосходит

$$p^\alpha,\ \alpha = r + nl - 0.5u_1(u_1 - 1) - \cdots - 0.5u_r(u_r - 1).$$

Полной рациональной тригонометрической суммой по модулю q называют сумму вида

$$S = S(q; f(x)) = \sum_{x=1}^{q} e^{2\pi i \frac{f(x)}{q}},$$

где $q > 1$ — натуральное число и $f(x) = a_n x^n + \cdots + a_1 x$ — многочлен с целыми рациональными коэффициентами.

Положим $w = \left[\frac{\ln n}{\ln p}\right]$.

Теорема Е. *Пусть $g(x)$ — многочлен с целыми рациональными коэффициентами, которые в совокупности взаимно просты с p, и ξ не является корнем сравнения*

$$p^{-\tau} g'(x) \equiv 0 \pmod{p},$$

где τ — наивысшая степень числа p, делящая все коэффициенты многочлена $g'(x)$. Тогда при $l > 2w + 1$ имеем

$$\sum_{x=1}^{p^{l-1}} e^{\frac{2\pi i g(\xi + px)}{p^l}} = 0.$$

Отсюда следует равенство

$$S(p^l; f(x)) = \sum_{\xi} p^{u_1 - 1} e^{\frac{f(\xi)}{p^l}} \sum_{x=1}^{p^{l-u_1}} e^{\frac{2\pi i f_1(x)}{p^{l-u_1}}},$$

где ξ пробегает по всем корням сравнения

$$p^{-\tau} f'(x) \equiv 0 \pmod{p}.$$

5.3. Полиномиальные сравнения от нескольких переменных по модулю, равному степени простого числа. Здесь мы построим решение сравнения

$$F(x_1, \ldots, x_r) \equiv 0 \pmod{p^l},$$

где $F(x_1, \ldots, x_r)$ — многочлен с целыми рациональными коэффициентами, которые в совокупности взаимно просты с p, $r > 1, a(0, \ldots, 0) = 0$ и

$$F(x_1, \ldots, x_r) = \sum_{t_1=0}^{n_1} \cdots \sum_{t_r=0}^{n_r} a(t_1, \ldots, t_r) x_1^{t_1} \ldots x_r^{t_r}.$$

Рассмотрим решение $x_{s,0}+px_{s,1}+\cdots+p^t x_{s,t}, s=1,\ldots,r$ системы сравнений

$$\begin{cases} F'_{x_1}(x_1,\ldots,x_r)\equiv 0 \pmod{p^l}, \\ \cdots \qquad\qquad \cdots \\ F'_{x_r}(x_1,\ldots,x_r)\equiv 0 \pmod{p^l}. \end{cases}$$

Определим последовательность многочленов $F_1(x_1,\ldots,x_r),\ldots, F_t(x_1,\ldots,x_r)$ и набор показателей $u_1,\ldots,u_t$ из следующих соотношений

$$p^{u_1}F_1(x_1,\ldots,x_r)=F(x_{1,0}+px_1,\ldots,x_{r,0}+px_r)-F(x_{1,0},\ldots,x_{r,0}),$$

где коэффициенты многочлена $F_1(x_1,\ldots,x_r)$ в совокупности взаимно просты с p.

Аналогично определяются многочлены $F_s(x_1,\ldots,x_r)$, $s=2,\ldots,t$,

$$p^{u_s}F_s(x_1,\ldots,x_r)=F_{s-1}(x_{1,0}+px_1,\ldots,x_{r,0}+px_r)-F_{s-1}(x_{1,0},\ldots,x_{r,0}).$$

Отсюда имеем

$$p^{-u_1-\cdots-u_s}F_s(x_1,\ldots,x_r)=$$

$$=F(x_{1,0}+px_{1,1}+\cdots+p^{s-1}x_{1,s-1}+p^s x_1,\ldots,x_{r,0}+\cdots+p^{s-1}x_{r,s-1}+p^s x_r)-$$

$$-F(x_{1,0}+px_{1,1}+\cdots+p^{s-1}x_{1,s-1},\ldots,x_{r,0}+px_{r,1}+\cdots+p^{s-1}x_{r,s-1}).$$

Заметим, что показатели u_s, $s=1,\ldots,t$, удовлетворяют условиям

$$n\geq u_1\geq u_2\geq\cdots\geq u_r\geq 2,$$

и количество многочленов с данным набором показателей не превосходит

$$p^\alpha,\ \alpha=t+nl-0.5ru_1(u_1-1)^r-\cdots-0.5ru_t(u_t-1)^r.$$

В качестве приложения построенного множества решений дадим оценку тригонометрической суммы (см., например, [3, с. 77]).

Полной кратной рациональной тригонометрической суммой по модулю q называют сумму вида

$$S=S(q;F(x_1,\ldots,x_r))=\sum_{x_1=1}^{q}\cdots\sum_{x_r=1}^{q}e^{2\pi i\frac{F(x_1,\ldots,x_r)}{q}},$$

где $q > 1$ — натуральное число и

$$F(x_1, \dots, x_r) = \sum_{t_1=0}^{n_1} \cdots \sum_{t_r=0}^{n_r} a(t_1, \dots, t_r) x_1^{t_1} \dots x_r^{t_r}$$

есть многочлен с целыми рациональными коэффициентами.

В основе оценки лежит следующая теорема.

Положим $n = \max(n_1, \dots, n_r)$, $w = \left[\frac{\ln n}{\ln p}\right]$.

Теорема. *Пусть $F(x_1, \dots, x_r)$ — многочлен с целыми рациональными коэффициентами, которые в совокупности взаимно просты с p, и $(\xi_1, \dots, \xi_r)$ не является корнем системы сравнений*

$$\begin{cases} p^{-\tau_1} F'_{x_1}(x_1, \dots, x_r) \equiv 0 \pmod p, \\ \dots \qquad\qquad \dots \\ p^{-\tau_r} F'_{x_r}(x_1, \dots, x_r) \equiv 0 \pmod p. \end{cases}$$

где $\tau_s, s = 1, \dots, r$ — наивысшая степень числа p, делящая все коэффициенты многочлена $F'_{x_s}(x_1, \dots, x_r)$. Тогда при $l > 2w+1$ имеем

$$\sum_{x_1=1}^{p^{l-1}} \cdots \sum_{x_r=1}^{p^{l-1}} e^{\frac{2\pi i F(\xi_1 + p x_1, \dots, \xi_r + p x_r)}{p^l}} = 0.$$

Отсюда следует равенство

$$S(p^l; F(x_1, \dots, x_r)) =$$

$$= \sum_{(\xi_1, \dots, \xi_r)} p^{r(u_1-1)} e^{\frac{F(\xi_1, \dots, \xi_r)}{p^l}} \sum_{x_1=1}^{p^{l-u_1}} \cdots \sum_{x_1=1}^{p^{l-u_1}} e^{\frac{2\pi i F_1(x_1, \dots, x_r)}{p^{l-u_1} s}},$$

где наборы $(\xi_1, \dots, \xi_r)$ пробегают по всем корням системы сравнений

$$\begin{cases} p^{-\tau_1} F'_{x_1}(x_1, \dots, x_r) \equiv 0 \pmod p, \\ \dots \qquad\qquad \dots \\ p^{-\tau_r} F'_{x_r}(x_1, \dots, x_r) \equiv 0 \pmod p. \end{cases}$$

Таким образом получена рекуррентная формула для полной кратной рациональной тригонометрической суммы по модулю, равному степени простого числа p. Она позволяет получить оценку этой суммы. К сожалению, найти аналог теоремы Д пока не удалось.

Работа выполнена при финансовой поддержке РФФИ, грант № 10-01-00433-а.

Список литературы

1. Ax J., Kochen S. Diophantine problems over local fields. I // American J. Math. — 1965. — V. 87. — P. 605–630.

2. Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. Основы криптографии: Учебное пособие, 2-е изд., испр. и доп. — М.: Гелиос АРВ, 2002.

3. Архипов Г. И., Карацуба А. А., Чубариков В. Н. Теория кратных тригонометрических сумм. — М.: Наука. Физматлит, 1987.

4. Аршинов М. Н., Садовский Л. Е. Коды и математика. — М.: Наука, 1983.

5. Бабаш А. В., Шанкин Г. П. Криптография. — М.: СОЛОН-ПРЕСС, 2007.

6. Баричев С. Криптография без секретов // `http://www.artele-com.ru/library/books/swos/index/html`.

7. Birch B. J., McCann K. A criterion for the p-adic solubility of diophantine equations // Quart. J. Math. — 1967. — V. 18, № 69. — P. 59–63.

8. Боревич З. И., Шафаревич И. Р. Теория чисел. — М.: Наука. Физматлит, 1972.

9. Вейль Г. Классические группы, их инварианты и представления. — М.: Изд-во иностр. лит, 1947.

10. Виноградов И. М. Основы теории чисел. — М.: Наука, 1983.

11. Гашков С. Б., Чубариков В. Н. Арифметика. Алгоритмы. Сложность вычислений. — М.: Наука, 1996.

12. Гольев Ю. И., Ларин Д. А., Тришин А. Е., Шанкин Г. П. Криптография: страницы истории тайных операций. — М.: Гелиос АРВ, 2008.

13. Жельников В. Криптография от папируса до компьютера. — М.: ABF, 1996.

14. Коблиц Н. Курс теории чисел и криптографии. — М.: Научное изд-во ТВП, 2001.

15. Копьев Д. В., Минеев М. П., Чубариков В. Н. О некоторых арифметических подходах к задачам криптографии // Совр. пробл. матем., мех. и прил. — 2009. — Т. 3, вып. 1. — С. 56–66.

16. Минеев М. П., Чубариков В. Н. Задача об искажении частоты появления знаков в шифре простой замены // Математические вопросы кибернетики. Вып. 16. — М.: Наука, 2007. — С. 242–245.

17. Минеев М. П., Чубариков В. Н. Об одном методе искажения частоты появления знаков в шифре простой замены // Докл. РАН. — 2008. — Т. 420, № 6. — С. 736–738.

18. Минеев М. П., Чубариков В. Н. К вопросу об искажении частот появления знаков в шифре простой замены // Докл. РАН. — 2009. — Т. 426, № 1. — С. 6–8.

19. Минеев М. П., Чубариков В. Н. Об одном применении китайской теоремы об остатках к шифру Виженера // Докл. РАН. — 2010. — Т. 430, № 1. — С. 21–22.

20. Минеев М. П., Чубариков В. Н. Лекции по арифметическим вопросам криптографии. Уч. пос. — М.: Изд-во мех.-матем. фак-та МГУ, 2010.

21. Минеев М. П., Чубариков В. Н. Об одной цифровой подписи и новом блочном шифре // Докл. РАН. — 2011. — Т. 439, № 3. — С. 308–310.

22. Молдовян Н. А., Молдовян А. А. Введение в криптосистемы с открытым ключом. — СПб.: БХВ-Петербург, 2005.

23. Молдовян А. А., Молдовян Н. А., Советов Б. Я. Криптография. — СПб.: Лань, 2001.

24. Нечаев В. И. Элементы криптографии (Основы теории защиты информации). — М.: Высшая школа, 1999.

25. Rabin M. O. Digitalized signatures and public key functions as itractable as factorization // Techn. Rept. MIT/LCS/TR-212.MIT. — Lab. Computer Science, 1979.

26. Саломаа А. Криптография с открытым ключом. — М.: Мир, 1996.

27. Сингх С. Книга шифров: тайная история шифров и их расшифровки. — М.: Астрель, 2007.

28. Смарт Н. Криптография. — М.: Техносфера, 2006.

29. Hua L.-k. On the number of solutions of Tarry's problem // Acta Sci. Sinica. — 1952. — V. 1. — P. 1–76.

30. Hua L.-k. Introduction to number theory. — Springer-Verlag. 1982.

31. Чубариков В. Н. Элементы арифметики. — М.: Изд-во Механико-математического ф-та МГУ, 2007.

О СЛОЖНОСТИ ИНДИВИДУАЛЬНЫХ БУЛЕВЫХ ФУНКЦИЙ

Н. П. Редькин (Москва)

Одно из главных направлений математической кибернетики — это построение оптимальных, в том или ином смысле, управляющих систем, в частности, построение минимальных схем из функциональных элементов [1] для конкретных булевых функций. Существенные затруднения возникают на этапе доказательства необходимых нижних оценок для сложности схем. Здесь рассматриваются некоторые продвижения и новые результаты по указанному направлению.

Получение нижних оценок сложности методом замены базиса.

Разработанные к настоящему времени способы получения нижних оценок сложности схем зачастую ориентированы на конкретные базисы, и даже те из них, которые обладают относительной универсальностью (например, метод «забивания» переменных на входах схем булевыми константами [2]), всё-таки предполагают использование достаточно простых базисов, включающих элементы с небольшим числом входов. Однако полученные нижние оценки сложности схем в простых базисах можно эффективно использовать для получения аналогичных оценок для схем в более сложных базисах. Суть рассматриваемого подхода [3] к получению новых нижних оценок заключается в замене одного (быть может, достаточно сложного) базиса на другой, существенно (в том или ином смысле) более простой базис. (Можно усмотреть некоторую, пусть даже и отдалённую, аналогию этого метода с заменой переменной при интегрировании.)

Пусть B — произвольный (не обязательно полный) базис с положительными весами элементов, а S — схема в базисе B. Как обычно, сумму весов всех элементов из S будем считать сложностью схемы S и обозначать через $L_B(F)$. Для произвольной реализуемой в базисе B булевой функции f положим $L_B(f) = \min L_B(S)$, где минимум берётся по всем схемам в базисе B, реализующим f. Число $L_B(f)$ задаёт по определению сложность реализации функции схемами в базисе B (или просто сложность булевой функции f); схему S в базисе B, реализующую функцию f, будем считать минимальной, если $L_B(S) = L_B(f)$.

Пусть имеются два произвольных базиса B, B' и базис B состоит из элементов $E_1, \ldots, E_a$ с весами $P(E_1), \ldots, P(E_a)$, а базис B' состоит из элементов $E'_1, \ldots, E'_b$ с весами $P(E'_1), \ldots, P(E'_b)$.

Пусть элементы $E_1, \ldots, E_a$ реализуют функции $\phi_1, \ldots, \phi_a$, а элементы $E'_1, \ldots, E'_b$ — соответственно функции $\phi'_1, \ldots, \phi'_b$. Справедливо следующее утверждение о соотношении сложностей реализации одной и той же булевой функции схемами из функциональных элементов в разных базисах.

Теорема 1. *Пусть булева функция f реализуема схемой в базисе B', а функции базиса B' реализуемы схемами в базисе B и выполняются соотношения*

$$L_B(\phi'_i) \le P(E'_i), \quad 1 \le i \le b. \tag{1}$$

Тогда выполняется неравенство

$$L_{B'}(f) \ge L_B(f). \tag{2}$$

Приведём примеры использования теоремы 1.

Пример 1. Оценка сложности монотонных симметрических пороговых функций.

Возьмём базис B' из элементов E'_1, E'_2, E'_3, реализующих соответственно функции $\phi'_1 = x_1 \& \ldots \& x_l$, $\phi'_2 = x_1 \vee \ldots \vee x_l$, $\phi'_3 = \overline{x}$, где l — некоторое заданное натуральное число, не меньшее трёх, а вес каждого элемента равен единице (т. е. сложность схемы определяется числом элементов в ней). Найдём асимптотику для сложности реализации функции $f_2^n(\tilde{x}) = \bigvee\limits_{1 \le i < j \le n} x_i x_j$ схемами в базисе B'.

Верхняя оценка $L'_B(f_2^n) \lesssim \frac{2n}{l-1}$ получается с использованием конструкции М. И. Гринчука из [4], основанной на представлении f_2^n в виде

$$f_2^n(x_1, \ldots, x_n) = f_2^m(y_1, \ldots, y_m) \vee f_2^m(z_1, \ldots, z_m),$$

где $m = \lceil \sqrt{n} \rceil$, а каждая новая переменная y_i (и z_i) представляет собой дизъюнкцию не более чем m переменных из $\{x_1, \ldots, x_n\}$.

Нижнюю оценку получим заменой базиса B' на новый базис B, содержащий двухвходовый конъюнктор, двухвходовый дизъюнктор и инвертор. Вес каждого элемента из B положим равным $\frac{1}{l-1}$; в таком случае условия теоремы 1 будут выполнены. Согласно теореме 1 из [4] общее число элементов из базиса B в любой схеме для f_2^n не меньше чем $2n - 3$; отсюда следует, что сложность любой схемы в базисе B для функции f_2^n не меньше чем $\frac{2n-3}{l-1}$, т. е.

$$L_B(f_2^n) \ge \frac{2n-3}{l-1}. \tag{3}$$

Применяя теорему 1 из неравенств (2) и (3) получаем оценку

$$L_{B'}(f_2^n) \geq \frac{2n-3}{l-1},$$

которая совместно с приведённой выше верхней оценкой при растущем n даёт асимптотику

$$L_{B'}(f_2^n) \sim \frac{2n}{l-1}.$$

Пример 2. Оценка сложности булевых функций с малым числом единиц.

Возьмём класс $F_{n,k}$, состоящий из всех тех булевых функций от n переменных, каждая из которых обращается в единицу ровно на k наборах значений переменных. Известна [5] асимптотика для сложности реализации каждой функции из $F_{n,k}$ в случае, когда выполняется условие

$$1 \leq k \leq \log_2 n - c \log_2 \log_2 n, \tag{4}$$

где c — произвольная бóльшая единицы константа, а базис B содержит элементы, реализующие все булевы функции от двух переменных, кроме линейных функций $x \oplus y$ и $x \oplus y \oplus 1$; вес каждого элемента полагается равным единице. В рассматриваемом здесь примере предполагается, что условие (4) выполняется, а базис B' содержит 2^{l+1} элементов, реализующих всевозможные конъюнкции $x_1^{\sigma_1} \& \ldots \& x_l^{\sigma_l}$ и дизъюнкции $x_1^{\sigma_1} \vee \ldots \vee x_l^{\sigma_l}$, где $\sigma_1, \ldots, \sigma_l \in \{0,1\}$, а l — заданное натуральное число, не меньшее трёх; вес каждого элемента предполагается равным единице.

Пусть $f(x_1, \ldots, x_n)$ — произвольная булева функция из $F_{n,k}$, обращающаяся в единицу на наборах $\widetilde{\sigma_1}, \ldots, \widetilde{\sigma_k}$, где $\widetilde{\sigma_i} = (\sigma_{i,1}, \ldots, \sigma_{i,n})$, $i = 1, \ldots, k$. Пусть M_f — это $(k \times n)$-матрица, строками которой являются наборы $\widetilde{\sigma_1}, \ldots, \widetilde{\sigma_k}$, а j-й столбец отвечает переменной x_j, $j = 1, \ldots, n$. Столбцы матрицы M_f разобьём на группы одинаковых между собой столбцов; через $M_{\widetilde{\tau}}$ обозначим группу столбцов, т. е. подматрицу матрицы M_f, составленную из всех столбцов, равных $\widetilde{\tau}$ (для каких-то $\widetilde{\tau}$ группы $M_{\widetilde{\tau}}$ могут оказаться пустыми). Непустую группу столбцов $M_{\widetilde{\tau}}$ считаем сильной, если она содержит не менее двух столбцов $\widetilde{\tau}$ и в этих столбцах имеются как нули, так и единицы; переменные, отвечающие столбцам из сильной группы, также считаем сильными.

Теорема 2. *Пусть у функции f из класса F_{n,k_n} имеется m_n сильных переменных, а для последовательности $\{k_n\}$ при достаточно больших n выполняется условие* (4). *Тогда*

$$L_{B'}(f(x_1,\ldots,x_n)) \sim \frac{n+m_n}{l-1}.$$

При доказательстве последнего соотношения верхняя оценка получается конструктивно путём модификации схемы S, представленной в разделе 5 из [5]. Нижнюю оценку получим при переходе от базиса B' к новому базису B из элементов, реализующих все булевы функции от двух переменных x и y, кроме $x \oplus y$, $x \oplus y \oplus 1$. Вес каждого элемента из B положим равным $\frac{1}{l-1}$; как нетрудно заметить, условие (1) теоремы 1 будет выполнено.

Согласно теореме (1) из [5] общее число элементов из B в любой схеме, реализующей функцию $f(x_1,\ldots,x_n)$ из F_{n,k_n} с m_n сильными переменными, асимптотически не меньше $n+m_n$. Поэтому по теореме 1 сложность любой схемы для f в базисе B' асимптотически не меньше чем $\frac{n+m_n}{l-1}$.

Пусть $B = \{\phi_1,\ldots,\phi_8\}$ — множество из восьми булевых функций, каждая из которых есть либо конъюнкция $x^\alpha \& y^\beta$, либо дизъюнкция $x^\alpha \vee y^\beta$, где $\alpha,\beta \in \{0,1\}$. При заданном натуральном l, $l \geq 3$, через B' обозначим множество тех булевых функций, каждая из которых существенно зависит ровно от l переменных $x_1,\ldots,x_l$ и может быть реализована формулой над B, содержащей $l-1$ функциональных символов из B. Похожий на второй, но только более сложный пример использования теоремы 1 можно получить теперь, если рассматривать схемы (для функций с малым числом единиц) в базисе B', полагая вес каждого элемента равным единице.

Метод замены базиса применим и к самокорректирующимся схемам из функциональных элементов; покажем, как в этом случае можно использовать соответствующий аналог теоремы 1 из [6].

Будем рассматривать схемы в базисе B, содержащие надёжные и ненадёжные функциональные элементы. Всякий надёжный элемент имеет неотрицательный вес и всегда реализует некоторую приписанную ему функцию из B. Всякий ненадёжный элемент также имеет неотрицательный вес и в исправном состоянии реализует некоторую приписанную ему функцию из B, а в неисправном состоянии — некоторую фиксированную для всех элементов схемы константу δ ($\delta \in \{0,1\}$). Схема в базисе B называется k-самокорректирующейся

относительно неисправностей типа δ, если при переходе в неисправное состояние не более чем k ненадёжных элементов она реализует ту же булеву функцию, что и при исправном состоянии всех её элементов. Сложность схем, сложность (реализации) булевых функций, минимальность схем определяется и обозначается так же, как и выше, но только теперь применительно к рассматриваемым k-самокорректирующимся схемам.

Представим теперь, что имеются два произвольных конечных базиса $B = \{\phi_1, \ldots, \phi_a\}$ и $B' = \{\psi_1, \ldots, \psi_b\}$. Первый базис B содержит надёжные элементы $D_1, \ldots, D_a$ с весами $P(D_1), \ldots, P(D_a)$, реализующие соответственно функции $\phi_1, \ldots, \phi_a$, и ненадёжные элементы $E_1, \ldots, E_a$ с весами $P(E_1), \ldots, P(E_a)$, реализующие (в исправном состоянии) те же самые функции $\phi_1, \ldots, \phi_a$. Аналогичным образом, второй базис B' содержит надёжные элементы $F_1, \ldots, F_b$ с весами $P(F_1), \ldots, P(F_b)$ и ненадёжные элементы $G_1, \ldots, G_b$ с весами $P(G_1), \ldots, P(G_b)$; элементы базиса B' реализуют функции $\psi_1, \ldots, \psi_b$.

Базис B согласован с базисом B', если для каждого надёжного элемента F_i базиса B существует подсхема (блок) F_i^* из надёжных элементов базиса B и для каждого ненадёжного элемента G_i существует подсхема G_i^* из элементов базиса B такие, что выполняются следующие условия согласованности:

1) подсхема F_i^* реализует функцию ψ_i и $L_B(F_i^*) \leq P(F_i)$;

2) подсхема G_i^* реализует (при исправном состоянии всех её ненадёжных элементов) функцию ψ_i и $L_B(G_i^*) \leq P(G_i)$;

3) при наличии в подсхеме G_i^* не более чем k неисправных элементов значение на выходе этой подсхемы на любом входном наборе (значений переменных) $\pi = (\pi_1, \ldots, \pi_{r_i})$ равно либо $\psi_i(\widetilde{\pi})$, либо δ $(i = 1, \ldots, b)$.

Теорема 3. *Пусть базис B согласован с базисом B', а f — произвольная булева функция. Тогда*

$$L^k_{B'}(f) \geq L^k_B(f),$$

где верхний индекс k означает, что используются k-самокорректирующиеся схемы.

Приведём пример использования теоремы 3. В работе [7] найдены асимптотики для сложности k-самокорректирующихся схем в базисах $B = \{x\&y, x \vee y, \overline{x}\}$ и $B_1 = \{x\&y, x \vee y\}$ для монотонных симметричных пороговых функций f_2^n в случае однотипных константных

неисправностей типа δ, $\delta \in \{0,1\}$, на выходах элементов. В этой работе предполагалось, что вес каждого надёжного элемента равен p, а вес каждого ненадёжного элемента равен 1, и были установлены следующие асимптотики.

Для схем в базисе B в случае $p \geq k+1$ выполняется асимптотическое (при $n \to \infty$) равенство

$$L_B^k(f_2^n) \sim (k+2)n, \tag{5}$$

а для схем в базисе B_1 при $\delta = 0$ и $p > 0$ получена асимптотика

$$L_{B_1}^k(f_2^n) \sim n \cdot \min\{2p, k+2\}.$$

Заменим в базисах B и B_1 двухвходовые конъюнкторы и дизъюнкторы на l-входовые, $l \geq 3$, оставляя прежние веса элементов, т. е. p для каждого надёжного элемента и 1 для ненадёжного, и перейдём к новым базисам B' и B_1' соответственно. Верхние оценки для сложности k-самокорректрующихся схем, реализующих f_2^n, получаются конструктивно, почти так же, как и верхние оценки в [6]. А вот для получения нижних оценок воспользуемся теоремой 3. В итоге получим следующие асимптотики.

Теорема 4. *Для базиса B', однотипных константных неисправностей типа δ ($\delta \in \{0,1\}$) на выходах элементов, $p \geq k+1$ и последовательности булевых функций f_2^n, $n = 2, 3, \ldots$, выполняется равенство*

$$L_{B'}^k(f_2^n) \sim \frac{(k+2)n}{l-1}.$$

Теорема 5. *Для базиса B_1', однотипных константных неисправностей типа 0 на выходах элементов, $p \geq 1$ и последовательности булевых функций f_2^n, $n = 2, 3, \ldots$, выполняется равенство*

$$L_{B'}^k(f_2^n) \sim \frac{n \cdot \min\{2p, k+2\}}{l-1}.$$

Заметим, что согласованность базисов B и B', а также B_1 и B_1' можно обеспечить, если положить веса надёжных элементов в базисах B и B' равными $\frac{p}{l-1}$, а ненадёжных — равными $\frac{1}{l-1}$ и реализовать конъюнкции и дизъюнкции ранга l с помощью цепочек длины $l-1$ из соответствующих двухвходовых элементов.

Асимптотические оценки сложности схем для монотонных симметрических пороговых функций.

Первая асимптотика для сложности реализации функции f_2^n была установлена М. И. Гринчуком [4] при использовании элементов

базиса $\{x\&y, x \vee y, \overline{x}\}$ (или монотонного базиса $\{x\&y, x \vee y\}$), а затем в работах автора [3, 6, 7]. Существенной особенностью результатов из этих работ является предположение о наличии в базисе элементов, реализующих дизъюнкции. За последние несколько лет Т. И. Красновой и В. М. Красновым установлены новые асимптотики сложности функции f_2^n для существенно иных базисов и иных мер сложности схем.

В работе [8] установлена асимптотика для сложности реализации f_n^2 схемами в базисе $B = \{\&, -\}$:

$$L_B(f_2^n) \sim 3n$$

(сложность схем здесь определяется числом элементов в них). При получении асимптотики верхняя оценка получается конструктивно с использованием несложной модификации метода М. И. Гринчука.

Нижняя оценка получается методом забивания переменных на входах схем константами. Принципиально новым моментом при использовании этого метода является ещё и учёт наличия хотя бы одного инвертора в любой цепи, ведущей от входа схемы к её выходу.

В [9] исследуются k-самокорректирующиеся схемы для f_2^n в базисе $B = \{x\&\overline{y}, 1\}$. Веса надёжных элементов равны p, ненадёжных — 1; неисправные элементы выдают некоторую фиксированную булеву константу δ. Установлено, что при любых фиксированных k, p и δ, удовлетворяющих условию $p > k + 2$, справедлива асимптотика

$$L_B^k(f_2^n) \sim (k + 2)n.$$

В [10] рассматриваются k-самокорректирующиеся схемы из функциональных элементов в базисе $\{x\&y, \overline{x}\}$. Предполагается, что каждый надёжный инвертор имеет вес p. Каждый ненадёжный инвертор имеет вес 1 и в исправном состоянии реализует инверсию, а в неисправном состоянии — некоторую (заданную) булеву константу δ. Все конъюнкторы считаются надёжными элементами с нулевым весом. Установлено, что при любых фиксированных k и p, удовлетворяющих условию $p \geq k + 1$,

$$L_-^k(f_2^n) \sim (k + 1)n$$

(нижний индекс «$-$» означает, что в данном случае имеется в виду так называемая «инверсионная» сложность схем). Отметим, что формально полагая в данном случае $k = 0$, получим асимптотику для инверсионной сложности функции f_2^n.

В [11] найдена асимптотика для конъюнкторной сложности реализации функции f_2^n k-самокорректирующимися схемами в базисе $B = \{x\&y, \overline{x}\}$. Здесь предполагается, что вес надёжного конъюнктора равен p, ненадёжного — единице, а инверторы — надёжные элементы с нулевыми весами. Каждый неисправный ненадёжный элемент реализует (заранее известную фиксированную) константу δ. При $p \geq k + 2$ установлено соотношение

$$L_B^k(f_2^n) \sim (k + 2)n.$$

О сложности и структуре минимальных схем для линейных функций.

Линейные булевы функции относятся к числу наиболее изученных индивидуальных функций с точки зрения реализации их схемами из функциональных элементов. Ряд новых результатов по сложности линейных функций получен в работах Ю. А. Комбарова [12–14]. В работе [12] рассматриваются схемы для линейных булевых функций в базисе $\{x \to y, \overline{x}\&y\}$. Установлено, что для реализации любой из функций $l_n = x_1 \oplus \ldots \oplus x_n$, $\overline{l}_n = x_1 \oplus \ldots \oplus x_n \oplus 1$ необходимо и достаточно $3n - 3$ элементов. Ещё один важный результат этой работы заключается в том, что в ней устанавливается структура минимальных схем. Оказывается, любая минимальная схема для линейной функции в этом базисе может быть разбита на попарно непересекающиеся блоки (подсхемы) всего лишь двух типов. Блок первого типа имеет два входа и содержит два элемента E_1, E_2 «$x \to y$» и один элемент E_3 «$\overline{x}\&y$», причём входы элементов E_1, E_3 соединены со входами блока, выходы элементов E_1, E_3 соединены только со входами элемента E_2, выход которого также является и выходом блока. Блок второго типа получается из блока первого типа заменой элементов «$x \to y$» на элементы «$\overline{x} \to y$» и элемента «$\overline{x} \to y$», наоборот, на элемент «$x \to y$».

Минимальные реализации линейных функций l_n и $\overline{l}_n$ схемами в базисе $B = \{E_1, \ldots, E_k, E^-\}$, где $1 \leq k \leq 6$, элементы $E_1, \ldots, E_k$ — это различные двухвходовые функциональные элементы, реализующие функции из $\{x\&y, x \vee y, \overline{x}\&y, \overline{x} \vee y, \overline{x\&y}, \overline{x \vee y}\}$, а E^- — инвертор, рассматриваются в [13]. Здесь сложность каждой схемы определяется числом двухвходовых функциональных элементов в ней (веса инверторов полагаются равными нулю). Установлено, что сложность реализации каждой из функций $l_n, \overline{l}_n$ при указанных исходных предположениях равна $3n - 3$. Относительно структуры минимальных схем установлено, что в каждой из них можно выделить $n - 1$ непе-

ресекающихся «стандартных» блоков, содержащих по три двухвходовых элемента (и ещё, быть может, несколько «бесплатных» инверторов, взятых в наименьшем количестве).

В работе [14] исследуется структура всех минимальных схем в базисе $\{x\&y, x \vee y, \overline{x}\}$, реализующих линейные функции l и $\overline{l}$. Каждая из этих схем разбивается на $n-1$ взаимно непересекающихся «стандартных» блоков. Каждый из стандартных блоков (всего их 2) представляет собой некоторую схему из четырёх функциональных элементов, реализующую одну из функций l_2, $\overline{l}_2$.

Работа выполнена при финансовой поддержке РФФИ, проект № 11-01-00508.

Список литературы

1. Лупанов О. Б. Асимптотические оценки сложности управляющих систем. — М.: Изд-во МГУ, 1984.

2. Редькин Н. П. Доказательство минимальности некоторых схем из функциональных элементов // Проблемы кибернетики. Вып. 23. — М.: Наука, 1970. — С. 83–101.

3. Редькин Н. П. Об оценках сложности схем из многовходовых функциональных элементов // Дискретная математика. — 2010. — Т. 22, № 1. — С. 50–57.

4. Гринчук М. И. О монотонной сложности пороговых функций // Методы дискретного анализа в теории графов и сложности. Вып. 52. — Новосибирск. Ин-т математики СО РАН, 1992. — С. 41–48.

5. Редькин Н. П. О сложности булевых функций с малым числом единиц // Дискретная математика. — 2004. — Т. 16, № 4. — С. 20–31.

6. Редькин Н. П. Доказательство нижних оценок сложности самокорректирущихся схем методом замены базиса // Вестн. Моск. ун-та. Сер. 1. Матем. Механ. — 2010. — № 3. — С. 14–18.

7. Редькин Н. П. Асимптотически минимальные самокорректирующиеся схемы для одной последовательности булевых функций // Дискретный анализ и исследование операций. — 1996. — Т. 3, № 2. — С. 62–79.

8. Краснова Т. И. Асимптотически минимальные схемы для одной последовательности булевых функций // Вестн. Моск. ун-та. Сер. 15. Вычислит. матем. и киберн. — 2009. — № 3. — С. 53–56.

9. Краснов В. М. О сложности самокорректирующихся схем для симметрических пороговых функций // Материалы X Международного семинара «Дискретная математика и её приложения» (Москва,

1–6 февраля 2010 г.). — М.: Изд-во механико-математического факультета МГУ. — 2010. — С. 117–119.

10. Краснова Т. И. Об инверсионной сложности самокорректирующихся схем для одной последовательности булевых функций // Материалы X Международного семинара «Дискретная математика и её приложения» (Москва, 1–6 февраля 2010 г.). — М.: Изд-во механико-математического факультета МГУ. — 2010. — С. 120–122.

11. Краснова Т. И. О конъюнкторной сложности самокорректирующихся схем для одной последовательности булевых функций // Материалы XVI Международной конференции «Проблемы теоретической кибернетики» (Нижний Новгород, 20–25 июня 2011 г.). — Нижний Новгород: Изд-во Нижегородского госуниверситета. — 2011. — С. 246–249.

12. Комбаров Ю. А. О минимальных реализациях линейных булевых функций схемами из функциональных элементов в базисе $\{x \to y, \overline{x}\&y\}$ // Труды VIII Международной конференции «Дискретные модели в теории управляющих систем» (Москва, 6–9 апреля 2009 г.). — М.: МАКС Пресс. — 2009. — С. 145–149.

13. Комбаров Ю. А. О минимальных реализациях линейных булевых функций схемами из функциональных элементов в некотором базисе // Материалы XVI Международной конференции «Проблемы теоретической кибернетики» (Нижний Новгород, 20–25 июня 2011 г.). — Нижний Новгород: Изд-во Нижегородского госуниверситета. — 2011. — С. 215–218.

14. Комбаров Ю. А. О минимальных схемах для линейных булевых функций // Вестн. Моск. ун-та. Сер. 1. Матем. Механ. — 2011. — № 6. — С. 41–44.

СИСТЕМЫ УПРАВЛЕНИЯ КОНФЛИКТНЫМИ ПОТОКАМИ НЕОДНОРОДНЫХ ТРЕБОВАНИЙ И ПРИНЦИП ЛЯПУНОВА–ЯБЛОНСКОГО

М. А. Федоткин (Нижний Новгород)

1. Введение. В работе [1] впервые предлагается неклассический способ описания и изучения потоков движущихся требований с использованием статистической связи пространственной и временной

характеристик. При этом в потоке различаются два типа требований, а именно, требования с медленным движением и требования с быстрым движением. Это и означает неоднородность требований потока. Также предполагается, что только требования с быстрым движением имеют возможность обгона требований с медленным движением.

Далее рассмотрим вероятностное пространство $(\Omega, \mathcal{F}, \mathbf{P}(\cdot))$. Здесь Ω — достоверный исход, $\omega \in \Omega$ — описание некоторого элементарного исхода случайного эксперимента, определяющего процессы движения входных потоков требований в пространстве, их обслуживание системой и управление ими. Множество наблюдаемых исходов $A \subset \Omega$ данного эксперимента составляет σ-алгебру $\mathcal{F}$, на которой задана вероятностная функция $\mathbf{P}(\cdot)$. Иногда не будем явно фиксировать символ ω как аргумент каких-либо функций или величин. Однако, все случайные события и случайные элементы рассматриваются на указанном пространстве $(\Omega, \mathcal{F}, \mathbf{P}(\cdot))$. Пусть $\eta_j(t) = \eta_j(\omega; t)$ при $t \geq 0$ подсчитывает число всех типов требований потока Π_j, поступающих в систему обслуживания за время $[0, t)$. Тогда случайный процесс $\{\eta_j(t)\colon t \geq 0\}$ — описание временной характеристики потока. В [1] дано обоснование, когда и при каких условиях возникают неординарные потоки Пуассона Π_j, для которых семейство $\varphi_j(k,t) = \mathbf{P}(\{\omega\colon \eta_j(\omega; t) = k\})$, $k \geq 0$, из одномерных распределений имеет вид: $\varphi_j(0,t) = e^{-\lambda_j t}$, $\varphi_j(1,t) = \lambda_j t p_j e^{-\lambda_j t}$,

$$\varphi_j(k,t) = e^{-\lambda_j t} \sum_{w=0}^{[\frac{k}{2}]} \sum_{v=0}^{[\frac{k-2w}{3}]} \frac{p_j^{k-2w-3v} q_j^w s_j^v (\lambda_j t)^{k-w-2v}}{w! v! (k-2w-3v)!}, \quad k \geq 2.$$

Здесь $\lambda_j > 0$ — интенсивность поступления в систему требований с медленным движением. В любой вызывающий момент поступает одна заявка с вероятностью p_j, две — с вероятностью q_j, три — с вероятностью s_j и $p_j + q_j + s_j = 1$. Неординарные потоки такого типа, которые зависят от параметров λ_j, p_j и q_j, обозначаем символом $\Pi_j = \Pi(\lambda_j, p_j, q_j)$.

2. Постановка задачи и основные результаты. При кибернетическом подходе [2] для любой управляющей системы обслуживания необходимо выделить схему, информацию, координаты и функцию. Схема включает структурные блоки: *a*) статистические независимые входные потоки $\Pi_1 = \Pi(\lambda_1, p_1, q_1)$, $\Pi_2 = \Pi(\lambda_2, p_2, q_2)$, ..., $\Pi_m = \Pi(\lambda_m, p_m, q_m)$ неоднородных требований — первый уровень входных полюсов; *b*) статистические независимые потоки на-

сыщения $\Pi_1^{(н)}$, $\Pi_2^{(н)}$, ..., $\Pi_m^{(н)}$ (выходные потоки при максимальной загрузке и эффективном функционировании системы) — второй уровень входных полюсов; *c*) неограниченные накопители $N^{(1)}$, $N^{(2)}$, ..., $N^{(m)}$ очередей соответственно по потокам Π_1, Π_2, ..., Π_m — внешняя память; *d*) устройства δ_1, δ_2, ..., δ_m по организации дисциплины очередей в накопителях — блок по переработке информации внешней памяти; *e*) обслуживающее устройство с $2m$ состояниями $\Gamma^{(1)}$, $\Gamma^{(2)}$, ..., $\Gamma^{(2m)}$ — внутренняя память; *f*) циклический граф переключений этих состояний, когда после состояния $\Gamma^{(r)}$ осуществляется мгновенный переход в состояние $\Gamma^{(r+1)}$ при $r < 2m$ и в состояние $\Gamma^{(1)}$ при $r = 2m$, — блок по переработке информации внутренней памяти; *g*) выходные потоки $\overline{\Pi}_1$, $\overline{\Pi}_2$, ..., $\overline{\Pi}_m$ — выходные полюса. Общая схема таких управляющих систем обслуживания представлена на рис. 1 в работе [2]. Набор состояний очередей в накопителях, множество состояний обслуживающего устройства, входных потоков, потоков насыщения и потоков обслуженных требований определяют информацию системы обслуживания. Номера всех входных потоков, потоков насыщения, выходных потоков, накопителей, механизмов формирования очередей и номера состояний обслуживающего устройства задают координаты системы обслуживания, которые определяют расположение блоков на схеме. Функция системы это циклическое управление конфликтными [2] потоками (разрешение или запрещение начала обслуживания каждого из них) и непосредственно обслуживание неоднородных требований. При фиксированном $j \in \{1, 2, \ldots, m\}$ в состоянии $\Gamma^{(2j-1)}$ в течение времени T_{2j-1} согласно экстремальной стратегии [2] обслуживаются только требования потока Π_j в количестве не более величины $l_j = [\mu_j T_{2j-1}]$, а в состоянии $\Gamma^{(2j)}$ в течение времени T_{2j} запрещается обслуживание потоков. Здесь параметр μ_j^{-1} определяет среднее время обслуживания требования потока Π_j, или μ_j есть интенсивность потока насыщения $\Pi_j^{(н)}$.

Пусть моменты τ_i, $i = 0, 1, \ldots$, суть моменты переключений состояний обслуживающего устройства. В дальнейшем будем отслеживать значения интересующих нас величин в дискретные моменты переключений состояний обслуживающего устройства. Случайную последовательность этих моментов времени обозначим через множество $\tau = \{\tau_i; i = 0, 1, \ldots\}$. Элементы множества τ, вообще говоря, случайны, так как значения T_1, T_2, ..., T_{2m} являются различными, и можно задать вероятность того или иного состояния обслужива-

ющего устройства в начальный момент времени τ_0. При $j = \overline{1,m}$ и $i \geq 0$ введем следующие случайные величины и элементы: 1) $\eta_{j,i}$ — число заявок потока Π_j на промежутке $[\tau_i, \tau_{i+1})$; 2) $\xi_{j,i}$ — максимально возможное число заявок потока Π_j, которые система может обслужить за промежуток $[\tau_i, \tau_{i+1})$; 3) Γ_i — состояние обслуживающего устройства на промежутке $[\tau_i, \tau_{i+1})$; 4) $\kappa_{j,i}$ — число требований потока Π_j в системе в момент τ_i; 5) $\xi'_{j,i}$ — число заявок потока Π_j, которые в действительности покидают систему на промежутке $[\tau_i, \tau_{i+1})$; 6) $\xi'_{j,-1}$ — число заявок потока Π_j, которые в действительности покидают систему на промежутке $[0, \tau_0)$. Каждый из случайных элементов Γ_i, $i \in \{0, 1, \dots\}$, принимает значения из набора $\Gamma = \{\Gamma^{(1)}, \Gamma^{(2)}, \dots, \Gamma^{(2m)}\}$ состояний обслуживающего устройства. Случайные величины $\kappa_{j,i}$, $1 \leq j \leq m$, $i \geq 0$, принимают значения из множества $X = \{0, 1, \dots\}$ возможного числа требований в очереди. Случайные величины $\xi_{j,i}$, $1 \leq j \leq m$, $i \geq 0$, могут принимать значения 0 или l_j, где l_1, l_2, $\dots$, l_m суть заданные натуральные числа. Случайные величины $\xi'_{j,i-1}$, принимают значения из конечного множества $Y_j = \{0, 1, \dots, l_j\}$. Элемент множества Y_j определяет число требований, которые в действительности могут покинуть систему массового обслуживания по j-му направлению.

Перейдем к математическому описанию структурных блоков схемы. Входной полюс первого уровня с номером j (входной поток Π_j) будем описывать с помощью условных одномерных распределений $\mathbf{P}(\eta_{j,i} = k | \Gamma_i = \Gamma^{(s)}) = \varphi_j(k, T_s)$, $k = 0, 1, \dots$ для последовательности случайных величин $\{\eta_{j,i}; i \geq 0\}$. Введем функцию $\beta_j(b; \Gamma^{(s)})$, которая равна единице при $b = l_j$ и $\Gamma^{(s)} = \Gamma^{(2j-1)}$, равна единице при $b = 0$ и $\Gamma^{(s)} \in \Gamma \setminus \{\Gamma^{(2j-1)}\}$, и, наконец, равна нулю в остальных случаях. Входной полюс второго уровня с номером j (поток насыщения $\Pi_j^{(\text{н})}$) будем описывать с помощью условных одномерных распределений $\mathbf{P}(\xi_{j,i} = b | \Gamma_i = \Gamma^{(s)}) = \beta(b; \Gamma^{(s)})$, $b = 0, 1, \dots$, $\Gamma^{(s)} \in \Gamma$, для последовательности случайных величин $\{\xi_{j,i}; i \geq 0\}$. Внешнюю память по потоку Π_j будем математически описывать случайной последовательностью $\{\kappa_{j,i}; i \geq 0\}$. Математическое описание устройства по переработке информации внешней памяти задается рекуррентным соотношением $\kappa_{j,i+1} = \max\{0, \kappa_{j,i} + \eta_{j,i} - \xi_{j,i}\}$. Математическое описание внутренней памяти задается случайной последовательностью $\{\Gamma_i; i \geq 0\}$. Определим отображение $u(\cdot)\colon \Gamma \to \Gamma$ соотношениями $u(\Gamma^{(s)}) = \Gamma^{(s+1)}$ при $1 \leq s < 2m$ и $u(\Gamma^{(2m)}) = \Gamma^{(1)}$.

Тогда математическое описание устройства по переработке информации внутренней памяти задается рекуррентным соотношением $\Gamma_{i+1} = u(\Gamma_i)$. Математическое описание выходного полюса с номером j (выходного потока $\overline{\Pi}_j$) будем задавать последовательностью $\{\xi'_{j,i}; i \geq 0\}$, для которой имеет место рекуррентное соотношение $\xi'_{j,i} = \min\{\kappa_{j,i} + \eta_{j,i}, \xi_{j,i}\}$.

Теорема 1. *Если значение функци* $u(\Gamma^{(r)})$ *равно* $\Gamma^{(1)}$ *при* $r = 2m$ *и равно* $\Gamma^{(r+1)}$ *при* $r = 1, 2, ..., 2m-1$, *то имеет место равенство* $(\Gamma_{i+1}, \kappa_{j,i+1}, \xi'_{j,i}) = (u(\Gamma_i), \max\{0, \kappa_{j,i} + \eta_{j,i} - \xi_{j,i}\}, \min\{\kappa_{j,i} + \eta_{j,i}, \xi_{j,i}\})$.

Теорема 2. *При каждом* $j \in \{1, 2, \ldots, m\}$ *и заданном распределении* $\{\mathbf{P}(\Gamma_0 = \Gamma^{(s)}, \kappa_{j,0} = x, \xi'_{j,-1} = y)\colon \Gamma^{(s)} \in \Gamma, x \in X, y \in Y_j\}$, $j \in \{1, 2, \ldots, m\}$ *начального вектора* $(\Gamma_0, \kappa_{j,0}, \xi'_{j,-1})$ *случайная последовательность*

$$\{(\Gamma_i, \kappa_{j,i}, \xi'_{j,i-1}); i = 0, 1, \ldots\}$$

является управляемой однородной марковской цепью со счетным множеством $\Gamma \times X \times Y_j$ *состояний.*

Теорема 3. *Для одномерных распределений*

$$\{Q_{j,i}(\Gamma^{(s)}, x, y)\colon \Gamma^{(s)} \in \Gamma, x \in X, y \in Y_j\}$$

векторной последовательности $\{(\Gamma_i, \kappa_{j,i}, \xi'_{j,i-1}); i = 1, 2, \ldots\}$ *выполняются по времени* i *следующие рекуррентные соотношения:*

$$Q_{j,i+1}(\Gamma^{(2j)}, 0, y) = \sum_{v=0}^{y} Q_{j,i}(\Gamma^{(2j-1)}, v, 0)\varphi_j(y - v; T_{2j-1}),$$

$$Q_{j,i+1}(\Gamma^{(2j)}, x, l_j) = \sum_{v=0}^{x+l_j} Q_{j,i}(\Gamma^{(2j-1)}, v, 0)\varphi_j(x + l_j - v; T_{2j-1}),$$

$$Q_{j,i+1}(\Gamma^{(2j+1)}, x, 0) = \sum_{w=0}^{l_j-1} Q_{j,i}(\Gamma^{(2j)}, 0, w)\varphi_j(x; T_{2j}) +$$

$$+ \sum_{v=0}^{x} Q_{j,i}(\Gamma^{(2j)}, v, l_j)\varphi_j(x - v; T_{2j}),$$

$$Q_{j,i+1}(\Gamma^{(r)}, x, 0) = \sum_{v=0}^{x} Q_{j,i}(\Gamma^{(r-1)}, v, 0)\varphi_j(x - v; T_{r-1}),$$

где $\Gamma^{(r)} \in \Gamma(j) = \Gamma \setminus \{\Gamma^{(2j)}, \Gamma^{(2j+1)}\}$, $y \in \{0, 1, \ldots, l_j - 1\}$, $x \in X$ *и* $i = 1, 2, \ldots$.

Теорема 4. *Пространство* $\Gamma \times X \times Y_j$ *состояний управляемой векторной марковской последовательности*

$$\{(\Gamma_i, \kappa_{j,i}, \xi'_{j,i-1}), i = 0, 1, \ldots\}$$

разбивается на незамкнутое подмножество

$$\{(\Gamma^{(r)}, x, y)\colon \Gamma^{(r)} \in \Gamma \setminus \{\Gamma^{(2j)}\}, x \in X, y = \overline{1, l_j}\} \cup$$

$$\cup \{(\Gamma^{(2j)}, x, y)\colon x > 0, y = \overline{0, l_j - 1}\}$$

несущественных состояний и на замкнутое подмножество вида $\bigcup_{r=1}^{2m} E_j(\Gamma^{(r)})$ *существенных периодических состояний с периодом* $2m$, *где*

$$E_j(\Gamma^{(s)}) = \{(\Gamma^{(s)}, x, 0)\colon x \in X\}, \Gamma^{(s)} \in \Gamma \setminus \{\Gamma^{(2j)}\},$$

$$E_j(\Gamma^{(2j)}) = \{(\Gamma^{(2j)}, x, l_j)\colon x \in X\} \cup \{(\Gamma^{(2j)}, 0, y)\colon y = 0, 1, \ldots, l_j - 1\}.$$

Теорема 5. *Пусть при* $\Gamma^{(s)} \in \Gamma$ *и* $y \in Y_j$ *следующее равенство* $\Phi_{j,i}(\Gamma^{(s)}, z, y) = \sum_{x=0}^{\infty} Q_{j,i}(\Gamma^{(s)}, x, y) z^x$ *определяет производящую функцию по* z, $|z| \le 1$, *которая соответствует семейству вероятностей* $Q_{j,i}(\Gamma^{(s)}, x, y)$, $x \in X$. *Тогда для производящих функций* $\Phi_{j,i+1}(\Gamma^{(2j)}, z, l_j)$, $\Phi_{j,i+1}(\Gamma^{(2j+1)}, z, 0)$, $\Phi_{j,i+1}(\Gamma^{(r)}, z, 0)$, *где* $\Gamma^{(r)} \in \in \Gamma(j)$, *выполняются следующие рекуррентные по* $i = 1, 2, \ldots$ *соотношения:*

$$\Phi_{j,i+1}(\Gamma^{(2j)}, z, l_j) = z^{-l_j} \Phi_{j,i}(\Gamma^{(2j-1)}, z, 0) \Psi_j(T_{2j-1}, z) -$$

$$- z^{-l_j} \sum_{v=0}^{l_j - 1} Q_{j,i}(\Gamma^{(2j-1)}, v, 0) z^v \sum_{k=0}^{l_j - v - 1} z^k \varphi_j(k; T_{2j-1}),$$

$$\Phi_{j,i+1}(\Gamma^{(2j+1)}, z, 0) = \Phi_{j,i}(\Gamma^{(2j)}, z, l_j) \Psi_j(T_{2j}, z) +$$

$$+ \sum_{w=0}^{l_j - 1} Q_{j,i}(\Gamma^{(2j)}, 0, w) \Psi_j(T_{2j}, z),$$

$$\Phi_{j,i+1}(\Gamma^{(r)}, z, 0) = \Phi_{j,i}(\Gamma^{(r-1)}, z, 0) \Psi_j(T_{r-1}, z), \quad r \notin \{2j, 2j+1\},$$

где $\Psi_j(T_k,z)=\exp\{\lambda_j T_k(s_jz^3+q_jz^2+p_jz-1)\}$, $k=\overline{1,2m}$.

Теорема 6. *Пусть* $T=T_1+T_2+\cdots+T_{2m}$. *Производящие функции* $\Phi_{j,2m(i+1)}(\Gamma^{(2j)},z,l_j)$, $\Phi_{j,2m(i+1)}(\Gamma^{(2j+1)},z,0)$, $\Phi_{j,2m(i+1)}(\Gamma^{(r)},z,0)$, *где* $\Gamma^{(r)}\in\Gamma^{(j)}$, $|z|\le 1$, *удовлетворяют следующим соотношениям:*

$$\Phi_{j,2m(i+1)}(\Gamma^{(2j)},z,l_j)=z^{-l_j}e^{\lambda_jT(p_jz+q_jz^2-1)}\Phi_{j,2mi}(\Gamma^{(2j)},z,l_j)+$$

$$+z^{-l_j}e^{\lambda_jT(p_jz+q_jz^2-1)}\sum_{w=0}^{l_j-1}Q_{j,i}(\Gamma^{(2j)},0,w)-$$

$$-z^{-l_j}\sum_{v=0}^{l_j-1}Q_{j,2m(i+1)-1}(\Gamma^{(2j-1)},v,0)z^v\sum_{k=0}^{l_j-v-1}z^k\varphi_j(k;T_{2j-1}),$$

$$\Phi_{j,2m(i+1)}(\Gamma^{(2j+1)},z,0)=z^{-l_j}e^{\lambda_jT(p_jz+q_jz^2-1)}\Phi_{j,2mi}(\Gamma^{(2j+1)},z,0)+$$

$$+\sum_{w=0}^{l_j-1}Q_{j,2m(i+1)-1}(\Gamma^{(2j)},0,w)\Psi_j(T_{2j},z)-$$

$$-z^{-l_j}\sum_{v=0}^{l_j-1}Q_{j,i}(\Gamma^{(2j-1)},v,0)z^v\sum_{k=0}^{l_j-v-1}z^k\varphi_j(k;T_{2j-1})\Psi_j(T_{2j},z),$$

$$\Phi_{j,2m(i+1)}(\Gamma^{(r)},z,0)=z^{-l_j}e^{\lambda_jT(p_jz+q_jz^2-1)}\Phi_{j,2mi}(\Gamma^{(r)},z,0)-$$

$$-z^{-l_j}\Psi_j(T_{r-1},z)\Psi_j(T_{r-2},z)\times\cdots\times\Psi_j(T_{2j-1},z)\times$$

$$\times\sum_{v=0}^{l_j-1}Q_{j,2m(i+1)-s-2}(\Gamma^{(2j-1)},v,0)z^v\sum_{k=0}^{l_j-v-1}z^k\varphi_j(k;T_{2j-1})+$$

$$+\Psi_j(T_{r-1},z)\Psi_j(T_{r-2},z)\times\cdots\times\Psi_j(T_{2j-1},z)\times$$

$$\times\sum_{w=0}^{l_j-1}Q_{j,2m(i+1)-s-1}(\Gamma^{(2j)},0,w)\Psi_j(T_{2j},z),$$

где $\Gamma^{(r)}\in\Gamma(j)$, $s=r-2j-1$, *если* $r>2j+1$, *или* $s=r+2m-2j-1$, *если* $r<2j$.

Теорема 7. *Последовательность* $\{(\Gamma_i,\kappa_{j,i},\xi'_{j,i-1});i=0,1,\ldots\}$ *при начальном распределении вектора* $(\Gamma_0,\kappa_{j,0},\xi'_{j,-1})$ *является марковской и неравенство* $\lambda_jT(1+q_j+2s_j)-[\mu_jT_{2j-1}]<0$ *является*

необходимым и достаточным условием для существования единственного стационарного режима в системе по потоку Π_j.

Используя эти утверждения в работе исследована математическая модель выходных потоков, возникающих в системе обслуживания и управления m конфликтными потоками типа $\Pi(\lambda, p, q)$ в классе циклических алгоритмов. Доказано, что нелокальное описание выходных потоков в таких неклассических системах обслуживания можно выполнить с помощью маркированного точечного процесса с выделенной дискретной компонентой [2].

Работа выполнена в рамках госбюджетной НИР ННГУ по теме «Математическое моделирование и создание новых методов анализа эволюционных систем и систем оптимизации — № Н-040-0» (регистрационный номер 01201252499) и совместного гранта РФФИ и ГФФИ Украины «Моделирование и анализ систем управления взаимодействующими транспортными потоками высокой интенсивности» (регистрационный номер 01201263419).

Список литературы

1. Федоткин М. А., Рачинская М. А. Исследование математической модели трафика автомобилей на основе подхода Ляпунова–Яблонского // Сборник докладов XVI Международной конференции «Проблемы теоретической кибернетики». — Нижний Новгород: Изд–во ННГУ, 2011. — С. 508–512.

2. Федоткин М. А. Процессы обслуживания и управляющие системы // Мат. вопросы кибернетики. — 1996. — Вып. 6. — С. 51–70.

РЕШЕНИЕ ПРОБЛЕМЫ ОПИСАНИЯ ГРАНИЦ РЕКУРСИВНЫХ КЛАССОВ ОБРАТИМЫХ КЛЕТОЧНЫХ АВТОМАТОВ

И. В. Кучеренко (Москва)

Клеточные автоматы (КА) являются дискретными математическими моделями широкого класса реальных систем вместе с протекающими в них процессами. Важное семейство клеточных автоматов образуют обратимые КА, т. е. такие, в которых не происходит потери информации в процессе их функционирования. Эти объекты имеют много приложений, в том числе в вопросах защиты информации.

Первые исследования обратимых клеточных автоматов относятся к шестидесятым годам двадцатого века. Было замечено, что обратимость эквивалентна сюръективности глобальной функции переходов клеточного автомата (теорема «о райском саде» Мура—Майхилла, [1]). Следующим естественным вопросом, возникшим перед исследователями, стала задача распознавания свойства обратимости. Первым значимым классом, для которого были получены продвижения в этой задаче, стал класс КА с одномерным пространством ячеек. В работе [2] было установлено, что в этом классе существует алгоритм для распознавания обратимости. В той же работе высказана гипотеза, что для многомерных КА свойство обратимости также разрешимо, и даже было предложено попытаться обобщить на них технику одномерного случая. Однако, долгое время прогресса в решении задачи распознавания свойства обратимости многомерных КА не было. Только в девяностые годы было установлено, что эта задача является алгоритмически неразрешимой [3].

Следующим вопросом, связанным с обратимыми КА, является вопрос о доле их в множестве всех клеточных автоматов. С помощью усиления теоремы Мура-Майхилла можно показать, что почти все клеточные автоматы являются необратимыми. До настоящего времени в литературе обратимые КА часто упоминали как экзотический класс малой мощности. Однако, такая точка зрения не отражает реальное положение вещей. В работе [4] было установлено, что асимптотика логарифма числа обратимых клеточных автоматов в любом классе КА с фиксированным шаблоном соседства совпадает с асимптотикой числа всех клеточных автоматов. Это было сделано с помощью явного построения богатого класса обратимых КА с разрешимым свойством обратимости — гранично-перестановочных клеточных автоматов (ГПКА). Одним из замечательных свойств этого класса является возможность моделирования в нем произвольных клеточных автоматов. В частности, в $(k+1)$-мерном ГПКА без увеличения числа состояний можно смоделировать любой k-мерный клеточный автомат, что является усилением известного результата [5].

Отметим, что классификация клеточных автоматов по размерности множества ячеек является довольно грубой и не отражает многих особенностей функционирования КА. В работе приводятся результаты исследования границы между теми классами клеточных автоматов, для которых свойство обратимости является алгоритмически разрешимым, и теми, для которых оно является алгоритмически неразрешимым. Рассматривались семейства классов КА, получающиеся независимыми ограничениями на размерность про-

странства ячеек, число состояний ячейки, шаблон соседства и локальную функцию переходов. Для всех таких семейств классов, не содержащих ограничений на локальную функцию переходов, получены критерии разрешимости свойства обратимости в соответствующем семействе [6]. Для классов бинарных КА, локальные функции переходов которых образуют класс Поста, получен критерий разрешимости свойства обратимости путем явного указания верхних классов Поста для разрешимых случаев [7]. Установлено, что для классов двумерных бинарных клеточных автоматов с малым числом переменных локальной функции переходов свойство обратимости является алгоритмически разрешимым. При этом конструктивно построен класс бинарных КА с фиксированной локальной функцией переходов с 91 переменной, в котором свойство обратимости уже является алгоритмически неразрешимым [8]. Также было построено два класса двумерных клеточных автоматов, отличающихся возможностью конструирования в одном из них одного дополнительного бинарного сигнала, для которых в одном из классов свойство обратимости разрешимо, а в другом — нет [9].

Приведем необходимые определения и сформулируем теоремы, составляющие основные результаты работы.

Формально *клеточный автомат* σ представляет из себя четверку вида $(\mathbb{Z}^k,\ E_n,\ V,\ \varphi)$, где $\mathbb{Z}^k$ — совокупность всех k-мерных векторов с целочисленными координатами; $E_n = \{0,\ 1, \ldots,\ n-1\}$; $V = (v_1,\ v_2, \ldots,\ v_m)$, $m \in \mathbb{N}$, — упорядоченный набор различных ненулевых векторов из $\mathbb{Z}^k$; $\varphi : (E_n)^{m+1} \mapsto E_n$, $\varphi(0, 0, \ldots, 0) = 0$. Элементы множества $\mathbb{Z}^k$ называются *ячейками*, E_n — *состояниями ячеек,* 0 — *состояние покоя.* При помощи *шаблона соседства* V каждой ячейке α ставится в соответствие набор ячеек $V(\alpha) = (\alpha,\ \alpha + v_1,\ \alpha + v_2, \ldots,\ \alpha + v_m)$, который называется *окрестностью ячейки.* Функция φ называется *локальной функцией переходов* клеточного автомата.

Функции $g : \mathbb{Z}^k \mapsto E_n$ называются *состояниями КА. Основная функция переходов* Φ задается как отображение множества всех состояний клеточного автомата σ в себя, причем если $g = \Phi(g')$, то $g(\alpha) = \varphi(g'(\alpha), g'(\alpha + v_1), g'(\alpha + v_2), \ldots, g'(\alpha + v_m)), \forall \alpha \in \mathbb{Z}^k$. *Функционирование КА* определяется как последовательность его состояний $g_0, g_1, g_2, \ldots$, получающаяся в результате применения основной функции переходов к некоторому его состоянию g_0, т. е. $g_t = \Phi(g_{t-1}) = \Phi^t(g_0)$, t — натуральное число. Состояние клеточного автомата, в котором только конечное число ячеек находится в ненулевом состоянии, называется *конфигурацией.*

Клеточный автомат, основная функция переходов которого инъ-

ективна на множестве всех конфигураций, называется *обратимым клеточным автоматом.* По теореме Мура-Майхилла множество обратимых клеточных автоматов совпадает с множеством КА, основная функция переходов которых является сюръективной.

Серия теорем 1–3 ниже связана с классом гранично-перестановочных клеточных автоматов [4]. Обозначим через $NRCA(k,n,V)$ число обратимых клеточных автоматов вида $(\mathbb{Z}^k, E_n, V, \varphi)$.

Теорема 1. *Справедлива следующая оценка*

$$\frac{1}{n}(n!)^{n^m} \leqslant NRCA(k,n,V) \leqslant \frac{n^{m+1}!}{(n^m!)^n},$$

где m — число векторов в шаблоне соседства V.

Обозначим через $NCA_{(k,*,V)}(n)$, где $NCA_{(k,*,V)} : \mathbb{N} \mapsto \mathbb{N}_0$, число клеточных автоматов вида $(\mathbb{Z}^k, E_n, V, \varphi)$. Назовем $NCA_{(k,*,V)}(n)$ функцией роста числа клеточных автоматов с фиксированным шаблоном соседства относительно числа состояний ячейки. С ростом n отношение $NRCA_{(k,*,V)}(n)$ и $NCA_{(k,*,V)}(n)$ стремится к нулю [1]. Тем не менее, имеет место следующее утверждение.

Теорема 2. *Для логарифма функции роста числа обратимых клеточных автоматов $NRCA_{(k,*,V)}(n)$ с фиксированным шаблоном соседства относительно числа состояний ячейки выполняется следующее соотношение*:

$$\lim_{n\to\infty} \frac{\ln NRCA_{(k,*,V)}(n)}{\ln NCA_{(k,*,V)}(n)} = 1.$$

Обозначим через $CA(k,n)$ множество k-мерных клеточных автоматов с n состояниями ячейки. Будем говорить, что клеточный автомат $\sigma \in CA(k,n)$ *вкладывается* в КА $\sigma' \in CA(k',n')$, если выполняются следующие условия.

1) $k \leqslant k'$, $n \leqslant n'$ (полагаем, что $E_n \subset E_{n'}$).

2) Существует $T : \mathbb{R}^k \mapsto \mathbb{R}^{k'}$, T — линейный оператор ранга k такой, что для любой ячейки α, $\alpha \in \mathbb{Z}^k$, выполнено $T(\alpha) \in \mathbb{Z}^{k'}$.

3) Для любого начального состояния f_0 клеточного автомата σ существует начальное состояние f'_0 клеточного автомата σ' такое, что для любого момента времени t, $t \in \mathbb{N}_0$, и для любой ячейки α, $\alpha \in \mathbb{Z}^k$, выполнено $f_t(\alpha) = \Phi^t(f_0)(\alpha) = \Phi'^t(f'_0)(T(\alpha)) = f'_t(T(\alpha))$.

Теорема 3. *Любой k-мерный клеточный автомат вкладывается в $k+1$-мерный обратимый КА с количеством состояний, равным числу состояний исходного клеточного автомата.*

Следующая теорема дает критерий разрешимости свойства обратимости в классах КА с фиксированным шаблоном соседства [6]. Обозначим через $CA(k, *, V)$ класс k-мерных клеточных автоматов с шаблоном соседства V. Клеточный автомат $(\mathbb{Z}^k, E_n, V, \varphi)$, шаблон соседства $V = (v_1, v_2, \ldots, v_m)$ которого удовлетворяет следующему условию

$$\forall i,\ 1 \le i \le m,\ \exists c \in \mathbb{R} \setminus \{0\} :\ v_i = c \cdot v_1,$$

назовем *клеточным автоматом с одномерным шаблоном соседства.*

Теорема 4. *В классе клеточных автоматов $CA(k, *, V)$ свойство обратимости разрешимо тогда и только тогда, когда шаблон соседства V является одномерным.*

Автором было исследовано влияние числа состояний ячейки на разрешимость свойства обратимости [6]. Теорема 5 показывает, что существенной зависимости разрешимости от этого параметра нет.

Теорема 5. *В классе клеточных автоматов $CA(k, n)$ свойство обратимости алгоритмически неразрешимо тогда и только тогда, когда $n > 1$ и $k > 1$.*

Обозначим через $\mathrm{BCA}(K)$ класс бинарных клеточных автоматов с локальными функциями переходов, принадлежащими некоторому классу Поста K [10]. В теореме 5 установлено, что конструктивного способа проверки на обратимость для класса $\mathrm{BCA}(P_2)$ не существует. Следующее утверждение дает усиление указанного результата.

Теорема 6. *В классе* $\mathrm{BCA}(K)$ *свойство обратимости неразрешимо тогда и только тогда, когда $K \supseteq D_1$.*

Теорема 4 позволяет предположить, что свойство обратимости разрешимо в классах КА с фиксированным числом состояний ячейки и шаблонами, близкими к одномерному. Как оказалось, уже в простейшем случае это предположение оказывается неверным.

Г-шаблоном соседства диаметра l будем называть двумерный шаблон $V^{\Gamma}{}_l = ((0,-1),\ (1,0),\ (2,0), \ldots, (l,0))$. Обозначим множество двумерных КА с n состояниями ячейки и Г-шаблоном соседства V^{Γ} через $\mathrm{CA}^{\Gamma}(n)$.

Теорема 7. *В классе* $\mathrm{CA}^{\Gamma}(16)$ *свойство обратимости алгоритмически неразрешимо.*

Обозначим через $CA(2, 2, m, \varphi)$ множество двумерных бинарных клеточных автоматов с фиксированной локальной функцией переходов φ, зависящей от $m+1$ переменных. Автором конструктивно

построен рекордный по значению m класс двумерных бинарных КА с неразрешимым свойством обратимости. Построение является технически очень сложным, занимая порядка семидесяти журнальных страниц [8].

Теорема 8. *Существует булева функция $\varphi(x_0, x_1, \ldots, x_m)$ с 91 переменной ($m = 90$) такая, что в классе $CA(2, 2, m, \varphi)$ свойство обратимости алгоритмически неразрешимо.*

Нами будет рассматриваться один подкласс КА специального вида. Пусть состояния клеточного автомата μ представляют из себя пары вида (x, y), $x \in E_{n_1}$, $y \in E_{n_2}$. Тогда локальную функцию переходов φ можно рассматривать как вектор-функцию (ψ, ϕ), а шаблон соседства V — как пару шаблонов (V_1, V_2), состояние f КА — как пару состояний (f_x, f_y). При этом формула для вычисления значения образа g состояния f будет иметь вид

$$\begin{aligned} g_x(\alpha) = \quad & \psi(f_x(\alpha), f_x(\alpha + v_1^1), \ldots, f_x(\alpha + v_{m_1}^1), \\ & f_y(\alpha), f_y(\alpha + v_1^2), \ldots, f_y(\alpha + v_{m_2}^2)), \\ g_y(\alpha) = \quad & \phi(f_x(\alpha), f_x(\alpha + v_1^1), \ldots, f_x(\alpha + v_{m_1}^1), \\ & f_y(\alpha), f_y(\alpha + v_1^2), \ldots, f_y(\alpha + v_{m_2}^2)), \end{aligned}$$

где $V_1 = (v_1^1, \ldots, v_{m_1}^1)$, $V_2 = (v_1^2, \ldots, v_{m_2}^2)$, $m_1, m_2 \in \mathbb{N}$.

Будем называть клеточный автомат μ *клеточным автоматом с переменной структурой* (КАПС), если вторая компонента состояния ячейки не меняется в процессе функционирования μ, т. е.

$$\phi(x_0, x_1, \ldots, x_{m_1}, y_0, y_1, \ldots, y_{m_2}) = y_0.$$

Для удобства, значение второй компоненты состояния ячейки будем называть основанием, а первой — активным состоянием. Записывать КАПС μ будем в виде шестерки $(\mathbb{Z}^k, E_{n_1}, E_{n_2}, V_1, V_2, \psi)$. В случае, если $n_1 = 2$, будем называть КАПС бинарным.

На клеточные автоматы с переменной структурой распространяется определение обратимости, данное выше для КА. В классе КАПС автору удалось построить наиболее бедный из известных подкласс, в котором можно провести границу между случаями разрешимости и неразрешимости свойства обратимости [9].

Будем считать, что множество ячеек вложено естественным образом в евклидово пространство $\mathbb{R}^k$. Двумерный шаблон соседства V будем называть *полуплоскостным,* если все его вектора находятся в некоторой полуплоскости. Формально это означает, что для шаблона V существует ненулевой вектор $w \in \mathbb{R}^2$ такой, что $\forall v \in V$ $(w, v) \geqslant 0$, где $(\cdot, \cdot)$ — евклидово скалярное произведение.

Будем называть КАПС линейным, если для любого фиксированного значения переменных основания его локальная функция переходов является линейной функцией. Обозначим класс двумерных бинарных линейных клеточных автоматов с переменной структурой, шаблон соседства V_1 которых является полуплоскостным, через $\mathrm{VCA}^{\swarrow}(2,\cdot)$.

Теорема 9. *В классе клеточных автоматов* $\mathrm{VCA}^{\swarrow}(2,\cdot)$ *свойство обратимости разрешимо.*

T-шаблоном соседства радиуса r будем называть двумерный шаблон $V_r^{\top} = ((0,-1), (-r,1), (-r+1,1), \ldots, (r,1))$. Обозначим класс двумерных бинарных линейных КАПС с бинарным основанием, для которых существует $r \in \mathbb{N}$, что $V_1 = V_1^{\top}$, $V_2 = V_r^{\top}$, через $\mathrm{VCA}^{\top}(2,2)$.

Теорема 10. *В классе клеточных автоматов* $\mathrm{VCA}^{\top}(2,2)$ *свойство обратимости алгоритмически неразрешимо.*

Автор выражает благодарность своему научному руководителю академику Кудрявцеву Валерию Борисовичу за постановку задачи и постоянное внимание к работе.

Список литературы

1. Кудрявцев В. Б., Подколзин А. С., Болотов А. А. Основы теории однородных структур. — М.: Наука, 1990.

2. Amoroso S., Patt Y. N. Decision procedures for surjectivity and injectivity of parallel maps for tessellation structures // Journal of Computer and System Sciences. — 1972. — V. 6, № 5. — P. 448–464.

3. Kari J. Reversibility of 2D cellular automata is undecidable // Physica D. — 1994. — Т. 45. — С. 379–385.

4. Кучеренко И. В. О числе обратимых однородных структур // Дискретная математика. — 2003. — Т. 15, вып. 2. — С. 123–127.

5. Toffoli T. Computation and construction universality of reversible cellular automata // Journal of Computer and System Sciences. — 1977. — V. 15, № 2. — P. 213–231.

6. Кучеренко И. В. О разрешимости обратимости клеточных автоматов // Интеллектуальные системы. — 2004. — Т. 8, вып. 1–4. — С. 465–482.

7. Кучеренко И. В. О структуризации класса обратимых бинарных клеточных автоматов // Интеллектуальные системы. — 2005. — Т. 9, вып. 1–4. — С. 445–456.

8. Кучеренко И. В. О минимизации монофункциональных классов бинарных клеточных автоматов с неразрешимым свойством обратимости // Интеллектуальные системы. — В печати.

9. Кучеренко И. В. О структуризации класса обратимых клеточных автоматов // Дискретная математика. — 2007. — Т. 19,

вып. 3. — С. 102–121.

10. Яблонский С. В., Гаврилов Г. П., Кудрявцев В. Б. Функции алгебры логики и классы Поста. — М.: Наука, 1966.

ТРИАНГУЛЯЦИИ ВЫПУКЛЫХ КОНУСОВ И РЕАЛИЗАЦИЯ ИХ f-ВЕКТОРОВ

В. Н. Шевченко (Нижний Новгород)

1. Пусть $\mathbf{Q}$ — поле рациональных чисел, $\mathbf{R}$ — поле вещественных чисел и $\mathbf{F}$ — поле, такое, что $\mathbf{Q} \subseteq \mathbf{F} \subseteq \mathbf{R}$, $\mathbf{Z}$ — кольцо целых чисел, $\mathbf{F}^d$ — линейное пространство d-мерных столбцов (аналогично $\mathbf{F}_d$ — пространство строк), $\mathbf{F}^{m\times n}$ — множество $(m \times n)$-матриц с элементами из $\mathbf{F}$ и $\mathbf{Z}^{m\times n}$ — его подмножество целочисленных матриц. Через A^T обозначим матрицу, транспонированную к A, через $a_{i\bullet}$ и $a_{\bullet j}$ — i-ю строку и j-й столбец матрицы A соответственно и через $r_A = rankA$ — ранг матрицы A. С матрицей A из $\mathbf{F}^{m\times n}$ можно связать четыре многогранных полиэдральных конуса: два конечнопорожденных $A^{\angle} = \{y = Ax/x \in \mathbf{F}^n, x \geq 0\}, A_{\angle} = \{v = uA/u \in \mathbf{F}_m, u \geq 0\}$ и два конечноопределенных $A^* = \{x \in \mathbf{F}^n/y = Ax \geq 0\}, A_* = \{u \in \mathbf{F}_m/v = uA \geq 0\}$.

Следующий фундаментальный факт состоит в том, что понятия конечнопорожденного и конечноопределенного конусов совпадают (см., например, [1, 3, 10, 14]).

Теорема 1 (Г. Минковский, Ю. Фаркаш, Г. Вейль).

1.1. $\forall A \in \mathbf{F}^{m\times d} \ \exists \ B \in \mathbf{F}^{d\times n}/A^* = B^{\angle}$.

1.2. $\forall B \in \mathbf{F}^{d\times n} \ \exists \ A \in \mathbf{F}^{m\times d}/B^{\angle} = A^*$.

1.3. $A^* = B^{\angle} \Leftrightarrow A_{\angle} = B_*$.

Проблема получения по одному описанию конуса его двойственного описания (получения по матрице A матрицы B и наоборот) представляет большой практический и теоретический интерес, и имеется много алгоритмов (см., например, [9] и имеющуюся там библиографию), решающих ее.

Пример 1. Пусть ранг матрицы $B \in \mathbf{Q}^{n\times r}$ равен r, ранг матрицы $A \in \mathbf{Q}^{(n-r)\times n}$ равен $(n - r)$, $AB = 0$, L — линейная оболочка столбцов $b_{\bullet,1}, ..., b_{\bullet,r}$, $L^{\perp}$ — линейная оболочка строк

$a_{1\bullet}, a_{2\bullet}, ..., a_{n-r\bullet}$ матрицы A. Тогда L можно представить двумя способами: $L = (B, -B)^{\angle}$ и $L = \{x \in R^d \ / \ Ax \geq 0, -Ax \geq 0\} = \binom{A}{-A}^*$. Аналогично, $L^{\perp} = \binom{A}{-A}_{\angle} = (B, -B)_*$. Заметим, что эти представления *неприводимы*, т. е. ни один из элементов, порождающих конус, выбросить нельзя, но не минимальны. Положив $b_{\bullet 0} = -\sum_{j=1}^{r} b_{\bullet j}$, получим минимальное (с наименьшим числом порождающих векторов) представление линейного пространства $L = (b_{\bullet 0}, B)^{\angle}$ в виде конечно-порожденного конуса.

Пример 2. Если $m = d = r$, то в качестве B можно взять A^{-1}.

В докладе рассматриваются связи между параметрами матриц A и B.

2. Пусть $F = A^* = B^{\angle}$, $A \in Z^{m \times d}$, $B \in Z^{d \times n}$, $AB = C = (c_{ij}),,$ при $I \in \{1, ..., m\}$ $A(I) = \{a_{i\bullet} \ / i \in I\}$, $A(\overline{I}) = \{a_{i\bullet} / i \notin I\}$ при $J \in \{1, ..., n\}$ $B(J) = \{b_{\bullet j} / \ j \in J\}$, $B(\overline{J}) = \{b_{\bullet j} \ / j \notin J\}$, $I_j = \{i / c_{ij} = 0\}$, $J_i = \{i / c_{ij} = 0\}$. Число r_B назовем *размерностью конуса* A^* и положим $dim A^* = r_B$.

Для каждого $a \in A_{\angle}$ определим *грань* $F(a)$ *конуса* A^* равенством $F(a) = \{x \in A^* / ax = 0\}$ и рассмотрим множество $\Gamma(A^*) = \{A^*(a) / a \in A_{\angle}\}$ всех граней конуса A^*, частично упорядоченное отношением включения. Терминологию и необходимые сведения по частично упорядоченным множествам и решеткам можно получить, например, в [2, 10, 14]. Ясно, что при $J(a) = \{j / ab_{\bullet j} = 0\}$ $F(a) = B^{\angle}(J(a))$. В частности, $F(0) = A^*-$ максимальная грань A^*, а наибольшее из подпространств пространства $\mathbf{F}^d$ $A^{\perp} = \{x \in \mathbf{F}^d / Ax = 0\}-$ минимальная грань A^*. Если $A^{\perp} = \{0\}$, то *конус* A^* называется *острым*.

Число $\rho(a) = rank B(J(a)) + r_A - d$ назовем рангом грани $F(a)$, в частности, число $\rho = \rho(0)$ назовем рангом конуса A^*. Если $\rho(a) = k$, то $F(a)$ назовем k-*гранью* конуса A^* и перенумеруем их. Пусть $|\Gamma_k(F)| = f_k$ и $J^k = \{J_{\mu}^{(k)}, \mu = 0, ..., f_k\}$, где $B^{\angle}(J_{\mu}^{(k)})-$ μ-я k- грань конуса A^*. Она называется симплициальной, если $\left|J_{\mu}^{(k)}\right| = k$. Итак, $\Gamma(A^*) = \bigcup_{i=0}^{\rho} \Gamma_i(A^*)$ является *полиэдральным комплексом*. Множество $\partial(A^*) = \bigcup_{i=0}^{\rho-1} \Gamma_i(A^*)$ называется *граничным* комплексом конуса A^*. При $\rho > 0$ грани множества $\Gamma_{\rho-1}(A^*)$, т. е. максимальные грани $\partial(A^*)$ называются *фасетами конуса* A^*. Если все они симплициальны, то конус A^* называется симплициальным.

Теорема 2.

2.1 *Конус* A^* *можно разложить в прямую сумму* $A^* = B^{\angle}(J_0) + B^{\angle}(\overline{J_0})$, *где* $B^{\angle}(J_0) = A^{\perp}$, *а* $B^{\angle}(\overline{J_0}) = A^* \cap B^{\perp}(J_0)-$ *острый конус.*

2.2. *Комплексы* $\Gamma(A^*)$ *и* $\Gamma(B^{\angle}(\overline{J_0}))$ *изоморфны.*

2.3. *Комплексы* $\partial(A^*)$ *и* $\partial(B^{\angle}(\overline{J_0}))$ *изоморфны.*

Теорема 3 [14].

3.1. $\Gamma(A^*)$ — *градуированная решетка длины* ρ.

3.2. *Если* $G \subseteq F$, *то интервал* $[G, F]$, *т. е. множество граней* H *из* $\Gamma(A^*)$ *таких, что* $G \subseteq H \subseteq F$, *градуированная подрешетка длины* $\rho(F) - \rho(G)$.

3.3. *Каждый интервал длины* 2 *имеет ровно четыре элемента.*

Теорема 4. *Решетки* $\Gamma(A^*)$ *и* $\Gamma(A_{\angle})$ *антиизоморфны.*

Теорема 5 [8]. *Если* $\rho > 0$, *то множество фасет* $F_{\rho-1}(A^*)$ *можно упорядочить так, что при* $i = 1, ..., f_{\rho-1} - 1$ *выполняется условие*

$$F_{i+1} \cap \cup_{k=1}^{i} F_k \subseteq \Gamma_{\rho-2}(F_{i+1}). \tag{1}$$

Начальную и конечную фасеты можно выбрать произвольно.

Условие (1) останется верным, если последовательность граней заменить на противоположную.

Следствие 1. При замене **F** на **Z** все утверждения теорем 1–5 верны.

3. Будем считать теперь, что $A \in \mathbf{Z}^{m\times d}$, $B \in \mathbf{Z}^{d\times n}$ и $r = r_B$ и **F**= **Q**.

Триангуляцией конуса A^* *с узлами из множества* B назовём [4, 11, 12, 14] множество $T(B) = \{S_1, ..., S_t\}$ таких S_τ, для которых выполнены следующие условия:

1) $S_\tau \subseteq \{1, ..., n\}$,

2) $|S_\tau| = r = rankB(S_\tau)$,

3) $B^{\angle} = \bigcup_{\tau=1}^{t} B^{\angle}(S_\tau)$,

4) $B^{\angle}(S_\tau) \cap B^{\angle}(S_\sigma) = B^{\angle}(S_\tau \cap S_\sigma)$.

Множество $\triangle(T(B)) = \bigcup_{\tau=1}^{t} \Gamma(S_\tau)$ даёт пример геометрической реализации d-мерного однородного симплициального комплекса (с.к.) [1]. При $k = 0, ..., d$ обозначим через $\triangle_k = \bigcup_{\tau=1}^{t} \Gamma_k(S_\tau)$ множество k-мерных граней с.к. $\triangle$, положим $f_k(\triangle) = |\triangle_k|$, $f(\triangle) = (f_0(\triangle), ..., f_d(\triangle))$ и

$$f(\lambda, \Delta) = \sum_{k=0}^{d} f_k(\Delta)\lambda^k. \tag{2}$$

Через $\partial\triangle = \Delta \cap \partial P$ обозначим граничный подкомплекс с.к. Δ, и определим многочлен $f(\lambda, \partial\Delta)$ аналогично.

Представим многочлен $f(\lambda, \Delta)$ в виде $f(\lambda, \Delta) = \sum_{k \in \mathbf{Z}_+} \gamma_k(\Delta)\lambda^k (1+\lambda)^{d-k}$ и назовем целочисленную последовательность $\gamma = (\gamma_0, \gamma_1, ...)$ (d, n)-реализуемой, если $\gamma_k = \gamma_k(\Delta)$ при $k = 0, 1, ..., d$ и $\gamma_k = 0$ при $k > d$.

Для формулировки критерия реализуемости необходимо следующее понятие.

Для любых натуральных чисел a и i существует единственное *биномиальное i-разложение числа* $a = \binom{a_i}{i} + \binom{a_{i-1}}{i-1} + ... + \binom{a_j}{j}$, где $a_i > a_{i-1} > ... > a_j \geq j \geq 1$. Тогда число $a^{<i>} = \binom{1+a_i}{1+i} + ... + \binom{1+a_j}{1+j}$ называется *i-й псевдостепенью числа a.*

Утверждение 1. *Если найдется такое k, при котором $\gamma_{k+1} > \gamma_k^{<k>}$, то γ не реализуема ни при каком d. Если $\gamma_{k+1} \leq \gamma_k^{<k>}$, при $k = 1, ..., d-1$, то γ — $(2d)$-реализуема.*

Следующая теорема позволяет находить минимальные d, при которых последовательность γ является d-реализуемой.

Утверждение 2. *Для d-реализуемости целочисленной последовательности $\gamma = (\gamma_0, \gamma_1, \dots)$ необходимо и достаточно, чтобы выполнялись следующие условия:*

1) $\gamma_0 = 1$, $\gamma_i \geq 0$ *при* $i = 1, \dots, d$ *и* $\gamma_k = 0$ *при целых* $k \geq d$,

2) $\gamma_i \leq \gamma_{d-i} \leq \gamma_{d-i-1}$ *при* $i = 1, \dots, \lfloor \frac{d}{2} \rfloor$,

3) $\gamma_{i+1} - \gamma_{j-i} \leq (\gamma_i - \gamma_{j+1-i})^{<i>}$ *при* $j = d, \dots, 2d$ *и* $i = 1, \dots, \lfloor \frac{j}{2} \rfloor$.

Эта теорема обобщает ранее полученный для случая острого конуса результат [6] на случай произвольного конуса и доказывается применением результатов из [5] к с.к. $\triangle(T(B)) \bigcap \Gamma(\partial A^*)$. При этом существенно использовались работы [7, 8, 12, 13].

Список литературы

1. Емеличев В. А., Ковалев М. М., Кравцов М. К. Многогранники, графы, оптимизация. — М.: Наука, 1981.

2. Скорняков Л. А. Элементы алгебры. — М.: Наука, Главная редакция физико-математической литературы, 1980.

3. Черников С. Н. Линейные неравенства. — М.: Наука 1968.

4. Шевченко В. Н. Триангуляции выпуклых многогранников и их булевы функции // Математические вопросы кибернетики. Вып. 16. — М.: Физматлит, 2007. — С. 43–56.

5. Шевченко В. Н. Триангуляции выпуклых многогранников и реализация их f-векторов // Российская конференция "Дискретная оптимизация и исследование операций": Материалы конференции

(Алтай, 27 июня – 3 июля 2010). — Новосибирск: Изд-во Ин-та математики, 2010. — С. 75–81.

6. Шевченко В. Н. Триангуляции многогранных конусов и булевы функции // Информационный бюллетень Ассоциации математического программирования. № 12. (XIV Всероссийская конференция "Математическое программирование и приложения", Екатеринбург, 28 февраля – 4 марта 2011 г.). — Екатеринбург: УрО РАН, 2011. — С. 221–222.

7. Шевченко В. Н., Груздев Д. В. Об f-векторах пирамидальных триангуляций точечных конфигураций // Дискретный анализ и исследование операций. Сер. 2. — 2008. — Т. 15, № 3. — С. 74–90.

8. Bruggesser H., Mani P. Shellable decompositions of cells and spheres // Math. Scand. — 1971. — V. 29. — P. 197–205.

9. Fukuda K., Prodon A. // Lecture Notes in Computer Science. — 1996. — V. 1120. — P. 91–111.

10. Grunbaum B. Convex polytopes. — N-Y: Wiley and Sons, 1967.

11. Kleinschmidt P., Smilansky Z. New results for simplicial spherical polytopes // Discrete and Computation Geometry. DIMACS Series in Discrete Mathematics and Theoretical Computer Science. — 1991. — V. 6, AMS. — P. 187–197.

12. Lee C. Regular triangulations of convex politopes // Applied Geometry and Discrete Mathematics. The Victor Klee Festschrift. DIMACS Series in Discrete Mathematics and Theoretical Computer Science. — 1991. — V. 4, AMS. — P. 443–456.

13. Macaulay F. S. Some properties of enumeration in the theory of modular systems // Proceedings of the London Mathematical Society. — 1927. — V. 26. — P. 531–555.

14. Ziegler G. Lectures on polytopes. — Berlin: Springer-Verlag, 1995.

МОДЕЛИ И АЛГОРИТМЫ В ЗАДАЧЕ ПРОВЕРКИ ЭКВИВАЛЕНТНОСТИ ПРОГРАММ

В. А. Захаров (Москва)

Проблема эквивалентности программ состоит в том, чтобы для произвольной заданной пары программ выяснить, имеют ли эти программы одинаковое поведение. Строгие определения терминов «программа» и «поведение», фигурирующих в этой формулировке, могут варьироваться, и поэтому проблема эквивалентности программ

охватывает целый спектр задач проверки схожести разных видов поведения программ в различных моделях вычислений.

Проблема эквивалентности является одной из первичных проблем в теории вычислений: для ее формулировки в любой модели вычислений достаточно располагать определениями всего лишь двух базовых понятий — программы и ее вычисления.

Велика эпистемологическая значимость проблемы эквивалентности. Изучая методы решения и сложность этой задачи, мы тем самым оцениваем уровень математических средств и объем вычислительных ресурсов, которые потребуются для решения других задач смыслового (семантического) анализа программ.

Проблема эквивалентности возникает при решении ряда задач системного программирования и компьютерной безопасности, включая задачи оптимизации, реорганизации, обфускации и верификации программ, задачи обнаружения метаморфных и полиморфных вирусов, проверки стойкости криптографичесмких протоколов и др.

Отправной точкой в решении задач семантического анализа программ является теорема Райса—Успенского [1], которая гласит о том, что в любой «естественной» универсальной системе программирования любое нетривиальное функциональное свойство программ нерекурсивно. Эта теорема не отменяет возможности получения эффективно проверяемых достаточных условий функциональной эквивалентности программ, но утверждает, что ни одно из этих достаточных условий не будет необходимым. Чтобы установить как можно более общие алгоритмически вычислимые признаки функциональной эквивалентности программ, можно исследовать более сильные виды эквивалентности программ, которые включаются (в теоретико-множественном смысле) в отношение функциональной эквивалентности, не ограничивая при этом класс рассматриваемых программ. В рамках этого направления были построены многочисленные математические модели программ, обнаружены взаимосвязи между этими моделями программ и другими моделями вычислений, используемыми для решения различных прикладных задач (синтаксического анализа и трансляции формальных языков, моделирования систем управления и др.), созданы разрешающие алгоритмы, некоторые из которых нашли применение в системном программировании.

В этой заметке приводится краткий обзор результатов исследований проблемы эквивалентности программ в различных моделях вычислений. Шестидесятилетний период исследования этой проблемы разделен на пять этапов. На каждом этапе выделены наиболее

актуальные для того времени (по мнению автора) задачи, перечислены основные результаты их исследований.

Первые идеи — схемы программ: 1953–63. Первой математической моделью программ можно считать схемы программ Ляпунова—Янова. Концепция этих схем программ была предложена А. А. Ляпуновым и опубликована в статьях [2, 3]. В этих работах высказана мысль о том, что программы, подобно алгебраическим выражениям, могут быть описаны формулами специального вида — схемами программ, — состоящими из элементарных операторов и логических условий (тестов), связь между которыми определяется структурой формулы. Предполагалось, что для схем программ удастся создать такую алгебру или формальное исчисление, правила и законы которых на основании общих сведений об алгебраических свойствах операторов и предикатов, используемых в программах, позволят проводить целенаправленную манипуляцию схемами программ.

Эти ожидания удалось осуществить Ю. И. Янову в статье [4]. В ней были определены семантика схем программ Ляпунова—Янова, отношение эквивалентности схем программ, разработан алгоритм проверки эквивалентности схем программ и описано корректное и полное эквациональное исчисление схем программ.

Первые положительные результаты стимулировали разработку новых видов схем программ и их применение для решения задач системного программирования.

Разнообразие моделей программ: 1964–1973. Пионерская работа Ю. И. Янова [4] не вызвала немедленного отклика ни в математическом мире, ни в зарождающемся сообществе программистов. Новые понятия и задачи, которые привнесло в математику программирование, требовали создания новых, более удобных для понимания форм их представления. Решающую роль в этом сыграли работы В. М. Глушкова и А. П. Ершова.

В. М. Глушков установил взаимосвязь конечных автоматов и схем программ, описал технологию применения теории конечных автоматов для проектирования и оптимизации программ. В совместной работе с А. А. Летичевским [5] им были предложены две новые перспективные идеи. Было показано, что автоматы могут описывать не только поток управления в программах, но также и семантику компонентов программы — операторов и предикатов. Поэтому вычисление программы можно представить как процесс взаимодействия двух автоматов, один из которых задает поток управления в программе, а второй описывает семантику компонентов этой программы. Эта идея и составляет суть концепции дискретных пре-

образователей. Кроме того, опираясь на взаимосвязь между схемами программ, конечными автоматами и регулярными выражениями, В. М. Глушков предложил использовать операции алгебры регулярных выражений в качестве средств конструирования программ, создав таким образом алгебры программ, или алгоритмические алгебры.

Статья А. П. Ершова [6] придала новый импульс развитию теории схем программ. Теоретико-графовое представление схем программ существенно упростило результаты Янова и сократило количество правил в полной системе эквивалентных преобразований схем Ляпунова—Янова. Методы, предложенные в статье [6], был впоследствии развиты в теории статического анализа программ.

В этот период были созданы модели параллельных программ а также многочисленные модификации и обобщения схем Ляпунова—Янова. В работе Д. Лакхема, Д. Парка и М. Патерсона [7] был введен класс стандартных схем программ, а в заметке Дж. де Беккера и Д. Скотта [8] были введены рекурсивные схемы программ, применимые для моделирования функциональных программ.

Большое разнообразие моделей программ, созданных в этот период, привело к формированию нового направления в теоретическом программировании — теории схем программ. Обзор наиболее важных результатов в этой области, полученных к началу 70-х годов, был сделан в статье А. П. Ершова [9]. В ней было отмечено, что основными проблемами теории схем программ являются задачи построения алгоритмов проверки эквивалентности схем программ, создания полных систем эквивалентных преобразований и применения алгоритмов проверки эквивалентности и эквивалентных преобразований схем программ для решения задач системного программирования.

В 60-е годы был получен ряд важных результатов решения проблемы эквивалентности в моделях вычислений, возникших в рамках теории формальных языков и теории автоматов. Было показано, что проблема эквивалентности неразрешима для недетерминированных многоленточных автоматов, недетерминированных автоматов с магазинной памятью, недетерминированных обобщенных автоматов-преобразователей с конечным числом состояний (transducers), а также для детерминированных многоголовочных автоматов.

Проблемы эквивалентности разрешимые и неразрешимые: 1968–1985. В это время были получены почти все основные результаты, позволившие очертить границу между разрешимыми и неразрешимыми случаями проблемы эквивалентности схем программ в различных моделях программ.

М. Патерсон [7] доказал (см. также [10]) неразрешимость проблемы функциональной эквивалентности стандартных схем программ в классе свободных (эрбрановских) интерпретаций сведением к этой задаче проблемы пустоты многоголовочных автоматов. Эти результаты были усилены В. Э. Иткиным и З. Звиногродским [11]; они показали, что любая невырожденная эквивалентность стандартных схем программ, определенная на основе их вычислений во всевозможных интерпретациях, является нерекурсивным отношением. Тем не менее, М. Патерсону, А. А. Летичевскому, Г. Н. Петросяну, А. Б. Годлевскому и В. К. Сабельфельду удалось доказать разрешимость проблемы эквивалентности в некоторых специальных классах свободных стандартных схем программ. В других классах стандартных схем программ, выделенных М. Патерсоном, вопрос о разрешимости этой проблемы остается открытым и по сей день. В статье [7] было отмечено, что задача проверки эквивалентности стандартных схем программ, составленных из одноместных предикатов и операторов присваивания вида `x:=f(x)`, взаимносводима к проблеме эквивалентности детерминированных многоленточных автоматов.

Другое направление исследований эквивалентности стандартных схем программ инициировал В. Э. Иткин; он ввел неинтерпретационное отношение логико-термальной (л.-т.) эквивалентности схем программ, аппроксимирующее отношение функциональной эквивалентности, и доказал его разрешимость [12]. Алгоритмы проверки л.-т. эквивалентности последовательно улучшались и вскоре В. К. Сабельфельду удалось построить полиномиальный по времени алгоритм проверки л.-т. эквивалентности стандартных схем программ [13].

В этот период интенсивно изучалась проблема эквивалентности дискретных преобразователей Глушкова—Летичевского для случаев, когда автоматы, задающие семантику базовых операторов, соответствуют полугруппам. А. А. Летичевский [5], применив технику следов и оригинальный метод устранения несущественных ветвлений, разработал рекурсивный алгоритм проверки эквивалентности дискретных преобразователей над классом разрешимых полугрупп с неразложимой единицей, обладающих свойством левого сокращения. Развивая далее этот результат, Летичевский описал достаточные условия, при которых разрешима проблема эквивалентности дискретных преобразователей над группами, а также установил необходимые и достаточные условия разрешимости проблемы эквивалентности дискретных преобразователей над классом полугрупп, удовлетворяющих законам левого и правого сокращения [14].

Изучение моделей рекурсивных программ также принесло ре-

зультаты. С. Гарленд и Д. Лакхем [15] доказали разрешимость проблемы функциональной эквивалентности в классе линейных унарных рекурсивных схем программ. Вместе с тем, Е. Ашкрофт, З. Манна и А. Пнуели [16], применив технику «альтернирующего стекинга», доказали разрешимость проблемы эквивалентности в классе свободных унарных рекурсивных схем программ. Обнаружилось также, что эта задача значительно труднее аналогичной задачи для стандартных схем программ. Авторами статьи [15] была предпринята попытка построить алгоритм проверки эквивалентности линейных унарных рекурсивных схем программ с константами, аналогичными операторам засылки констант в стандартных схемах программ. Однако оказалось, что эту задачу нельзя решить простой комбинацией известных методов проверки эквивалентности схем программ. Она долгое время оставалась открытой, пока Л. П. Лисовик [17] не сумел найти ее решение, разработав для этого метод «жестких множеств». Но уже для произвольных унарных рекурсивных схем программ с операторами засылки констант, как было впоследствии установлено в статье [18], проблема эквивалентности неразрешима. Одним из важных результатов этого периода была теорема Е. Фридмана [19], показывающая, что проблема эквивалентности унарных рекурсивных схем программ взаимносводима к проблеме эквивалентности детерминированных магазинных автоматов.

Смена ориентиров: 1983–1993. Период 80-х годов — это время пересмотра парадигм и ориентиров, сложившихся на ранних этапах развития программирования, открытие новых задач и направлений исследований. Техническое совершенствование элементной базы вычислительных устройств привело к тому, что компьютеры становились все более дешевыми, компактными и производительными, и поэтому острота многих проблем, приведших к возникновению и развитию теории схем программ, была сглажена. Программирование нуждалось в новых инструментальных средствах, позволяющих сократить издержки при разработке качественных программ. В этот период окрепло понимание того, что разработка математических методов, обеспечивающих корректность программ, — это одна из главных задач теоретического программирования.

Многочисленные модели операторных программ с различными отношениями эквивалентности схем программ потребовали проведения исследований взаимосвязи между этими отношениями эквивалентности с целью обеспечения корректности перенесения результатов проверки эквивалентности, полученных для одних классов схем программ, на другие классы схем программ и сами программы. В статье [20] Р. И. Подловченко предложила новый класс моделей про-

грамм — алгебраические модели программ, — в которых синтаксис схем программ Ляпунова—Янова, отражающий основные особенности устройства императивных программ, сочетается с аппаратом описания семантических свойств программных операторов и логических условий, используемом в модели вычислений дискретных преобразователей Глушкова—Летичевского.

Настойчивые попытки отыскать решение проблемы эквивалентности детерминированных многоленточных автоматов увенчались успехом: Т. Харью и Ю. Кархюмяки [21], применив комбинацию методов теории групп, теории автоматов и теории формальных языков, сумели доказать алгоритмическую разрешимость этой задачи. Однако ее сложность не удалось установить до сих пор.

Значительным достижением теории вычислений в рассматриваемый период было создание семейства новых формальных математических моделей, описывающих устройство и поведение систем взаимодействующих процессов — исчисления взаимодействующих систем Милнера, языка взаимодействующих последовательных процессов Хоара и, позднее, алгебры взаимодействующих процессов Бергстры—Клопа. Наряду с сетями Петри, они стали основными математическими моделями распределенных программ. Для них были определены другие виды эквивалентности, отражающие различные аспекты схожести поведения таких систем — трассовая эквивалентность, наблюдаемая эквивалентность и др. Но наиболее важным для этих теорий оказалось концепция бисимуляции. Именно задача проверки бисимуляционной эквивалентности для различных видов бисимуляции стала одной из центральных проблем в теории систем взаимодействующих процессов. Из наиболее значимых результатов решения задач проверки бисимуляционной эквивалентности для моделей параллельных вычислений можно выделить следующие: 1) построение полиномиальных по времени алгоритмов проверки бисимуляционной эквивалентности между конечными размеченными системами переходов (недетерминированными конечными автоматами) [22] и 2) доказательство разрешимости бисимуляционной эквивалентности для последовательных (BPA) и параллельных (BPP) контекстно-свободных процессов [23, 24].

Проблемы эквивалентности легкоразрешимые и трудноразрешимые: 1991–2012. Отличительная особенность изучения проблемы эквивалентности в этот период — это повышенное внимание, которое уделялось вопросам сложности проверки эквивалентности программ и автоматов, построению как можно более эффективных алгоритмов проверки эквивалентности и расширению области применения методов решения проблемы эквивалентности. В связи с

этим был проведен пересмотр некоторых из ранее полученных результатов о разрешимости проблемы эквивалентности с целью повышения эффективности разрешающих процедур и уточнения оценок сложности задач проверки эквивалентности программ и автоматов.

Наиболее значимый результат этого периода — решение Ж. Сенизергом проблемы эквивалентности детерминированных автоматов с магазинной памятью [25], остававшейся открытой более 30 лет.

Полиномиальные по времени алгоритмы проверки эквивалентности были построены для целого ряда моделей программ, включая машины со сцепленными состояниями, конечные автоматы-преобразователи, детерминированные счетчиковые автоматы, нормированные контекстно-свободные процессы и др.

М. Абади и Э. Гордон, разработавшие исчисление мобильных процессов, предложили использовать отношение тестирующей эквивалентности для проверки свойств конфиденциальности и целостности криптографических протоколов. Алгоритм проверки тестирующей эквивалентности для процессов spi-исчисления, не содержащих операторов репликации или иных средств рекурсивного вычисления, был предложен в статье [26].

В заключение заметим, что в этот период были предложены также новые подходы к решению проблемы функциональной эквивалентности в рамках алгебраической теории моделей программ. Эти подходы преследовали цель разработки эффективных (полиномиальных по времени) процедур проверки эквивалентности и проведения эквивалентных преобразований последовательных программ в моделях, позволяющих описывать и учитывать семантические свойства базовых компонентов программ — операторов и предикатов. Именно эту задачу А. П. Ершов выделил в обзорной статье [9] как одну из основных задач теории схем программ. Для ее решения в работах Р. И. Подловченко [27] и В. А. Захарова [28–30] были предложены полиномиальные по времени алгоритмы проверки эквивалентности последовательных и рекурсивных схем программ.

Список литературы

1. Rice H. G. Classes of recurcively enumerable sets and their decision problems // Trans. of American Math. Soc. — 1953. — V. 74, № 2.

2. Ляпунов А. А., Янов Ю. И. О логических схемах программ // Труды конференции “Пути развития советского математического машиностроения и приборостроения”. Часть 3. — 1956. — С. 5–8.

3. Ляпунов А. А. О логических схемах программ // Проблемы кибернетики. Вып. 1. — М.: Физматгиз, 1958. — С. 46–74.

4. Янов Ю. И. О логических схемах алгоритмов // Проблемы кибернетики. Вып. 1. — М.: Физматгиз, 1958. — С. 75–127.

5. Глушков В. М., Летичевский А. А. Теория дискретных преобразователей // Избранные вопросы алгебры и логики. — Новосибирск: Наука, 1973. — С. 5–39.

6. Ершов А. П. Операторные схемы (Об операторных схемах Янова) // Проблемы кибернетики. Вып. 20. — М.: Наука, 1967. — С. 181–200.

7. Luckham D. C., Park D. M., Paterson M. S. On formalized computer programs // Journal of Computer and System Science. — 1970. — V. 4, № 3. — P. 220–249.

8. De Bakker J. W., Scott D. A. Theory of programs. Unpublished notes. — Vienna: IBM Seminar, 1969.

9. Ершов А. П. Современное состояние теории схем программ // Проблемы кибернетики. Вып. 27. — М.: Наука, 1973. — С. 87–110.

10. Летичевский А. А. Функциональная эквивалентность дискретных преобразователей II // Кибернетика. — 1970. — № 2. — С. 14–28.

11. Itkin V. E., Zwinogrodski Z. On program schemata equivalence // Journal of Computer and System Science. — 1972. — V. 6, № 1. — P. 88–101.

12. Иткин В. Э. Логико-термальная эквивалентность схем программ // Кибернетика. — 1972. — № 1. — С. 5–27.

13. Сабельфельд В. К. Полиномиальная оценка сложности распознавания логико-термальной эквивалентности // Доклады АН СССР. — 1979. — Т. 249, № 4. — С. 793–796.

14. Летичевский А. А. Эквивалентность автоматов относительно полугрупп с сокращением // Проблемы кибернетики. Вып.27. — М.: Наука, 1973. — С. 195–212.

15. Garlend S. J., Luckham D. C. Program schemes, recursion schemes and formal languages // Journal of Computer and System Science. — 1973. — V. 7, № 2. — P. 119–160.

16. Ashcroft E., Manna Z., Pnueli A. A decidable properties of monadic functional schemes // Journal of the ACM. — 1973. — V. 20, № 3. — P. 489–499.

17. Лисовик Л. П. Металинейные схемы с засылками констант // Программирование. — 1985. — № 2. — С. 29–38.

18. Лисовик Л. П. Стандартные схемы с магазинами // Доклады АН УССР. — 1989. — № 12. — С. 23–27.

19. Friedman E. P. Equivalence problems for deterministic languages and monadic recursion schemes // Journal of Computer System Science. — 1977. — V. 14. — P. 362–399.

20. Подловченко Р. И. Моделирование программ схемами и построение систем преобразований схем // Кибернетика. — 1982. — № 6. — С. 23–29.

21. Harju T., Karhumaki J. The equivalence of multi-tape finite automata // Theoretical Computer Science – 1991. – V. 78, № 2. — P. 347–355.

22. Kanellakis P. C., Smolka S. A. CCS expressions, finite state processes, and three problems of equivalence // Information and Computation. — 1990. — V. 86, № 1. — P. 43–68.

23. Baeten J. C. M., Bergstra J. A., Klop J. W. Decidability of bisimulation equivalence for processes generating context-free languages // Lecture Notes in Computer Science. — 1987. — V. 259. — P. 93–114.

24. Christensen S, Hirshfeld Y., Moller F. Bisimulation equivalence is decidable for basic parallel processes // Lecture Notes in Computer Science. — 1993. — V. 715. — P. 143–157.

25. Senizergues G. The equivalence problem for deterministic pushdown automata is decidable // Lecture Notes in Computer Science. — 1997. — V. 1256. — P. 271–281.

26. Durante L., Sisto R., Valenzano A. Automatic testing equivalence verification of spi calculus // Journal ACM Transactions on Software Engineering and Methodology. — 2003. — V. 12, № 2.

27. Подловченко Р. И. К вопросу о полиномиальной разрешимости проблемы эквивалентности в алгебраических моделях программ // Кибернетика и системный анализ. — 2012. — № 4.

28. Zakharov V. A. An efficient and unified approach to the decidability of equivalence for propositional program schemes // Lecture Notes in Computer Science. — 1998. — V. 1443. — P. 247–258.

29. Zakharov V. A. On the decidability of the equivalence problem for monadic recursive programs // Theoretical Informatics and Applications — 2000. — V. 34, № 2. — P. 157–171.

30. Захаров В. А. Проверка эквивалентности программ при помощи двухленточных автоматов // Кибернетика и системный анализ. — 2010. — № 4. — С. 39–48.

СЛОЖНОСТЬ РАСШИФРОВКИ ПОРОГОВЫХ ФУНКЦИЙ МНОГОЗНАЧНОЙ ЛОГИКИ

Н. Ю. Золотых, А. Ю. Чирков (Нижний Новгород)

Введение

Пусть $E_k^n = \{0, 1, \ldots, k-1\}^n$, $k \geq 2$, $n \geq 1$. Обозначим $\mathcal{F}(n,k)$ множество всех функций $f : E_k^n \to \{0,1\}$, в частности, $\mathcal{F}(n,2)$ — множество всех булевых функций n переменных. Рассмотрим некоторый класс $\mathcal{F}' \subseteq \mathcal{F}(n,k)$. Под *расшифровкой* функции в классе $\mathcal{F}'$ понимают восстановление значений заранее не известной функции f из известного класса $\mathcal{F}'$ с помощью обращений к оракулу этой функции. Под *оракулом* функции f понимают некоторую процедуру, которая по заданному $x \in E_k^n$ возвращает $f(x)$.

Впервые задача расшифровки рассматривалась В. К. Коробковым и Т. Л. Резником [1] и В. К. Коробковым [2, 3] для класса монотонных булевых функций. Сложность расшифровки монотонных булевых функций установил G. Hansel [4]. Оптимальный по числу вопросов и используемой памяти алгоритм расшифровки предложил Н. А. Соколов [5]. Задачу расшифровки монотонных функций многозначной логики рассматривали В. К. Коробков [6], В. Б. Алексеев [7], А. В. Сержантов [8] и др. М. В. Горяинов и А. А. Сапоженко [9] предложили алгоритм расшифровки монотонных функций на частично упорядоченных множествах. Другие сведения о монотонных функциях и задаче расшифровки монотонных функций приведены в обзоре А. Д. Коршунова [10].

Рассматриваются задачи расшифровки функций из других классов (А. А. Вороненко, В. В. Осокин, Э. Э. Гасанов и др.) Задача интенсивно изучается в рамках теории тестов [11] и вычислительной теории машинного обучения (Computational Learning Theory) [12].

Для функции $f \in \mathcal{F}(n,k)$ обозначим

$$M_\nu(f) = \{x \in E_k^n : \ f(x) = \nu\} \qquad (\nu = 0, 1).$$

Функция $f \in \mathcal{F}(n,k)$ называется *пороговой*, если существуют вещественные числа $a_0, a_1, \ldots, a_n$, такие, что

$$M_0(f) = \left\{ x \in E_k^n : \ \sum_{j=1}^{n} a_j x_j \leq a_0 \right\},$$

при этом неравенство

$$\sum_{j=1}^{n} a_j x_j \le a_0$$

называется *пороговым*. Очевидно, его коэффициенты можно сделать целыми. Обозначим $\mathcal{T}(n,k)$ множество всех пороговых функций, заданных на E_k^n, т. е. множество пороговых функций k-значной логики n переменных. В частности, $\mathcal{T}(n,2)$ — множество всех булевых пороговых функций n переменных.

Задачу расшифровки пороговых функций k-значной логики поставил В. Н. Шевченко [13]. В случае пороговых функций уточним термин «расшифровка»: под *расшифровкой пороговой функции* будем понимать алгоритм поиска коэффициентов порогового неравенства заранее не известной функции f с помощью обращений к ее оракулу.

Задача расшифровки пороговых функций тесно связана с проблемой оценки числа таких функций. Заметим, что задача оценки числа пороговых функция является весьма сложной. До сих пор не известна асимптотика числа пороговых булевых функций. Из результатов Л. Шлёфли [14] о числе открытых областей, получаемых при разбиении n-мерного пространства K гиперплоскостями, легко получить верхнюю оценку:

$$|\mathcal{T}(n,2)| < 2\sum_{j=0}^{n} \left(\begin{array}{c} 2^n - 1 \\ j \end{array} \right) < 2^{n^2}.$$

С. Яджима и Т. Ибараки [15] получили первую нетривиальную нижнюю оценку:

$$|\mathcal{T}(n,2)| > 2^{n^2/2}.$$

Ю. А. Зуев [16, 17] доказал, что

$$|\mathcal{T}(n,2)| > 2^{n^2(1-10/\ln n)},$$

тем самым установив асимптотику логарифма числа булевых пороговых функций:

$$\log_2 |\mathcal{T}(n,2)| \sim n^2 \qquad (n \to \infty). \tag{1}$$

При этом использовался один комбинаторно-вероятностный результат о ± 1-матрицах, полученный А. М. Одлыжко [18]. Другой подход

к получению асимптотики (1), также использующий лемму Одлыжко, предложил А. А. Ирматов [19].

Обстоятельный обзор результатов по пороговым булевым функциям и пороговым представлениям булевых функций содержится в [20].

Для числа пороговых функций k-значной логики А. А. Ирматов и Ж. Д. Ковиянич [21] получили нижнюю оценку:

$$|\mathcal{T}(n,k)| \geq \frac{1}{2} \left(\begin{array}{c} k^n \\ \lfloor n - 4 - 2n/\log_k n \rfloor \end{array} \right) |\mathcal{T}(\lfloor 2n/\log_k n + 4 \rfloor,\, k)|,$$

справделивую для достаточно больших n. Отсюда и из результатов Л. Шлёфли получается асимптотика логарифма числа таких функций:

$$\log_2 |\mathcal{T}(n,k)| \sim n^2 \log_2 k \qquad (n \to \infty).$$

Для пороговых функций k-значной логики двух переменных в [22] получена оценка:

$$|\mathcal{T}(2,k)| = \frac{6k^4}{\pi^2} + O(k^3 \log k) \qquad (k \to \infty).$$

Рассмотрим несколько областей, в которых возникает задача расшифровки функции из разных классов, в том числе из класса пороговых функций. В вычислительной теории машинного обучения Д. Англуин [12] предложила следующую модель обучения с помощью *вопросов принадлежности* (membership queries). Пусть M — конечное множество, $\mathcal{C} \subseteq M$, $\mathsf{C} \subseteq 2^M$. Назовем M *пространством примеров* (instance space), $\mathcal{C}$ — *понятием* (concept), C — *классом понятий* (concept class). *Ученик* с помощью вопросов вида «$x \in \mathcal{C}$?», где $x \in M$, должен дать описание заранее не известного $\mathcal{C}$ из некоторого известного класса C.

Одной из важнейших задач целочисленного линейного программирования является *задача о рюкзаке*. Рассмотрим один из ее вариантов: необходимо найти

$$\max \sum_{j=1}^{n} c_j x_j$$

при ограничениях

$$x \in \mathcal{C} \equiv \left\{ x \in E_k^n : \ \sum_{j=1}^{n} a_j x_j \leq a_0 \right\}.$$

Предположим, что k, n, $(c_1, c_2, \ldots, c_n) \in \mathbf{Z}^n$ известны, а $\mathcal{C}$ задано с помощью оракула, позволяющего по произвольной точке $x \in E_k^n$ отвечать на вопрос «$x \in \mathcal{C}$?». Очевидно, что эту задачу можно свести к расшифровке пороговой функции, заданной оракулом.

Пусть $\mathcal{A}$ — алгоритм расшифровки в классе $\mathcal{F}' \subseteq \mathcal{F}(n,k)$. Обозначим через $\tau(\mathcal{A}, f)$ число обращений к оракулу при расшифровке функции $f \in \mathcal{F}'$, а через $\rho(\mathcal{A}, f)$ — количество операций при расшифровке функции $f \in \mathcal{F}'$.

Оракульной сложностью алгоритма $\mathcal{A}$ назовем

$$\tau(\mathcal{A}) = \max_{f \in \mathcal{F}'} \tau(\mathcal{A}, f).$$

Вычислительной трудоемкостью алгоритма $\mathcal{A}$ назовем

$$\rho(\mathcal{A}) = \max_{f \in \mathcal{F}'} \rho(\mathcal{A}, f).$$

Оракульной сложностью расшифровки в классе $\mathcal{F}'$ называется

$$\tau(\mathcal{F}') = \min_{\mathcal{A}} \tau(\mathcal{A}) = \min_{\mathcal{A}} \max_{f \in \mathcal{F}'} \tau(\mathcal{A}, f).$$

Вычислительной трудоемкостью расшифровки в классе $\mathcal{F}'$ называется

$$\rho(\mathcal{F}') = \min_{\mathcal{A}} \rho(\mathcal{A}) = \min_{\mathcal{A}} \max_{f \in \mathcal{F}'} \rho(\mathcal{A}, f).$$

Множество $T \subseteq E_k^n$ называется *разрешающим* (также используется термин *проверочный тест*) для $f \in \mathcal{F}'$ относительно класса $\mathcal{F}'$, если для любой функции $g \in \mathcal{F}'$, $f \neq g$, найдется по крайней мере одна точка $z \in T$, такая, что $g(z) \neq f(z)$. Понятие разрешающего множества введено В. К. Коробковым и Т. Л. Резником [1] в контексте монотонных булевых функций. Разрешающее множество, никакое собственное подмножество которого не является разрешающим для f, называется *тупиковым*. Разрешающее множество функции f минимальной мощности называется ее *наименьшим* разрешающим множеством. Например, тупиковое разрешающее множество монотонной функции единственно и составлено из ее верхних нулей и нижних единиц [1, 7].

Пусть $\sigma(f, \mathcal{F}')$ — мощность наименьшего разрешающего множества для $f \in \mathcal{F}'$ относительно класса $\mathcal{F}'$. *Длиной обучения* в классе $\mathcal{F}'$ называется

$$\sigma(\mathcal{F}') = \max_{f \in \mathcal{F}'} \sigma(f, \mathcal{F}').$$

Нетрудно видеть, что

$$\sigma(f, \mathcal{F}') = \min_{\mathcal{A}} \tau(\mathcal{A}, f),$$

поэтому

$$\sigma(\mathcal{F}') = \max_{f \in \mathcal{F}'} \min_{\mathcal{A}} \tau(\mathcal{A}, f).$$

Нетрудно видеть, что для любого класса $\mathcal{F}'$

$$\sigma(\mathcal{F}') \le \tau(\mathcal{F}').$$

Обозначим

$$\tau(n,k) = \tau\big(\mathcal{T}(n,k)\big), \qquad \sigma(n,k) = \sigma\big(\mathcal{T}(n,k)\big).$$

Если P — полиэдр (выпуклое многогранное множество) в $\mathbf{R}^n$, то обозначим $\operatorname{Vert} P$ множество его вершин. Если $X \subseteq \mathbf{R}^n$, то обозначим $\operatorname{Conv} X$ — выпуклую оболочку множества X, а $\operatorname{Cone} X$ — коническую оболочку этого множества (множество всех неотрицательных линейных комбинаций).

1. Характеризация разрешающего множества и оценки длины обучения

Легко видеть, что для любого алгоритма $\mathcal{A}$ расшифровки функций из класса $\mathcal{T}(E_2^n)$ справедливо

$$\tau(\mathcal{A}) = 2^n = |E_2^n|,$$

откуда

$$\tau(n,k) \ge \sigma(n,k) \ge \tau(n,2) = \sigma(n,2) = 2^n.$$

Итак, алгоритма расшифровки пороговой функции k-значной логики с полиномиальной от n оракульной сложностью не существует. Поэтому в первую очередь нас будет интересовать асимптотика величин $\tau(n,k)$ и $\sigma(n,k)$ при $k \to \infty$ и фиксированном n.

С каждой функцией $f \in \mathcal{T}(n,k)$ в пространстве коэффициентов $a_0, a_1, \ldots, a_n$ свяжем так называемый *конус $C(f)$ разделяющих функционалов*, заданный как множество решений следующей системы:

$$\begin{cases} \sum\limits_{j=1}^{n} a_j x_j \le a_0 & \text{при всех} \quad (x_1, \ldots, x_n) \in M_0(f); \\ \sum\limits_{j=1}^{n} a_j x_j > a_0 & \text{при всех} \quad (x_1, \ldots, x_n) \in M_1(f). \end{cases} \tag{2}$$

Пусть $T_\nu \subseteq M_\nu(f)$ $(\nu = 0, 1)$. Рассмотрим подсистему системы (2):

$$\begin{cases} \sum\limits_{j=1}^{n} a_j x_j \le a_0 & \text{при всех} \quad (x_1, \ldots, x_n) \in T_0; \\ \sum\limits_{j=1}^{n} a_j x_j > a_0 & \text{при всех} \quad (x_1, \ldots, x_n) \in T_1. \end{cases} \tag{3}$$

Утверждение. *Для того, чтобы множество $T = T_0 \cup T_1$, $T_\nu \subseteq M_\nu(f)$ $(\nu = 0, 1)$ было разрешающим для $f \in \mathcal{T}(n, k)$, необходимо и достаточно, чтобы система неравенств* (2) *была эквивалентна системе неравенств* (3).

Можно доказать, что в системе (2) найдется минимальная подсистема, эквивалентная всей системе:

$$\begin{cases} \sum\limits_{j=1}^{n} a_j x_j \le a_0 & \text{при всех} \quad (x_1, \ldots, x_n) \in T_0(f); \\ \sum\limits_{j=1}^{n} a_j x_j > a_0 & \text{при всех} \quad (x_1, \ldots, x_n) \in T_1(f). \end{cases}$$

Следствие 1. *Для любой $f \in \mathcal{T}(n, k)$ множество $T = T_0 \cup T_1$, где $T_\nu \subseteq M_\nu(n, k)$ $(\nu = 0, 1)$, является тупиковым разрешающим тогда и только тогда, когда $T_\nu = T_\nu(f)$ $(\nu = 0, 1)$.*

Следствие 2. *Для любой $f \in \mathcal{T}(n, k)$ существует единственное тупиковое разрешающее множество $T(f) = T_0(f) \cup T_1(f)$.*

Обозначим $P_\nu(f) = \operatorname{Conv} M_\nu(f)$ $(\nu = 0, 1)$. В. Н. Шевченко [23] показал, что для любой $f \in \mathcal{T}(n, k)$ множество $\operatorname{Vert} P_0(f) \cup \operatorname{Vert} P_1(f)$ является разрешающим. Оценивая $|\operatorname{Vert} P_0(f) \cup \operatorname{Vert} P_1(f)|$ сверху, В. Н. Шевченко доказал, что

$$\sigma(n, k) \le 2^n \log_2^n (k + 1).$$

Более точную (при фиксированном n) оценку получил T. Hegedüs [24] на основе результатов [25] о числе вершин в неявно заданных целочисленных полиэдрах:

$$\sigma(n, k) = O(\log_2^{n-1} k) \qquad (k \to \infty).$$

Первая нетривиальная оценка снизу получена В. Н. Шевченко, Н. Ю. Золотых [26, 27]: при любом фиксированном $n \ge 2$

$$\sigma(n, k) = \Omega(\log_2^{n-2} k) \qquad (k \to \infty).$$

Прогресс на пути построения более точных верхних и нижних оценок для величины $\sigma(n,k)$ происходил за счет использования новых результатов о числе вершин в неявно заданных целочисленных полиэдрах. Полиэдр называется *целочисленным*, если все его вершины целые. В частности, в [28] получена двусторонняя оценка:

$$\frac{\Big(\frac{1}{2}\log k - n - 3 - (n-1)\log(n-2)\Big)^{n-2}}{4(n-1)3^{n-1}(n-2)^{n-2}\Big((n-2)!\Big)^2} \le$$

$$\le \sigma(n,k) \le 2n\log(2n)\Big(1+\log(k+1)\Big)^{n-1}.$$

Существует гипотеза, утверждающая, что при любом фиксированном $n \ge 2$

$$\sigma(n,k) = \Theta(\log_2^{n-2} k) \qquad (k \to \infty).$$

Ниже эта гипотеза будет доказана.

Рассмотрим полиэдр $P = \{x \in \mathbf{R}^n : \ Ax \le a_0\}$, где $A \in \mathbf{Z}^{m\times n}$, $a_0 \in \mathbf{Z}^m$, и целочисленный полиэдр $P_{\mathbf{Z}} = \mathrm{Conv}(P \cap \mathbf{Z}^n)$. Проблемой получения оценок $|\operatorname{Vert} P_{\mathbf{Z}}|$ занимались В. Н. Шевченко, С. И. Веселов, А. Ю. Чирков, A. S. Hayes, D. C. Larman, I. Bárány, R. Howe, L. Lovász, W. Cook, M. Hartmann, R. Kannan, C. McDiarmid и др. См. обзор работ в [29].

Одним из основных инструментов при оценке числа вершин неявно заданных целочисленных полиэдров является подход, впервые предложенный В. Н. Шевченко [30] и основанный на отображении множества $\operatorname{Vert} P_{\mathbf{Z}}$ на множество, обладающее свойством разделенности. Говорят, что множество $G \subset \mathbf{Z}_+^n$ обладает *свойством разделенности* [30], если из условий $x, y \in G$, $x \ne y$ следует $2x - y \notin \mathbf{Z}_+^n$, где $\mathbf{Z}_+^n = \{x \in \mathbf{R}^n : \ x \ge 0\}$.

Лемма [30]. *Пусть множество $G \subset \mathbf{Z}_+^n$ обладает свойством разделенности и для каждого $x = (x_1, x_2, \ldots, x_n) \in G$ выполнено $\alpha_i \le x_j \le \beta_j$ $(j = 1, \ldots, n-1)$, где $\alpha_1, \alpha_2, \ldots, \alpha_{n-1}$, $\beta_1, \beta_2, \ldots, \beta_{n-1}$ — неотрицательные числа, тогда*

$$|G| \le \prod_{j=1}^{n-1} \left\lfloor 1 + \log_2 \frac{\beta_j + 2}{\alpha_j + 1} \right\rfloor.$$

Наилучшая (при фиксированном n) из известных оценок для $|\operatorname{Vert} P_{\mathbf{Z}}|$ получена в [29].

Теорема 1 [29]. *Пусть* $P = \{x \in \mathbf{R}^n : Ax \le a_0\}$, $A \in \mathbf{Z}^{m\times n}$, $a_0 \in \mathbf{Z}^m$, *тогда*

$$|\operatorname{Vert} P_{\mathbf{Z}}| \le (n+1)^{n+1} n!\, \xi_n(m) \left(1 + \frac{1}{2}\log(n+1) + \log\Delta\right)^{n-1},$$

где

$$\xi_n(m) = \binom{m - \lfloor\frac{n-1}{2}\rfloor - 1}{\lfloor\frac{n}{2}\rfloor} + \binom{m - \lfloor\frac{n}{2}\rfloor - 1}{\lfloor\frac{n-1}{2}\rfloor},$$

Δ *равно максимуму из абсолютных значений миноров порядка* $n+1$ *матрицы*

$$\begin{pmatrix} A & a_0 \\ 0 & 1 \end{pmatrix}.$$

Точка $x \in P \cap \mathbf{Z}$ называется *неприводимой*, если ее нельзя представить в виде полусуммы двух других точек из $P \cap \mathbf{Z}$. Легко видеть, что всякая вершина целочисленного полиэдра $P_{\mathbf{Z}}$ неприводима. Обратное, вообще говоря, не верно. Как отмечено, например, в [31], все известные подходы к оценке числа $|\operatorname{Vert} P_{\mathbf{Z}}|$ основаны на оценке количества неприводимых точек.

Пусть $f \in \mathcal{T}(n,k)$. Обозначим $K(f) = \operatorname{Cone}\big(M_1(f) - M_0(f)\big)$, $F_0(f) = \operatorname{Conv} M_0(f) - K(f)$, $F_1(f) = \operatorname{Conv} M_1(f) + K(f)$.

В [32] дано описание множества $T(f)$ в терминах $F_0(f)$, $F_1(f)$.

Теорема 2 [32]. *Пусть* $f \in \mathcal{T}(n,k)$, *тогда* $T_\nu(f) = \operatorname{Vert} F_\nu(f)$ $(\nu = 0,1)$.

Следствие. *Пусть* $f \in \mathcal{T}(n,k)$, $x, y \in T_\nu(f)$ $(\nu = 0,1)$, $x \ne y$. *Тогда*

$$2x - y \notin F_0(f) \cup F_1(f). \tag{4}$$

Удобного описания множества $F_0(f) \cup F_1(f)$ в общем случае не известно. Рассмотрим однако множество $\mathcal{T}'(n,k)$ таких пороговых функций f, для каждой из которых найдется пороговое неравенство, для которого

$$a_0 \in \mathbf{Z}, \quad a_j \in \mathbf{Z}, \quad 0 < a_0 < a_j(k-1) \qquad (j = 1,2,\ldots,n).$$

Если $f \in \mathcal{T}'(n,k)$, то $F_0(f) \cup F_1(f) = \mathbf{Z}^n_+$ и свойство (4) эквивалентно *свойству разделенности*.

Теорема 3 [32]. *Для любой* $f \in \mathcal{T}'(n,k)$ *при* $n \geq 2$

$$|T_\nu(f)| \leq n(1+\log_2 n)\Big(1+\log_2(k+1)\Big)^{n-2} \qquad (\nu = 0,1).$$

Теорема 4. *При любом фиксированном* $n \geq 2$

$$\sigma(n,k) = O(\log_2^{n-2} k) \qquad (k \to \infty).$$

Доказательство. Не нарушая общности, предположим, что коэффициенты порогового неравенства функции $f \in \mathcal{T}(n,k)$ удовлетворяют неравенствам $a_1 \geq a_2 \geq \cdots \geq a_n \geq 0$.

Если $a_0 \leq (k-1)a_n$, то доказываемая оценка следует из теоремы 3. Рассмотрим случай, когда $a_0 > (k-1)a_n$. Если $e_n \notin K(f)$, то из $x \in T_\nu(f)$ следует $x_n = 0$ или $x_n = k-1$, поэтому $|T_\nu(f)| \leq 2\sigma(n-1,k)$.

Пусть $e_n \in K(f)$. Положим

$$T_0'(f) = \{x \in T_0(f) : \sum_{j=1}^{n-1} a_j x_j \leq a_0 - (k-1)a_n\},$$

$$T_0''(f) = \{x \in T_0(f) : \sum_{j=1}^{n-1} a_j x_j > a_0 - (k-1)a_n\},$$

$$T_1'(f) = \{x \in T_1(f) : \sum_{j=1}^{n-1} a_j x_j > a_0\},$$

$$T_1''(f) = \{x \in T_1(f) : \sum_{j=1}^{n-1} a_j x_j \leq a_0\}.$$

Если $x \in T_\nu'(f)$ $(\nu = 0,1)$, то $x_n = 0$ или $x_n = k-1$, следовательно, $|T_\nu'(f)| \leq 2\sigma(n-1,k)$.

Пусть

$$P = \left\{ x \in E_k^n : \ a_0 - (k-1)a_n < \sum_{j=1}^{n-1} a_j x_j \leq a_0, \ x_n = 0 \right\}.$$

Если $y \in P$, то учитывая, что $e_n \in K(f)$, получаем:

$$\{y + \alpha e_n : \ \alpha \in Z\} \subset F_0(f) \cup F_1(f).$$

Следовательно, по следствию из теоремы 2, $|T''_\nu(f)|$ не превосходит количества неприводимых точек в P. Поскольку размерность полиэдра Conv не выше $n-1$, то по теореме 1 количество неприводимых точек в P при фиксированном n есть $O(\log_2^{n-2} k)$. Теорема доказана.

Итак, доказано, что при фиксированном $n \geq 2$

$$\sigma(n,k) = \Theta(\log_2^{n-2} k) \qquad (k \to \infty).$$

Отдельно в литературе рассматривался случай $n = 2$. Можно показать [26, 33], что для любого $k \geq 2$

$$\sigma(2,k) = 4.$$

Отсюда получаем интересное геометрическое

Следствие. *Среди ограниченных областей, получаемых при разбиении плоскости параметров a_1, a_2 прямыми $a_1x_1 + a_2x_2 = 1$, где $(x_1, x_2) \in \{0, 1, \ldots, k-1\}^2$, встречаются только треугольники и четырехугольники.*

Такой же результат получается, если разбивать плоскость параметров a_1, a_2 прямыми $a_1x_1 + a_2x_2 = 1$, где $(x_1, x_2) \in \{1, 2, \ldots, k\}^2$ и т. п.

Под *средней мощностью тупикового разрешающего множества* в классе $\mathcal{F}'$ понимаем величину

$$\overline{\sigma}(\mathcal{F}') = \frac{1}{|\mathcal{F}'|} \sum_{f \in \mathcal{F}'} \sigma(f).$$

Обозначим: $\overline{\sigma}(n,k) = \overline{\sigma}\big(\mathcal{T}(n,k)\big)$.

M. Antony, G. Brightwell, D. Cohen, J. Shawe-Taylor [34] показали, что

$$\overline{\sigma}(n,2) \leq n^2.$$

Этот результат можно обобщить (см. [35]) на случай пороговых функций k-значной логики:

$$\overline{\sigma}(n,k) \leq n^2 \log_2 k.$$

Ю. А. Зуев [20] ввел понятие *графа* (булевых) *пороговых функций*. Это понятие легко обобщается на случай пороговых функций k-значной логики (а также на любой другой класс $\mathcal{F}' \subseteq \mathcal{F}(n,k)$). Пусть $f \in \mathcal{F}(n,k)$, $g \in \mathcal{F}(n,k)$,

$$\operatorname{dist}(f,g) = |\{x \in E_k^n : \ f(x) \neq g(x)\}|.$$

Графом класса $\mathcal{F}'$ называется простой граф, в котором множество вершин есть $\mathcal{F}'$, а $\{f, g\}$ является ребром тогда и только тогда, когда $\operatorname{dist}(f, g) = 1$.

Среди задач, связанных с пороговыми функциями и представляющими наибольший интерес, Ю. А. Зуев (1994) называет исследование свойств графа пороговых функций. Приведенные результаты о $\sigma(n, k)$ и $\overline{\sigma}(n, k)$ можно интерпретировать в этих терминах: $\sigma(n, k)$ есть максимальная, а $\overline{\sigma}(n, k)$ — средняя степень вершины графа.

2. Алгоритмы расшифровки пороговых функций

В. Н. Шевченко [13] предложил алгоритм $\mathcal{A}_0$ расшифровки пороговых функций, для которого при любом фиксированном n величины $\tau(\mathcal{A}_0)$ и $\rho(\mathcal{A}_0)$ ограничены полиномом от $\log_2 k$. T. Hegedüs [24] показал, что

$$\tau(\mathcal{A}_0) = O\Big(\log_2^{\lfloor n/2 \rfloor (n-1)+n} k\Big).$$

Н. Ю. Золотых, В. Н. Шевченко [36] и T. Hegedüs [37] построили алгоритм $\mathcal{A}_1$, для которого $\tau(\mathcal{A}_1) = O(\log_2^n k)$, $\rho(\mathcal{A}_1)$ ограничено полиномом от $\log_2 k$. Из теоремы 4 следует, что $\tau(\mathcal{A}_1) = O(\log_2^{n-1} k)$.

Более того, применяя результаты М. Ю. Мошкова [38, 39] в теории тестов, можно построить (ср. [37]) алгоритм $\mathcal{A}'$, для которого

$$\tau(\mathcal{A}') = O\left(\frac{\log_2^{n-1} k}{\log\log k}\right) \qquad (k \to \infty),$$

но $\rho(\mathcal{A}')$ ограничить полиномом от $\log_2 k$ (при фиксированном n) нельзя.

Итак,

$$\tau(n, k) = O\left(\frac{\log_2^{n-1} k}{\log\log k}\right), \quad \tau(n, k) \geq \sigma(n, k) = \Omega(\log_2^{n-2} k) \quad (k \to \infty).$$

Для $n = 2$ в [26, 40] построен алгоритм $\mathcal{A}_2$, для которого

$$\tau(\mathcal{A}_2) \leq 6 \log_2(k-1) + 4, \qquad \rho(\mathcal{A}_2) = O(\log_2^2 k).$$

3. Расшифровка с помощью расширенного оракула

В отличие от «обычного» оракула *расширенный* оракул принимает на вход произвольные точки из $\mathbf{Q}^n$, а не только из E_k^n. По

заданной точке $x \in \mathbf{Q}^n$ он возвращает 0, если пороговое неравенство выполнено, и 1 в противном случае. Под *расшифровкой пороговой функции* f, заданной с помощью расширенного оракула, будем понимать процедуру восстановления коэффициентов любого ее возможного порогового неравенства с помощью обращений к этому оракулу.

Теорема 5 [41]. *Существует алгоритм* $\mathcal{A}_{\text{ext}}$ *расшифровки функций из* $\mathcal{T}(n,k)$*, заданных расширенным оракулом, причем*

$$\tau(\mathcal{A}_{\text{ext}}) \le \frac{(6n^2+n+11)(n+1)n}{12}\log_2(n+1) + n^2(2n-1)\log_2 k,$$

а $\rho(\mathcal{A}_{\text{ext}})$ *при фиксированном* n *ограничено полиномом от* $\log_2 k$.

Работа выполнена в рамках ФЦП «Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2007–2013 годы», госконтракт 11.519.11.4015.

Список литературы

1. Коробков В. К., Резник Т. Л. О некоторых алгоритмах вычисления монотонных функций алгебры логики // Доклады АН СССР. — 1962. — Т. 147, № 5. — С. 1022–1025.

2. Коробков В. К. Оценка числа монотонных функций алгебры логики и сложности алгоритма отыскания разрешающего множества для произвольной монотонной функции алгебры логики // Доклады АН СССР. — 1963. — Т. 150, № 4. — С. 744–747.

3. Коробков В. К. О монотонных функциях алгебры логики // Проблемы кибернетики. Вып. 13. — М.: Наука, 1965. — С. 5–28.

4. Hansel G. Sur le nombre des fonctions booléennes monotones de n variables // C. R. Acad. Sci. — Paris, 1966. — V. 262, № 20. — P. 1088–1090.

5. Соколов Н. А. Оптимальная расшифровка монотонных булевых функций // Журн. вычисл. математики и матем. физики. — 1987. — Т. 27, № 12. — С. 1878–1887.

6. Коробков В. К. Некоторые обобщения задачи «расшифровки» монотонных функций алгебры логики // Дискретный анализ. Сб. тр. Вып. 5. — Новосибирск: изд-во Ин-та матем. СО АН СССР, 1965. — С. 19–25.

7. Алексеев В. Б. О расшифровке некоторых классов монотонных многозначных функций // Журн. вычисл. математики и матем. физики. — 1976. — Т. 16, № 1. — С. 189–198.

8. Сержантов А. В. Оптимальный алгоритм расшифровки некоторых классов монотонных функций // Журн. вычисл. математики и матем. физики. — 1983. — Т. 23, № 1. — С. 206–212.

9. Горяинов М. В., Сапоженко А. А. О расшифровке монотонных функций на частично упорядоченных множествах // Дискретный анализ и исследование операций. — 1995. — Т. 2, № 3. — С. 79–80.

10. Коршунов А. Д. Монотонные булевы функции // Успехи матем. наук. — 2003. — Т. 58, № 5. — С. 5–108.

11. Чегис И. А., Яблонский С. В. Логические способы контроля работы электрических схем // Тр. Матем. ин-та АН СССР. — 1958. — Т. 51. — С. 270–360.

12. Angluin D. Queries and concept learning // Machine Learning. — 1988. — V. 2, № 4. — P. 319–342.

13. Шевченко В. Н. О расшифровке пороговых функции многозначной логики // Комбинаторно-алгебраические методы в прикл. матем. — Горький: Горьковский гос. ун-т, 1987. — С. 155–163.

14. Schläfli L. Gesammelte mathematisce Abhanglugen. Band 1. — Basel: Verlag Birkhäuzer, 1950.

15. Yajima S., Ibaraki T. A lower bound of the number of threshold functions // IEEE Trans. on Electronic Comput. — 1965. — V. 14, № 6. — P. 929–929.

16. Зуев Ю. А. Асимптотика логарифма числа пороговых функций алгебры логики // Доклады АН СССР. – 1989. – Т. 306, № 3. – С. 528–530.

17. Зуев Ю. А. Комбинаторно-вероятностные и геометрические методы в пороговой логике // Дискретная математика. — 1991. – Т. 3, № 2. – С. 47–57.

18. Odlyzko A. M. On subspaces spanned by random selection of ± 1 vectors // J. Combin. Theory, A. — 1988. – V. 47, № 1. — С. 124–133.

19. Ирматов А. А. О числе пороговых функций // Дискретная математика. — 1993. – Т. 5, № 3. – С. 40–43.

20. Зуев Ю. А. Пороговые функции и пороговые представления булевых функций // Матем. вопросы кибернетики. Вып. 5. — М.: Физматлит, 1994. — С. 5–61.

21. Ирматов А. А., Ковиянич Ж. Д. Об асимптотике логарифма числа пороговых функций k-значной логики // Дискретная математика. — 1998. – Т. 10, № 3. – С. 35–56.

22. Koplowitz J., Lindenbaum M., Bruckstein A. M. The number of digital straight lines on an $N \times N$ grid // IEEE Trans. Inform. Theory. — 1990. — V. 36. — P. 192–197.

23. Шевченко В. Н. О некоторых функциях многозначной логики, связанных с целочисленным программированием // Методы дискретного анализа в теории графов и схем. Вып. 42. — Новосибирск: Ин-т матем. СО АН СССР, 1985. — С. 99–108.

24. Hegedüs T. Geometrical concept learning and convex polytopes // Proc. 7th Ann. ACM Conf. on Computational Learning Theory. — New York: ACM Press, 1994. — P. 228–236.

25. Cook W., Hartmann M., Kannan R., McDiarmid C. On integer points in polyhedra // Combinatorica. — 1992. — V. 12, № 1. — P. 27–37.

26. Шевченко В. Н., Золотых Н. Ю. О сложности расшифровки пороговых функций k-значной логики // Доклады Академии наук. — 1998. — Т. 362, № 5. — С. 606–608.

27. Золотых Н. Ю., Шевченко В. Н. О нижней оценке сложности расшифровки пороговых функций k-значной логики // Журн. вычисл. матем. и матем. физики. — 1999. — Т. 39, № 2. — С. 346–352.

28. Золотых Н. Ю. Оценки мощности минимального разрешающего множества пороговой функции многозначной логики // Матем. вопросы кибернетики. Вып. 17. — М.: Физматлит, 2008. — С. 159–168.

29. Веселов С. И., Чирков А. Ю. Оценки числа вершин целых полиэдров // Дискретный анализ и исследование операций. Серия 2. — 2007. — Т. 14, № 2. — С. 14–31.

30. Шевченко В. Н. О числе крайних точек в целочисленном программировании // Кибернетика. — 1981. — № 2. — С. 133–134.

31. Веселов С. И., Чирков А. Ю. О вершинах неявно заданных целых полиэдров // Вестник Нижегород. гос. ун-та им. Н. И. Лобачевского. — 2008. — № 1. — С. 118–123.

32. Золотых Н. Ю., Чирков А. Ю. О верхней оценке мощности минимального разрешающего множества пороговой функции // Дискретный анализ и исследование операций (в печати).

33. Золотых Н. Ю. О сложности расшифровки пороговых функций, зависящих от двух переменных // Материалы XI Межгосударственной школы-семинара «Синтез и сложность управляющих систем». Часть I. — М.: Изд-во Центра прикладных исследований при механико-матем. ф-те МГУ, 2001. — С. 74–79.

34. Antony M., Brightwell G., Shawe-Taylor J. On exact specification by labelled examples // Discrete Applied Mathematics. — 1995. — V. 61, № 1. — С. 1–25.

35. Вировлянская М. А., Золотых Н. Ю. Верхняя оценка средней мощности минимального разрешающего множества пороговой функции многозначной логики // Вестник Нижегород. гос. ун-та им. Н. И. Лобачевского. Матем. моделирование и оптимальное управление. — Нижний Новгород.: изд-во ННГУ, 2003. — С. 238–246.

36. Золотых Н. Ю., Шевченко В. Н. Расшифровка пороговых

функций k-значной логики // Дискретный анализ и иссл. операций. — 1995. — Т. 2, № 3. — С. 18–23.

37. Hegedüs T. Generalized teaching dimensions and the query complexity of learning // Proc. 8th Ann. ACM Conf. on Computational Learning Theory (COLT'95). — New York: ACM Press, 1995. — P. 108–117.

38. Мошков М. Ю. Об условных тестах // Доклады АН СССР. — 1982. — Т. 265, № 3. — С. 550–552.

39. Мошков М. Ю. Условные тесты // Проблемы кибернетики. Вып. 40. — М.: Наука, 1983. — С. 131–170.

40. Золотых Н. Ю. Пороговые функции, зависящие от двух переменных: сложность расшифровки и мощность разрешающего множества // Материалы четвертой молодежной научной школы по дискретной математике и ее приложениям. — М.: Изд-во механико-матем. факультета МГУ, 2000. — С. 48–54.

41. Золотых Н. Ю. Расшифровка пороговой функции, заданной расширенным оракулом // Вестник Нижегородского государственного ун-та им. Н. И. Лобачевского (в печати).

Секция «Синтез, сложность и надежность управляющих систем»

КВАНТОВЫЙ МЕТОД ОТПЕЧАТКОВ ДЛЯ МОДЕЛИ КВАНТОВЫХ КОММУНИКАЦИОННЫХ ВЫЧИСЛЕНИЙ

Ф. М. Аблаев, А. В. Васильев (Казань)

Данная работа посвящена разработке эффективных квантовых коммуникационных протоколов на основе предложенного нами ранее квантового метода отпечатков. Учитывая тесную связь коммуникационной модели вычислений и модели упорядоченных ветвящихся программ [3] и используя полиномиальные представления булевых функций, конструируется обобщенный квантовый метод отпечатков для односторонней квантовой коммуникационной модели.

Нами предложен вариант обобщенного квантового метода отпечатков для квантовых коммуникационных вычислений, основанный на представлении булевых функций множествами характеристических полиномов, которые мы называем *характеристиками*.

Формально, назовем множество χ_f^m полиномов над некоторым кольцом $\mathbb{Z}_m$ *характеристикой* булевой функции f, если для всех $\sigma \in \{0,1\}^n$ выполняется: $f(\sigma) = 1$ тогда и только тогда, когда $\forall g \in \chi_f^m \mid g(\sigma) = 0$.

Обобщенный метод отпечатков для квантовых коммуникационных вычислений.

1. Для булевой функции f зафиксируем некоторое $\epsilon \in (0,1)$ и выберем два таких множества $G = \{g_1, \ldots, g_l\}$ и $H = \{h_1, \ldots, h_l\}$ полиномов над кольцом $\mathbb{Z}_m$, что множество полиномов $\chi_f^m = \{g_1 + h_1, \ldots, g_l + h_l\}$ образует характеристику функции f над $\mathbb{Z}_m$.

2. На основе входного набора $\sigma = \sigma_1 \ldots \sigma_{n_1}$ вычислитель A строит его отпечаток $|h_\sigma\rangle$, соединяющий в себе $t \cdot l$ ($t = 2^{\lceil \log_2((2/\epsilon)\ln(2m))\rceil} = O\left(\frac{\log m}{\epsilon}\right)$) однокубитных отпечатков $\left|h_\sigma^{i,j}\right\rangle$ ($1 \leq$

$i \le t$, $1 \le j \le l$):

$$\begin{aligned} \left|h_\sigma^{i,j}\right\rangle &= \cos\tfrac{\pi k_i g_j(\sigma)}{m}\left|0\right\rangle + \sin\tfrac{\pi k_i g_j(\sigma)}{m}\left|1\right\rangle \\ \left|h_\sigma\right\rangle &= \tfrac{1}{\sqrt{t}}\sum_{i=1}^{t}\left|i\right\rangle\left|h_\sigma^{i,1}\right\rangle\left|h_\sigma^{i,2}\right\rangle\ldots\left|h_\sigma^{i,l}\right\rangle. \end{aligned}$$

3. Отпечаток $|h_\sigma\rangle$ передается вычислителю B, который на основе своей части входных данных $\gamma = \gamma_1 \ldots \gamma_{n_2}$ переводит его в состояние

$$\begin{aligned} \left|h_{\sigma,\gamma}^{i,j}\right\rangle &= \cos\tfrac{\pi k_i (g_j(\sigma)+h_j(\gamma))}{m}\left|0\right\rangle + \sin\tfrac{\pi k_i (g_j(\sigma)+h_j(\gamma))}{m}\left|1\right\rangle \\ \left|h_{\sigma,\gamma}\right\rangle &= \tfrac{1}{\sqrt{t}}\sum_{i=1}^{t}\left|i\right\rangle\left|h_{\sigma,\gamma}^{i,1}\right\rangle\left|h_{\sigma,\gamma}^{i,2}\right\rangle\ldots\left|h_{\sigma,\gamma}^{i,l}\right\rangle. \end{aligned}$$

4. Вычислитель B измеряет состояние $|h_{\sigma,\gamma}\rangle$ относительно стандартного вычислительного базиса и выдает ответ 1 (принимает входной набор), только если последние l кубит находятся в состоянии $|0\rangle$.

В случаях, когда $f(\sigma,\gamma) = 1$, данный протокол будет приводить к безошибочным результатам. Если же $f(\sigma,\gamma) = 1$, то, выбрав множество параметров $K = \{k_1, \ldots, k_t\}$ "хорошим" в смысле определения статьи [1], вычислители A и B получат неправильный ответ с вероятностью, не превосходящей $\sqrt{\epsilon}/2 + 1/2$.

Сложность коммуникационных протоколов, основанных на описанном выше методе, будет порядка $O\left(\log\log m + |\chi_f^m|\right)$. В случае, когда $|\chi_f| = O(\log n)$ и $m = 2^{n^{O(1)}}$, коммуникационная сложность такого протокола будет порядка $O(\log n)$, что экспоненциально лучше тривиальной оценки.

Отметим, что единственным существенным ограничением при построении такого квантового коммуникационного протокола для булевых функций является наличие характеристики, допускающей разложение каждого из ее полиномов на сумму двух полиномов, зависящих от непересекающихся наборов переменных. Простейшим вариантом таких характеристик являются линейные характеристики, для которых нами ранее была доказана возможность эффективного вычисления в модели квантовых ветвящихся программ [1].

Кроме того, нами получено обобщение предложенного нами ранее полиномиального представления булевых функций, позволившего расширить класс функций эффективно вычислимых нашим квантовым методом отпечатков. Доказано, что данный класс включает функции с "ограниченно-нелинейными" представлениями [2].

Ввиду тесной связи между квантовыми OBDD и квантовыми односторонними коммуникационными протоколами, данные результаты также имеют непосредственные аналоги в модели квантовых коммуникационных вычислений.

Работа выполнена при финансовой поддержке РФФИ, проекты 11-07-00465-а и 12-07-97019-р_поволжье_а.

Список литературы

1. Ablayev F., Vasiliev A. Algorithms for quantum branching programs based on fingerprinting // Electronic Proceedings in Theoretical Computer Science. — 2009. — V. 9. — P. 1–11.

2. Ablayev F., Vasiliev A. Classical and quantum parallelism in the quantum fingerprinting Method // Parallel Computing Technologies. Lecture Notes in Computer Science. — Springer, 2011. — V. 6873. — P. 1–12.

3. Wegener I. Branching programs and binary decision diagrams. — SIAM Press, 2000.

УТОЧНЕНИЕ ИЕРАРХИИ КЛАССОВ БУЛЕВЫХ ФУНКЦИЙ, ПРЕДСТАВИМЫХ В МОДЕЛЯХ k-OBDD ВЕТВЯЩИХСЯ ПРОГРАММ

Ф. М. Аблаев, К. Р. Хадиев (Казань)

Мы рассматриваем известную модель ветвящихся программ — k-$OBDD$. Ветвящиеся программы и их модификации $OBDD$ и k-$OBDD$ определены в книге [1].

$OBDD$ на множестве переменных $X = \{x_1, x_2, \ldots, x_n\}$ — это ветвящаяся программа, обладающая следующими свойствами. Ее вершины разбиты на n уровней $1, \ldots, n$ таким образом, что для каждого i ребра из вершин уровня i ведут только в вершины уровня $(i+1)$. На каждом уровне i считывается значение только одной переменной x_{i_j}. На любом пути вычисления каждая переменная считывается один раз. Говорят, что $OBDD$ P читает переменные в порядке $\theta = (i_1, \ldots, i_n)$. Различные $OBDD$ могут использовать различные порядки θ считывания переменных.

K-$OBDD$ — это ветвящаяся программа P, которую можно разделить на k слоев, каждый из которых является $OBDD$, причем порядок θ чтения переменных во всех слоях программы P одинаковый.

Сложность $S(P)$ ветвящейся программы P — это число ее внутренних вершин.

Через k-$OBDD$ обозначим класс булевых функций, которые вычислимы k-$OBDD$ полиномиальной сложности.

В работе [2] доказана следующая иерархия (иерархия BSSW): для $k = o(n^{1/2}/\log^{3/2} n)$ выполняется собственное включение

$$(k-1)-OBDD \subset k-OBDD.$$

Доказательство иерархии BSSW основано на нижней оценки вычисления булевых функций в k-раундовых коммуникационных протоколах [3].

Нами разработан метод функционального описания булевой функции, представимой в k-$OBDD$, на основе которого мы уточняем иерархию BSSW.

Введем следующее определение. *Ширина* $w(P)$ программы k-$OBDD$ P — это максимум от количества вершин на уровне, взятый по всем уровням P.

Замечание 1. *В силу определения k-$OBDD$ P имеем $w(P) \leq S(P) \leq k \cdot w(P) \cdot n$. Понятно, что для k-$OBDD$ P полиномиальной сложности, ее ширина $w(P)$ не более чем полином.*

Теорема 1. *Пусть булева функция $f(X)$ представима в k-$OBDD$ ширины w и пусть $w^{2k-2} < 2^n$. Тогда существуют такие булевы функции g_j, h_j, $1 \leq j \leq w^{2k-2}$, что h_j представима в $OBDD$ ширины w и выполняется следующее равенство*

$$f(X) = \bigvee_{j=1}^{w^{2k-2}} g_j(X) h_j(X).$$

Теорема 1 предоставляет нам достаточное условие непредставимости булевой функции в k-$OBDD$, на основе которого доказываются следующие иерархии.

Через k-$OBDD_w$ обозначим класс булевых функций, которые вычислимы k-$OBDD$ ширины w полиномиальной сложности.

Теорема 2. *Для $k = o(n/\log w)$, выполняется собственное включение*

$$\left(\frac{k}{c}\right)-OBDD_w \subset k-OBDD_w,$$

где c — некоторая константа и $c \geq 9$.

Полученная иерархия является "более грубой" чем иерархия BSSW, однако существенно продолжает иерархию по параметру k (до $k = o(n/\log n)$ см. замечание 1).

Необходимое условие представления булевой функции в k-$OBDD$ (теорема 1) позволяет доказывать иерархию классов булевых функций, представимых в k-$OBDD$ более чем полиномиальной ширины (а следовательно и более чем полиномиальной сложности).

Через k-$\widetilde{OBDD}_w$ обозначим класс булевых функций, которые вычислимы k-$OBDD$ ширины $w \succ pol(n)$, где $pol(n)$ — это функции вида $n^t, t \geq 1$.

Теорема 3. *Для $k = o(n/\log^2 n)$, выполняется*

$$\left(\frac{k}{c}\right)\text{-}\widetilde{OBDD}_w \subset k\text{-}\widetilde{OBDD}_w,$$

где c — некоторая константа и $c \geq 9$.

Список литературы

1. Wegener I. Branching programs and binary decision diagrams: theory and applications // Society for Industrial and Applied Mathematics. — Philadelphia, 2000.

2. Bolling B., Sauerhoff M., Sieling D., Wegener I. Hierarchy theorems for k-OBDDs and k-IBDDs. — 1996.

3. Nisan N., Widgerson A. Rounds in communication complexity revisited // SIAM Journal on Computing. — 1993. — V. 22. — P. 211–219.

О БИЛИНЕЙНОЙ СЛОЖНОСТИ ПЕРЕМНОЖЕНИЯ МАТРИЦ РАЗМЕРОВ 2×4 И 4×2.

В. Б. Алексеев (Москва)

Билинейными алгоритмами для вычисления системы билинейных форм называются алгоритмы, в которых сначала вычисляются произведения некоторых линейных форм от первого множества переменных на некоторые линейные формы от второго множества переменных, а затем из этих произведений сложением получаются нужные билинейные формы. При этом число умножений называется *билинейной сложностью алгоритма. Билинейной сложностью задачи* вычисления системы билинейных форм называется минимальная

билинейная сложность алгоритмов, вычисляющих данную систему билинейных форм.

Одной из важных задач вычисления системы билинейных форм является задача умножения двух матриц. Алгоритм Штрассена [1] для умножения матриц порядка n со сложностью $O(n^{\log_2 7})$ основан на найденном им билинейном алгоритме умножения двух квадратных матриц порядка 2 с билинейной сложностью 7. Виноград [2] показал, что эту оценку нельзя понизить, то есть билинейная сложность задачи умножения двух матриц порядка 2 равна 7.

Несмотря на простоту постановки, задача определения билинейной сложности умножения двух матриц оказывается тяжелой даже для малых размеров матриц. Так, про билинейную сложность задачи умножения двух матриц порядка 3 известно только, что она не больше 23 [3] и не меньше 19 [4]. Из результата Штрассена легко вытекает, что для умножения матрицы размером $2 \times m$ на матрицу размером $m \times 2$ существует билинейный алгоритм с числом умножений $\lceil \frac{7m}{2} \rceil$. Хопкрофт и Керр [5] показали, что эту оценку нельзя понизить для задачи умножения таких матриц над полем из 2 элементов. Для произвольных полей и произвольных m неизвестно, является ли эта оценка неулучшаемой. В работе автора [6] было показано, что при $m = 3$ любой билинейный алгоритм имеет билинейную сложность не меньше 11 над произвольным полем, то есть билинейная сложность задачи умножения матрицы размером 2×3 на матрицу размером 3×2 равна 11 над любым полем.

Данная работа посвящена случаю $m = 4$. Тогда верхняя оценка равна 14.

Теорема. *Любой билинейный алгоритм для умножения матрицы размером* 2×4 *на матрицу размером* 4×2 *над произвольным полем требует не менее* 14 *умножений, то есть билинейная сложность задачи умножения матрицы размером* 2×4 *на матрицу размером* 4×2 *равна* 14 *над любым полем.*

Доказательство ведется от противного. Доказывается, что для указанной задачи не существует билинейного алгоритма с 13 умножениями. Как показано в [6], это утверждение равносильно отсутствию решения у следующей задачи.

Пусть A — произвольная невырожденная матрица размером 8×8, разбитая на подматрицы размером 8×2: $A = |A_1|A_2|A_3|A_4|$. Пусть A_{i1} — матрица размером 8×4 вида $|A_i|0|$, а A_{i2} — матрица размером 8×4 вида $|0|A_i|$. Спрашивается, существуют ли 13 матриц `первого ранга` $D_1 - D_{13}$ размером 8×4 такие, что все 8 матриц $A_{i1}, i = \overline{1,4}$ и $A_{i2}, i = \overline{1,4}$ являются линейными комбинациями матриц $D_1 - D_{13}$.

Надо доказать, что эта задача не имеет решения ни для какой невырожденной матрицы A.

Идея доказательства состоит в том, чтобы из произвольного решения этой задачи получать решение более простого вида, а уже для этого более простого вида доказать невозможность. Укажем здесь только некоторые переходы.

Пусть матрицы $D_t, t = \overline{1,13}$ дают решение для некоторой невырожденной матрицы A. Представим их в виде $D_t = |D_t^1|D_t^2|$, где матрицы D_t^1, D_t^2 имеют размер 8×2. По условию все $A_i, i = \overline{1,4}$ являются линейными комбинациями матриц $D_1^1 - D_{13}^1$. Так как ранг столбцов в матрице A равен 8, то среди матриц $D_1^1 - D_{13}^1$ (ранга 1) должны существовать 8 матриц, отличные от 0 и построенные на 8 линейно независимых столбцах (пусть это матрицы $D_1 - D_8$). Умножая слева все матрицы $D_1 - D_{13}$ и A на произвольную невырожденную матрицу P, мы получим опять решение нашей задачи (для другой невырожденной матрицы PA). При этом можно подобрать P так, что после преобразования каждая матрица ранга 1 $D_t, t = \overline{1,8}$ будет построена на вектор-столбце с одной единицей в строке с номером t и, следовательно, матрица D_t будет равна 0 во всех строках, кроме строки с номером t. Это резко упрощает рассмотрение случаев.

Другое упрощение основано на следующем. Поскольку матрица A невырожденная, то матрицы A_1, A_2, A_3, A_4 линейно независимы, а значит и 4 матрицы A_{i2} линейно независимы. По условию 4 матрицы A_{i2} должны быть линейными комбинациями матриц $D_1 - D_{13}$. Но тогда эти 4 линейные комбинации матриц $D_1 - D_{13}$ должны быть линейно независимыми, при этом для подматриц $D_1^1 - D_{13}^1$ они должны давать 0, а это значит, что среди матриц $D_1^1 - D_{13}^1$ не может быть более 9 линейно независимых матриц. С учетом предыдущего абзаца получаем, что рассмотрение распадается на 2 случая: 1) среди матриц $D_1^1 - D_{13}^1$ имеется ровно 8 линейно независимых ($D_1 - D_8$); 2) среди матриц $D_1^1 - D_{13}^1$ имеется ровно 9 линейно независимых ($D_1 - D_8$ и D_9).

В случае 1) каждая матрица $D_t^1, t = \overline{9,13}$ должна быть линейной комбинацией матриц $D_t^1, t = \overline{1,8}$, при этом она должна быть матрицей первого ранга, поэтому в соответствующей линейной комбинации могут участвовать только матрицы из $D_t^1, t = \overline{1,8}$, у которых (единственные) ненулевые строки пропорциональны. Это приводит к рассмотрению небольшого числа разных случаев в зависимости от того, сколько пропорциональных строк имеется в разных

$D_t^1, t = \overline{1,8}$.

Случай 2) рассматривается аналогично. Все варианты приводят к противоречию. Этим завершается доказательство теоремы.

Работа выполнена при финансовой поддержке РФФИ (проект 12-01-91331-ННИО-а).

Список литературы

1. Strassen V. Gaussian elimination is not optimal // Numer. Math. — 1969. — V. 13. — P. 354–356.

2. Winograd S. On multiplication of 2×2 matrices // Linear Algebra and Appl. — 1971. — V. 4. — P. 381–388.

3. Laderman J. D. A noncommutative algorithm for multiplying 3×3 matrices using 23 multiplications // Bull. Amer. Math. Soc. — 1976. — V. 82, №. 1. — P. 126–128.

4. Bläser M. On the complexity of the multiplication of matrices of small formats // J. Complexity. — 2003. — V. 19. — P. 43–60.

5. Hopcroft J. E., Kerr L. R. On minimizing the number of multiplications necessary for matrix multiplication // SIAM J. Appl. Math. — 1971. — V. 20, №. 1. — P. 127–148.

6. Alekseyev V. B. On the complexity of some algorithms of matrix multiplication // Journal of Algorithms. — 1985. — V. 6. — P. 71–85.

О СЛОЖНОСТИ АСИМПТОТИЧЕСКИ ОПТИМАЛЬНЫХ ПО НАДЕЖНОСТИ СХЕМ ПРИ ОДНОТИПНЫХ КОНСТАНТНЫХ НЕИСПРАВНОСТЯХ НА ВЫХОДАХ ЭЛЕМЕНТОВ

М. А. Алехина (Пенза)

Рассматривается реализация булевых функций схемами из ненадежных функциональных элементов в полном конечном базисе $B = \{e_1, e_2, ..., e_m\}$, $m \in N$. Каждому элементу базиса E_i приписано положительное число $v(E_i)$ – вес данного элемента. Сложностью $L(S)$ схемы S называется сумма весов всех входящих в нее элементов.

Предполагается, что все элементы схемы независимо друг от друга с вероятностью γ ($\gamma \in (0, 1/2)$ переходят в неисправные состояния типа 0 на выходах элементов. Эти неисправности характеризуются тем, что в исправном состоянии функциональный элемент реализует приписанную ему булеву функцию φ, а в неисправном –

константу 0. Неисправности типа 1 на выходах элементов определяются аналогично. Далее считаем, что базисные элементы подвержены неисправностям типа 0 на выходах.

Пусть схема S реализует функцию $f(\mathbf{x})$ ($\mathbf{x} = (x_1, x_2, ..., x_n)$). Пусть $P_{\bar{f}(\mathbf{a})}(S, \mathbf{a})$ — вероятность появления значения $\bar{f}(\mathbf{a})$ на выходе схемы S при входном наборе $\mathbf{a}$. *Ненадежность* $P_\gamma(S)$ схемы S, реализующей булеву функцию $f(\mathbf{x})$, равна $P_\gamma(S) = \max\limits_{\mathbf{a}} P_{\bar{f}(\mathbf{a})}(S, \mathbf{a})$, где максимум берется по всем возможным входным наборам $\mathbf{a}$.

Пусть $P_\gamma(f) = \inf P_\gamma(S)$, где инфимум берется по всем схемам S из ненадежных элементов, реализующим функцию f. Схему A, реализующую функцию f, назовем асимптотически оптимальной по надежности, если $P_\gamma(A) \sim P_\gamma(f)$ при $\gamma \to 0$.

Известно [1], что в произвольном полном конечном базисе любую булеву функцию можно реализовать такой схемой, что ее ненадежность при всех $\gamma \in (0, 1/960]$ не больше $3\gamma + 100\gamma^2$.

Доказано [2], что при константных неисправностях на выходах элементов в любом неприводимом полном базисе B из двухвходовых элементов (исключая три случая) почти все булевы функции можно реализовать асимптотически оптимальными по надежности схемами S, функционирующими с ненадежностью $P(S)$, асимптотически равной $c\varepsilon$ (т. е. $P(S) \sim c\varepsilon$) при $\varepsilon \to 0$. Константа c зависит только от базиса, $c \in \{1, 2, 3\}$. Для почти всех функций сложность таких схем удовлетворяет соотношению $L(S) \lesssim k_B \cdot 2^n/n$, причем мультипликативная константа k_B зависит только от базиса B, $40 \leq k_B \leq 168$.

Пусть B – полный конечный базис. Число c назовем *коэффициентом ненадежности* базиса B, если любую булеву функцию в нем можно реализовать схемой с ненадежностью, асимптотически не больше $c\varepsilon$ при $\varepsilon \to 0$, и найдется функция, которую нельзя реализовать схемой, ненадежность которой асимптотически меньше $c\varepsilon$.

Заметим (см. [1]), что коэффициент ненадежности любого полного конечного базиса $c \in \{1, 2, 3\}$.

Эта работа посвящается сложности асимптотически оптимальных по надежности схем: константу k_B удалось понизить до 3, причем не только в полных базисах из двухвходовых элементов, но и в произвольном полном конечном базисе (теорема 2).

Введем функцию Шеннона $L_{p,\gamma}(n) = \max\limits_{f} \min\limits_{S} L(S)$, характеризующую сложность схем, реализующих функции от n переменных в базисе B, где минимум берется по всем схемам S из ненадежных элементов, реализующим функцию $f(x_1, x_2, ..., x_n)$ с ненадежностью

$P(S) \leq p$, а максимум — по всем булевым функциям f от n переменных.

Пусть N_g — минимальное число надежных элементов, необходимое для реализации функции голосования $g(x_1, x_2, x_3) = x_1x_2 \vee x_1x_3 \vee x_2x_3$ в рассматриваемом базисе B.

Теорема 1. *Для любых, сколь угодно малых чисел b и h $(b, h > 0)$ существует число $\gamma_1 (\gamma_1 \in (0, 1/2))$ такое, что при любом $\gamma \in (0, \gamma_1]$, и любом p, удовлетворяющем условию $(1 + h)\gamma N_g \leq p \leq 1/2$, справедливо соотношение $L_{p,\gamma}(n) \lesssim (1+b)\rho \cdot 2^n/n$, где ρ – приведенный вес.*

Доказательство этой теоремы опирается на результат Д. Улиг [3] для инверсных неисправностей на выходах элементов с вероятностью ошибки ε в предположении, что $\varepsilon = \gamma$. Инверсные неисправности на выходах элементов характеризуются тем, что в исправном состоянии элемент реализует приписанную ему функцию φ, а в неисправном состоянии, в которое он переходит независимо от других элементов схемы с вероятностью $\varepsilon \in (0; 1/2)$, реализует функцию $\bar{\varphi}$.

Схемы, которые удовлетворяют условиям теоремы 1 в общем случае могут не быть асимптотически оптимальными по надежности. Оценка сложности этих схем получена в теореме 2.

Теорема 2. *Пусть B – полный конечный базис, c — коэффициент ненадежности базиса B. Для любого $b > 0$ существуют такие константы $\gamma_2 \in (0, 1/2)$ и $d > 0$, что при любом $n \geq 3$ любую булеву функцию $f(x_1, x_2, \ldots, x_n)$ можно реализовать схемой S, для которой*

$P(S) \leq c\gamma + d\gamma^2$ *при любом* $\gamma \in (0, \gamma_2]$,

$L(S) \lesssim 3(1 + b)\rho 2^n/n$ *при* $n \to \infty$.

Таким образом, асимптотически оптимальные по надежности схемы можно строить со сложностью, которая для почти всех функций отличается от сложности минимальных схем, построенных из абсолютно надежных элементов в $3(1 + b)$ раз, где b — любое, сколь угодно малое положительное число.

Поскольку ненадежности двойственных схем равны [4], теоремы 1 и 2 верны при неисправностях типа 1 на выходах базисных элементов.

Работа выполнена при финансовой поддержке РФФИ (проект 11-01-00212).

Список литературы

1. Алехина М. А. О надежности схем при однотипных константных неисправностях на выходах элементов // Материалы X Международного семинара "Дискретная математика и ее приложения"

(г. Москва, 1–6 февраля 2010 г.). — М.: Изд-во мех.-мат. ф-та МГУ, 2010. — С. 83–85.

2. Алехина М. А. Синтез асимптотически оптимальных по надежности схем. Монография. — Пенза: ИИЦ ПГУ, 2006.

3. Uhlig D. Reliable networks from unreliable gates with almost minimal comlexity // Fundamentals of Computation Theory. Intern. conf. FCT'87 (Kazan, June 1987). Proc. — Berlin: Springer-Verl., 1987. — P. 462–469. (Lecture Notes in Comput. Sci. — V. 278.)

4. Алехина М. А., Пичугина П. Г. О надежности двойственных схем в полном конечном базисе // Материалы XVIII Международной школы-семинара "Синтез и сложность управляющих систем" (г. Пенза 28 сентября – 3 октября 2009 г.). — М.: Изд-во мех.-мат. ф-та МГУ, 2009. — С. 10–13.

ОБ ОДНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ ФУНКЦИЙ МНОГОЗНАЧНОЙ ЛОГИКИ

А. А. Андреев (Москва)

Рассматривается задача о реализации функций многозначной логики формулами [1]. Известно, что в двузначной логике сложность реализации функций формулами над конечными системами имеет не более чем экспоненциальный порядок роста от числа переменных [2, 3]. В работе [4] приводится пример последовательности функций 5-значной логики, сложность которых в классе формул над некоторой конечной системой превосходит $2^{C_n^{n/2}}$, где n — число переменных. В работе [5] аналогичный результат получен для последовательности функций 4-значной логики. В работе автора [6] приводится последовательность $f_n(x_1, \ldots, x_n)$ функций из P_{10}, сложность которых в классе формул над некоторой конечной системой превосходит 2^{3^n}.

В настоящей работе приводится метод, позволяющий для любых натуральных m и r при $k(r) = r + 3$ строить последовательность функций из $P_{k(r)}$, сложность которых превосходит m^{r^n}. В частности, на основе этого метода можно привести последовательность

функций из P_6, сложность которых в классе формул над некоторой конечной системой превосходит 2^{3^n}.

Обозначим через P_k множество всех функций k–значной логики, $k \geq 4$. Обозначим через E^n $(n \geq 1)$ множество всех наборов $(\alpha_1, \ldots, \alpha_n)$, таких, что $\alpha_1, \ldots, \alpha_n \in E_k = \{0, 1, \ldots, k-1\}$, а через H_n — множество всех наборов из E^n, состоящих только из символов $3, \ldots, k-1$, причем тройки есть обязательно. Определим функции $\lambda(x, y)$, $\mu(x, y, z)$, $\varphi_m(x, y)$ $(m \in \{3, \ldots, k-1\})$ и $f_n(y, x_1, \ldots x_n)$ из P_k следующим образом. Положим

$$\lambda(x,y) = \begin{cases} 0, & \text{если } x = 0,\ y = 2; \\ 1, & \text{если } x = 1 \text{ или } x = 0,\ y = 3; \\ 2, & \text{в остальных случаях;} \end{cases}$$

$$\mu(x,y,z) = \begin{cases} \lambda(x,z), & \text{если } x = y; \\ 2, & \text{в противном случае;} \end{cases}$$

$$\varphi_m(x,y) = \begin{cases} 3, & \text{если } x = 3,\ y = m; \\ 2, & \text{в остальных случаях;} \end{cases}$$

$$f_n(y,x_1,\ldots,x_n) = \begin{cases} 0, & \text{если } y = 0,\ (x_1, \ldots x_n) \notin H_n; \\ 1, & \text{если } y = 1 \text{ или } y = 0,\ (x_1, \ldots x_n) \in H_n; \\ 2, & \text{в остальных случаях.} \end{cases}$$

Положим $\mathfrak{B} = \{\mu, \varphi_3, \ldots, \varphi_{k-1}, 2\}$, $\mathfrak{A} = \mathfrak{B} \cup \{\lambda\}$. Имеет место следующее утверждение.

Теорема. *При всех $n \geq 1$, $k \geq 4$ для последовательности f_n функций k-значной логики имеет место равенство*

$$L_{\mathfrak{B}}(f_n) = (n+1) \cdot 2^{n((k-3)^n - (k-4)^n)} - n.$$

Из этой теоремы (при $k = 6$) получаем

Следствие 1. *При всех $n \geq 1$ для последовательности f_n функций 6–значной логики имеет место равенство*

$$L_{\mathfrak{B}}(f_n) = (n+1) \cdot 2^{n(3^n - 2^n)} - n.$$

Следует отметить, что это следствие является усилением результата упомянутой выше работы [6].

Рассуждая аналогично доказательству теоремы, непосредственно получается следующее утверждение.

Следствие 2. *При всех натуральных m и r для последовательности f_n функций $r+3$-значной логики при $n \longrightarrow \infty$ выполняется соотношение*

$$L_{\mathfrak{B}}(f_n) \gtrsim m^{r^n}.$$

При доказательстве теоремы была использована следующая лемма.

Лемма. *Пусть Φ — произвольная формула над $\mathfrak{A}$, реализующая функцию $f_n(y, x_1, \ldots, x_n)$ из P_k и имеющая вид*

$$\Phi = \lambda(\lambda(\ldots\lambda(\lambda(y, Z_1), Z_2), \ldots), Z_N),$$

где $Z_1, \ldots, Z_N$ — формулы над $\mathfrak{A}$, $k \geq 4$, n и N — натуральные. Пусть $L(\Phi) = L_{\mathfrak{A}}(f_n)$. Тогда

$$N \geq (k-3)^n - (k-4)^n,$$

и для всех $i = 1, \ldots, N$ выполняются неравенства

$$L(Z_i) \geq n.$$

Список литературы

1. Лупанов О. Б. Асимптотические оценки сложности управляющих систем. — М.: Изд-во МГУ, 1984.

2. Угольников А. Б. О глубине формул в неполных базисах // Математические вопросы кибернетики. Вып. 1. — М.: Наука, 1988. — С. 242–245.

3. Угольников А. Б. О глубине и сложности формул, реализующих функции из замкнутых классов // Доклады АН СССР — 1988. — Т. 298, № 6. — С. 1341–1344.

4. Угольников А. Б. О сложности реализации формулами одной последовательности функций многозначной логики // Математические вопросы кибернетики. Вып. 2. — 1989. — С. 174–176.

5. Угольников А. Б. О сложности реализации формулами одной последовательности функций 4-значной логики // Вестник Московского университета. Сер. 1. Математика. Механика. — 2004. — № 3. — С. 52–55.

6. Андреев А. А. Об одной последовательности функций многозначной логики // Вестник Московского университета. Сер. 1. Математика. Механика. — 2011. — № 6. — С. 3–7.

О ЧИСЛЕ ПОЛНЫХ БАЗИСОВ ИЗ ДВУХВХОДОВЫХ ЭЛЕМЕНТОВ С ЗАДАННЫМ КОЭФФИЦИЕНТОМ НЕНАДЕЖНОСТИ

О. Ю. Барсукова (Пенза)

Рассматривается реализация булевых функций схемами из функциональных элементов в полных базисах, содержащих функции не более чем двух переменных. Предполагается, что все элементы схемы ненадежны и независимо друг от друга с вероятностью ε ($\varepsilon \in (0, 1/2)$) подвержены инверсным неисправностям на выходах. Эти неисправности характеризуются тем, что элемент с приписанной ему булевой функцией φ в неисправном состоянии реализует функцию $\bar{\varphi}$.

Пусть $f(x_1, ..., x_n)$ ($n \geq 1$) — произвольная булева функция, а S — любая схема, реализующая $f(\tilde{x})$ ($\tilde{x} = (x_1, ..., x_n)$).

Пусть $P_{\bar{f}(\tilde{a})}(S, \tilde{a})$ — вероятность появления значения $\bar{f}(\tilde{a})$ на выходе схемы S, реализующей функцию $f(\tilde{a})$, на входном наборе $\tilde{a}$. Ненадежность $P(S)$ схемы S есть $P(S) = \max\limits_{\tilde{a}}\{P_{\bar{f}(\tilde{a})}(S, \tilde{a})\}$, где максимум берется по всем входным наборам $\tilde{a}$ схемы S.

Обозначим $P_\varepsilon(f) = \inf P(S)$, где инфимум берется по всем схемам S из ненадежных элементов, реализующим булеву функцию $f(x_1, ..., x_n)$.

Схему A из ненадежных элементов, реализующую булеву функцию $f(x_1, ..., x_n)$, назовем асимптотически оптимальной по надежности, если $P(A) \sim P_\varepsilon(f)$ при $\varepsilon \to 0$, т. е. $\lim\limits_{\varepsilon \to 0} \frac{P_\varepsilon(A)}{P(f)} = 1$.

Обозначим через B_2 множество всех булевых функций, зависящих не более чем от двух переменных x_1, x_2 ($|B_2| = 16$), а через B_3 — множество всех булевых функций, зависящих не более чем от трех переменных x_1, x_2, x_3.

Известно [1], что для любого полного базиса $B \subseteq B_3$ найдется единственная константа k ($k \in \{1, 2, 3, 4, 5\}$) такая, что почти все функции можно реализовать асимптотически оптимальными по надежности схемами, функционирующими с ненадежностью, асимптотически равной $k\varepsilon$ при $\varepsilon \to 0$.

Число k, зависящее только от базиса, будем называть коэффициентом ненадежности базиса.

В данной работе подсчитано число всех полных базисов в B_2, а также для каждого значения коэффициента ненадежности k ($k \in \{1, 2, 3, 4, 5\}$) найдено число $N(k)$ полных базисов из двухвходовых элементов.

В B_2 были рассмотрены всевозможные подмножества булевых функций. Число этих подмножеств равно $2^{16} = 65536$.

С помощью ЭВМ было найдено число всевозможных полных различных базисов в B_2. Это число равно 64801.

Оказалось, что число $N(k)$ полных базисов с коэффициентом ненадежности k (т. е. базисов, в которых почти все функции можно реализовать асимптотически оптимальными по надежности схемами, функционирующими с ненадежностью асимптотически равной $k\varepsilon$ при $\varepsilon \to 0$) равно:

$N(k) = 0$, если $k = 1$;

$N(k) = 43776$, если $k = 2$;

$N(k) = 18624$, если $k = 3$;

$N(k) = 1872$, если $k = 4$;

$N(k) = 528$, если $k = 5$.

Таким образом, 99 % подмножеств множества B_2 являются полными, причем в 68% случаев из них коэффициент ненадежности равен 2, и менее 1% полных базисов имеют коэффициент ненадежности 5.

Работа выполнена при финансовой поддержке РФФИ, номер проекта 11-01-00212а.

Список литературы

1. Васин А. В. Асимптотически оптимальные по надежности схемы в полных базисах из трехвходовых элементов. — Дисс. ... канд. физ.-мат. наук. — Пенза, 2010.

МУЛЬТИАГЕНТНАЯ ГЕОМЕТРИЧЕСКАЯ ЗАДАЧА О НАЗНАЧЕНИЯХ: ИНФОРМАЦИОННЫЙ АСПЕКТ

А. Ю. Бернштейн, Н. В. Шилов (Новосибирск)

Распределённая система — это группа децентрализованных взаимодействующих исполнителей [2]. *Распределённый алгоритм* — это протокол работы и взаимодействия исполнителей в распределённой системе, превращающий децентрализованную группу в коллектив, совместно решающий некоторую задачу [3].

Мультиагентная система — это распределённая система, состоящая из агентов [4]. *Агент* — это автономный (воспринимающий мир разделённым на *себя* и *среду*, включающей всё остальное), реагирующий (способный взаимодействовать со средой и отвечать на

воздействия среды) объект (в объектно-ориентированном смысле), внутреннее состояние которого можно характеризовать в терминах *мнений* или *веры* (Believes), *целей* (Desires), и *намерений* (Intentions) агента. *Мультиагентный алгоритм* — это распределённый алгоритм для мультиагентной системы.

В работе исследуется следующая мультиагентная геометрическая задача о назначениях, которую мы для краткости будем называть задачей о *роботах в пространстве* (RinS — *Robot in Space*): *В евклидовом пространстве R^k ($k \geq 2$) находятся $n > 1$ автономных роботов и столько же укрытий в общем положении. Местоположение всех укрытий фиксировано и известно каждому роботу. Каждому роботу изначально назначено индивидуальное укрытие, о котором робот знает. Каждый робот знает свои координаты в пространстве, знает о существовании всех остальных роботов, но не знает их координаты, и знает, что всем роботам изначально назначены и известны индивидуальные укрытия. В некоторый момент времени все роботы останавливаются, фиксируют свои текущие позиции, и затем они все должны выбрать укрытия, чтобы двинуться к ним по прямолинейному маршруту. Ясно, что роботам нельзя сталкиваться. Роботы могут взаимодействовать каждый с каждым попарно, вести переговоры в парах и обмениваться укрытиями. Задача: разработать анонимный параметрический мультиагентный алгоритм переговоров, гарантирующий, что каждый робот когда-нибудь будет точно знать, что его маршрут к укрытию, которое он выбрал в результате переговоров, не пересекается и никогда не будет пересекаться с маршрутами остальных роботов.* Эта задача "выросла" из ранее рассмотренной задачи о роботах на Марсе (*Mars Robot Puzzle* — MRP), которая докладывалась на X Международном семинаре "Дискретная математика и ее приложения" и была опубликована в [1]. Отметим, что MRP является частным случаем RinS на плоскости.

Будем называть *протоколом распределения укрытий* произвольный мультиагентный алгоритм, решающий задачу RinS. Такой протокол может состоять из алгоритма переговоров для индивидуальных роботов и алгоритма-планировщика общения между роботами мультиагентной системы. Будем говорить, что алгоритм-планировщик общения между роботами удовлетворяет условию *справедливости*, если в любой момент времени для любого робота, желающего контактировать в этот момент с каким-либо другим роботом-партнёром, обязательно наступит в будущем момент времени, когда партнёр будет готов к общению с данным роботом. Мы не будем обсуждать варианты алгоритма-планировщика, а рекомендуем

обратиться для этого к работе [1].

Шелчок — это алгоритм переговоров между парой роботов, позволяющий этим роботам проверить, нужно ли им обмениваться укрытиями, который удовлетворяет следующим двум условиям:
• если текущие пути роботов пересекаются, то они должны совершить обмен;
• после обмена укрытиями суммарная длина путей строго уменьшается.
Два крайних случая щелчка — это *простой щелчок*, при котором обмен укрытиями выполняется тогда и только тогда, когда пути пересекаются, и *щелчком со сравнением*, при котором обмен укрытиями выполняется тогда и только тогда, когда сумма длин путей уменьшается. В рамках данного исследования для нас не важно, как именно устроин щелчок, но существенно то, что при исполнении этого протокола роботы сообщают друг другу что-либо о своём положении.

В рамках исследования информационного аспекта задачи RinS в качестве входных данных будут рассматриваться действительные числа. При этом нас не будет интересовать то, как роботы хранят их в памяти. Основная величина, которая будет нас интересовать, — это общее количество бит/сообщений, переданное участниками друг другу в ходе исполнения протокола. Будем называть протокол *финитным*, если при любых допустимых значениях входных данных его работа завершается после передачи конечного количества бит.

Теорема. *Существует финитный мультиагентный алгоритм распределения укрытий, основанный на протоколе щелчка и справедливом планировщике общения между агентами.*

Будем называть протокол *ограниченным*, если существует такая константа N, что при любых допустимых значениях входных данных его работа завершается после передачи не более N бит. Будем называть протокол *ограниченным по сообщениям*, если существует такая константа N, что при любых допустимых значениях входных данных его работа завершается после передачи не более N сообщений.

Теорема. *Пусть бесконечное множество точек $S \subseteq R^k$, $k \geq 2$, лежащих в общем положении, обладает следующим свойством: существует непрерывная замкнутая плоская кривая содержащая S и ограничивающая выпуклое плоское множество. Тогда не существует ограниченного протокол распределения укрытий между $n \geq 2$ участниками, входные данные для которого (положения роботов и укрытий) принадлежат множеству S; кроме того, если множество S более чем счётно, то не существует ограниченного по сообщениям протокол распределения укрытий.*

Работа выполнена в рамках проекта СО РАН 15/10 на 2012-14 гг.

Список литературы

1. Бодин Е. В., Гаранина Н. О., Шилов Н. В. Задача о роботах на Марсе (мультиагентный подход к задаче Дейкстры) // Моделирование и анализ информационных систем. — 2011. — Т. 18, вып. 2. — С.111–126.

2. Таненбаум Э., ван Стеен М. Распределенные системы. Принципы и парадигмы. — СПб.: Питер, 2003.

3. Тель Ж. Введение в распределенные алгоритмы. — М.: МЦНМО, 2009.

4. Wooldridge M. An introduction to multiagent systems. — John Willey & Sons Ltd, 2002.

О ПОЧТИ БИЛИНЕЙНЫХ АЛГОРИТМАХ ДЛЯ ЛОКАЛЬНЫХ И СВЕРХОСНОВНЫХ АЛГЕБР

М. Блезер (Саарбрюкен, Германия), Б. В. Чокаев (Москва)

Одной из важных задач в алгебраической теории сложности является задача сложности вычисления билинейных форм. Для линейного пространства V, обозначим через V^* двойственное пространство к V, то есть, линейное пространство всех линейных форм на V.

Пусть k — поле, U, V, и W конечномерные линейные пространства над k, и $\phi : U \times V \to W$ — билинейное отображение.

Последовательность $\beta = (f_1, g_1, w_1, \ldots, f_\ell, g_\ell, w_\ell)$ такая, что $f_\lambda, g_\lambda \in (U \times V)^*$ и $w_\lambda \in W$ называется *квадратическим алгоритмом* длины ℓ для ϕ если

$$\phi(u, v) = \sum_{\lambda=1}^{\ell} f_\lambda(u, v) g_\lambda(u, v) w_\lambda \quad \text{for all } u \in U, v \in V.$$

Длина кратчайшего квадратического алгоритма для ϕ называется *мультипликативной сложностью* ϕ и обозначается $C(\phi)$.

Если A — конечномерная ассоциативная k-алгебра, то мультипликативная сложность алгебры A определяется как мультипликативная сложность умножения в A, которое является билинейным отображением $A \times A \to A$. Мультипликативная сложность алгебры A обозначается как $C(A)$.

Если в определении, $f_\lambda \in U^*$ и $g_\lambda \in V^*$, то алгоритм называется *билинейным* а длина кратчайшего алгоритма называется *билинейной сложностью или рангом*. Ранг ϕ и A, соответсвенно обозначаются через $R(\phi)$ и $R(A)$.

Как ранг и мультипликативная сложности соотносятся между собой? Очевидно, $C(A) \leq R(A)$ и несложно видеть, что $R(A) \leq 2C(A)$. Существуют примеры, где мультипликативная сложность и ранг различаются, например, мультипликативная сложность умножения матрицы 2×2 на матрицу 2×3 равна 10 [1] над полями характеристики не 2, тогда как ранг этого умножения равен 11 [2]. Однако, до сих пор не известен пример алгебры, для которой эти две сложности различаются.

Фундаментальной нижней оценкой для мультипликативной сложности ассоциативной алгебры A является оценка Алдера—Штрассена [3]:

$$C(A) \geq 2 \dim A - t_A, \tag{1}$$

где t_A — число максимальных двусторонних идеалов в A. Это оценка является точной в том смысле, что существуют алгебры, для которых неравенство обрашается в равенство. Такие алгебры называются *алгебрами минимальной мультипликативной сложности*. Если это неравенство обрашается в равенство для билинейной сложности, то соответсвующая алгебра называется *алгеброй минимального ранга*. Все алгебры минимального ранга найдены в работе [4].

Одним из интересных вопросов касающийся соотношения билинейной и мультипликативной сложностей алгебры является определить существует ли для данной алгебры оптимальный квадратический алгоритм, который не является билинейным. В 1981 г. доказано [5], что любой оптимальный квадратический алгоритм для алгебры с делением (алгебра называется алгеброй с делением, если каждый ненулевой ее элемент является обратимым) минимальной мультипликативной сложности является существенно билинейным. Одной из открытых проблем на данный момент является найти все алгебры, для которых любой оптимальный квадратический алгоритм является существенно билинейным [6]. Решение данной задачи для всех алгебр сразу не представляется возможным. Вместо этого можно зафиксировать некоторый класс алгебр и определить какие алгебры из данного класса удовлетворяют этому условию. Целью данной работы является исследование данного вопроса для локальных и сверхосновных алгебр.

Для того, чтобы сформулировать основную теорему данной работы дадим некоторые определения. Пусть A — алгебра над полем

k. Радикалом A называется пересечение всех ее максимальных двусторонних идеалов и обозначается $\operatorname{rad} A$. Левым (правым) аннигилятором $\operatorname{rad} A$ называется множество $L_A = \{x \in \operatorname{rad} A \mid x(\operatorname{rad} A) = \{0\}\}$ ($R_A = \{x \in \operatorname{rad} A \mid (\operatorname{rad} A)x = \{0\}\}$).

Алгебра A называется *локальной*, если фактор алгебра $A/\operatorname{rad} A \cong D$ является алгеброй с делением. Алгебра A называется *сверхосновной*, если фактор алгебра $A/\operatorname{rad} A \cong k \times \ldots \times k$ изоморфна прямому произведению некоторого количества полей.

Теорема. *Пусть A — локальная или сверхосновная алгебра минимальной мультипликативной сложности, $\beta = (f_1, g_1, w_1, \ldots, f_\ell, g_\ell, w_\ell)$ — оптимальный квадратический алгоритм для A. Если $w_\lambda \notin L_A \cap R_A$ для всех λ, то β является существенно билинейным, то есть после перестановки некоторых f_λ с g_λ, имеем $f_\lambda(x, y) = f_\lambda(x, 0)$ и $g_\lambda(x, y) = g_\lambda(0, y)$ для всех $x, y \in A$.*

Назовем квадратический алгоритм для алгебры A *почти билинейным*, если не выполняется предпосылка этой теоремы, то есть, если существует λ такое, что $w_\lambda \in L_A \cap R_A$. Из теоремы следует, что любой оптимальный квадратический алгоритм для локальной или сверхосновной алгебры минимальной мультипликативной сложности является либо существенно билинейным, либо почти билинейным. Следующий пример показывает, что не все алгоритмы для таких алгебр являются существенно билинейными.

Пример. Пусть k — поле характеристики отличной от двух. Алгебра $k[X]/(X^2)$ является локальной и сверхосновной, но имеет квадратический алгоритм, который не является существенно билинейным (но естественно является почти билинейным): мы можем вычислить коэффициенты $(a + bX)(a' + b'X)$ как aa' и $ab' + ba' = \frac{1}{2}(b + b')(a + a') + \frac{1}{2}(b - b')(-a + a')$. Заметим, что $X \in L_{k[X]/(X^2)} = R_{k[X]/(X^2)}$.

Работа выполнена при поддержке следующих грантов: гранта DFG BL 511/10-1, гранта РФФИ № 12-01-91331-ННИО_а, и гранта Президента РФ № МД-757.2011.9.

Список литературы

1. A. Waksman. On Winograd's algorithm for inner products // IEEE Trans. Comp. — 1970. — V. 19. — P. 360–361.

2. Valery B. Alekseyev. On the complexity of some algorithms of matrix multiplication //J. Algorithms. — 1985. — V. 6, № 1. — P. 71–85.

3. A. Alder and V. Strassen. On the algorithmic complexity of associative algebras //Theoret. Comput. Sci. — 1981. — V. 15. — P. 201–211.

4. Markus Bläser. A complete characterization of the algebras of minimal bilinear complexity //SIAM J. Comput. — 2004. — V. 34, № 2. — P. 277–298.

5. Ephraim Feig. On systems of bilinear forms whose minimal division-free algorithms are all bilinear //J. Algorithms. — 1981. — V. 2, № 3. — P. 261–281.

6. Peter Bürgisser, Michael Clausen, and M. Amin Shokrollahi. Algebraic complexity theory. — Springer, 1997.

О СИНТЕЗЕ РЕКУРСИВНЫХ СХЕМ ИЗ ФУНКЦИОНАЛЬНЫХ ЭЛЕМЕНТОВ С ОГРАНИЧЕННОЙ ГЛУБИНОЙ РЕКУРСИИ

С. В. Блинов, С. А. Ложкин (Москва)

В данной работе рассматривается одна из моделей программ, вычисляющих функции алгебры логики (ФАЛ), — рекурсивные схемы из функциональных элементов (РСФЭ). Эта модель управляющих систем, функционально эквивалентная модели схем из функциональных элементов, впервые она была рассмотрена в работе [1]. В этой работе была установлена линейная относительно числа переменных асимптотика функции Шеннона для сложности РСФЭ, что существенно отличает модель РСФЭ от других моделей программ и, в частности, моделей [2].

Определим РСФЭ *общего вида* над базисом Б, опираясь на понятие схемы из функциональных элементов (СФЭ) [3] и используя индукцию по рекурсивной глубине РСФЭ.

Любая РСФЭ общего вида рекурсивной глубины $d \geq 1$ представляет собой упорядоченный набор из d СФЭ.

Шаг 1. РСФЭ F_1 рекурсивной глубины 1 над базисом Б включает в себя единственную СФЭ G_1 над базисом Б. Эта РСФЭ реализует ту же ФАЛ, что и составляющая ее СФЭ. Будем говорить, что этой РСФЭ соответствует расширенный базис $\text{Б}_1 = \text{Б}$.

Шаг $S + 1$. Пусть построена РСФЭ F_S рекурсивной глубины S над базисом Б, причем F_S реализует функцию f_S и этой РСФЭ соответствует расширенный базис Б_S. Пусть D_S — функциональный элемент, реализующий функцию f_S. Построим базис $\text{Б}_{S+1} = \text{Б}_S \cup D_S$, а также построим СФЭ G_{S+1} над базисом Б_{S+1}. Тогда набор $F_{S+1} = F_S \cup G_{S+1}$ является РСФЭ рекурсивной глубины $S + 1$. Эта РСФЭ

реализует ту же функцию, что и G_{S+1} и ей соответствует расширенный базис Б_{S+1}.

Сложность $L_{\text{Б}}(F)$ РСФЭ F общего вида над базисом Б равна общему числу функциональных элементов во всех СФЭ, составляющих РСФЭ F. Стандартным образом вводится сложность $L_{\text{Б}}(f)$ ФАЛ f и функции Шеннона $L_{\text{Б}}(n)$ в классе РСФЭ над базисом Б, а также для фиксированного натрального d, $d \geq 1$, — сложность $L_{\text{Б}}^{(d)}(f)$ ФАЛ f и функция Шеннона $L_{\text{Б}}^{(d)}(n)$ в классе РСФЭ рекурсивной глубины не более, чем d, над базисом Б.

В статье [1] показано, что выбор базиса на сложность РСФЭ влияет очень слабо (переход от одного базиса к другому изменяет сложность ФАЛ не более, чем на константу) и что функция Шеннона $L_{\text{Б}}(n)$ асимптотически равна $\frac{3n}{\log_2 3}$.

Теорема. *Для базиса* $Б_0 = \{\vee, \&, \neg\}$ *справедливы следующие оценки:*

$$L^{(2)}(n) \leq 3\sqrt{\frac{2^n}{n}}(1 + o(1)),$$

$$L^{(2)}(n) \geq 2\sqrt{2}\sqrt{\frac{2^n}{n}}(1 - o(1)).$$

Список литературы

1. Грибок С. В. Об одной модели рекурсивных схем их функциональных элементов // Вестник Московского университета. Серия 15. Вычислительная математика и кибернетика. — 2002. — № 4. — С. 31–36.

2. Кузьмин В. Ф. Оценка сложности реализации функций алгебры логики простейшими видами бинарных программ // Методы дискретного анализа в теории кодов и схем. — Вып. 29. — 1976. — С. 11–39.

3. Лупанов О. Б. Асимптотические оценки сложности управляющих систем. — М.: Изд-во МГУ, 1984.

О СЛОЖНОСТИ МУЛЬТИПЛЕКСОРНОЙ ФУНКЦИИ В КЛАССЕ СХЕМ ИЗ ФУНКЦИОНАЛЬНЫХ ЭЛЕМЕНТОВ

Н. В. Власов (Москва)

Рассматривается задача оптимальной по сложности реализации мультиплексорной функции алгебры логики (ФАЛ) в классе схем из функциональных элементов (СФЭ) в стандартном базисе $Б_0 = \{x \,\&\, y, x \vee y, \overline{x}\}$ (см., например, [1, 2]).

Мультиплексорной ФАЛ (мультиплексором) μ_n порядка n называется ФАЛ от $n + 2^n$ булевых переменных (БП), где первые n переменных называются "адресными", оставшиеся 2^n — "информационными", а значение функции равно значению той ее информационной БП, номер которой задается значениями адресных БП.

Задача синтеза решается в классе СФЭ в стандартном базисе $Б_0 = \{x \,\&\, y, x \vee y, \overline{x}\}$. Сложность $L(\Sigma)$ СФЭ Σ определяется как число функциональных элементов (ФЭ) "&", "$\vee$" и "$\neg$" в ней.

Сложность мультиплексорной ФАЛ изучалась в ряде работ. Известно (см., например, [3]), что сложность реализации ФАЛ μ_n, $n = 1, 2, \ldots$, как СФЭ, так и формулами в стандартном базисе $Б_0$, асимптотически равна 2^{n+1}. В работе [4] получена нижняя оценка вида $2^{n+1} + c_1 \cdot 2^{n/2} - O\left(2^{n/4}\right)$ и верхняя оценка вида $2^{n+1} + c_2 \cdot 2^{n/2} + O\left(2^{n/4}\right)$, для сложности реализации мультиплексора порядка n в классе СФЭ над базисом $Б_0$, где $c_1 = 1/3$, $c_2 = 2$, если n четно, и $c_1 = 0,32$, $c_2 = 3/\sqrt{2}$, если n нечетно. Кроме того, в [3] была установлена асимптотика сложности ФАЛ μ_n в классе СФЭ в базисе $\{x\&y, x \oplus y, \overline{x}\}$, равная 2^{n+1}. В работе [5] были получены асимптотические оценки высокой степени точности [6] вида $2^{n+1}\left(1 + \frac{1}{2n} \pm O\left(\frac{1}{n \log_2 n}\right)\right)$ для сложности ее реализации в классе π-схем, а в [7] были установлены близкие к ним оценки вида $2^{n+1}\left(1 + \frac{c(n)}{n} \pm O\left(\frac{1}{n \log_2 n}\right)\right)$, где $c(n) \in \left[\frac{1}{2}, 1\right]$, для сложности реализации мультиплексора порядка n в классе формул в стандартном базисе.

В работе [8] доказано, что значение глубины мультиплексорной ФАЛ порядка n в стандартном базисе в случае, если ФЭ "&" и "$\vee$" имеют единичную глубину, а ФЭ "$\neg$" — нулевую, равно 2, если $n = 2$, и равно $n + 2$, если $1 < n \leqslant 5$ или $n \geqslant 20$. Для случая $5 < n < 20$ устанавливаются нижняя оценка $(n + 2)$ и верхняя оценка $(n + 3)$ глубины ФАЛ μ_n. Аналогичные результаты справедливы также для

базиса, состоящего из всех элементарных конъюнкций и дизъюнкций от двух переменных.

Теорема. *Для любой СФЭ* Σ *в базисе* $Б_0$*, реализующей ФАЛ* μ_n*,* $n \geqslant 2$*, справедливо:*

$$L(\Sigma) \geqslant 2^{n+1} + \frac{\sqrt{2}}{2} 2^{\frac{n}{2}} - O(n).$$

Работа выполнена при финансовой поддержке РФФИ (грант №12-01-00964-а).

Список литературы

1. Лупанов О. Б. Асимптотические оценки сложности управляющих систем. — М.: Изд-во МГУ, 1984.

2. Ложкин С. А. Лекции по основам кибернетики. — М.: Издательский отдел ф-та ВМиК МГУ, 2004.

3. Коровин В. В. О сложности реализации универсальной функции схемами из функциональных элементов // Дискретная математика. — 1995. — Т. 7, вып. 2. — С. 95–102.

4. Румянцев П. В. О сложности реализации мультиплексорной функции схемами из функциональных элементов. // Проблемы теоретической кибернетики. Тезисы докладов XIV международной конференции (Пенза, 23–28 мая 2005 г.). — М.: Изд-во механико-математического факультета МГУ, 2005. — С. 133.

5. Ложкин С. А., Власов Н. В. О сложности мультиплексорной функции в классе π-схем. // Ученые записки Казан. ун-та. Сер. Физ.-матем. науки. — 2009. — Т. 151, кн. 2. — С. 98–106.

6. Ложкин С. А. О синтезе формул, сложность и глубина которых не превосходят асимптотически наилучших оценок высокой степени точности. // Вестн. Моск. ун-та Сер. 1. Математика. Механика. — 2007. — № 3. — С. 20–26.

7. Власов Н. В. О сложности мультиплексорной функции в классе формул // Проблемы теоретической кибернетики. Материалы XVI Международной конференции (Нижний Новгород, 20–25 июня 2011 г.). Нижний Новгород: Изд-во Нижегородского госуниверситета, 2011. — С. 96–97.

8. Ложкин С. А., Власов Н. В. О глубине мультиплексорной функции // Вестн. Моск. ун-та. Сер. 15. Вычисл. матем. и киберн. — 2011. — № 2. — С. 40–46.

ОБ УНИВЕРСАЛЬНЫХ ФУНКЦИЯХ ДЛЯ КЛАССА ЛИНЕЙНЫХ БУЛЕВЫХ

А. А. Вороненко, Б. В. Кибза (Москва)

Будем называть линейной функцию, представимую в виде $\alpha_0 + \alpha_1 x_1 + ... + \alpha_n x_n$. Назовём не всюду определённую (далее частичную) булеву функцию n переменных универсальной, если для любой линейной функции g тех же переменных существует $n+1$ набор из области определения f такой, что единственной линейной функцией, совпадающей с f на этих наборах, является g.

Обозначим через $\gamma(x_1, x_2, x_3, x_4, x_5, x_6)$ функцию, равную нулю на нулевом наборе и всех наборах вида $\mathbf{e_i} + \mathbf{e_{i+2}} + \mathbf{e_{i+3}}$, единице на единичном наборе и наборах вида $\mathbf{e_i}$, $\mathbf{e_i} + \mathbf{e_{i+2}}$, где $\mathbf{e_i}$ единичный вектор, имеющий единицу только в i-ой позиции, и неопределённую на всех остальных наборах. Индексы расположены по кругу и принимают значения 1, 2, 3, 4, 5, 6, операция сложения индексов означает движение по кругу.

Лемма 1. *Функция $\gamma(x_1, x_2, x_3, x_4, x_5, x_6)$ является универсальной функцией шести переменных.*

Доказательство. В силу симметричности функции

$$\gamma(x_1, x_2, x_3, x_4, x_5, x_6)$$

относительно группы перестановок достаточно рассмотреть соответствующие наборы. Лемма доказана.

Определим функцию Г таким образом, что

$$\Gamma(x_{1,1}, x_{1,2}, ..., x_{k,6}) = \gamma(x_{i,1}, x_{i,2}, ..., x_{i,6}),$$

если все $x_{j,s}$ равны нулю при $j \neq i$. На остальных наборах функция Г неопределена.

Лемма 2. *Функция $\Gamma(x_{1,1}, x_{1,2}, ..., x_{k,1}, x_{k,2}, ..., x_{k,6})$ является универсальной функцией $6k$ переменных.*

Доказательство. Рассмотрим произвольную линейную функцию g зависящую от $6k$ переменных: $g = \beta_{1,1}x_{1,1} + \beta_{1,2}x_{1,2} + ... + \beta_{1,6}x_{1,6} + ... + \beta_{k,1}x_{k,1} + \beta_{k,2}x_{k,2} + ... + \beta_{k,6}x_{k,6} + \delta$.

Если все $x_{j,s}$ равны нулю при $j \neq i$, то функция g равна $\beta_{i,1}x_{i,1} + \beta_{i,2}x_{i,2} + ... + \beta_{i,6}x_{i,6} + \delta$. Применив лемму 1, мы можем подобрать такие 7 наборов на соответствующем подкубе размера шесть, что функция g будет единственной линейной, совпадающей с Г. Проделав эту процедуру для всех i, получим множество наборов функции Г, однозначно задающих g среди всех линейных. Применив теорему Кронекера — Капелли [1, с. 96, с. 137], избавимся от лишних наборов. Теорема доказана.

Лемма 3. *Пусть $g(x_1, ..., x_n)$ — универсальная функция n переменных. Пусть функция $f(x_1, ..., x_{n+1})$ совпадает с g при $x_{n+1} = 0$ и определена на произвольном квадрате при $x_{n+1} = 1$ нелинейным образом. Тогда $f(x_1, ..., x_{n+1})$ — универсальная функция $n+1$ переменной.*

Доказательство. Значения при $x_{n+1} = 0$ в силу условий леммы определяют произвольную линейную функцию с точностью до слагаемого $\alpha_{n+1}x_{n+1}$. Поскольку нелинейная функция на квадрате не совпадает ни с одной линейной, то как для функции, так и для её отрицания найдётся набор с координатой $x_{n+1} = 1$, на котором они совпадут. Лемма доказана.

Теорема 1. *При $n \geq 6$ существует универсальная функция, заданная на $3\frac{1}{6}n + \frac{5}{6}(n \bmod 6) + 1$ наборах.*

Доказательство. Применим лемму 2 для наибольшего целого, кратного шести и не превосходящего n. После этого применим лемму 3 необходимое число раз. Теорема доказана.

Работа выполнена на факультете ВМК МГУ имени М.В. Ломоносова при поддержке гранта Президента РФ МД-757.2011.9.

Список литературы

1. Ильин В. А., Ким Г. Д. Линейная алгебра и аналитическая геометрия. — Мю: Изд-во Московского университетата, 1998.

2. Вороненко А. А. Об универсальных частичных функциях для класса линейных // Дискретная математика. — В печати.

О СЛОЖНОСТИ УМНОЖЕНИЯ И ИНВЕРТИРОВАНИЯ В НЕКОТОРЫХ КОЛЬЦАХ МНОГОЧЛЕНОВ

С. Б. Гашков, И. С. Сергеев (Москва)

В настоящей работе рассматривается реализация умножения и инвертирования в некоторых фактор-кольцах вида $\mathbf{K}[x]/(f(x))$ схемами над кольцом $\mathbf{K}$. Схемы над $\mathbf{K}$ — это схемы из функциональных элементов над арифметическим базисом $\{\pm, *, /\} \cup \{ax \mid a \in \mathbf{K}\}$. Умножение реализуется в базисе без операции деления.

Пусть $\mathbf{K}$ — кольцо с единицей, p — некоторое простое число. Обозначим

$$\mathbf{K}_{p,n}(x) = \mathbf{K}[x]/\left(x^{(p-1)p^n} + x^{(p-2)p^n} + \ldots + x^{p^n} + 1\right).$$

В известной статье [9] А. Шёнхаге и Ф. Штрассен фактически построили алгоритм умножения в кольцах $\mathbf{K}_{2,n}(x)$ (как составную часть метода умножения чисел) в случае, когда в кольце $\mathbf{K}$ обратима двойка, имеющий сложность $O(2^n n \log n)$. Метод основан на применении ДПФ порядка степени двойки. Аккуратная оценка сложности метода составляет $(3+o(1))2^n n \log_2 n$: асимптотически вся сложность сосредоточена в ДПФ порядка 2. Как следствие, многочлены суммарной степени $< N$ над $\mathbf{K}$ можно перемножать со сложностью $(3 + o(1))N \log_2 N \log_2 \log N$.

В случае кольца $\mathbf{K}$, в котором двойка не обязательно обратима, зато обратима тройка, Шёнхаге [8] предложил модификацию алгоритма [9] для умножения в $\mathbf{K}_{3,n}(x)$ сложности $O(3^n n \log n)$. Метод основан на применении ДПФ порядка степени тройки. Впоследствии Д. Кантор и Э. Калтофен [5] обобщили метод Шёнхаге на случай кольца $\mathbf{K}_{p,n}(x)$ с обратимым p, а также указали способ умножения многочленов над произвольным кольцом $\mathbf{K}$.

Троичный метод Шёнхаге [8] является теоретически самым эффективным известным средством реализации умножения многочленов над кольцами характеристики 2 — в них необратима двойка, поэтому неприменим двоичный метод [9]. Перечислим известные аккуратные оценки сложности метода [8] (или его модификаций) умножения в $\mathbf{K}_{3,n}(x)$, $\operatorname{char} \mathbf{K} = 2$, приведенные к виду $(A+o(1))3^n n \log_2 n$: $A = 24$ [6], $A = 18$ [4] и $A = 16,5$ [7]. Авторами в работе [1] была построена модификация метода [8], позволившая понизить оценку сложности до $A = 11,25$ с последующим уточнением до $A = 10,5$ [2]. На самом деле, справедлива

Теорема 1. *Пусть* $3^{-1} \in \mathbf{K}$. *Тогда умножение в кольце* $\mathbf{K}_{3,n}(x)$ *можно реализовать схемой сложности* $(13+o(1))3^n n \log_2 n$ *и глубины* $O(n)$. *В случае* $\operatorname{char} \mathbf{K} = 2$ *можно построить схему сложности* $(10 + o(1))3^n n \log_2 n$ *и глубины* $(6 + o(1))n$.

Как следствие, многочлены суммарной степени $< N$ над кольцом $\mathbf{K}$ характеристики 2 можно перемножать со сложностью $(3,16 + o(1))N \log_2 N \log_2 \log N$. Теорема 1 также позволяет оценить сложность метода [5] умножения многочленов суммарной степени $< N$ над произвольным кольцом $\mathbf{K}$ как $(B + o(1))N \log_2 N \log_2 \log N$, где $B = 3 + 6,5 \log_3 2 < 7,11$.

Результат теоремы 1 является окончательным в следующем (хотя и достаточно слабом) смысле: асимптотически вся сложность сосредоточена в ДПФ порядка 3, которые являются неустранимой частью троичного метода [8] (более точно, в предлагаемом методе вместо

ДПФ порядка 3 используются композиции ДПФ порядка 3 и некоторых простых преобразований, имеющие тем не менее такую же сложность, как одно ДПФ порядка 3).

Стандартным образом из теоремы 1 извлекаются следствия для сложности умножения в фактор-кольцах $\mathbf{K}[x]/(f(x))$, в частности, в кольцах $\mathbf{K}_{p,n}(x)$. Можно показать, что в некоторых случаях (например, $p = 5$ и $\mathrm{char}\,\mathbf{K} = 2$) умножение в $\mathbf{K}_{p,n}(x)$ быстрее выполнять в духе метода [5], опираясь на эффективную реализацию ДПФ порядка p.

Инвертирование (вычисление мультипликативного обратного элемента) также может быть реализовано эффективно в кольце $\mathbf{K}_{p,n}(x)$ — особенный интерес представляет случай, когда это кольцо является полем. Такой случай возникает, например, если $\mathbf{K} = GF(2)$, 2 — первообразный корень по модулю p, и p^2 не делит $2^{p-1} - 1$, см. [3].

Методом [1] с применением теоремы 1 доказывается

Теорема 2. *Пусть* $\mathbf{K} = GF(2)$ *и* $\mathbf{K}_{p,n}(x) \cong GF(2^N)$, *где* $N = (p-1)p^n$. *Тогда инвертирование в* $\mathbf{K}_{p,n}(x)$ *можно реализовать схемой сложности* $O(\log p)N \log N \log\log N$ *и глубины* $O(\log^2 N)$. *В случае* $p = 3$ *для сложности схемы справедлива оценка* $(25+o(1))3^n n \log_2 n$.

Работа выполнена при финансовой поддержке РФФИ, проекты 11–01–00508 и 11–01–00792, и программы фундаментальных исследований Отделения математических наук РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения» (проект «Задачи оптимального синтеза управляющих систем»).

Список литературы

1. Гашков С. Б., Сергеев И. С. О сложности и глубине схем для умножения и инвертирования в в некоторых полях $GF(2^n)$ // Вестник Моск. ун-та. Серия 1. Математика. Механика. — 2009. — № 4. — С. 3–7.

2. Гашков С. Б., Сергеев И. С. Алгоритмы быстрого преобразования Фурье // Сб. «Дискретная математика и ее приложения». Часть V. — М.: Изд-во ИПМ РАН, 2009. — С. 3–23.

3. Лидл Р., Нидеррайтер Х. Конечные поля. Т. 1. — М.: Мир, 1988.

4. Bernstein D. J. Multidigit multiplication for mathematicians. — Manuscript, 2001. — http://cr.yp.to/papers.html#m3.

5. Cantor D., Kaltofen E. On fast multiplication of polynomials over arbitrary algebras // Acta Inf. — 1991. — V. 28, № 7. — P. 693–701.

6. von zur Gathen J., Gerhard J. Modern computer algebra. — Cambridge: Cambridge University Press, 1999.

7. Mateer T. Fast Fourier algorithms with applications. — Ph. D. Thesis, Clemson Univ., 2008.

8. Schönhage A. Schnelle multiplikation von polynomen über körpern der charakteristik 2 // Acta Inf. — 1977. — V. 7. — P. 395–398.

9. Schönhage A., Strassen V. Schnelle multiplikation großer zahlen // Computing. — 1971. — V. 7. — P. 271–282. [Русский перевод: Шёнхаге А., Штрассен В. Быстрое умножение больших чисел // Кибернетический сборник. Вып. 10. — М.: Мир, 1973. — С. 87–98.]

ПОЛИНОМИАЛЬНЫЙ АЛГОРИТМ НАХОЖДЕНИЯ ПРИБЛИЖЕННОГО РЕШЕНИЯ ЗАДАЧИ О РАЗБИЕНИИ С ГАРАНТИРОВАННОЙ ОЦЕНКОЙ ТОЧНОСТИ

М. А. Герасимов (Санкт-Петербург)

Рассматривается жадный полиномиальный по времени (для детерминированной одноленточной машины Тьюринга) алгоритм нахождения приближенного задачи о разбиении множества неотрицательных целых чисел на K равных по весу подмножеств, где $K > 1$. Алгоритм позволяет находить приближенное решение задачи о разбиении с точностью, определяемой наибольшим во входном потоке данных числом. Имеется возможность находить разбиения (как точные, так и приближенные) и в тех случаях, когда широко известный полиномиальный алгоритм Кармаркара-Карпа [1] не работает.

Рассматриваемая реализация алгоритма использует линейный список входных элементов, занумерованных натуральными числами $X = \{x_1, , x_M\}$ и имеющих положительные веса $\{w_1, , w_M\}$ соответственно. Обозначим через W(X) суммарный вес элементов множества X:

$$W(X) = \sum_{i=1}^{M} w_i.$$

Пусть множество X разбито на K дизъюнктных подмножеств, $K \geq 2$, $X_1, X_2, ..., X_K : X_i \cap X_j = \oslash$, $X_1 \cup X_2 ... \cup X_K = X$. Согласно [1] весом разбиения назовем величину

$$F(X_1, X_2, ..., X_K) = \max\{W(X_1), W(X_2), ..., W(X_K)\}$$

Требуется найти такое разбиение множества X на K подмножеств $X_1^*, X_2^*, ..., X_K^*$, что

$$F(X_1^*, X_2^*, ..., X_K^*) = \min\{F(X_1, X_2, ..., X_K)\}$$

Нахождение разбиения $\{X_1^*, X_2^*, ...X_K^*\}$ множества X и точного значения $F(X_1^*, X_2^*, ..., X_K^*)$ для заданного множества элементов X является NP - полной задачей [2]. Одним из направлений исследования возможностей приближенного решения этой задачи за полиномиальное время на детерминированной машине Тьюринга является поиск решения $F(X_1, X_2, ..., X_K)$, достаточно близкого к $F(X_1^*, X_2^*, ..., X_K^*)$ за полиномиальное время.

Алгоритм работает в три этапа, для каждого из которых есть полиномиальная временная оценка. Для дальнейшей идентификации данный алгоритм будет называться "алгоритмом гребенки".

Первый этап работы алгоритма заключается в сортировке входных неотрицательных целых чисел в порядке убывания их весов. В дальнейшем будем полагать, что они поступают последовательно от большего по весу числа к меньшему.

Второй этап работы алгоритма заключается в разбиении полученного входного потока чисел на K подмножеств, где $K \geq 2$. При этом входные элементы с индексами, кратными по модулю K единице попадают в первое множества, кратные по модулю K двойке во второе, и т.д. Например, если $K = 2$, то элементы с четным индексом попадают во второе множество, а с нечетным — в первое. После завершения работы этого этапа получаем K множеств, отличающихся по весу не более чем на вес первого элемента отсортированного набора данных.

Теорема 1. *Вес K-го (последнего) множества алгоритма гребенки после второго этапа работы отличается от веса первого множества не более чем на вес первого элемента отсортированного потока входных чисел.*

Доказательство может быть произведено методом полной математической индукции по числу входных элементов.

Третий этап заключается в поиске перестановок элементов различных множеств, которые уменьшают погрешность найденного разбиения. Для этого вычисляется общий вес всех элементов входного набора данных W(X) и делится на K, что дает так называемый идеальный вес множества, который может быть достигнут тольКо в случае, Когда задача точного разбиения имеет решение. В некоторых случаях, Когда W(X) не кратен K, получается некоторое рациональное число (пара целых чисел), задающее идеальный вес для приближенного разбиения.

Далее для каждого из полученных множеств с индексом i считается величина G_i, определяющая избыток или недостаток веса относительно идеального разбиения. В случае избытка величина G_i будет больше нуля, в случае недостатка — меньше. Все множества сортируются по убыванию веса. Далее берем последнее из множеств и ищем для него один или несколько элементов в первом множестве, таких, что их суммарный вес будет равен (или меньше) $-G_i$ последнего множества. Если хоть один элемент был найден, то формируем набор множеств второго уровня по следующему правилу: все множества кроме первого и последнего сохраняют свой состав. Первое множество теряет найденный элемент (элементы), последнее множество приобретает этот элемент (элементы). Список вновь полученных множеств сортируется в порядке убывания их весов. Пересчитываются величины G_i.

Процесс продолжается до тех пор, пока хоть один подходящий элемент будет найден, либо хоть одна из величин G_i не равна нулю. Если ни одного элемента найти не удалось, либо все G_i равны нулю, процесс завершается. Получившийся набор множеств и есть приближенное разбиение исходного множества на K подмножеств. Максимальная по абсолютной величине G_i дает оценку точности полученного разбиения. Если все G_i равны нулю, полученное разбиение является точным разбиением исходного множества на K подмножеств.

Теорема 2. *Алгоритм гребенки завершает свою работу за полиномиальное время от размера входных данных на одноленточной, одноголовочной машине Тьюринга со входом и выходом.*

Список литературы

1. Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи. — М.: Мир, 1982.

2. Fischetti M., Martello S. Wost-case analysis of the differencing method for the partition problem // Math. Programming. — 1987. — V. 37, № 1. — P. 117–120.

3. Минский М. Вычисления и автоматы. — М., 1971.

4. Horowits E., Sahni S. Fundamentals of Computer Algorithms. — Computer Science Press, 1978.

ДЛИНА МИНИМАЛЬНОГО УСЛОВНОГО ТЕСТА ДЛЯ МОНОТОННЫХ ФУНКЦИЙ НА НЕКОТОРЫХ ГРАФАХ

М. В. Горяинов, К. А. Зыков (Москва)

В работах [1, 2] исследовалась задача о длине минимальных условных тестов для монотонных функций, заданных на частично упорядоченных множествах и принимающих только значения 0 и 1. В частности, М. В. Горяинов рассматривал минимальные условные тесты для монотонных функций, заданных на ориентированных графах из следующих трех классов.

Граф первого класса, обозначаемый далее $\Gamma(n,k)$, n,k — натуральные, $n>1$, содержит k ярусов по 2^{n-1} вершин в каждом. Ярусы пронумерованы числами от 1 до k. Каждой из вершин графа сопоставлен булев набор длины n, причем различным вершинам в одном ярусе соответствуют различные наборы. Если ярус имеет четный номер, то его вершинам сопоставлены наборы с четным числом единиц, а если ярус имеет нечетный номер, то его вершинам сопоставлены наборы с нечетным числом единиц. Две вершины графа соединены ребром в том и только том случае, когда эти вершины находятся в соседних ярусах, и расстояние Хемминга между соответствующими наборами равно 1.

Граф второго класса, обозначаемый далее $H(n,k)$, $n\geq 3$, определен для нечетных n. Его строение аналогично строению графа первого класса. Единственное различие — ярусы графа $H(n,k)$ содержат $C_n^{(n-1)/2}$ вершин, а соответствующие вершинам булевы наборы содержат либо $(n-1)/2$, либо $(n+1)/2$ единиц (в зависимости от четности номера яруса).

Граф третьего класса, обозначаемый далее $G(n,k)$, n,k — натуральные, $n>1$, содержит k ярусов, пронумерованных числами от 1 до k. Если ярус имеет четный номер, то он содержит 2^n вершин. Каждой из вершин сопоставлен булев набор длины n, причем различным вершинам в одном ярусе соответствуют различные наборы. Если ярус имеет нечетный номер, то он содержит $n2^{n-1}$ вершин, которым сопоставлены наборы длины n, содержащие ровно в одной из позиций «-» — прочерк, а в остальных позициях — 0 или 1. Две вершины графа соединены ребром в том и только том случае, когда эти вершины находятся в соседних ярусах, и соответствующие наборы совпадают во всех позициях, кроме позиции, содержащей «-».

Во всех случаях ребра ориентированы от вершин, лежащих в ярусе с меньшим номером. На множестве вершин установлен частичный порядок следующим образом. Вершина v графа Q ($Q=\Gamma(n,k)$,

$H(n,k)$ или $G(n,k)$) меньше вершины u, если существует ориентированный путь с началом v и концом u. Естественным образом определяются монотонные функции, определенные на множестве вершин этих графов и принимающие значения из множества $\{0,1\}$. Через $M(Q)$ обозначим множество таких функций для графа Q. Рассмотрим также $M_i(Q)$ — множество монотонных функций, имеющих по крайней мере одно нулевое значение на i-м ярусе графа Q и по крайней мере одно единичное значение на $(i+1)$-ом ярусе. Через $t(Q)$ (соответственно, $t_i(Q)$) обозначим длину минимального условного теста, определяющего монотонную функцию из множества $M(Q)$ (соответственно, $M_i(Q)$). М. В. Горяинов показал, что для $Q = \Gamma(n,k)$ и $Q = H(n,k)$ величина $t_i(Q)$ совпадает, а для $Q = G(n,k)$ совпадает или на единицу больше, чем число вершин в двух соседних ярусах графа Q. К. А. Зыков понизил верхнюю оценку для графов $G(n,k)$ на единицу. Объединяя эти результаты, получим следующее утверждение.

Теорема. *Справедливы равенства*

$$t_i(\Gamma(n,k)) = 2^n, \quad t_i(H(n,k)) = 2C_n^{(n-1)/2}, \quad t_i(G(n,k)) = 2^n + n2^{n-1}.$$

Можно показать, что для рассматриваемых графов $t(Q) = t_i(Q) + [\log_2 k] - 1$.

Отметим, что для доказательства нижних оценок достаточно ограничиться функциями, равными константе на каждом из ярусов графа, и функциями, отличными от них ровно в одной вершине.

Работа второго автора выполнена при финансовой поддержке РФФИ (проект 11-01-00508).

Список литературы

1. Горяинов М. В. О длине минимального условного теста для монотонных функций на некоторых графах. Дипломная работа. — Факультет ВМК МГУ, 1995.

2. Горяинов М. В., Сапоженко А. А. О расшифровке монотонных функций на частично упорядоченных множествах // Дискретный анализ и исследование операций. — 1995. — Т. 2, № 3. — С. 79–80.

АСИМПТОТИЧЕСКИ ОПТИМАЛЬНЫЕ ПО НАДЕЖНОСТИ НЕВЕТВЯЩИЕСЯ ПРОГРАММЫ С АБСОЛЮТНО НАДЕЖНЫМ СТОП-ОПЕРАТОРОМ

С. М. Грабовская (Пенза)

Рассматривается реализация булевых функций неветвящимися программами с операторами условной остановки (стоп-операторами) [1] в произвольном полном конечном базисе B. *Программы с оператором условной* остановки характеризуются наличием управляющей команды — команды условной остановки, дающей возможность досрочного прекращения работы при выполнении определенного условия, а именно, при поступлении единицы на вход оператора условной остановки (который еще называют стоп-оператором). Введем необходимые определения и понятия.

Будем считать, что операторы условной остановки абсолютно надежны, а все вычислительные операторы независимо друг от друга с вероятностью ε ($\varepsilon \in (0,\ 1/2)$) подвержены *инверсным неисправностям* на выходах. *Инверсные неисправности на выходах операторов* характеризуются тем, что в исправном состоянии вычислительный оператор реализует приписанную ему булеву функцию φ, а в неисправном — функцию $\bar{\varphi}$.

Считаем, что программа с ненадежными операторами реализует булеву функцию $f(\mathbf{x})$ ($\mathbf{x} = (x_1,\ x_2,\ \ldots,\ x_n)$), если при отсутствии неисправностей во всех ее операторах на каждом входном наборе $\mathbf{a} = (a_1,\ a_2,\ \ldots,\ a_n)$) значение выходной переменной z равно $f(\mathbf{a})$.

Ненадежностью $N_\varepsilon(Pr)$ программы Pr назовем максимальную вероятность ошибки на выходе программы Pr при всевозможных входных наборах. *Надежность* программы Pr равна $1 - N_\varepsilon(Pr)$. Обозначим $N_\varepsilon(f) = \inf N_\varepsilon(Pr)$, где инфимум берется по всем программам Pr, реализующим булеву функцию f. Программа Pr, реализующая функцию f, называется *асимптотически оптимальной по надежности*, если $N_\varepsilon(Pr) \sim N_\varepsilon(f)$ при $\varepsilon \to 0$, т. е. $\lim\limits_{\varepsilon\to 0} \frac{N_\varepsilon(f)}{N_\varepsilon(Pr)} = 1$.

Временем работы $T(Pr,\ \mathbf{a})$ неветвящейся программы Pr на входном наборе $\mathbf{a}$ назовем число команд программы, выполненных до остановки.

Величину $T(Pr) = (\sum T(Pr,\ \mathbf{a}))/2^n$, где суммирование производится по всем двоичным наборам $\mathbf{a}$ длины n, назовем *средним временем работы* программы Pr.

Величину $T(f) = \min T(Pr)$, где минимум берется по всем неветвящимся программам, вычисляющим f, назовем *средним временем вычисления* (*средней сложностью*) функции f.

Программу Pr, вычисляющую функцию f, назовем *минимальной* программой, если для нее справедливо равенство $T(Pr) = T(f)$.

Обозначим через $Subst(h)$ множество всех функций, зависящих от n переменных $x_1, x_2, ..., x_n$ $(n \geq 3)$ и полученных из функции h всевозможными подстановками переменных (т. е. заменой и/или отождествлением переменных).

Обозначим $A_0(n) = \{x_1, \ ..., \ x_n\}$, $A_r(n) = Subst(f_r(x_1, \ ..., \ x_{2r+1}))$, где $f_r(x_1, \ ..., \ x_{2r+1}) = x_1x_2 \vee \bar{x}_1x_3x_4 \vee \bar{x}_1\bar{x}_3x_5x_6 \vee ... \vee \bar{x}_1\bar{x}_3...\bar{x}_{2r-3}x_{2r-1}$ $x_{2r} \vee \bar{x}_1\bar{x}_3...\bar{x}_{2r-3}\bar{x}_{2r-1}x_{2r+1}$ $(r \geq 1, \ x_i \in \{x_1, \ ..., \ x_n\}$ при всех $i \in \mathbf{N})$.

Обозначим $A(n) = \bigcup\limits_{k=0}^{\infty} A_k(n)$.

Пусть $K(n)$ – множество всех неконстантных булевых функций, зависящих от переменных $x_1, x_2, \ \ldots, \ x_n$ $(n \geq 3)$, не принадлежащих множеству $A(n)$. Обозначим $K = \bigcup\limits_{n=3}^{\infty} K(n)$.

Замечание. *Мощность множества $A(n)$ удовлетворяет неравенству*

$$|A(n)| \leq n^{2n-1}.$$

Поэтому $\frac{|A(n)|}{2^{2^n}} \to 0$ при $n \to \infty$. Следовательно, $\frac{|K(n)|}{2^{2^n}} \to 1$, а множество K содержит почти все булевы функции.

Теорема 1 [2]. *В любом полном конечном базисе для любой булевой функции f существует такая неветвящаяся программа Pr_f с абсолютно надежными операторами условной остановки, реализующая f, для которой*

$$N_\varepsilon(Pr_f) \leq \varepsilon + 4\varepsilon^2,$$

и для любой булевой функции $f \in K$

$$N_\varepsilon(f) \geq \varepsilon - c_1\varepsilon^2$$

при всех $\varepsilon \in (0, 1/960]$, где c_1 — некоторая положительная константа.

Теорема 2 [2]. *Для произвольного полного конечного базиса B, любого действительного числа $\tau > 0$ существует константа $\varepsilon_1 \in (0, 1/2)$, такая, что при любом $n \geq 3$ всякую булеву функцию $f \in K(n)$ можно реализовать программой Pr_f с абсолютно надежными*

операторами условной остановки, для которой при всех $\varepsilon \in (0, \varepsilon_1]$

$$N_\varepsilon(Pr_f) - N_\varepsilon(f) \le c_2\varepsilon^2,$$

и

$$T(Pr_f) \lesssim 3(1+\tau)\rho 2^n/n$$

при $n \to \infty$, *где* c_2 — *некоторая положительная константа.*

Из теорем 1 и 2 следует, что в произвольном полном конечном базисе любую булеву функцию $f \in K$ можно реализовать асимптотически оптимальной по надежности неветвящейся программой Pr_f, ненадежность которой $N_\varepsilon(Pr_f) \sim \varepsilon$ при $\varepsilon \to 0$. Среднее время работы таких программ для почти всех функций асимптотически не больше чем в $9(1+\tau)$ раз превышает среднее время работы минимальных программ, построенных из абсолютно надежных операторов, если $B \subseteq B_2$, и асимптотически не больше чем в $6(1+\tau)$ раз — во всех остальных базисах (τ — любое сколь угодно малое положительное число).

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (номер проекта 11-01-00212а).

Список литературы

1. Чашкин А. В. О среднем времени вычисления значений булевых функций // Дискретный анализ и исследование операций. — 1997. — Т. 4, № 1. — С. 3–17.

2. Грабовская С. М. Асимптотически оптимальные по надежности неветвящиеся программы с оператором условной остановки // Дис. ... канд. физ.-мат. наук. — Пенза : ИИЦ ПГУ, 2012.

О СЛОЖНОСТИ ПРЕДСТАВЛЕНИЯ АЛГЕБРАИЧЕСКОГО ЧИСЛА ПЕРИОДИЧЕСКОЙ ВЕТВЯЩЕЙСЯ ДРОБЬЮ С НАТУРАЛЬНЫМИ ЭЛЕМЕНТАМИ

Д. В. Грибанов (Нижний Новгород)

Следуя [1], будем $T^{(1)}$ называть периодической ветвящейся дробью с натуральными элементами(везде далее ПВЦД) если:

$$\left\{\begin{array}{lcl} T^{(1)} & = & \frac{a^{(1)}}{c_0^1 \ + \ \sum_{i=1}^{d} c_i^{(1)} T^{(i)}} \\ & \cdots & \\ T^{(k)} & = & \frac{a^{(k)}}{c_0^k \ + \ \sum_{i=1}^{d} c_i^{(k)} T^{(i)}} \\ & \cdots & \\ T^{(d)} & = & \frac{a^{(d)}}{c_0^k \ + \ \sum_{i=1}^{d} c_i^{(d)} T^{(i)}} \end{array}\right. , \qquad (1)$$

$$\text{где } c_i^{(k)} \in \mathbb{R}^+, \ a^{(k)} \in \mathbb{R}^+, \ a^{(k)} > 0, \ c_0^{(k)} > 0, \ \text{для } i,k \in \{1,2,...,d\}. \qquad (2)$$

Таким образом при $k \in \{2,...,d\}$ $T^{(k)}$ тоже является ПВЦД.

$T_s^{(k)}$ будем называть s-й подходящей дробью для $T^{(k)}$, если

$$T_s^{(k)} \ = \ \frac{a^{(k)}}{c_0^k \ + \ \sum_{i=1}^{d} c_i^{(k)} T_{s-1}^{(i)}}, \ \text{где } T_1^{(k)} \ = \ \frac{a^{(k)}}{c_0^{(k)}}.$$

Будем говорить, что ПВЦД $T^{(k)}$ сходится и представляет число $\gamma^{(k)}$, если существует предел последовательности чисел $T_s^{(k)}$, и $\gamma^{(k)} \ = \ \lim_{s\to\infty} T_s^{(k)}$.

В [1] доказана сходимость $T^{(k)}$ при условиях (2).

Пусть $a_i \in \mathbb{R}^+$, для $i \in \{0,1,...,d+1\}$, $a_{d+1} > 0$, $a_1 > 0$, $a_0 > 0$ и алгебраическое число γ является корнем многочлена $a_{d+1}x^{d+1} + a_d x^d + ... + a_1 x = a_0$ (в [1] показано, что для любого алгебраического числа γ существует такой многочлен).

Положим $\alpha_{max} = \max_{i\in\{1,2,...,d+1\}}\{a_i\}$, $\alpha_{min} = \min_{i\in\{1,2,...,d+1\}}\{a_i\}$. Также положим $\eta_{max} = a_0 + \alpha_{max}$, $\eta_{min} = a_0 + \alpha_{min}$.

Алгоритм построения ПВЦД (1) для алгебраического числа γ был предложен Закировым в работе [1], сложность алгоритма не оценивалась. Обозначим его А1. Здесь построена целочисленная модификация алгоритма А1 и оценена сложность иэтой модификации. Назовем модификацию алгоритмом А2.

Теорема 1. *А2 строит ПВЦД* (1), *что* $T^{(k)} = \lim_{s\to\infty} T_s^{(k)} = \gamma^k$. *Пусть* m *— число ненулевых коэффициентов многочлена представляющего* γ. *Тогда алгоритм затрачивает* $d^2 + 3md + O(d) + O(m)$ *умножений,* $2md + O(d) + O(m)$ *сложений натуральных чисел. Числа, возникающие в процессе вычислений не превышают* $\alpha_{max}^2(\alpha_{max} + a_0)^d$.

Получив представление алгебраического числа γ в виде (1), будем приближать γ^k дробями $T_s^{(k)}$. В этом процессе параллельно будут приближаться все степени γ^k от 1 до d.

Теорема 2. *Положим* $\xi = C_1 a_0^{d-1}\eta_{min}^{d-1}(1 - min\{1,\ C_2\frac{1}{\eta_{min}^{d-1}} + \frac{1}{C_1}\frac{1}{a_0^{d-1}\eta_{min}^{d-1}}\})^2$. *Тогда* $|T_{s+1}^{(k)} - T_s^{(k)}| \le C_0(\frac{1}{1+\xi})^s$, *для* $d \ge 2$, *где* $C_0 = \frac{(\sqrt{5}+1)^3}{8}a_0^{k+d}\alpha_{max}^2\eta_{max}^{d-1}$, $C_1 = \alpha_{max}^2$, $C_2 = \frac{a_0\alpha_{max}}{\alpha_{min}^2}$.

Таким образом для приближения алгебраического числа с точностью ε нужно не более $\log_{1+\xi}(\frac{C_1}{\varepsilon})$ итераций.

Дополнительными результатами являются теоремы, описывающие свойства ПВЦД. Будем рассматривать ПВЦД (1) и её коэффициенты (2).

$$\text{Положим } Q_s^{(k)} = \frac{a^{(k)}}{T_s^{(k)}},\ \text{тогда } Q_s^{(k)} = c_0^{(k)} + \sum_{i=1}^{d}\frac{c_i^{(k)}a^{(i)}}{Q_{s-1}^{(i)}}.$$

Теорема 3. *Пусть* $m > n$, *а* $i_0 = k$, *тогда*

$$|T_m^{(i_0)} - T_n^{(i_0)}| = (-1)^n\frac{a^{(i_0)}}{Q_m^{(i_0)}Q_n^{(i_0)}}\sum_{i_1=1}^{d}\frac{c_{i_1}^{(i_0)}a^{(i_1)}}{Q_{m-1}^{(i_1)}Q_{n-1}^{(i_1)}}(\sum_{i_2=1}^{d}\frac{c_{i_2}^{(i_1)}a^{(i_2)}}{Q_{m-2}^{(i_2)}Q_{n-2}^{(i_2)}}\cdots$$
$$(\sum_{i_{n-1}}^{d}\frac{c_{i_{n-1}}^{(i_{n-2})}a^{(i_{n-1})}}{Q_{m-n+1}^{(i_{n-1})}Q_1^{i_{n-1}}}(\sum_{i_n=1}^{d}\frac{c_{i_n}^{(i_{n-1})}a^{(i_n)}}{Q_{m-n}^{(i_n)}}))).$$

Теорема 3 является частным случаем формулы из [3].

Следствие.

$$|T_{n+1}^{(i_0)} - T_n^{(i_0)}| = (-1)^n\frac{a^{(i_0)}}{Q_{n+1}^{(i_0)}Q_n^{(i_0)}}\sum_{i_1=1}^{d}\frac{c_{i_1}^{(i_0)}a^{(i_1)}}{Q_n^{(i_1)}Q_{n-1}^{(i_1)}}(\sum_{i_2=1}^{d}\frac{c_{i_2}^{(i_1)}a^{(i_2)}}{Q_{n-1}^{(i_2)}Q_{n-2}^{(i_2)}}\cdots$$
$$(\sum_{i_{n-1}}^{d}\frac{c_{i_{n-1}}^{(i_{n-2})}a^{(i_{n-1})}}{Q_2^{(i_{n-1})}Q_1^{i_{n-1}}}(\sum_{i_n=1}^{d}\frac{c_{i_n}^{(i_{n-1})}a^{(i_n)}}{Q_1^{(i_n)}}))).$$

Положим:

$$\beta^{(k)} = \sum_{i=1}^{d}a^{(i)}c_i^{(k)},$$
$$\beta_{min} = \min_{k\in\{1,2,\ldots,d\}}\{\beta^{(k)}\},\ \beta_{max} = \max_{k\in\{1,2,\ldots,d\}}\{\beta^{(k)}\},$$
$$\Delta_\beta = \beta_{max} - \beta_{min}.$$

Теорема 4. *Справедливо неравенство*

$$|T_{n+1}^{(k)} - T_n^{(k)}| \le \widetilde{C_1}(\frac{\beta_{max}}{\beta_{max} + (\Delta_\beta - 1)\frac{(\Delta_\beta - 1) + \sqrt{(\Delta_\beta - 1)^2 + 4\beta_{max}}}{2}})^n.$$

Оценки достигаются при $\Delta_\beta = 0$.

Пример 1. Приведем пример нетривиальной ПВЦД (1), чьи оценки из теоремы 4 достигаются:

$$\begin{cases} T^{(1)} & = & \frac{2}{1+3T^{(1)}+T^{(2)}} \\ T^{(2)} & = & \frac{4}{1+T^{(1)}+2T^{(2)}} \end{cases} .$$

Здесь $\beta^{(1)} = \beta^{(2)} = 10$.

Пример 2. Приведем пример представления $\gamma = 2^{1/3} - 1$ в виде ПВЦД. $f(x) = x^3 + 3x^2 + 3x - 1,\ f(\gamma) = 0$.

$$\begin{cases} T^{(1)} & = & \frac{1}{T^{(2)}+3T^{(1)}+3} \\ T^{(2)} & = & \frac{1}{3T^{(2)}+9T^{(1)}+12} \end{cases} ,$$

$$|T^{(1)}_{n+1} - T^{(1)}_n| \leq 3(\frac{1}{16})^n.$$

Автор выражает благодарность Валерию Николаевичу Шевченко за постановку задачи и неоценимую помощь в работе.

Список литературы

1. Закиров Н. Р. О представлении произвольного алгебраического числа периодической ветвящейся дробью // Математические вопросы кибернетики. Вып. 15. — М.: Физматлит, 2006. — С. 65–78.

2. Марченков С. С. Конечные автоматы и периодические разложения действительных чисел // Математические вопросы кибернетики. Вып. 6. — М.: Наука, 1999. — С. 304–311.

3. Скоробогатько В. Я. Теория ветвящихся цепных дробей и её применения в вычислительной математике. — М.: Наука, 1983.

ОБ ОДНОВРЕМЕННОЙ МИНИМИЗАЦИИ СЛОЖНОСТИ И МОЩНОСТИ КЛЕТОЧНЫХ СХЕМ, РЕАЛИЗУЮЩИХ НЕКОТОРЫЕ СИСТЕМЫ ФУНКЦИЙ

Ю. В. Гусева (Москва)

В настоящем сообщении рассматриваются схемы из функциональных элементов специального вида — плоские клеточные схемы. Понятие схемы из клеточных элементов было введено в работе

С. С. Кравцова [1]. Элементы таких схем имеют форму единичного квадрата и могут быть повернуты на угол, кратный $\pi/2$. Функциональные элементы реализуют булевы функции, а коммутационные осуществляют соединение функциональных. В данной работе рассматриваются функциональные элементы базиса $\{\vee, \&, -\}$.

Прямоугольник, составленный из клеточных элементов, будем называть *схемой*, если при замене клеточных функциональных элементов на обычные функциональные элементы и при соединении их, определяемом коммутационными элементами, получим обычную схему из функциональных элементов.

Будем рассматривать две меры сложности плоских схем: собственно *сложность* схемы, т.е. общее количество элементов, участвующих в ее построении (площадь схемы), и *мощность (активность)* схемы, одну из естественных мер сложности, соответствующую количеству элементов схемы, хотя бы один из выходов которых принимает значение 1.

Первые оценки сложности были получены, по-видимому, в работах С. С. Кравцова [1], Н. А. Шкаликовой [2] и А. А. Альбрехта [3].

Впервые понятие мощности схем из функциональных элементов рассматривалась М. Н. Вайнцвайгом [4]. В его работе и, позднее, в работе О. М. Касим-Заде [5] исследовалось поведение функции Шеннона мощности схем из функциональных элементов, отвечающей различным конечным базисам.

Для произвольной клеточной схемы S обозначим за $L(S)$ сложность этой схемы. *Сложностью системы булевых функций* A будем называть величину $L(A) = \min L(S)$, где минимум берется по всем клеточным схемам S, реализующим A.

Н. А. Шкаликовой [2] установлен порядок роста сложности клеточных схем, реализующих некоторые системы функций, в том числе следующие:

1. $U(n)$ — система всех булевых функций от n переменных: $L(U(n)) \asymp n \cdot 2^{2^n}$ при $n \to \infty$.

2. $B(n)$ — система всех симметрических функций от n переменных: $L(B(n)) \asymp n \log_2 n$ при $n \to \infty$.

В работе О. В. Черемисина [6] впервые рассматривался вопрос об одновременной минимизации сложности и мощности плоских клеточных схем для заданной системы функций. Для системы всех элементаных конъюнкций доказана невозможность одновременного достижения минимального порядка роста сложности и мощности.

Дадим точные определения, касающиеся мощности плоских схем из функциональных элементов.

Пусть S — произвольная плоская клеточная схема, имеющая n полюсов (входов). *Мощность (активность) схемы* S на наборе $\tilde{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ — это количество элементов схемы, принимающих значение 1 при подаче набора $\tilde{\alpha}$ на входы схемы (обозначение $E_{\tilde{\alpha}}(S)$).

Максимальной активностью схемы S назовем величину $E_{\max}(S) = \max_{\tilde{\alpha}} E_{\tilde{\alpha}}(S)$, где максимум берется по всем наборам $\tilde{\alpha}$ длины n, где n — число входов схемы. *Средней активностью схемы* S назовем величину $E_{cp}(S) = \frac{1}{2^n} \sum_{\tilde{\alpha}} E_{\tilde{\alpha}}(S)$, где суммирование ведется по всем наборам $\tilde{\alpha}$ длины n.

Максимальной (средней) активностью системы булевых функций M будем называть соответственно величины:

$$E_{max}(M) = \min_{\mathrm{S}} E_{max}(S),\ E_{cp}(M) = \min_{\mathrm{S}} E_{cp}(S),$$

где минимумы берутся по всем клеточным схемам S, реализующим систему M.

Выделим одну из содержательных интерпретаций мощности схемы — тепловую. При этой интерпретации считается, что каждый элемент выделяет тепло, если хотя бы один из его выходов принимает значение 1. Таким образом $E_{\tilde{\alpha}}(S)$, мощность схемы на наборе $\tilde{\alpha}$, интерпретируется как количество тепла, выделяемое всей схемой при данном входном наборе.

Теорема 1. *Для любого n существует клеточная схема W_n, реализующая систему $U(n)$, такая что $E_{cp}(W_n) \asymp E_{max}(W_n) \asymp 2^{2^n}$ при $n \to \infty$.*

Эти схемы являются минимальными по порядку роста мощности для данной системы в классе клеточных схем: с учетом теоремы 1 нетрудно показать, что $E_{cp}(U(n)) \asymp E_{max}(U(n)) \asymp 2^{2^n}$ при $n \to \infty$.

Теорема 2. *Для любой последовательности схем P_n, реализующих системы $U(n)$ с минимальной по порядку роста сложностью, то есть таких, что $L(P_n) \asymp n \cdot 2^{2^n}$, выполняются соотношения: $E_{max}(P_n) \succeq n \cdot 2^{2^n}$, $E_{cp}(P_n) \succeq n \cdot 2^{2^n}$, при $n \to \infty$.*

Это утверждение показывает, что одновременная минимизация порядков роста сложности и мощности для данных систем невозможна.

Теорема 3. *Для любой последовательности схем Q_n, реализующих системы $B(n)$ с минимальной по порядку роста сложностью, то есть таких, что $L(Q_n) \asymp n \log_2 n$, верно $E_{max}(Q_n) \succcurlyeq n \log_2 n$, $E_{cp}(Q_n) \succcurlyeq n \log_2 n$, при $n \to \infty$.*

Таким образом, невозможно построить последовательность схем, минимальных по порядку роста сложности, имеющих порядок роста мощности меньший, чем у схем из из работы [2].

Можно показать, что $E_{cp}(B(n)) \succcurlyeq n, E_{max}(B(n)) \succcurlyeq n$ при $n \to \infty$.

Список литературы

1. Кравцов С. С. О реализации функции алгебры логики в одном классе схем из функциональных и коммутационных элементов // Проблемы кибернетики. Вып. 19. — М.: Наука, 1967. — С. 285–293.

2. Шкаликова Н. А. О реализации булевых функций схемами из клеточных элементов // Математические вопросы кибернетики. Вып. 2. — М.: Наука, 1989. — С. 177–197.

3. Альбрехт А. А. О схемах из клеточных элементов // Проблемы кибернетики. Вып. 33. — М.: Наука, 1978. — С. 285–293.

4. Вайнцвайг М. Н. О мощности схем из функциональных элементов // Доклады АН СССР, 1961. — Т. 139, № 2. — С. 320–323.

5. Касим-Заде О. М. Об одной мере сложности схем из функциональных элементов // Проблемы кибернетики. Вып. 38. — М.: Наука, 1981. — С. 117–179.

6. Черемисин О. В. Об активности схем из клеточных элементов, реализующих систему всех конъюнкции // Дискретная математика. — 2003. — Т. 15, вып. 2. — С. 113–122.

ОБ ЭКВИВАЛЕНТНОСТИ ПОТОКОВЫХ ПРОГРАММ

В. А. Захаров (Москва)

Необходимость проектирования потоковых алгоритмов возникает при решении многих прикладных оптимизационных задач, к числу которых относятся задача загрузки кеш-памяти, задача о назначении, задача упаковки и др. В статье [1] в качестве математической модели потоковых алгоритмов была предложена модификация конечных автоматов-преобразователей; для этой модели был исследован ряд алгоритмических задач, включая проблему эквивалентности, и установлены их оценки сложности. Однако и в этой,

и во всех ранее рассмотренных математических моделях потоковых алгоритмов не предусмотрена возможность учета семантических свойств выполняемых операций. Поэтому с их помощью нельзя проводить подробный анализ поведения потоковых алгоритмов (например, проверять их правильность и проводить оптимизацию). Нами предлагается более общая математическая модель потоковых программ, пригодная для описания и анализа поведения потоковых алгоритмов.

Пусть заданы два конечных множества $\mathcal{A}$ *операторов* и $\mathcal{C}$ *событий. Потоковые программы*, работающие в оперативном режиме, могут быть описаны системой переходов $\pi = \langle V, \mathbf{start}, V_{out}, T\rangle$, состоящей из множества *точек программы* V, *точки входа* **start**, множества *точек выхода* V_{out} и *функции переходов* $T : V \times \mathcal{C} \to V \times \mathcal{A}^*$, определяющей реакцию программы на каждое событие в каждой точке программы. Интерпретация операторов задается полугруппой $\mathcal{F} = (S, \circ, e)$ с множеством образующих $\mathcal{A}$. Элементы полугруппы играют роль состояний данных, а нейтральный элемент e является начальным состоянием данных. Конечная последовательность операторов h, $h \in \mathcal{A}^*$, вычисляет элемент полугруппы $[h]_S$, который является результатом применения операторов цепочки h к начальному состоянию данных. *Поток событий* представляет собой конечную последовательность событий $\alpha = \Delta_0, \Delta_1, \ldots, \Delta_N$. Для заданного потока событий α потоковая программа π осуществляет вычисление, переходя из одних точек программы в другие и выполняя приписанные этим переходам последовательности операторов. При достижении точки выхода программа выдает в качестве результата вычисленное состояние данных, которое расценивается как реакция программы на поток событий α.

Для заданного потока событий $\alpha = \Delta_0, \Delta_1, \ldots, \Delta_N$ *вычислением* потоковой программы π называется последовательность пар $\pi(\alpha) = (v_0, s_0), (v_1, s_1), \ldots, (v_N, s_N),$, удовлетворяющая следующим двум требованиям:

1) $v_0 = \mathbf{start}$, $s_0 = e$,

2) для любого i, $1 \le i, \le N$, если $T(v_{i-1}, \Delta_i) = (u, h)$, то $v_i = u$, $s_i = s_{i-1} \circ [h]_S$.

Если $v_N \in V_{out}$, то состояние данных s_N считается *результатом вычисления* $\pi(\alpha)$ и обозначается $[\pi(\alpha)]_S$. Если $v_N \notin V_{out}$, то вычисление считается безрезультатным.

Две потоковые программы π_1 и π_2 называются *эквивалентными на полугруппе* операторов S (обозначается $\pi_1 \sim_S \pi_2$), если для любого потока событий α выполняется равенство $[\pi_1(\alpha)]_S = [\pi_1(\alpha)]_S$.

Теорема. Предположим, что полугруппа S вложима в группу G,

в которой проблема равенства слов разрешима за время $t(n)$, где n — длина слов. Тогда проблема эквивалентности потоковых программ $\pi_1 \sim_S \pi_2$ на полугруппе S разрешима за время $O(n^2 t(n^2))$, где n — суммарный размер программ π_1 и π_2.

Доказательство. Воспользуемся методом совместных вычислений для решения проблемы эквивалентности программ, предложенным в статье [2]. Не ограничивая общности, будем полагать, что в каждой из программ π_1 и π_2 из любой ее точки достижима хотя бы одна из точек выхода.

Для каждой операторной цепочки h, $h \in \mathcal{A}^*$, обозначим записью $[h]_S^{-1}$ элемент группы G, который является обратным для элемента полугруппы $[h]_S$.

Для проверки эквивалентности пары потоковых программ $\pi_i = \langle V_i, \mathbf{start}_i, V_{out,i}, T_i \rangle$, $i = 1,2$, рассмотрим граф совместных вычислений $\Gamma(\pi_1, \pi_2)$. Вершинами графа являются всевозможные тройки вида (v', v'', g), где v', v'' — точки в программах π_1 и π_2 соответственно, а g — элемент группы G. Для любого события Δ, $\Delta \in \mathcal{C}$, из каждой вершины (v', v'', g) графа $\Gamma(\pi_1, \pi_2)$ исходит дуга с пометкой Δ, ведущая в такую вершину $(u', u'', \widehat{g})$, для которой выполняются равенства $T_1(v', \Delta) = (u', h')$, $T_2(v'', \Delta) = (u'', h'')$, $\widehat{g} = [h'']_S^{-1} \circ g \circ [h']_S$. Вершину $(\mathbf{start}_1, \mathbf{start}_2, e)$ назовем *начальной вершиной* графа. *Опровергающими вершинами* назовем тройки (v', v'', g), удовлетворяющие одному из следующих трех требований: 1) $v' \in V_{out,1}$, $v'' \notin V_{out,2}$, 2) $v' \notin V_{out,1}$, $v'' \in V_{out,2}$, 3) $v' \in V_{out,1}$, $v'' \in V_{out,2}$, $g \neq e$.

Для определенного таким образом графа совместных вычислений $\Gamma(\pi_1, \pi_2)$ справедливы следующие три леммы, непосредственным следствием которых и является сформулированная выше теорема.

Лемма 1. Для любого потока событий $\alpha = \Delta_0, \Delta_1, \ldots, \Delta_N$ в графе $\Gamma(\pi_1, \pi_2)$ из начальной вершины ведет маршрут

$$(\mathbf{start}_1, \mathbf{start}_1, e) \xrightarrow{\Delta_1} (v'_1, v''_1, g_1) \xrightarrow{\Delta_2} \cdots \xrightarrow{\Delta_N} (v'_N, v''_N, \Delta_N)$$

тогда и только тогда, когда

$$\begin{aligned} \pi_1(\alpha) &= (\mathbf{start}_1, e), (v'_1, s'_1), \ldots, (v'_N, s'_N), \\ \pi_2(\alpha) &= (\mathbf{start}_2, e), (v''_1, s''_1), \ldots, (v''_N, s''_N), \end{aligned}$$

и при этом для любого i, $1 \leq i \leq N$, верно равенство $g_i = (s''_i)^{-1} \circ s'_i$.

Лемма 2. Потоковые программы π_1 и π_2 эквивалентны на полугруппе S тогда и только тогда, когда ни одна опровергающая

вершина графа совместных вычислений $\Gamma(\pi_1, \pi_2)$ не достижима из начальной вершины.

Лемма 3. Если из начальной вершины графа совместных вычислений $\Gamma(\pi_1, \pi_2)$ достижимы две вершины (u, v, g_1) и (u, v, g_2) и при этом $g_1 \neq g_2$, то хотя бы одна опровергающая вершина также достижима из начальной вершины графа $\Gamma(\pi_1, \pi_2)$.

Работа выполнена при финансовой поддержке гранта РФФИ (проект 12-01-00706).

Список литературы

1. Alur R., Deshmukh J.V. Nondeterministic streaming string transducers // Lecture Notes in Computer Science. — 2011. — V. 6756. — P. 1–20.

2. Захаров В. А. Быстрые алгоритмы разрешения эквивалентности операторных программ на уравновешенных шкалах // Математические вопросы кибернетики. Вып. 7. — М.: Физматлит, 1998. — С. 303–324.

О СРЕДНЕМ ВРЕМЕНИ ПРЕБЫВАНИЯ ТРЕБОВАНИЙ ПРИ ЦИКЛИЧЕСКОМ УПРАВЛЕНИИ С ФИКСИРОВАННЫМ РИТМОМ

А. В. Зорин (Н. Новгород)

Рассматривается управляющая система массового обслуживания $m < \infty$ конфликтных стационарных потоков Π_1, Π_2, ..., Π_m по циклическому алгоритму с фиксированным ритмом [1]. Конфликтность потоков означает, что запрещено обслуживать в один отрезок времени требования разных потоков. Требования по потоку Π_j, $j = \overline{1, m}$, поступают группами в накопитель O_j неограниченного объема, причем поток групп пуассоновский с параметром $\lambda_j > 0$, а размер группы — случайная величина, принимающая значение b с вероятностью $p_b^{(j)}$, $b = 1, 2, \ldots$. Обслуживающее устройство имеет $2m$ состояний $\Gamma^{(j)}$, $j = \overline{1, 2m}$. В состоянии $\Gamma^{(2j-1)}$ обслуживаются только требования потока Π_j. В состоянии $\Gamma^{(2j)}$ требования не обслуживаются. При циклическом алгоритме после состояния $\Gamma^{(r)}$, $r < 2m$,

прибор переходит в состояние $\Gamma^{(r+1)}$. После состояния $\Gamma^{(2m)}$ следует состояние $\Gamma^{(1)}$. Длительность пребывания прибора в состоянии $\Gamma^{(r)}$ неслучайна и равна T_r. Всякий промежуток времени длительностью $T = T_1 + T_2 + \ldots + T_{2m}$, начинающийся в момент смены состояния прибора, будем называть *циклом обслуживания*. Предположим, что длительность обслуживания требования из очереди O_j неслучайна и равна μ_j^{-1}, так что при состоянии прибора $\Gamma^{(2j-1)}$ за время T_{2j-1} обслуживаются не больше $\ell_j = [\mu_j T_j]$ требований потока O_j.

Обозначим $\tau_{j,i}$ момент окончания i-го промежутка обслуживания требований очереди O_j, так что $\tau_{m,i-1} < \tau_{1,i} < \tau_{2,i} < \ldots < \tau_{m,i}$ для всех $i \geq i_0$. Пусть $\kappa_{j,i}$ — число требований в очереди O_j в момент $\tau_{j,i}$, $\zeta_{j,i}$ — полное время пребывания всех требований в очереди O_j за цикл $(\tau_{j,i}, \tau_{j,i+1}]$. Для оценки качества управления в данной системе обслуживания рассматривается величина $J_i = \mathbf{M}(\zeta_{1,i}+\zeta_{2,i}+\ldots+\zeta_{m,i})$ среднего времени пребывания всех требований в системе за цикл. Будем считать выполненым условие $\lambda_j T \sum\limits_{b=1}^{\infty} b p_b^{(j)} - \ell_j < 0$, $j = \overline{1,m}$, необходимое и достаточное для существования единственного стационарного распределения марковской цепи $\{(\kappa_{1,i}, \kappa_{2,i}, \ldots, \kappa_{m,i}); i = = 0, 1, \ldots\}$. Для $x = 0, 1, \ldots$ обозначим $Q_j(x)$ стационарную вероятность события $\kappa_{j,i} = x$. Введем функции $\varphi_j(x; t) = (\lambda_j t)^x (x!)^{-1} e^{-\lambda_j t}$, $x = 0, 1, \ldots$ с параметром $t > 0$. При $\ell_j = 1$ легко найти, что

$$Q_j(0) = e^{\lambda_j T}\Big(1 - \lambda_j T \sum_{b=1}^{\infty} b p_b^{(j)}\Big).$$

Теорема 1. *Пусть* $\ell_j > 1$, $\beta_j(l)$, $l = 1, 2, \ldots$, *и* $\alpha_j(k,l)$, $k = 0, 1, \ldots, \ell_j - 1$, $l = 1, 2, \ldots$ *удовлетворяют уравнениям* $\beta_j(l) = 0$ *при* $l > \ell_j$,

$$\beta_j(l) = \varphi_j(\ell_j - 1; T) + \sum_{r=1}^{\infty} \varphi_j(\ell_j - 1 + r; T)\alpha_j(l-1, r),\ l = \overline{1, \ell_j};$$

$$\alpha_j(k,l) = \beta_j(k+l) + \sum_{r=1}^{\min\{\ell_j - k, l-1\}} \beta_j(k+r)\alpha(0, l-r),$$

Тогда стационарные вероятности $Q_j(0)$, $Q_i(1)$, $\ldots$, $Q_j(\ell_j - 1)$ *удо-*

влетворяют системе алгебраических уравнений

$$Q_j(x) = \sum_{w=0}^{\ell_j-1} Q_j(w)\Bigg(\sum_{r=1}^{\infty}\varphi_j(2\ell_j + r - 1 - w; T)\alpha_j(\ell_j - 1 - x, r) + \\ + \varphi_j(x + \ell_j - w; T)\Bigg), \quad x = 1, 2, \ldots, \ell_j - 1;$$

$$1 = \sum_{w=0}^{\ell_j-1} Q_j(w)\,(1 - \\ - \frac{\sum\limits_{x=0}^{\infty}\Bigg(\varphi_j(2\ell_j + x - w; T) + \sum\limits_{r=1}^{\infty}\varphi_j(2\ell_j + x + r - w; T)\alpha_j(0, r)\Bigg)}{1 - \sum\limits_{x=0}^{\infty}\Bigg(\varphi_j(\ell_j + x; T) + \sum\limits_{r=1}^{\infty}\varphi_j(\ell_j + x + r; T)\alpha_j(0, r)\Bigg)}\Bigg).$$

Теорема 2. *Пусть величина $\kappa_{j,i}$ имеет стационарное распределение $\{Q_j(x); x = 0, 1, \ldots\}$ и входные потоки ординарные ($p_1^{(j)} = 1$, $j = 1, 2, \ldots, m$). Тогда справедливы соотношения*

$$\mathbf{M}(\zeta_{j,i}) = T\,M_j + \frac{\ell_j(\ell_j+1)}{2\mu_j} + \lambda_j T^2 - \lambda_j T T_{2j-1} - \ell_j T_{2j-1} + \\ + \sum_{x=0}^{\ell_j-1} Q_j(x)\Bigg(\sum_{b=0}^{\ell_j-x-1}\varphi_j(b; T - T_{2j-1})\Big(H\Big(\frac{x+b}{\mu_j}; T_{2j-1} - \frac{x+b}{\mu_j}\Big) + \\ + \frac{(x+b)(x+b+1)}{2\mu_j} - \frac{\ell_j(\ell_j+1)}{2\mu_j} + (\ell_j - x - b)T_{2j-1} - \\ - \frac{\lambda_j}{2}(T - T_{2j-1})^2\Big) - \varphi_j(\ell_j - x; T - T_{2j-1})\Big(\frac{\ell_j(\ell_j+1)}{2\mu_j} - \frac{x(x+1)}{2\mu_j}\Big)\Bigg).$$

где функция $H_j(u,t) = \int\limits_0^{u+t} \lambda e^{-\lambda s}(\max\{u-s, 0\} + \mu_j^{-1} + \frac{1}{2}\lambda_j(u-s+t)^2)\,ds$ *при* $u \geq 0$, $0 \leq t < \mu_j^{-1}$, *а при* $u \geq 0$, $t \geq \mu_j^{-1}$

$$H(u,t) = \int_0^u \lambda_j e^{-\lambda_j s}(u-s+\mu_j^{-1} + H(u-s+\mu_j^{-1}, t-\mu_j^{-1})\,ds +$$

$$+ \int_u^{u+t-\mu_j^{-1}} \lambda_j e^{-\lambda_j s}(\mu_j^{-1} + H(\mu_j^{-1}, t+u-s-\mu_j^{-1})\,ds +$$

$$+ \int_{u-t+\mu_j^{-1}}^{u+t} \lambda_j e^{-\lambda_j s}(\mu_j^{-1} + \frac{1}{2}\lambda_j(t+u-s)^2)\,ds,$$

$$M_j = (2(\ell_j - \lambda_j T))^{-1}\Bigg(\ell_j + \ell_j^2 + \lambda_j^2 T^2 - 2\ell_j\lambda_j T -$$

$$- \sum_{x+b<\ell_j} Q_j(x)\varphi_j(b;T)(x+b-\ell_j)(x+b-\ell_j-1)\Bigg).$$

Работа выполнена по госбюджетной НИР ННГУ по теме «Математическое моделирование и создание новых методов анализа эволюционных системи и систем оптимизации — № Н-040-0» и гранту РФФИ 12-01-90409-Укр_а.

Список литературы

1. Зорин А. В. Кибернетический подход к построению и анализу математической модели тандема двух перекрестков // Сборник докладов XVI Международной конференции «Проблемы теоретической кибернетики». — Н. Новгород: Изд-во Нижегородского госуниверситета им. Н. И. Лобачевского, 2011. — С. 179–183.

ОБ ОЦЕНКАХ ГЛУБИНЫ БУЛЕВЫХ ФУНКЦИЙ ПРИ РЕАЛИЗАЦИИ СХЕМАМИ НАД ПРОИЗВОЛЬНЫМ БЕСКОНЕЧНЫМ БАЗИСОМ

О. М. Касим-Заде (Москва)

Любое функционально полное множество булевых функций, т. е. такое, что суперпозициями функций этого множества можно реализовать любую булеву функцию, будем называть *базисом.* Базис будем называть *конечным,* если число существенных переменных входящих в него функций в совокупности ограничено сверху, и *бесконечным* в противном случае.

Рассмотрим реализацию булевых функций схемами из функциональных элементов над произвольным фиксированным базисом B. Под *глубиной схемы* понимается наибольшее число функциональных элементов, составляющих ориентированную цепь, ведущую от входов схемы к ее выходу. Наименьшая глубина схемы над базисом B, достаточная для реализации булевой функции f, называется *глубиной функции* f над базисом B и обозначается через $D_B(f)$. Базису B ставится в соответствие *функция Шеннона глубины* $D_B(n)$, определяемая соотношением

$$D_B(n) = \max_f D_B(f),$$

где максимум берется по всем булевым функциям f от n переменных. Подробные определения этих и других используемых в работе понятий см. в [1, 2].

Известно [1], что для всякого конечного базиса B асимптотика функции Шеннона глубины при $n \to \infty$ имеет вид $D_B(n) = \alpha n + o(n)$, где $\alpha = (\log_2 m)^{-1}$, m — наибольшее число существенных переменных у функций базиса B.

В работе [3] показано, что для всякого бесконечного базиса B порядок роста функции Шеннона глубины $D_B(n)$ при $n \to \infty$ равен либо 1, либо $\log n$. Этот результат уточнен в [4]. В настоящей работе результаты [3, 4] существенно усилены.

Предпошлем формулировке основных результатов ряд необходимых сведений.

Пусть p — простое число. Обозначим через F_p поле классов вычетов по модулю p, $F_p = \{0, 1, \ldots, p-1\}$. Известно [5] (см. также [3,4,6]), что всякую булеву функцию f можно представить, и притом единственным образом, в виде многочлена

$$f(x_1, \ldots, x_n) = a_0 + \sum_{s=1}^{n} \sum_{1 \le i_1 < \ldots < i_s \le n} a_{i_1 \ldots i_s} x_{i_1} \ldots x_{i_s} \pmod{p}$$

с коэффициентами $a_0, a_{i_1 \ldots i_s} \in F_p$ (булевы значения $0, 1$ естественным образом погружаются в поле F_p, и булева функция f рассматривается как отображение $f\colon \{0,1\}^n \to F_p$). Степень этого многочлена (т. е. наибольшее число s такое, что хотя бы один из коэфициентов $a_{i_1 \ldots i_s} \neq 0$, или ноль, если все эти коэффициенты нулевые) называется *p-степенью функции* f и обозначается через $\deg_p f$.

Пусть A — множество булевых функций. Если среди p-степеней входящих в это множество функций существует наибольшая, то

будем называть ее *p-степенью множества A* и обозначать через $\deg_p A$. Если же множество A содержит функции сколь угодно большой p-степени, то будем говорить, что p-степень этого множества *бесконечна*, и писать символически $\deg_p A = \infty$.

В работе [4] доказано, что для всякого бесконечного базиса B имеет место один из двух случаев: либо $\deg_p B = \infty$ при всех простых p, либо существует единственное простое число p такое, что $\deg_p B < \infty$ и $\deg_q B = \infty$ при всех простых $q \neq p$. В первом случае говорят, что B есть базис *бесконечной характеристики*, во втором — что это базис *конечной характеристики p*. Подробнее об этом см. [3, 4].

Основной результат настоящей работы содержится в следующем утверждении.

Теорема 1. *Для всякого бесконечного базиса B либо существует постоянная β, $1 \leq \beta \leq 6$, такая, что $D_B(n) = \beta$ при всех достаточно больших n, либо выполняются соотношения*

$$\lceil \log_\gamma n \rceil \leq D_B(n) \leq \lceil \log_\gamma n \rceil + 5$$

при всех n, причем последнее имеет место тогда и только тогда, когда B есть базис конечной характеристики p, и тогда $\gamma = \deg_p B$.

Доказательство этого утверждения опирается на следующие утверждения, представляющие самостоятельный интерес.

Теорема 2. *Для всякого базиса B бесконечной характеристики и для всякой нетривиальной (т. е. отличной от селекторной) булевой функции f выполняются соотношения $1 \leq D_B(f) \leq 6$.*

Теорема 3. *Для всякого бесконечного базиса B конечной характеристики p и для всякой булевой функции f, отличной от констант, выполняются соотношения*

$$\lceil \log_\gamma \deg_p f \rceil \leq D_B(f) \leq \lceil \log_\gamma \deg_p f \rceil + 5,$$

где $\gamma = \deg_p B$.

Таким образом, для всех бесконечных базисов получены двусторонние оценки функции Шеннона глубины, различающиеся лишь на небольшую аддитивную постоянную. Более того, для всех бесконечных базисов и всех булевых функций указаны оценки глубины с точностью до небольшой аддитивной постоянной.

Работа выполнена при финансовой поддержке РФФИ (проект № 11-01-00508) и Программы фундаментальных исследований Отделения математических наук РАН «Алгебраические и комбинаторные

методы математической кибернетики и информационные системы нового поколения» (проект «Задачи оптимального синтеза управляющих систем»).

Список литературы

1. Лупанов О. Б. О схемах из функциональных элементов с задержками // Проблемы кибернетики. Вып. 23. — М.: Наука, 1970. — С. 43–81.

2. Savage J. E. The complexity of computing. — New York: Wiley, 1976 (имеется перевод: Сэведж Дж. Э. Сложность вычислений. М.: Факториал, 1998).

3. Касим-Заде О. М. О глубине булевых функций при реализации схемами над произвольным базисом // Вестник Московского университета. Серия 1. Математика. Механика. — 2007. — № 1. — С. 18–21.

4. Касим-Заде О. М. О глубине булевых функций над произвольным бесконечным базисом // Дискретный анализ и исследование операций. Серия 1. — 2007. — Том 14, № 1. — С. 45–69.

5. Smolensky R. Algebraic methods in the theory of lower bounds for Boolean circuit complexity // Proc. 19th Annual ACM Symposium on Theory of Computing. — New York: ACM Press, 1987. — P. 77–82.

6. Boppana R. B., Sipser M. The complexity of finite functions // Handbook of Theoretical Computer Science. Vol. A. Algorithms and complexity / Ed., J. van Leeuwen. — Amsterdam: Elsevier / Cambridge (Massachusetts): The MIT Press, 1990. — P. 757–804.

БИКРИТЕРИАЛЬНЫЕ ЗАДАЧИ ОБСЛУЖИВАНИЯ СТАЦИОНАРНЫХ ОБЪЕКТОВ В ОДНОМЕРНОЙ РАБОЧЕЙ ЗОНЕ ПРОЦЕССОРА

Д. И. Коган (Москва), Ю. С. Федосенко, Н. А. Дуничкина (Нижний Новгород)

Работа посвящена анализу бикритериальных модификаций рассмотренных в [1] задач обслуживания стационарных объектов, рассредоточенных в пределах одномерной рабочей зоны перемещающегося процессора. Необходимость указанного обобщения продиктована требованиями совершенствования управления конкретными типами транспортно-технологических систем, в частности, при

решении задач оперативного планирования снабжением топливом дизель-электрических добывающих комплексов, дислоцированных в крупномасштабном русловом полигоне [2].

Считается заданной группа $O_n = \{o_1, o_2, \ldots, o_n\}$ стационарных объектов, рассредоточенных в рабочей зоне L обслуживающего процессора P. Зона L одномерна, её начальная точка A является базовой для процессора; объекты считаем пронумерованными в порядке возрастания их расстояний от точки A; конечная точка B зоны L является местом расположения объекта o_n. Из точки A, начиная от момента времени $t = 0$, процессор поступательно перемещается к точке B (рейс λ_+), а затем, достигнув её, также поступательно возвращается в точку A (рейс λ_-).

При реализации цикла $\lambda_+\lambda_-$ процессор P выполняет однократное без прерываний обслуживание объектов группы O_n: часть объектов обслуживается в рейсе λ_+, все остальные — в рейсе λ_-. С каждым объектом o_j ассоциируются две монотонно возрастающие в нестрогом смысле функции индивидуального штрафа $\varphi_j(t)$ и $\psi_j(t)$, выражающие зависящие от момента t завершения его обслуживания величины потерь по первому и второму показателям соответственно. Примем обозначения: $1, 2, \ldots, n$ — точки зоны L, в которых расположены объекты $o_1, o_2, \ldots, o_n$ соответственно (точки n и B совпадают); τ_j — продолжительность обслуживания процессором P объекта o_j; $\gamma_{j-1,j}$ и $\gamma_{j,j-1}$ — затраты времени на перемещения процессора между точками $j-1$ и j в рейсах λ_+ и λ_- соответственно ($j = \overline{1,n}$), при этом $\gamma_{0,1}$ и $\gamma_{1,0}$ — затраты времени на перемещение процессора между точкой A и точкой 1 в прямом и обратном рейсах. Все числа τ_j, $\gamma_{j-1,j}$, $\gamma_{j,j-1}$ считаем целыми положительными.

Стратегией обслуживания именуем произвольное подмножество элементов V из совокупности индексов $N = \{1, 2, \ldots, n\}$; объекты o_j, где $j \in V$, в реализации стратегии V обслуживаются процессором в рейсе λ_+, все остальные объекты группы O_n – в рейсе λ_-. Для определенности полагаем, что объект o_n обслуживается при завершении процессором рейса λ_+. Для объекта o_j, $j = \overline{1,n}$, через $t_j^*(V)$ обозначим момент завершения его обслуживания при реализации стратегии V. Рассматриваются бикритериальные задачи

$$\min_{V \subseteq N} \Big(\sum_{j=1}^{n} \varphi_j(t_j^*(V)), \max \psi_j(t_j^*(V))\Big); \qquad (1)$$

$$\min_{V \subseteq N} \left(\sum_{j=1}^{n} \varphi_j(t_j^*(V)), \sum_{j=1}^{n} \psi_j(t_j^*(V)) \right). \qquad (2)$$

Принимается концепция решения, предусматривающая построение для каждой введенной задачи полной совокупности эффективных оценок E с одновременным обеспечением возможности синтеза по любой выбираемой в E оценке порождающей её паретооптимальной стратегии [3].

Конструируются решающие алгоритмы, основанные на построении полных совокупностей эффективных оценок методом динамического программирования в его бикритериальном обобщении [4, 5].

Для задач (1–2) и ряда их конкретизаций доказываются результаты о вычислительной сложности (NP-трудности, полиномиальной разрешимости). Рассматриваются вопросы определения максимального числа эффективных оценок.

Список литературы

1. Коган Д. И., Федосенко Ю. С. Задачи синтеза оптимальных стратегий обслуживания стационарных объектов в одномерной рабочей зоне процессора // Автоматика и телемеханика. — 2010. — № 10. — С. 50–62.

2. Коган Д. И., Федосенко Ю. С., Шлюгаев А. Ю. Задача одностадийного обслуживания добывающих комплексов в крупномасштабной акватории // Труды V Московской международной конференции по исследованию операций (ORM2007). — М.: МАКС Пресс, 2007. — С. 60–62.

3. Подиновский В. В., Ногин В. Д. Парето-оптимальные решения многокритериальных задач. — М.: Физматлит, 2007.

4. Коган Д. И. Динамическое программирование и дискретная многокритериальная оптимизация. — Н. Новгород: Изд-во Нижегородского госуниверситета, 2005.

5. Бугаев Ю. В., Чикунов С. В. Обобщение схемы динамического программирования // Автоматика и телемеханика. — 2009. — № 2. — С. 90–100.

О СЛОЖНОСТИ РЕАЛИЗАЦИИ ЛИНЕЙНЫХ БУЛЕВЫХ ФУНКЦИЙ В ОДНОМ БАЗИСЕ

Ю. А. Комбаров (Москва)

Одними из наиболее изученных с точки зрения их минимальных реализаций являются линейные булевы функции, представляемые в виде $l_n(x_1, \ldots, x_n) = x_1 \oplus \ldots \oplus x_n$ или в виде $\overline{l_n}(x_1, \ldots, x_n) = x_1 \oplus \ldots \oplus x_n \oplus 1$, где "$\oplus$" означает сложение по модулю два [1]. Первый результат в этом направлении был получен в 1952 г. Кардо [2]: для реализации линейной булевой функции (существенно зависящей) от n переменных контактной схемой необходимо и достаточно $4n - 4$ контактов. Сложность реализации линейных функций схемами из функциональных элементов [3] (определяемая обычно как наименьшее возможное число функциональных элементов, достаточное для реализации функции f схемой в заданном базисе и обозначаемая как $L(f)$) известна для многих базисов, состоящих из не более, чем двухвходовых функциональных элементов. Так, в работе [4] показано, что $L(l_n) = L(\overline{l_n}) = 4n - 4$ в базисе $\{x\&y, x \vee y, \overline{x}\}$ и $L(l_n) = L(\overline{l_n}) = 7n - 7$ в базисах $\{x\&y, \overline{x}\}$ и $\{x \vee y, \overline{x}\}$, а в работе [5] показано, что $L(l_n) = L(\overline{l_n}) = 3n - 3$ в базисе $\{x \to y, \overline{x}\&y\}$. Для некоторых базисов известны очень точные оценки для сложности реализации линейных функций, например, в работе [6] доказано, что $L(l_n) = 4n - 4$ и $4n - 4 \leq L(\overline{l_n}) \leq 4n - 3$ в базисе $\{\overline{x\&y}\}$, а в работе [7] доказано, что $L(l_n) = 4n - 4$ и $4n - 4 \leq L(\overline{l_n}) \leq 4n - 3$ в базисе $\{x \to y, \overline{x}\}$. Для некоторых базисов есть описание устройства минимальных схем. Например, в работе [5] показано, что все минимальные схемы, реализующие линейные функции в базисе $\{x \to y, \overline{x}\&y\}$ имеют определенную блочную структуру, а в работе [8] аналогичный результат доказан для минимальных схем, реализующих линейные функции в базисе $\{x\&y, x \vee y, \overline{x}\}$.

В настоящей работе устанавливается точное значение сложности функции $\overline{l_n}$ в базисе B, состоящем из единственного функционального элемента — штриха Шеффера, а также описывается структура всех минимальных схем, реализующих функцию l_n в том же базисе.

Для схемы S в базисе B через $L(S)$ обозначается количество функциональных элементов в S; число $L(S)$ называется *сложностью* схемы S. *Сложностью реализации* произвольной булевой функции f в базисе B называется число $\min L(S)$, где минимум берется по всем схемам S, реализующим функцию f в базисе B. Сложность реализации функции f в базисе B будем обозначать через $L(f)$.

Стандартным блоком будем называть схему с двумя входами, состоящую из четырех элементов E_1, E_2, E_3 и E_4, такую, что первый вход схемы соединен со входами элементов E_1 и E_2, второй вход схемы соединен со входами элементов E_1 и E_3, выход элемента E_1 соединен со входами элементов E_2 и E_3, а выходы элементов E_2 и E_3 соединены со входами элемента E_4. Элемент E_4 будем называть *выходным элементом* стандартного блока. Отметим, что на выходе выходного элемента стандартного блока реализуется сумма по модулю два функций, поданных на его входы. Будем говорить, что стандартный блок входит в некоторую схему S *правильно*, если выходы всех элементов этого блока, кроме выходных, не подаются на входы элементов, не принадлежащих блоку, а входы блока соединены с выходом некоторого элемента схемы S или с некоторым входом схемы S.

Основными результатами работы являются следующие теоремы.

Теорема 1. *Всякая минимальная схема в базисе B, реализующая линейную функцию $l_n = x_1 \oplus \ldots \oplus x_n$, состоит из $n-1$ стандартных блоков, каждый из которых входит в схему правильно.*

В следующей теореме устанавливается точное значение сложности функции $\overline{l_n}$ в базисе B.

Теорема 2. *При любом натуральном n сложность реализации линейной функции $\overline{l_n} = x_1 \oplus \ldots \oplus x_n \oplus 1$, $n \geq 2$, в базисе B составляет $4n-3$.*

Из теорем 1 и 2, а также из результатов работы [6], пользуясь соображениями двойственности, несложно получить аналогичные утверждения для базиса $\{\overline{x \vee y}\}$, состоящего из единственного функционального элемента — стрелки Пирса. А именно, верны следующие теоремы.

Теорема 3. *Всякая минимальная схема в базисе $\{\overline{x \vee y}\}$, реализующая линейную функцию $x_1 + \ldots + x_n + n + 1$ (mod 2), состоит из $n-1$ стандартных блоков, каждый из которых входит в схему правильно.*

Теорема 4. *В базисе $\{\overline{x \vee y}\}$ при четных n выполняются равенства $L(l_n) = 4n-3$ и $L(\overline{l_n}) = 4n-4$, а при нечетных n выполняются равенства $L(l_n) = 4n-4$ и $L(\overline{l_n}) = 4n-3$.*

В заключение автор благодарит своего научного руководителя проф. Н. П. Редькина за помощь в работе.

Работа выполнена при финансовой поддержке РФФИ, проект 11-01-00.

Список литературы

1. Яблонский С. В. Введение в дискретную математику. — М.:

Наука, 1986.

2. Cardot C. Quelques rézultats sur l'application de l'algébre de Boole á la synthése des circuits á relais // Ann. Telecomm. — 1952. — 7, № 2. — С. 75–84.

3. Лупанов О. Б. Асимптотические оценки сложности управляющих систем. — М.: МГУ, 1984.

4. Редькин Н.П. Доказательство минимальности некоторых схем из функциональных элементов // Проблемы кибернетики. — 1970. — Вып. 23. — С. 83–101.

5. Комбаров Ю. А. О минимальных реализациях линейных булевых функций схемами из функциональных элементов в базисе $\{x \to y, \overline{x}\&y\}$ // Труды VIII Международной конференции "Дискретные модели в теории управляющих систем" (Москва, 6–9 апреля 2009 г.) — М.: МАКС Пресс, 2009. — С. 145–149.

6. Редькин Н. П. О минимальной реализации линейной функции схемой из функциональных элементов // Кибернетика. — 1971. — № 6. – С. 31–38.

7. Шкребела И. С. О сложности реализации линейных булевых функций схемами из функциональных элементов в базисе $\{x \to y, \overline{x}\}$ // Дискретная математика. — 2003. — Т. 15, № 4. — С. 100–112.

8. Комбаров Ю. А. О минимальных схемах для линейных булевых функций // Вестник Московского университета. Серия 1. Математика. Механика. — 2011. — № 6. — С. 41–44.

О ГЛУБИНЕ ФУНКЦИЙ МНОГОЗНАЧНОЙ ЛОГИКИ

А. В. Кочергин (Москва)

В работе рассматривается глубина функций k-значной ($k \geq 2$) логики при реализации схемами из функциональных элементов над произвольным базисом. Под базисом понимается произвольное множество функций k-значной логики, такое, что его замыкание относительно операции суперпозиции совпадает с множеством всех функций k-значной логики. Базис называется бесконечным, если для любого натурального числа m найдется функция из этого базиса, зависящая существенно не менее, чем от m переменных. В противном случае базис называется конечным. Вообще говоря, число функций в конечном базисе может быть бесконечным. Однако, по-существу,

конечный базис с точностью до добавления и изъятия несущественных переменных содержит лишь конечное число различных функций. Далее при рассмотрении вопросов алгоритмической разрешимости будем считать, что конечный базис задается как конечное множество функций k-значной логики.

Под глубиной схемы понимается максимальное число функциональных элементов в ориентированных цепях, ведущих от какого-либо входа схемы к её выходу. Глубиной функции f над базисом B, обозначаемой через $D_B(f)$, называется минимальная глубина схем, реализующих функцию f над базисом B. Для произвольного базиса B исследуется поведение функции Шенноны глубины, обозначаемой через $D_B(n)$ и определяемой при любом натуральном n соотношением $D_B(n) = \max D_B(f)$, где максимум берется по всем функциям f, зависящим от n переменных.

В [1] установлено, что в случае двузначной логики ($k = 2$) для любого конечного базиса B при $n \to \infty$ выполняется соотношение $D_B(n) \sim \beta n$, где $\beta = (\log_2 m)^{-1}$ и m — максимальное число существенных переменных у функций из базиса B.

В случае k-значной логики ($k \geq 2$) имеют место следующие утверждения.

Теорема 1. *Для всякого конечного базиса B функций k-значной логики существует такая положительная константа α_B, что при $n \to \infty$ выполняется соотношение*

$$D_B(n) \sim \alpha_B n.$$

Теорема 2. *Для всякого конечного базиса B функций k-значной логики константа α_B имеет вид $\alpha_B = \log_k \lambda_B$, где λ_B является алгебраическим числом.*

Теорема 3. *Существует алгоритм нахождения по произвольному конечному базису B функций k-значной логики многочлена с целыми коэффициентами, максимальным действительным корнем которого является число λ_B.*

В [2] показано, что в двузначной логике ($k = 2$) для любого бесконечного базиса B порядок роста функции Шеннона глубины $D_B(n)$ равен либо 1, либо $\log_2 n$. В [3] этот результат усилен: доказано, что для любого бесконечного базиса булевых функций B либо существует константа $a \geq 1$ такая, что $D_B(n) = a$ при всех достаточно больших n, либо существует целочисленная константа $b \geq 2$ и константа d такие, что $\log_b n \leq D_B(n) \leq \log_b n + d$ при всех n.

В работе [4] результаты работы [2] перенесены на случай k-значной логики ($k \geq 2$). Доказано следующее утверждение.

Теорема 4 [4]. *Для любого бесконечного базиса B функций k-значной логики либо существует константа $\alpha \geq 1$, такая, что $D_B(n) = \alpha$ при всех достаточно больших n, либо существуют константы β, γ, δ, где $\beta > 0$, такие, что $\beta \log_2 n \leq D_B(n) \leq \gamma \log_2 n + \delta$ при всех n.*

Автор выражает искреннюю благодарность О. М. Касим-Заде за постоянное и всестороннее внимание к работе.

Работа выполнена при финансовой поддержке РФФИ (проект 11–01–00508) и Программы фундаментальных исследований Отделения математических наук РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения» (проект «Задачи оптимального синтеза управляющих систем»).

Список литературы

1. Лупанов О. Б. О схемах из функциональных элементов с задержками // Проблемы кибернетики. Вып. 23. — М.: Наука, 1970. — С. 43–81.

2. Касим-Заде О. М. О глубине булевых функций при реализации схемами над произвольным базисом // Вестник Моск. ун-та. Серия 1. Математика. Механика. — 2007. — № 1. — С. 18–21.

3. Касим-Заде О. М. О глубине булевых функций над произвольным бесконечным базисом // Дискретный анализ и исследование операций. Серия 1. — 2007. — Т. 14, № 1. — С. 45–69.

4. Кочергин А. В. О глубине функций k-значной логики в бесконечных базисах // Вестник Моск. ун-та. Серия 1. Математика. Механика. — 2011. — № 1. — С. 22–26.

НЕКОТОРЫЕ ЗАДАЧИ СЛОЖНОСТИ ВЫЧИСЛЕНИЯ ЭЛЕМЕНТОВ КОНЕЧНЫХ АБЕЛЕВЫХ ГРУПП

В. В. Кочергин (Москва)

Отправной точкой для доклада на семинаре и для данного текста стали сохранившиеся три листочка с записями Олега Борисовича Лупанова, датированными, по-видимому, 1988 годом, в которых автору, тогда еще студенту-пятикурснику, ставилась задача о сложности вычислений элементов конечных абелевых групп. С тех пор и в этом направлении, и для близких задач, были получены некоторые результаты, постановка задачи видоизменялась, расширялась,

переосмысливалась. Однако в данной заметке рассматривается задача именно в исходной постановке — решению задач в изначальной постановке О. Б. Лупанов придавал большое значение.

Пусть G — конечная абелева группа (групповую операцию будем называть умножением). Подмножество $B = \{a_1, \ldots, a_q\}$ элементов группы будем называть *базисом* в группе G, если G раскладывается в прямое произведение циклических подгрупп, порожденных элементами множества B:

$$G = \langle a_1 \rangle_{u_1} \times \ldots \times \langle a_q \rangle_{u_q},$$

где u_i — порядок элемента a_i, $i = 1, \ldots, q$.

Для каждого элемента g группы G определим его *сложность реализации над базисом* B, обозначаемую через $L(g; B)$ как минимальное число операций умножения, достаточное для вычисления элемента g с использованием элементов множества B (при этом все уже вычисленные элементы могут быть использованы многократно (в этом принципиальное отличие от другой меры сложности вычислений элементов в группах [1]).

Сложность $L(G; B)$ конечной абелевой группы G над базисом B определим так:

$$L(G; B) = \max_{g \in G} L(g; B).$$

Положим

$$LM(G) = \max_{B:\ B-\text{базис } G} L(G, B), \quad Lm(G) = \min_{B:\ B-\text{базис } G} L(G, B).$$

Так как конечная абелева группа G полностью определяется вектором $\mathbf{v} = (v_1, \ldots, v_q)$ порядков примарных циклических подгрупп группы G, то вместо обозначения $LM(G)$ можно использовать обозначение $M(\mathbf{v})$, а вместо $Lm(G)$ — $m(\mathbf{v})$.

Для вектора $\mathbf{v} = (v_1, \ldots, v_q)$ обозначим через $\|\mathbf{v}\|$ величину $v_1 v_2 \ldots v_q$. Положим

$$M(n) = \max_{\mathbf{v}:\ \|\mathbf{v}\| \le n} M(\mathbf{v}), \quad m(n) = \max_{\mathbf{v}:\ \|\mathbf{v}\| \le n} m(\mathbf{v}).$$

Задача (О. Б. Лупанов, 1988). Во-первых, найти числовые функции $f_1(\mathbf{v})$ и $f_2(\mathbf{v})$, определенные на векторах $\mathbf{v}$, характеризующих порядки примарных циклических групп, с помощью которых выражались бы величины $M(\mathbf{v})$ и $m(\mathbf{v})$ (хотя бы асимптотически или с

точностью до порядка при условии, что порядок всей группы стремится к бесконечности); во-вторых, исследовать рост функций $M(n)$ и $m(n)$ при $n \to \infty$.

Пусть $G = \langle a_1 \rangle_{u_1} \times \ldots \times \langle a_q \rangle_{u_q}$, т. е. $B = \{a_1, \ldots, a_q\}$ — базис в группе G. Из мощностных соображений вытекает следующий факт.

Утверждение 1. *Для произвольного положительного ε найдется такое положительное $m(\varepsilon)$, что для сложности любой конечной абелевой группы G над базисом B при выполнении условия $|G| > m(\varepsilon)$ справедлива оценка*

$$L(G; M_G) \geq \frac{\log |G|}{\log \log |G|} \left(1 + (1 - \varepsilon) \frac{\log \log \log |G|}{\log \log |G|}\right)$$

(*здесь и далее все логарифмы берутся по основанию* 2).

Из результатов работ [2–4] следует такая верхняя оценка.

Утверждение 2. *Пусть* $G = \langle a_1 \rangle_{u_1} \times \ldots \times \langle a_q \rangle_{u_q}$, $B = \{a_1, \ldots, a_q\}$. *Тогда при* $|G| \to \infty$

$$L(G, B) \leq \frac{\log |G|}{\log \log |G|}(1 + o(1)) + \log(\max_i u_i)(1 + o(1)) + O(q).$$

Теорема 1. *Пусть* $G = \langle a_1 \rangle_{u_1} \times \ldots \times \langle a_q \rangle_{u_q}$, $B = \{a_1, \ldots, a_q\}$. *Тогда при* $|G| \to \infty$ *справедливы соотношения*

$$\frac{\log |G|}{\log \log |G|} \lesssim L(G, B) \lesssim \frac{\log |G|}{\log \log |G|} + \log(\max_i u_i) + q.$$

Эта теорема вместе с простой нижней оценкой $L(G, B) \geq \log(\max_i u_i - 1) + q - 1$ при условии $|G| \to \infty$ устанавливает порядок роста функционала $L(G, B)$. Более того, при выполнении условия $q = o\left(\frac{\log |G|}{\log \log |G|} + \log(\max_i u_i)\right)$ теорема 1 дает асимптотику роста величины $L(G, B)$.

Теорема 2. *При* $\|\mathbf{v}\| \to \infty$ *выполняются соотношения*

$$\frac{\log \|\mathbf{v}\|}{\log \log \|\mathbf{v}\|} \lesssim m(\mathbf{v}) \leq M(\mathbf{v}) \lesssim \log \|\mathbf{v}\|.$$

В случае, когда все элементы вектора $\mathbf{v}$ являются степенями одного и того же простого числа, справедливо равенство $m(\mathbf{v}) = M(\mathbf{v})$.

Если же вектор $\mathbf{v}$ состоит из k различных простых чисел из отрезка $[2^k, 2^{2k}]$, то для него одновременно достигаются как нижняя оценка величины $m(\mathbf{v})$, так и верхняя оценка величины $M(\mathbf{v})$ из теоремы 2.

На самом деле теорема 1 дает серьезный инструмент для исследования поведения величин $M(\mathbf{v})$ и $m(\mathbf{v})$. На основе этой теоремы установлен порядок роста величин $M(\mathbf{v})$ и $m(\mathbf{v})$ (здесь формулировки соответствующих результатов не приводится из-за невозможности ввести все необходимые для точных формулировок определения).

Теорема 3. *При $n \to \infty$ справедливы равенства*

$$M(n) = \log n + \frac{\log n}{\log\log n}(1 + o(1)), \quad m(n) = \log n + \frac{\log n}{\log\log n}(1 + o(1)).$$

Работа выполнена при финансовой поддержке РФФИ, проект № 11-01-00508.

Список литературы

1. Глухов М. М., Зубов А. Ю. О длинах симметрических и знакопеременных групп подстановок в различных системах образующих // Математические вопросы кибернетики. Вып. 8. — М.: Наука, 1999. — С. 5–32.

2. Кочергин В. В. О сложности вычислений в конечных абелевых группах // ДАН СССР. — 1991. — Т. 317, № 2. — С. 291–294.

3. Кочергин В. В. О сложности вычислений в конечных абелевых группах // Математические вопросы кибернетики. Вып. 4. — М.: Наука, 1992. — С. 178–217.

4. Гашков С. Б., Кочергин В. В. Об аддитивных цепочках векторов, вентильных схемах и сложности вычисления степеней // Методы дискретного анализа в теории графов и сложности. — Новосибирск, 1992. — Вып. 52. — С. 22–40.

О КОНЪЮНКТОРНОЙ СЛОЖНОСТИ СХЕМ В БАЗИСЕ ЖЕГАЛКИНА ДЛЯ ОДНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ БУЛЕВЫХ ФУНКЦИЙ

Т. И. Краснова (Москва)

Будем рассматривать схемы из функциональных элементов в базисе Жегалкина $B = \{\&, \oplus, 1\}$ [1]. Под *конъюнкторной сложностью* $L_B^{\&}(f)$ понимается наименьшая из конъюнкторных сложностей схем

в базисе B, реализующих булеву функцию f; под *конъюнкторной сложностью* схемы понимается число конъюнкторов в этой схеме.

В данной работе исследуется конъюнкторная сложность функции $f_2^n(x_1, ..., x_n) = \bigvee\limits_{1 \le i < j \le n} x_i x_j$.

Теорема 1. *Если $n \ge 2$ — четное, то $L_B^{\&}(f_2^n) = n - 1$. Если $n \ge 3$ — нечетное, то $L_B^{\&}(f_2^n) = n - 2$.*

Теорема 2. *Пусть $deg(f)$ — степень полинома Жегалкина булевой функции f. Тогда имеем $L_B^{\&}(f) \ge deg(f) - 1$.*

Доказательство Теоремы 2 проведем индукцией по степени полинома Жегалкина булевой функции f.

База индукции $deg(f) = 1$. Очевидно, $L_B^{\&}(f) \ge 0$.

Пусть верно для $deg(f) = d$, докажем для $deg(f) = d + 1$.

Рассмотрим минимальную (относительно конъюнкторной сложности) схему S в базисе B, реализующую функцию $f(x_1, ..., x_n)$, для которой $deg(f) = d+1$. Заметим, что $d+1 \ge 2$, значит в схеме S есть хотя бы один конъюнктор. Введем в схеме монотонную нумерацию вершин [2] и рассмотрим конъюнктор $E_{\&}$ с минимальным номером. На его входы могут подаваться только линейные функции от переменных. Пусть на выходе конъюнктора $E_{\&}$ реализуется функция $g(x_1, ..., x_n)$. Теперь рассмотрим функцию $h(x_1, ..., x_n, x_{n+1})$, такую что $h(x_1, ..., x_n, g(x_1, ..., x_n)) = f(x_1, ..., x_n)$. Эту функцию можно реализовать слегка видоизмененной схемой S, в которой вместо выхода конъюнктора $E_{\&}$ на соответсвующие элементы подается новая переменная x_{n+1}. Заметим, что

$$L_B^{\&}(f) - 1 \ge L_B^{\&}(h). \qquad (*)$$

Предположим, что $deg(h) < d$, тогда подставим в полином Жегалкина вместо x_{n+1} полином Жегалкина функции g. Заметим, что степень каждого монома возрасла не более, чем на 1. Значит, степень полинома не могла возрасти более, чем на 1. Однако, $deg(f) = d + 1$. Из получившегося противоречия следует, что $deg(h) \ge d$.

Пусть $deg(h) > d$. В этом слкчае получаем способ переходить к функции со степенью полинома Жегалкина не меньшей, чем у исходной, а конъюнкторной сложностью как минимум на единицу меньшей, чем у исходной. Но такой переход нельзя повторять неограниченное число раз (если повторить $L_B^{\&}(f)$ раз, то в схеме не останется конъюнкторов), значит на каком-то шаге мы получим функцию со степенью полинома Жегалкина ровно d.

Если $deg(h) = d$, то по предположению индукции $L_B^{\&}(h) \geq deg(h) - 1 = d - 1$. Теперь, учитывая неравенство (*), получим $L_B^{\&}(f) \geq d = deg(f) - 1$.

Теорема 2 доказана.

Лемма. *При* $n \geq 2$ *имеем* $f_2^n(x_1, ..., x_n) = \bigoplus\limits_{2 \leq 2k \leq n} p_n^{2k}(x_1, ..., x_n)$, *где* $p_n^k(x_1, ..., x_n) = \bigoplus\limits_{1 \leq i_1 < ... < i_k \leq n} x_{i_1} \cdot ... \cdot x_{i_k}$.

Следствие 1. *Если* n — *четное, то* $deg(f_2^n) = n$. *Если* n — *нечетное, то* $deg(f_2^n) = n - 1$.

Следствие 2. *Если* n — *четное, то* $L_B^{\&}(f_2^n) \geq n - 1$. *Если* n — *нечетное, то* $L_B^{\&}(f_2^n) \geq n - 2$.

Из следствия 2 вытекают *нижние оценки* для теоремы 1.

Верхние оценки для теоремы 1 получим конструктивно индукцией по n.

Базис индукции. Для $n = 2$ построим схему по представлению $f_2^2(x_1, x_2) = x_1 \cdot x_2$ со сложностью $L_B^{\&}(f_2^2) = 1$.

Для $n = 3$ построим схему по представлению $f_2^3(x_1, x_2, x_3) = (x_1 \oplus x_2) \cdot (x_1 \oplus x_3) \oplus x_1$ со сложностью $L_B^{\&}(f_2^3) = 1$.

Для $n = 4$ построим схему по представлению $f_2^4(x_1, x_2, x_3, x_4) = f_2^3(x_1, x_2, x_3) \vee (x_1 \oplus x_2 \oplus x_3) \cdot x_4$ со сложностью $L_B^{\&}(f_2^4) = 3$.

Для $n = 5$ построим схему по представлению $f_2^5(x_1, x_2, x_3, x_4, x_5) = f_2^3(x_1, x_2, x_3) \vee f_2^3(x_1 \oplus x_2 \oplus x_3, x_4, x_5)$ со сложностью $L_B^{\&}(f_2^5) = 3$.

Переход. Пусть верно для $f_2^2, ..., f_{n-1}^2$. Докажем для f_n^2. При подсчете конъюнкторной сложности воспользуемся тем, что функцию $f_1^k(x_1, ..., x_k) = x_1 \vee ... \vee x_k$ можно реализовать схемой с конъюнкторной сложностью $k - 1$.

Случай 1а: $n = 3k$, k — четное. В этом случае n — четное. Воспользуемся представлением $f_2^n(x_1, y_1, z_1, ..., x_k, y_k, z_k) = f_2^k(x_1 \oplus y_1 \oplus z_1, ..., x_k \oplus y_k \oplus z_k) \vee f_1^k(f_2^3(x_1, y_1, z_1), ..., f_2^3(x_k, y_k, z_k))$. Конъюнкторная сложность полученной схемы равна $k-1+1+k-1+k = 3k-1 = n-1$.

Случай 1б: $n = 3k$, k — нечетное. В этом случае n — нечетное. Воспользуемся представлением $f_2^n(x_1, y_1, z_1, ..., x_k, y_k, z_k) = f_2^k(x_1 \oplus y_1 \oplus z_1, ..., x_k \oplus y_k \oplus z_k) \vee f_1^k(f_2^3(x_1, y_1, z_1), ..., f_2^3(x_k, y_k, z_k))$. Конъюнкторная сложность полученной схемы равна $k - 2 + 1 + k - 1 + k = 3k - 2 = n - 2$.

Случай 2а: $n = 3k + 1$, k — четное. В этом случае n — нечетное. Воспользуемся представлением $f_2^n(x_1, y_1, z_1, ..., x_k, y_k, z_k, x) = f_2^{k+1}(x_1 \oplus y_1 \oplus z_1, ..., x_k \oplus y_k \oplus z_k, x) \vee f_1^k(f_2^3(x_1, y_1, z_1), ..., f_2^3(x_k, y_k, z_k))$.

Конъюнкторная сложность полученной схемы равна $k+1-2+1+k-1+k=3k-1=n-2$.

Случай 2б: $n=3k+1$, k — нечетное. В этом случае n — четное. Воспользуемся представлением $f_2^n(x_1,y_1,z_1,...,x_k,y_k,z_k,x) = f_2^{k+1}(x_1\oplus y_1\oplus z_1,...,x_k\oplus y_k\oplus z_k,x)\vee f_1^k(f_2^3(x_1,y_1,z_1),...,f_2^3(x_k,y_k,z_k))$. Конъюнкторная сложность полученной схемы равна $k+1-1+1+k-1+k=3k=n-1$.

Случай 3а: $n=3k+2$, k — четное. В этом случае n — четное. Воспользуемся представлением $f_2^n(x_1,y_1,z_1,...,x_k,y_k,z_k,x,y) = f_2^{k+2}(x_1\oplus y_1\oplus z_1,...,x_k\oplus y_k\oplus z_k,x,y)\vee f_1^k(f_2^3(x_1,y_1,z_1),...,f_2^3(x_k,y_k,z_k))$. Конъюнкторная сложность полученной схемы равна $k+2-1+1+k-1+k=3k+1=n-1$.

Случай 3б: $n=3k+2$, k — нечетное. В этом случае n — нечетное. Воспользуемся представлением $f_2^n(x_1,y_1,z_1,...,x_k,y_k,z_k,x,y) = f_2^{k+2}(x_1\oplus y_1\oplus z_1,...,x_k\oplus y_k\oplus z_k,x,y)\vee f_1^k(f_2^3(x_1,y_1,z_1),...,f_2^3(x_k,y_k,z_k))$. Конъюнкторная сложность полученной схемы равна $k+2-2+1+k-1+k=3k=n-2$.

Теорема 1 доказана.

Выражаю признательность Н. П. Редькину за внимание к работе.

Работа выполнена при финансовой поддержке РФФИ, проект № 11-01-00508.

Список литературы

1. Лупанов О. Б. Асимптотические оценки сложности управляющих систем. — М.: Изд-во МГУ, 1984.

2. Редькин Н. П. Дискретная математика. — М.: Физматлит. 2009.

О БИЛИНЕЙНЫХ АЛГОРИТМАХ УМНОЖЕНИЯ ОБОБЩЕННЫХ КВАТЕРНИОНОВ

В. В. Лысиков (Москва)

В работе рассматривается сложность умножения в алгебрах обобщенных кватернионов с делением в модели билинейных алгоритмов. Данная задача связана с задачей классификации алгебр почти минимального ранга [1].

Билинейным алгоритмом сложности r для билинейного отображения $\varphi\colon U\times V\to W$ называется набор троек

$$(f_1,g_1,z_1;\ldots;f_r,g_r,z_r),\quad f_k\in U^*,g_k\in V^*,z_k\in W$$

такой, что

$$\varphi(u,v) = \sum_{k=1}^{r} f_k(u) g_k(v) z_k \quad \forall u \in U, v \in V.$$

Минимально возможная длина билинейного алгоритма называется *билинейной сложностью* или *рангом* отображения φ и обозначается $R(\varphi)$. *Билинейной сложностью алгебры* называется билинейная сложность умножения в ней.

Понятие ранга билинейного отображения допускает удобную интерпретацию в терминах мультилинейной алгебры. Тот факт, что набор троек является билинейным алгоритмом для φ, будем записывать следующим образом: $\varphi = \sum\limits_k f_k \otimes g_k \otimes z_k$.

Алгеброй обобщенных кватернионов над полем F называется четырехмерная алгебра с базисом $1, i, j, k$, удовлетворяющим соотношениям

$$i^2 = p, j^2 = q, ij = -ji = k$$

при некоторых $p, q \in F^\times$.

Любая алгебра обобщенных кватернионов H либо изоморфна алгебре матриц $F^{2\times 2}$, либо является некоммутативной алгеброй с делением. Известно, что некоммутативная алгебра с делением не может быть алгеброй минимального ранга [3], т.е. $R(H) \geq 8$.

Обозначим $\dim U = m$, $\dim V = n$. Результат о сложности умножения в алгебрах обобщенных кватернионов получен с помощью следующих общих утверждений о билинейных алгоритмах сложности $m + n$ для билинейных отображений специального вида.

Назовем элемент $u_0 \in U$ (левым) *φ-регулярным*, если линейный оператор $\varphi(u_0, \cdot)$ инъективен, т.е. $\varphi(u_0, v) = 0$ тогда и только тогда, когда $v = 0$

Билинейный алгоритм $\varphi = \sum_{k=1}^{r} f_k \otimes g_k \otimes z_k$ будем называть *двухкомпонентным*, если множество $\{1, \ldots, r\}$ можно разбить на непересекающиеся множества I и J такие, что $\{f_i | i \in I\}$ и $\{g_j | j \in J\}$ являются базисами пространств U^* и V^* соответственно.

Лемма 1. *Если $R(\varphi) = m + n$, $\operatorname{lker} \varphi = \mathbf{0}$, и в любом базисе пространства U найдется φ-регулярный элемент, то любой оптимальный билинейный алгоритм для φ является двухкомпонентным.*

Для доказательства этой леммы используется тот факт, что при выполнении указанных условий перестановкой слагаемых алгоритма можно добиться того, что $f_1, \ldots, f_m$ и $g_m, \ldots, g_{m+n-1}$ бу-

дут являтся базисами соответствующих пространств, причем вектор $u \in U$, являющийся общим нулем функционалов $f_1, \ldots, f_{m-1}$, φ-регулярен. Далее доказывается, что если $g_{m+1}, \ldots, g_{m+n}$ линейно зависимы, то в базисе $f_1, \ldots, f_m$ можно заменить f_m на какой-то из функционалов f_k, соответсвующих линейно зависимым g_k.

Лемма 2. *Двухкомпонентный билинейный алгоритм для φ существует тогда и только тогда, когда существует пара базисов $(u_1, \ldots, u_m)$ и $(v_1, \ldots, v_n)$ пространств U и V соответственно, и наборы $(z'_1, \ldots, z'_m)$ и $(z''_1, \ldots, z''_n)$ элементов W, удовлетворяющие условию $\varphi(u_i, v_j) \in \mathrm{lin}(\{z'_i, z''_j\})$.*

Доказательство. Пусть (u_i) и (v_j) — базисы U и V соответственно, а (f_i) и (g_j) — двойственные им базисы.

Билинейный алгоритм

$$\sum_{i=1}^{m} f_i \otimes (\sum_{j=1}^{n} \lambda_{ij} g_j) \otimes z'_i + \sum_{j=1}^{n} (\sum_{i=1}^{m} \mu_{ij} f_i) \otimes g_j \otimes z''_j$$

вычисляет φ тогда и только тогда, когда $\varphi(u_i, v_j) = \lambda_{ij} z'_i + \mu_{ij} z''_j$.

Следствие. *Пусть A — локальная алгебра, $\dim A = n$, и $R(A) \geq 2n$. $R(A) = 2n$ тогда и только тогда, когда в A существует пара базисов $(u_1 = 1, u_2, \ldots, u_n)$, $(v_1 = 1, v_2, \ldots, v_n)$ и пара наборов элементов $(z'_1, \ldots, z'_n)$, $(z''_1, \ldots, z''_n)$ такие, что $u_i v_j \in \mathrm{lin}(\{z'_i, z''_j\})$.*

Теорема 1. *Если H — алгебра обобщенных кватернионов с делением, то $R(H) = 8$.*

Доказательство. Воспользуемся доказанными вспомогательными утверждениями. В качестве (u_i) и (v_j) стандартный кватернионный базис: $(u_1, u_2, u_3, u_4) = (v_1, v_2, v_3, v_4) = (1, i, j, k)$, а наборы z'_i и z''_j определим следующим образом:

$$(z'_1, z'_2, z'_3, z'_4) = (1+\alpha i+\beta j+\gamma k, 1+\alpha i-\beta j-\gamma k, 1-\alpha i+\beta j-\gamma k, 1-\alpha i-\beta j+\gamma k);$$

$$(z''_1, z''_2, z''_3, z''_4) = (1-\alpha i-\beta j-\gamma k, 1-\alpha i+\beta j+\gamma k, 1+\alpha i-\beta j+\gamma k, 1+\alpha i+\beta j-\gamma k),$$

где α, β, γ — некоторые ненулевые константы из F. Непосредственно проверяется, что для этих наборов выполнено требуемое соотношение $u_i v_j \in \mathrm{lin}(\{z'_i, z''_j\})$.

Также доказано, что при некоторых значениях констант α, β, γ полученные алгоритмы являются неэквивалентными в смысле де Гроота [2].

Теорема 2. *Если H — алгебра обобщенных кватернионов с делением, то существует бесконечно много неэквивалентным оптимальных алгоритмов умножения в H.*

Автор благодарен В. Б. Алексееву за постановку задачи и внимание к работе.

Работа выполнена при финансовой поддержке РФФИ (грант 12-01-91331-ННИО_а)

Список литературы

1. Bläser, M., de Voltaire, A. M. Semisimple algebras of almost minimal rank over the reals // Theoretical Computer Science. — 2009. — V. 410, № 50. — С. 5202–5214.

2. de Groote, H. F. On varieties of optimal algorithms for the computation of bilinear mappings I // Theoretical Computer Science. — V. 7, № 1. — С. 1–24.

3. Bürgisser, P., Clausen, M., Shokrollahi, M. A. Algebraic complexity theory. — Springer Verlag, 1997.

О ПРОВЕРЯЮЩИХ ТЕСТАХ ОТНОСИТЕЛЬНО МНОЖЕСТВЕННЫХ ЛИНЕЙНЫХ СЛИПАНИЙ ПЕРЕМЕННЫХ

Е. В. Морозов, Д. С. Романов (Москва)

Будем говорить, что в булевой функции $f(x_1, ..., x_n)$ произошло Ф-*слипание* переменных $x_{i_1}, ..., x_{i_k}$, если вместо функции f реализуется булева функция, полученная в результате подстановки вместо каждой из этих переменных булевой функции $\phi(y_1, ..., y_k), k \geq 2$ от $x_{i_1}, ..., x_{i_k}$ из некоторого множества Ф. Назовем ϕ функцией слипания. Назовем Ф-слипание *множественным*, если существуют p непересекающихся подмножеств множества переменных функции $f(x_1, ..., x_n)$, для каждого из которых произошло Ф-слипание с некоторой своей функцией слипания. Через $\Psi = \Psi_{n,f,\Phi}$ обозначим множество функций, в которое входят $f(x_1, ..., x_n)$ и всевозможные различные функции, получающиеся из $f(x_1, ..., x_n)$ в результате множественных Ф-слипаний переменных с функциями слипания из множества Ф. Проверяющий тест T для системы $\Psi_{n,f,\Phi}$ (все неопределенные понятия можно найти в [1]) назовем *проверяющим тестом относительно множественных* Ф-*слипаний переменных*. Введем функцию Шеннона $L(n)$ длины проверяющего относительно множественных Ф-слипаний как максимум по всем булевым функциям $f(x_1, ..., x_n)$ длины минимального проверяющего теста относительно множественных Ф-слипаний переменных.

Ф-слипание назовем *линейным слипанием*, если Ф — множество всех линейных функций. В данной работе изучаются проверяющие тесты относительно множественных линейных слипаний.

Теорема. *При* $n \to \infty$ *справедливы соотношения*

$$\frac{n^2}{2} + O(n) \leq L(n) \leq n^2 + O(n).$$

Доказательство. Установим верхнюю оценку. Сначала рассмотрим только функции слипания без фиктивных переменных.

Проверяющей парой для переменных x_i, x_j назовем пару наборов $\tilde{\alpha'}, \tilde{\alpha''}$, таких, что $\alpha'_k = \alpha''_k$ при $k \neq i, j$, а при $k = i, j$ $\alpha'_k \neq \alpha''_k$ и $f(\tilde{\alpha'}) \neq f(\tilde{\alpha''})$. Под *проверкой* пары переменных будем понимать добавление в тест наборов, обнаруживающих неисправность, если эти переменные участвуют в одном слипании. Для всех пар переменных, у которых существует проверяющая пара наборов, добавим эти наборы в тест.

Пусть не существует проверяющей пары для переменных x_1, x_2. Разобьем переменные f на две группы. В первую войдут x_1, x_2 и переменные, не имеющие проверяющих пар с x_1 или x_2, во вторую — все остальные. Будем считать, что $x_1, ..., x_m$ — переменные первой группы. Тогда для любого набора $\tilde{\alpha} = (\alpha_3, ..., \alpha_n)$ верно $f(00\tilde{\alpha}) = f(11\tilde{\alpha}) = \sigma_1(\tilde{\alpha}), f(01\tilde{\alpha}) = f(10\tilde{\alpha}) = \sigma_2(\tilde{\alpha})$. Зафиксируем набор $\tilde{\alpha}$. Рассмотрим переменную x_3. Пусть $\tilde{\alpha} = \alpha_3\tilde{\gamma}$. Тогда видно, что и для $\overline{\alpha_3}\tilde{\gamma}$ верно: $f(00\overline{\alpha_3}\tilde{\gamma}) = f(11\overline{\alpha_3}\tilde{\gamma}) = \sigma_1(\overline{\alpha_3}\tilde{\gamma}), f(01\overline{\alpha_3}\tilde{\gamma}) = f(10\overline{\alpha_3}\tilde{\gamma}) = \sigma_2(\overline{\alpha_3}\tilde{\gamma})$. Так как не существует проверяющих пар для x_1, x_3 и x_2, x_3, получаем, что $\sigma_1(\alpha_3\tilde{\gamma}) = \sigma_2(\overline{\alpha_3}\tilde{\gamma})$, а $\sigma_2(\alpha_3\tilde{\gamma}) = \sigma_1(\overline{\alpha_3}\tilde{\gamma})$. Аналогично для $x_4, ..., x_m$. Тогда подфункция $f(x_1, ..., x_m, \beta_{m+1}, ..., \beta_n)$ — либо константа, либо линейная функция от всех переменных.

Предположим, что переменные первой группы могут слипаться только между собой. Если все переменные первой группы фиктивны, их слипание не меняет исходную функцию f. Пусть среди них есть хотя бы одна существенная переменная. Тогда существуют $(\beta_{m+1}, ..., \beta_n)$, при подстановке которых вместо переменных второй группы получаем линейную функцию, существенно зависящую от всех переменных первой группы. Зафиксируем этот набор. В случае слипания переменных из $x_1, ..., x_m$ будет реализовываться линейная функция m переменных. Добавим в тест $m+1$ набор для определения получившейся линейной функции. Если неисправность не обнаружена, то либо реализуется функция, не отличимая от исходной, либо были слипания во второй группе.

В результате слипаний переменных второй группы при подстановке набора $(\beta_{m+1}, ..., \beta_n)$ можем получить подфункцию из множества $\{0, 1, \xi(x_1, ..., x_m), \xi(x_1, ..., x_m) \oplus 1\}$. Неисправность могла быть не обнаружена, если $\xi \in \{l_m(x_1, ..., x_m), l_m(x_1, ..., x_m) \oplus 1\}$.

Аналогично можно разбить переменные $x_{m+1}, ..., x_n$, объединяя в одну группу переменные, не имеющие проверяющих пар между собой. Оставшиеся переменные объединим в последнюю, возможно пустую группу. Повторяя рассуждения для первой группы, получим, что неисправность могла быть не обнаружена, если f зависит от $l_{m_1}(x_1, ..., x_{m_1}), ..., l_{m_r - m_{r-1}+1}(x_{m_{r-1}+1}, ..., x_{m_r}), x_{m_r+1}, ..., x_n$, где $m_r + 1$, ..., n — индексы переменных последней группы. Тогда f представим суперпозицией: $f(x_1, ..., x_n) = g(y_1, ..., y_r, x_{m_r+1}, ..., x_n)$, $y_i = l_{m_i - m_{i-1}+1}(x_{m_{i-1}+1}, ..., x_{m_i})$. То есть непроверенные слипания эквивалентны инверсиям входов для g. Из [2] следует, для тестирования достаточно $r + n - m_r$ наборов.

Итак, для проверки одной пары достаточно либо двух наборов в тесте, либо проверить соответствующую группу из переменных. Если в группе m переменных, то для их проверки достаточно $(m+1)$ наборов. При $m \geq 3$ на одну пару переменных будет приходиться не более 2 наборов. Если же $m = 2$, то возможные функции слипания 2 переменных x_i, x_j есть $0, 1, x_i \oplus x_j, x_i \oplus x_j \oplus 1$, для различения их хватит 2 наборов $(0, 0)$ и $(1, 0)$. И в этом случае на пару переменных будет приходиться 2 набора. Плюс, возможно, понадобится линейное число наборов для тестирования функции f относительно инверсий групп.

Рассмотрим оставшиеся функции слипания. Если какая-то существенная переменная стала фиктивной, для обнаружения этого понадобится 2 набора. Если в слипание входит не менее 2 существенных переменных, то это эквивалентно некоторому слипанию с функцией слипания без фиктивных переменных. В противном случае результатом слипания может быть инверсия существенной переменной. Поэтому теста для инверсий входов f достаточно, чтобы найти подобные неисправности. Итого, добавляем еще некоторое линейное количество наборов.

Докажем нижнюю оценку. Рассмотрим функцию $f(x_1, ..., x_n) = x_1 \vee x_2 \vee ... \vee x_n$. Сузим класс неисправностей до единичного слипания 2 переменных с функцией слипания $\phi(x, y) = x \oplus y$. Для проверки переменных x_i, x_j понадобится набор, у которого в i-ой и j-ой позициях стоят единицы, во всех остальных нули. На любом другом наборе получившаяся функция неисправности неотличима от исходной. Для тестирования f необходимы все наборы с ровно двумя единицами.

Работа выполнена при поддержке грантов РФФИ № 12-01-00964 и № 10-01-00768.

Список литературы

1. Редькин Н. П. Надежность и диагностика схем. — М.: Изд-во МГУ, 1992.

2. Погосян Г. Р. О проверяющих тестах для логических схем. — М.: Изд-во ВЦ АН СССР, 1982.

О ЛОГИКО-ТЕРМАЛЬНОЙ ЭКВИВАЛЕНТНОСТИ СТАНДАРТНЫХ СХЕМ ПРОГРАММ

Т. А. Новикова (Астана), В. А. Захаров (Москва)

Логико-термальная (л.-т.) эквивалентность стандартных схем программ, предложенная в статье [1], — это неинтерпретационное отношение эквивалентности программ, обладающее двумя важными свойствами: это отношение разрешимо, и из л.-т. эквивалентности программ следует их функциональная эквивалентность. В статье [2] был предложен полиномиальный по времени алгоритм проверки л.-т. эквивалентности программ, использующий специальные представления инвариантов равенства в виде сетей. В статье [3] нами был разработан более простой алгоритм проверки л.-т. эквивалентности программ, основанный на алгебре подстановок с операциями композиции и антиунификации. В настоящей заметке мы покажем, что предложенный нами алгоритм имеет полиномиальную сложность.

Для множеств переменных $\mathcal{X}, \mathcal{Y}$ и множества функциональных символов $\mathcal{F}$ обозначим записью $Term(\mathcal{F}, \mathcal{X})$ множество термов, а записью $Subst(\mathcal{X}, \mathcal{F}, \mathcal{Y})$ — множество подстановок вида $\theta : \mathcal{X} \to Term(\mathcal{F}, \mathcal{Y})$, на котором обычным образом определяется операция композиции и отношение квазипорядка $\preceq$: для пары подстановок θ_1, θ_2 отношение $\theta_1 \preceq \theta_2$ выполняется, если есть такая подстановка $\eta \in Subst(\mathcal{Y}, \mathcal{F}, \mathcal{Y})$, что $\theta_2 = \theta_1\eta$. Если $\theta_1 \preceq \theta_2$, то подстановка θ_1 называется *шаблоном* θ_2. Множество $(Subst(\mathcal{X}, \mathcal{F}, \mathcal{Y})$ с отношением $\preceq$ образует полную квазирешетку, наименьшим элементом которой является пустая подстановка $\varepsilon = \{x_1/y_1, \ldots, x_n/y_n\}$, а наибольшим— специальная максимальная подстановка τ, удовлетворяющая равенству $\tau\theta = \theta\tau = \tau$ для любой подстановки θ. Операция взятия точной нижней грани в этой квазирешетке называется *антиунификацией* подстановок и обозначается символом $\downarrow$. Термы и

подстановки могут быть представлены ациклическими ориентированными графами (АОГ), вершинам которых приписаны переменные и функциональные символы.

Как показано в статье [3], задача проверки л.-т. эквивалентности стандартных схем программ равносильно следующей задаче анализа размеченных графов. Рассмотрим конечный ориентированный граф G с выделенной вершиной v_0. Каждой вершине v графа G сопоставлена пара (A'_v, A''_v) атомарных формул вида $P(t_1, \ldots, t_k)$, где P — предикатный символ, а $t_1, \ldots, t_k$ — термы из $Term(\mathcal{F}, \mathcal{X})$. Каждой дуге $\langle v, u\rangle$ в графе G приписана подстановка $\eta_{u,v}$ из $Subst(\mathcal{X}, \mathcal{F}, \mathcal{X})$. Каждому маршруту $Path = \langle v_0, v_1\rangle, \langle v_1, v_2\rangle, \ldots, \langle v_{n-1}, v_n\rangle$, исходящего из вершины v_0, может быть соспоставлена подстановка η_{Path}, являющаяся композицией $\eta_{v_{n-1},v_n} \cdots \eta_{v_1,v_2}\eta_{v_0,v_1}$ подстановок, приписанных дугам этого маршрута. Размеченный граф G называется *согласованным*, если для любого пути $Path$, ведущего из вершины v_0 в произвольную вершину v, верно равенство $A'_v\eta_{Path} = A''_v\eta_{Path}$. Упомянутая задача анализа графов — это задача проверки согласованности произвольных размеченных графов.

Для решения этой задачи мы выделим особый подкласс подстановок, в котором операция антиунификации выполняется наиболее эффективно. Подстановка θ из класса $Subst(\mathcal{X}, \mathcal{F}, \mathcal{Y})$ называется *редуцированной*, если для любой пары переменных x, $x \in \mathcal{X}$, и y, $y \in \mathcal{Y}$, если y входит в состав терма $\theta(x)$, то существует такая переменная x', $x' \in \mathcal{X}$, для которой выполняется равенство $\theta(x') = y$.

Утверждение 1. *Для любой подстановки θ, $\theta \in Subst(\mathcal{X}, \mathcal{F}, \mathcal{Y})$, существует наибольший по отношению $\preceq$ редуцированный шаблон θ', который может быть вычислен за время $O(n)$, где n — размер АОГ, представмющего θ.*

Подстановку θ', упомянутую в утверждении 1, условимся обозначать записью $msr(\theta)$. В классе подстановок $Subst(\mathcal{X}, \mathcal{F}, \mathcal{Y})$ введем операцию $\Downarrow$: для любой пары подстановок θ_1, θ_2 будем полагать $\theta_1 \Downarrow \theta_2 = msr(\theta_1 \downarrow \theta_2)$.

Утверждение 2. *Для любых подстановок θ_1, θ_2 из $Subst(\mathcal{X}, \mathcal{F}, \mathcal{Y})$, подстановки η из $Subst(\mathcal{X}, \mathcal{F}, \mathcal{X})$, и атомарных формул A', A'' справедливы соотношения*

1) $\eta\theta_1 \Downarrow \eta\theta_2 = \eta(\theta_1 \Downarrow \theta_2)$,

2) $A'\theta_1 = A''\theta_1 \wedge A'\theta_2 = A''\theta_2 \iff A'(\theta_1 \Downarrow \theta_2) = A''(\theta_1 \Downarrow \theta_2)$.

Нами предлагается следующий алгоритм проверки согласованности размеченного графа G. Каждая вершина v графа G помечается

подстановкой θ_v из класса $Subst(\mathcal{X}, \mathcal{F}, \mathcal{Y})$. Начальная разметка вершин такова: выделенная вершина v_0 помечается пустой подстановкой ε, а все остальные вершины помечаются наибольшей по отношению $\preceq$ подстановкой τ. Далее выполняется итеративная процедура: для каждой дуги $\langle u, v\rangle$ подстановка θ_v, приписанная вершине v, заменяется подстановкой $\theta_v \Downarrow \eta_{u,v}\theta_u$. Процедура выполняется до тех пор, пока для каждой дуги $\langle u, v\rangle$ не будет выполняться равенство $\theta_v = \theta_v \Downarrow \eta_{u,v}\theta_u$ (стационарная разметка).

Теорема 1. *Процедура разметки вершин графа G всегда завершается, и полученная при этом стационарная разметка θ_v обладает следующим свойством: граф G является согласованным тогда и только тогда, когда для любой вершины v, которой приписана пара атомарных формул (A'_v, A''_v), соблюдается равенство $A'_v\theta_v = A''_v\theta_v$.*

Доказательство этой теоремы опирается на утверждение 2 и следует схеме доказательства аналогичной теоремы из статьи [3]. Для оценки сложности процедуры вычисления стационарной разметки вершин графа G введем понятеи сложности подстановки. *Сложностью терма* назовем размер минимального АОГ, представляющего этот терм. *Сложностью $|\theta|$ подстановки θ* назовем сумму $N_1 + N_2$, где N_1 — суммарная сложность термов из множества $\{\theta(x) \ : \ x \in \mathcal{X}\}$, а N_2 — количество термов t, удовлетворяющих условию $\exists\, x_1, x_2 \ : \ (x_1 \neq x_2 \ \wedge \ t = \theta(x_1) = \theta(x_2))$.

Утверждение 3. *Если $\theta_0 = \eta\theta_1$, то $|\theta_0| = |\eta| + |\theta_1|$. Если $\theta_0 = \theta_1 \Downarrow \theta_2$ и при этом $\theta_0 \neq \theta_1$, $\theta_0 \neq \theta_2$, то $|\theta_0| < min(|\theta_1|, |\theta_2|)$.*

Из утверждения 3 и описания процедуры вычисления стационарной разметки следуют

Теорема 2. *Если граф G содержит k вершин, полустепень исхода которых не превосходит ℓ, и сложность каждой подстановки, приписанной дугам графа, ограничена величиной m, то стационарная разметка вершин графа G вычислима за время $O(\ell m^3 k^4)$.*

Теорема 3. *Проблема л.-т. эквивалентности стандартных схем программ разрешима за полиномиальное время.*

Список литературы

1. Иткин В. Э. Логико-термальная эквивалентность схем программ // Кибернетика. — 1972. — № 1. — С. 5–27.

2. Sabelfeld V. K. The logic-termal equivalence is polynomial-time deci dable // Inform. Proces. Lett. — 1980. — V. 10, № 2. — P. 57–62.

3. Захаров В. А., Новикова Т. А. Применение алгебры подстановок для унификации программ // Труды Института системного программирования РАН. — 2011. — Т. 21. — С. 162–176.

ОБ ОДНОМ СЕМЕЙСТВЕ ФУНКЦИОНАЛЬНО ПОЛНЫХ В P_k БАЗИСОВ

В. А. Орлов (Москва)

Оптимальная реализация дискретных отображений различными средствами является актуальной областью теоретической и технической кибернетики.

Функция, переменные которой принимают значения из алфавита $A_k = 0, 1, , k-1, k \geq 2$ и которая принимает значения из этого алфавита, называется k-*значной*. Множество всех k-значных функций обозначается через P_k. Функции из P_2 ч асто называют булевыми.

В работе критерием оптимальности схемы считаем сумму весов ее элементов. Эту сумму будем называть *сложностью схемы* S и обозначать через $L(S)$.

С практической точки зрения наиболее востребованной является задача нахождения функционала $L^B(f)$, равного минимальной сложности схем в базисе B, реализующих функцию f. В настоящее время эффективного метода (отличного от перебора схем) решения этой задачи нет. В виду этого часто рассматривают задачу исследования асимптотического поведения функционала $L^B(k, n)$, равного максимуму функционалов $L^B(f)$, где f — функция из P_k^n (множество k-значных функций от переменных $x_1, x_2, \ldots, x_n$). При этом полагают, что k фиксировано, а $n \to \infty$.

Обычно полагают, что функции из P_k^n определены на всех k^n наборах значений их переменных. Однако рассматривают и функции, значения которых на некоторых наборах безразличны. Такие функции называют *не всюду определенными*; при их реализации схемами необходимо полное доопределение. Реализация не всюду определенных *булевых* функций является хорошо исследованной областью синтеза управляющих систем (отметим работы Э. И. Нечипорука, Л. А. Шоломова, А. А. Андреева).

Пусть A^1 и A^2 — подалфавиты алфавита A_k. Функцию, значения аргументов (значения выходов) которой принадлежат A^1 (принадлежат A^2), будем называть (A^1, A^2)-функцией. Пусть $A^b = \{0, 1\}$. (A_k, A^b)-функцию ((A^b, A_k)-функцию) будем называть $(k, 2)$-функцией ($(2, k)$-функцией). При реализации функций из P_k будем допускать и базисы, в которых некоторые элементы реализуют (A^1, A^2)-функции. При этом на схему накладываются дополнительные естественные ограничения: вход элемента E нельзя присоединять к выходу элемента, выходные значения которого могут не принадлежать входному алфавиту элемента E.

Функцию f одного аргумента будем задавать вектором, i-й компонент которого, $0 \le i \le k-1$, равен $f(i)$. Систему $F = \{f_1, f_2, , f_r\}$ $(k,2)$-функций одного аргумента назовем $(k,2)$-*достаточной*, если все столбцы (r,k)-матрицы, строки которой суть векторы функций из F, различны. Отметим, что $r \ge \log_2 k$. Примером $(k,2)$-достаточной является следующая система

$$(0101011), (0011001), (0000111).$$

Пусть F_1 система функций из P_k такая, что с помощью операций суперпозиции над F_1 можно получить: функционально полную систему булевых функций F_1^b, $(k,2)$-достаточную систему функций F_1^2, функцию $f_{2,k}$, которая на булевых наборах значений ее аргументов принимает все значения из алфавита A_k. Нетрудно проверить, что объединение F_1^b и F_1^2 является $(k,2)$-полной системой.

Системе F_1 сопоставим базис B_1. Для простоты изложения будем полагать, что система F_1^b, состоит из функции штрих Шеффера. Пусть E_1 — элемент с двумя входами, реализующий эту функцию и имеющий вес 1. Пусть $E_1^2, E_2^2, \ldots, E_r^2$ суть элементы базиса B_1, реализующие функции из F_1^2 и имеющие вес k. Пусть $E_{2,k}$ — элемент базиса B_1, реализующий функцию $f_{2,k}$ и имеющий равный sk вес (s — число аргументов функции $f_{2,k}$).

Доказано, что базис B_1 функционально полон в P_k.

Исследуем асимптотическое поведение функционала $L^{B_1}(k,n)$. Вначале рассмотрим случай, когда k является степенью 2. Для произвольной функции f из P_k^n построена реализующая ее схема SF, состоящая из трех последовательно соединенных блоков $K2$, BF и $2K$ такая, что $L(SF) \lesssim k^n/n$. Блок $K2$ (блок $2K$) состоит из $(k,2)$ — (из $(2,k)$-функций. Элементы блока BF реализуют булевы функции. Такие схемы назовем 3-уровневыми. В случае, когда k не является степенью 2 можно построить 3-уровневую схему со сложностью асимптотически не превосходящей $(\lceil \log_2 k \rceil / \log_2 k) k^n/n$. Отказавшись от требования 3-уровневости и разлагая функцию f по переменным можно получить (асимптотически наилучшую) оценку k^n/n при любых k.

Список литературы

1. Лупанов О. Б. О синтезе некоторых классов управляющих систем // Проблемы кибернетики. Вып. 10. — М.: Физматгиз, 1963. — С. 3–97.

2. Лупанов О. Б. Об одном подходе к синтезу управляющих систем — принципе локального кодирования // Проблемы кибернетики. Вып. 14. — М.: Физматгиз, 1965. — С. 31–110.

3. Орлов В. А. О реализации k-значных функций схемами из функциональных элементов // Математические заметки. — 1998. — Т. 64, вып. 3. — С. 431–436.

ЧЕМ ПРИВЛЕКАТЕЛЬНЫ АЛГЕБРАИЧЕСКИЕ МОДЕЛИ ПРОГРАММ С ПРОЦЕДУРАМИ

Р. И. Подловченко, А. Э. Молчанов (Москва)

Алгебраические модели программ с процедурами введены в [1] для решения задачи, являющейся центральной в теории схем программ: разрабатывать эквивалентные преобразования программ на их схемах, специально конструируемых для этого.

Опишем, как строятся эти модели вычислений.

Фиксируется базис B, состоящий из элементов четырёх непустых и непересекающихся алфавитов — Y, C, R и P. Элементы первых трех называются символами соответственно операторов, вызовов и возвратов, элементы множества P — логическими переменными.

Схема программы над базисом B представляет собой конечный ориентированный граф с размеченными вершинами и дугами, состоящий из нескольких подграфов. Один из них называется главным, остальные, если они имеются, — подграфами процедур. В каждом подграфе выделены две вершины — вход и выход, не несущие меток. Остальные вершины подграфа помечены элементами базиса и в соответствии с этим называются: операторная вершина, вершина-вызов, вершина-возврат и распознаватель. Из распознавателя исходят две дуги, помеченные числами 0 и 1, из выхода главного подграфа дуги не исходят, остальные вершины, кроме выходов подграфов-процедур, имеют по одной исходящей дуге. Вход главного подграфа не имеет входящих дуг. Вызовы и возвраты находятся во взаимно-однозначном соответствии, составляя пары. Всякой паре присвоен свой номер, и она принадлежит общему для неё подграфу. Дуга из вызова ведёт во вход подграфа-процедуры (своего или чужого), и тогда из выхода этого подграфа исходит дуга, ведущая в парный вызову возврат. Иных дуг, кроме упомянутых, из выхода подграфа-процедуры не исходит. Дуги, исходящие из вершин, отличных от вызова, ведут в вершины того же подграфа, которому принадлежит их начало.

Используем обозначения: $B' = (Y \cup C \cup R)^*$, $X = \{x | x : P \to \{0,1\}\}$; элементы из B' называем операторными цепочками.

Функционирование схемы осуществляется на функциях типа $B' \to X$, они называются функциями разметки и составляют множество $\mathfrak{L}$. Выполнение схемы на функции μ из $\mathfrak{L}$ — это обход схемы, сопровождающийся построением операторной цепочки. Для детерминированности обхода, кроме μ, используется магазин, в который загружаются номера пар вызов-возврат. Обход начинается по дуге из входа главного подграфа при пустых магазине и операторной цепочке. Переход через вершину с символом сопровождается приписыванием его к текущей операторной цепочке. Если переходимая вершина — вызов, то в магазин загружается его номер. При переходе через выход подграфа-процедуры извлекается номер из магазина, и обход продолжается по дуге, ведущей к возврату с этим номером. При переходе через распознаватель с переменной p обход продолжается по дуге с меткой $\mu h(p)$, где h — текущая цепочка. Обход схемы прекращается при достижении выхода главного подграфа, и тогда текущая цепочка называется результатом выполнения схемы на μ; в ином случае выполнение безрезультатно.

Таким образом, всякая схема над базисом B осуществляет отображение множества $\mathfrak{L}$ в множество B'.

Все алгебраические модели программ с процедурами имеют одно и то же множество схем программ над B и отличаются друг от друга отношением эквивалентности схем. Оно вводится параметрическим образом. Пусть ν — эквивалентность в B', и $L \subseteq \mathfrak{L}$. Две схемы над B назовем (ν, L)-эквивалентными, если, какой бы ни была функция μ из L, результативное выполнение на ней одной из схем означает результативное выполнение на μ другой схемы, и результаты их выполнения ν-эквивалентны. С введением (ν, L)-эквивалентности возникает отдельная алгебраическая модель программ с процедурами, называемая (ν, L)-моделью.

В теории алгебраических моделей программ фундаментальной является задача построения системы э. п., полной в модели, т. е. обладающей свойством: для любых эквивалентных схем из модели возможно эффективное построение конечной цепочки э.п. из данной системы, трансформирующей одну из схем в другую. Эта задача выдвигает проблему эквивалентности в модели, т. е. построение алгоритма, распознающего эквивалентность схем в модели.

Остановимся на том, чем привлекательны алгебраические модели программ с процедурами.

1. Они построены для формализации программы, естественным образом абстрагирующейся от программы, записанной на импера-

тивном алгоритмическом языке программирования [1].

2. Переход от программы к её схеме обладает свойством: всякое структурное преобразование схемы одновременно является структурным преобразованием моделируемой ею программы.

3. Выделены аппроксимирующие модели программ, т.е. обладающие свойством: из эквивалентности схем программ в такой модели следует эквивалентность моделируемых ими программ [2].

4. Частным случаем моделей программ с процедурами являются модели программ без процедур, для которых разработаны два метода распознавания эквивалентности в модели [3, 4] и один метод построения системы э.п., полной в модели.

5. Описано в [2] множество аппроксимирующих моделей программ с процедурами, так называемые перегородчатые модели программ, для которых нами установлено следующее: проблема эквивалентности в перегородчатой модели программ сводится к решению двух проблем в индуцирующей её модели программ без процедур: проблеме эквивалентности и проблеме непустоты пересечения.

В связи с изложенным, актуальными и вместе с тем перспективными являются исследования семантических свойств алгебраических моделей программ с процедурами.

Список литературы

1. Подловченко Р. И. Рекурсивные программы и иерархия их моделей // Программирование. — 1991. — № 6. — С. 44–51.

2. Подловченко Р. И. От схем Янова к теории моделей программ // Математические вопросы кибернетики. — 1998. — Вып. 7. — С. 281–302.

3. Подловченко Р. И. Об одной методике распознавания эквивалентности в алгебраических моделях программ // Программирование. — 2011. — № 6. — С. 33–43.

4. Захаров В. А. Проверка эквивалентности программ при помощи двухленточных автоматов // Кибернетика и системный анализ. — 2010. — № 4. — С. 39–48.

ЧАСТИЧНО КОММУТАТИВНЫЕ МОДЕЛИ ПРОГРАММ

Р. И. Подловченко, Д. В. Скрынников (Москва)

Частично коммутативные модели программ — это частный случай широкого класса алгебраических моделей программ, для которых получены следующие результаты: доказана разрешимость проблемы эквивалентности и построены полные системы эквивалентных преобразований (э.п.).

Общего вида алгебраические модели программ введены в [1], а упомянутый их широкий класс исследован в [2–3]. Эти модели называются уравновешенными полугрупповыми моделями с левым сокращением. Данный доклад посвящен адаптации к частично коммутативным моделям результатов, о которых сказано выше. В нем описываются приемлемые по сложности алгоритмы, разрешающие эквивалентность в таких моделях, а приведением к канонической форме схем программ из этих моделей созданы полные в моделях системы э.п. Продемонстрировано, что сложность приведения существенно меньше общего случая.

Здесь исследуется фактически подмодель частично коммутативной модели. Основанием тому служат следующие факты, установленные в [2–4]: проблема эквивалентности в любой алгебраической модели программ сводится к проблеме эквивалентности матричных схем из этой модели; построена система э.п., в рамках которой осуществляется это сведение. Поэтому рассматривается подмодель, элементами которой являются матричные схемы, и строится система э.п., полная в этой подмодели. Обозначим ее $\mathcal{M}$.

Подмодель $\mathcal{M}$ строится над конечными алфавитами Y и P; элементы из Y называются операторными символами, а элементы из P — логическими переменными; каждая из них принимает значение из множества $\{0,1\}$.

Матричная схема над Y, P представляет собой конечный ориентированный граф, удовлетворяющий требованиям: в нём имеются три выделенные вершины — вход, выход, и loop; каждой из других вершин (они называются преобразователями) сопоставлен символ из Y; из любой вершины графа, кроме выхода и loop, исходят дуги в количестве, равном числу элементов в множестве X, где $X = \{x|x : P \to \{0,1\}\}$; всякая дуга помечена элементом x из X; любые две дуги из одной вершины имеют различные метки.

Функционирование матричной схемы (далее — просто схемы), осуществляется на отображениях множества Y^* (его элементы называются операторными цепочками) в множество X; эти отображения именуются функциями разметки; их множество обозначается $\mathfrak{L}$.

Пусть G — схема над Y, P и $\mu \in \mathfrak{L}$. Выполнение схемы G на μ представляет собой обход схемы, который начинается во входе схемы при пустой операторной цепочке и подчиняется следующим правилам. Пусть v — достигнутая вершина схемы, и h — цепочка, с которой пришли в v; если v — преобразователь с символом y, то текущая цепочка h преобразуется в цепочку hy, и переход из v осуществляется по дуге с меткой $\mu(hy)$; если v — выход схемы или вершина loop, то обход схемы прекращается, в первом случае — с результатом h, и во втором случае — безрезультатно. Таким образом, схемой G реализуется отображение множества $\mathfrak{L}$ в множество Y^*, частичное в общем случае.

Эквивалентность схем над Y, P индуцируется двумя параметрами — ν и L, где ν — это эквивалентность в Y^*, а $L \subseteq \mathfrak{L}$. Две схемы, по определению, (ν, L)-эквивалентны, если, какой бы ни была функция разметки μ из L, всякий раз, когда выполнение на μ одной из схем результативно, результативно и выполнение другой схемы на μ, и при этом полученные результаты — это ν-эквивалентные цепочки.

В случае подмодели $\mathcal{M}$ параметры ν и L задаются следующим образом. Эквивалентность ν индуцируется системой T, где $T \subseteq Y \times Y$; символы y_1, y_2, где $(y_1, y_2) \in T$, называются перестановочными; ν-эквивалентными объявляются равновеликие по длине операторные цепочки, одна из которых может быть получена из другой перестановками соседних и перестановочных символов. Множество L состоит из всех функций разметки, обладающих свойством: ν-эквивалентным цепочкам функция сопоставляет равные значения.

Используем алгоритм τ, распознающий эквивалентность матричных схем и описанный в [2]. Он строит для испытуемых схем сочетаемые в них маршруты, длина которых ограничивается числом, зависящим от размеров схем.

Маршрутом в схеме называется ориентированный путь в ней с началом во входе. Всякому конечному маршруту соответствует несомая им операторная цепочка, а сочетаемыми именуются маршруты, прокладываемые общей для них функцией разметки из L. Имеется критерий сочетаемости маршрутов, на основе которого работает алгоритм, реализующий продолжение сочетаемых маршрутов с сохранением свойства сочетаемости.

При построении сочетаемых маршрутов алгоритм τ проверяет необходимые условия эквивалентности схем из $\mathcal{M}$. Наиболее ёмким из них является следующее условие: из сопряжённых преобразователей, помеченных различающимися символами, вырастают сопряжённые кусты. Сопряжёнными называются концы сочетаемых маршру-

тов, несущих ν-эквивалентные операторные цепочки.

При адаптации алгоритма τ к случаю подмодели $\mathcal{M}$ нами построены алгоритмы ρ_1 и ρ_2, выявляющие, действительно ли из сопряжённых вершин с разными метками вырастают сопряжённые кусты. Алгоритм ρ_1 применяется в случае, когда перестановочность символов, задаваемая системой T, является транзитивной. В противном случае применяется алгоритм ρ_2. Для обоих алгоритмов даны оценки их временной сложности; они полиномиальны.

Построение системы э.п., полной в $\mathcal{M}$, проведено методом, разработанным в [3]. Согласно ему, конструируется алгоритм, приводящий каждую из двух эквивалентных схем к каноническому виду; последний подобен конечному минимальному автомату. Параллельно с этим выявляются аксиомы, реализующие действие алгоритма. Именно они и индуцируют полную в $\mathcal{M}$ систему э.п.

Список литературы

1. Подловченко Р. И. Иерархия моделей программ // Программирование. — 1981. — № 2. — С. 3–14.

2. Подловченко Р. И. Техника следов в разрешении проблемы эквивалентности в алгебраических моделях программ // Кибернетика и системный анализ. — 2009. — № 5. — С. 25–37.

3. Подловченко Р. И. Полные системы эквивалентных преобразований в уравновешенных полугрупповых моделях программ с левым сокращением // Программирование. — 2010. — № 3. — С. 3–18.

ОБ ЭКВИВАЛЕНТНОСТИ МЕТАЛИНЕЙНЫХ УНАРНЫХ РЕКУРСИВНЫХ ПРОГРАММ

В. В. Подымов, В. А. Захаров (Москва)

Проблема эквивалентности программ состоит в том, чтобы для заданной пары программ выяснить, имеют ли они одинаковое поведение. В качестве формализации понятия программы мы используем модель рекурсивных программ, описанную в статье [1]. В статье [2] была доказана эффективная разрешимость проблемы эквивалентности линейных унарных рекурсивных программ с использованием метода совместных вычислений. Цель данной работы состоит в обобщении предложенного метода для эффективной проверки сильной эквивалентности металинейных унарных рекурсивных программ.

Записью Σ^* обозначим множество слов в алфавите Σ, включая пустое слово λ. Записью $|h|$ будем обозначать длину слова h, полагая $|\lambda| = 0$. Записями $pref(h, n)$, $suf(h, n)$ будем обозначать, соответственно, максимальный префикс и максимальный суффикс слова h, длина которых не превосходит n.

Считаем заданными конечные алфавиты *операторов* $\mathfrak{A}$ и *предикатов* $\mathfrak{C}$, счетно-бесконечный алфавит *заголовков* $\mathfrak{F}$, множество *термов* $Term = (\mathfrak{A} \cup \mathfrak{F})^*$ и множество *базовых термов* $BTerm = \mathfrak{A}^*$.

Унарной рекурсивной программой будем называть систему $\pi = (t_0, F, D)$, где $t_0 \in Term \setminus \{\lambda\}$ — запрос, $F \subset \mathfrak{F}$ — конечное множество заголовков программы, $D : F \times \mathfrak{C} \to Term \cup \{\perp\}$ — описание функций (здесь $\perp$ — неопределенное значение). Унарная рекурсивная программа называется *металинейной* (для краткости — просто программой), если каждый терм из области значений функции D имеет вид tft', где $t, t' \in BTerm$, $f \in \mathfrak{F} \cup \{\lambda\}$. *Сложность* программы π характеризуется парой $|\pi| = (|t_0|, \sum_{f \in F, \delta \in \mathfrak{C}} |D(f, \delta)|)$.

Терм $wD(f, \delta)w'$, где $w \in BTerm$, $f \in \mathfrak{F}$, $\delta \in \mathfrak{C}$, будем называть *δ-преемником* терма wfw'. Базовый терм t' будем называть *раскрытием* терма t, если найдется последовательность термов $t_1, t_2, \ldots, t_n$, в которой $t_1 = t$, $t_n = t'$ и каждый терм t_{i+1} является преемником терма t_i, $1 \leq i < n$. Заголовок считается *завершаемым*, если существует хотя бы одно его раскрытие. Не умаляя общности, ограничимся рассмотрением программ $\pi = (t_0, F, D)$, в которых 1) $t_0 \in F^*$, 2) для любых $f \in F$, $\delta \in \mathfrak{C}$ верно $D(f, \delta) \in \{afh \mid a \in \mathfrak{A}, f \in F, h \in BTerm\} \cup \{\perp\}$, и 3) все заголовки из F являются завершаемыми.

Вычисление программы π — это непродолжаемая последовательность термов, в которой первым термом является запрос программы и каждый следующий терм является преемником предыдущего. Результатом конечного вычисления, оканчивающегося базовым термом, объявляется этот терм. Остальные вычисления безрезультатны.

Вычисления $T' = t'_1, t'_2, \ldots$ и $T'' = t''_1, t''_2, \ldots$ программ π_1, π_2 назовем *совместными* в том случае, когда для любой пары термов $t'_i = h'_i f'_i g'_i$ и $t''_j = h''_j f''_j g''_j$, входящих в состав вычислений T' и T'', где $h'_i, h'_j \in BTerm$, $f'_i, f''_j \in \mathfrak{F}$, выполняется следующее требование: если вычисления T' и T'' не оканчиваются термами t'_i и t''_j и $h'_i = h''_j$, то термы t'_{i+1} и t''_{j+1}, следующие за термами t'_i и t''_j соответственно в вычислениях T' и T'', являются δ-преемниками термов t'_i и t''_j для одного и того же предиката δ. Программы π_1, π_2 будем называть

сильно эквивалентными (и обозначать этот факт записью $\pi_1 \sim \pi_2$), если любые их совместные вычисления имеют одинаковый результат.

Весом терма t в программе π назовем число $\|t\|_\pi$ (или $\|t\|$, если программа ясна из контекста), которое определяется следующими соотношениями: 1) $\|\lambda\|_\pi = 0$; 2) $\|a\|_\pi = 1$, если $a \in \mathfrak{A}$; 3) $\|f\|_\pi$ есть наименьшая длина раскрытий заголовка f; 4) $\|t_1 t_2\|_\pi = \|t_1\|_\pi + \|t_2\|_\pi$.

Опишем *граф совместных вычислений* G_{π_1,π_2} программ $\pi_1 = (f_1 h_1, F_1, D_1)$, $\pi_2 = (f_2 h_2, F_2, D_2)$. Его вершинами являются наборы

$$(G_1, G_2, R_1, R_2, u_1, u_2, w_1, w_2), \qquad (1)$$

где $G_i \in \mathfrak{F} \cup \{\lambda\}$, $R_i \in \mathfrak{F}^*$, $u_i, w_i \in BTerm$, $i \in \{1,2\}$. В графе также выделены отличные от описанных вершины v_∞, v_{inf}. Вершина $(f_1, f_2, h_1, h_2, \lambda, \lambda, \lambda, \lambda)$ считается корневой.

Метки дуг, исходящих из вершины (1), различны и образуют множество: $\{(\delta,\delta)|\delta \in \mathfrak{C}\}$, если $G_1, G_2 \in \mathfrak{F}$; $\{(\varepsilon,\delta)|\delta \in \mathfrak{C}\}$, если $G_1 = \lambda$; $\{(\delta,\varepsilon)|\delta \in \mathfrak{C}\}$, если $G_2 = \lambda$. Из остальных вершин не исходит ни одной дуги. Для упрощения обозначений будем полагать, что $D_i(\lambda,\varepsilon) = \lambda$.

Дуга, исходящая из вершины (1) и помеченная парой (d_1, d_2), ведет в вершину v', описываемую следующим образом. Если $D_1(G_1, d_1) = D_2(G_2, d_2) = \perp$, то $v' = v_{inf}$. Если $D_{3-i}(G_{3-i}, d_{3-i}) \neq D_i(G_i, d_i) = \perp$ или $\|D_1(G_1, d_1)\| - \|D_2(G_2, d_2)\| \neq \|G_1\| - \|G_2\|$, то $v' = v_\infty$. Иначе считаем, что $D_i(G_i, d_i) = a_i G_i' t_i$, где $a_i \in \mathfrak{A}$, $G_i' \in \mathfrak{F} \cup \{\lambda\}$, $t_i \in BTerm$ ($D_i(G_i, d_i) = G_i' = \lambda$, если $d_i = \varepsilon$).

Если $d_1 = d_2 \in \mathfrak{C}$ и $\|G_j\| \leq \|G_{3-j}\|$, то поверяются следующие условия: $a_1 = a_2$; $\exists h : h_j h = h_{3-j}$, где $h_i = suf(t_i u_i, |t_i u_i| + \|G_i'\| - \|G_{3-i}'\|)$, $i \in \{1,2\}$. Если хотя бы одно из условий не выполнено, то $v' = v_\infty$. Иначе $u_i' = pref(t_i u_i, \|G_{3-i}'\| - \|G_i'\|)$ и $w_i' = suf(t_i w_i, \|R_{3-i}\| - \|R_i\|)$, $i \in \{1,2\}$.

Если $d_{3-i} = \varepsilon$, то проверяется следующее условие: $\exists h : u_{3-i} = a_i h t_i$. Если оно не выполнено, то $v' = v_\infty$. Иначе $u_i' = \lambda$, $u_{3-i}' = h$, $w_i' = suf(t_i w_i, \|R_{3-i}\| - \|R_i\|)$, $w_{3-i}' = w_{3-i}$.

Вершина $v' = (G_1'', G_2'', R_1'', R_2'', u_1'', u_2'', w_1'', w_2'')$ определяется следующим образом.

Если $G_i' = \lambda$, $G_{3-i}' \neq \lambda$ и $u_i' = \lambda$, то $G_i'' = f_i$, $G_{3-i}'' = G_{3-i}'$, $R_{3-i}'' = R_{3-i}$, $u_i'' = \lambda$, $u_{3-i}'' = pref(w_{3-i}', \|G_i''\| - \|G_{3-i}''\|)$, $w_i'' = \lambda$, $w_{3-i}'' = suf(w_{3-i}', |w_{3-i}'| - |u_{3-i}''|)$, где $R_i = f_i R_i''$.

Если $G_1' = G_2' = \lambda$ и для некоторого i верно $w_i' \neq \lambda$, то $G_i'' = \lambda$, $G_{3-i}'' = f_{3-i}$, $R_i'' = R_i$, $u_i'' = pref(w_i', \|G_{3-i}''\|)$, $u_{3-i}'' = \lambda$, $w_i'' = suf(w_i', |w_i'| - |u_i''|)$, $w_{3-i}'' = \lambda$, где $R_{3-i} = f_{3-i} R_{3-i}''$, $f_{3-i} \in \mathfrak{F}$.

Если $R_1 \neq G'_1 = G'_2 = w'_1 = w'_2 = \lambda$, то $v' = (f_1, f_2, R'_1, R'_2, \lambda, \lambda, \lambda, \lambda)$, где $R_i = f_i R'_i$, $f_i \in \mathfrak{F}$, $i \in \{1, 2\}$.

В остальных случаях $v' = (G'_1, G'_2, R_1, R_2, u'_1, u'_2, w'_1, w'_2)$.

Теорема 1. *$\pi_1 \nsim \pi_2$ тогда и только тогда, когда из корня графа G_{π_1,π_2} достижима вершина $v_\nsim$.*

Лемма. *Если из корня графа G_{π_1,π_2} достижимы различные вершины с одинаковыми первыми четырьмя компонентами, то $\pi_1 \nsim \pi_2$.*

Алгоритм проверки эквивалентности программ π_1, π_2, где $|\pi_i| = (k_i, n_i)$, $i \in \{1, 2\}$, состоит в построении связного подграфа графа G_{π_1,π_2}, содержащего корень графа. Если на очередном шаге построения была добавлена вершина $v_\nsim$ или число вершин превысило величину $k^2 n^3$, где $k = max\{k_1, k_2\}$, $n = max\{n_1, n_2\}$, то $\pi_1 \nsim \pi_2$. Иначе, если нельзя добавить ни одной вершины, то $\pi_1 \sim \pi_2$.

Теорема 2. *Проблема сильной эквивалентности металинейных унарных рекурсивных программ разрешима за полиномиальное время.*

Список литературы

1. Garlend S. J., Luckham D. C. Program schemes, recursion schemes and formal languages // Journal of Computer and System Science. — 1973. — V. 7, № 2. — P. 119–160.

2. Подымов В. В. Алгоритм проверки эквивалентности линейных унарных рекурсивных программ на упорядоченных полугрупповых шкалах // Вестн. Моск. ун-та. Сер. 15. Вычислительная математика и кибернетика. — 2012. — № 4.

ОБ ОЦЕНКАХ ФУНКЦИИ ШЕННОНА ДЛИНЫ ЕДИНИЧНОГО ПРОВЕРЯЮЩЕГО ТЕСТА ОТНОСИТЕЛЬНО ПРОИЗВОЛЬНЫХ КОНСТАНТНЫХ НЕИСПРАВНОСТЕЙ НА ВЫХОДАХ ЭЛЕМЕНТОВ

Д. С. Романов (Москва)

Пусть $f(\tilde{x}^n)$ — произвольная булева функция, формально зависящая от переменных $x_1, x_2, \ldots, x_n$, а S — схема из функциональных элементов в некотором базисе B, реализующая функцию f (все определения, не введенные в данной работе, можно найти в монографии [1]). Пусть на схему S действует источник одиночных неисправностей U, вызывающий инверсные или константные неисправности на

выходах функциональных элементов, то есть на выходе любого не более чем одного функционального элемента схемы вместо реализуемой на его выходе функции от его входов может реализовываться либо отрицание этой функции (случай инверсной неисправности), либо произвольная булева константа (случай константной неисправности). *Тривиальной* будем называть такую неисправность схемы S, при которой значение на выходе любого элемента E схемы S на всяком входном наборе равно значению на выходе элемента E при исправной работе схемы S. При этом мы для простоты будем считать, что тривиальная неисправность единственна. Неисправности, не являющиеся тривиальными, будем называть *нетривиальными*. Обозначим через $W(S)$ множество всех попарно неравных функций, каждая из которых может быть реализована схемой S в результате нетривиальной неисправности, вызванной действием на схему источника неисправностей U. Схема S называется *неизбыточной* тогда и только тогда, когда для любой функции $g(\tilde{x}^n) \in W(S)$ справедливо: $f(\tilde{x}^n) \not\equiv g(\tilde{x}^n)$. Множество T наборов значений переменных $x_1, x_2, \ldots, x_n$ называется *единичным проверяющим тестом для схемы S относительно инверсных и константных неисправностей на выходах элементов* тогда и только тогда, когда для любой функции $g \in W(S)$ такой, что $g(\tilde{x}^n) \not\equiv f(\tilde{x}^n)$, найдется набор $\tilde{\alpha}$ из T, для которого выполнено неравенство $f(\tilde{\alpha}) \neq g(\tilde{\alpha})$. Количество различных наборов в тесте T называется его *длиной* и обозначается через $l(T)$ или через $|T|$. Тест минимальной длины называется *минимальным*. Обозначим через $D(S)$ длину минимального единичного проверяющего теста относительно инверсных и константных неисправностей на выходах элементов в схеме S, через $D_B(f(\tilde{x}^n))$ — минимум величины $D(S)$ по всем неизбыточным реализующим $f(\tilde{x}^n)$ схемам S в базисе B. При этом будем считать, что если для какой-то функции f не существует неизбыточных схем, ее реализующих, то $D_B(f) = 0$. Пусть $\hat{P}_2^n$ — множество всех булевых функций, существенно зависящих от всех своих переменных $x_1, \ldots, x_n$. Через $D_B(n)$ обозначим *функцию Шеннона длины единичного проверяющего теста относительно инверсных и константных неисправностей на выходах элементов*, т. е. функцию $D_B(n) = \max\limits_{f(\tilde{x}^n) \in \hat{P}_2^n} D_B(f(\tilde{x}^n))$.

В [2] было доказано, что при $B = \{x\&y, x \oplus y, 1\}$ $D_B(n) \leqslant n+3$. В [3] было установлено, что в стандартном базисе $B_0 = \{x\&y, x \vee y, \bar{x}\}$ функция Шеннона длины полного проверяющего теста относительно однотипных константных неисправностей на выходах элементов не превосходит n, а в [4] показано, что функция Шеннона дли-

ны полного проверяющего теста относительно произвольных константных неисправностей на выходах элементов при всех натуральных n не превосходит $O(2^{n/2})$. В [5] установлено, что в случае $B = \{x\&y, x \oplus y, 1\}$ функция Шеннона длины единичного проверяющего теста относительно инверсных неисправностей на выходах элементов равна 1; в [6] доказано, что в произвольном полном базисе аналогичная функция Шеннона не превосходит 3. В [7] установлено, что в стандартном базисе B_0 функция Шеннона длины полного проверяющего теста относительно однотипных константных неисправностей на выходах элементов равна 2, в [8] доказано, что функция Шеннона длины единичного проверяющего теста относительно константных неисправностей типа 1 на выходах элементов в базисе Жегалкина равна 1, в [9] получено, что функция Шеннона длины полного проверяющего теста относительно константных неисправностей типа 0 на выходах элементов в базисе Жегалкина равна 1. В [10] опубликована формулировка и идея доказательства теоремы о том, что для любого $n \in \mathbb{N}$ в произвольном полном базисе функция Шеннона длины единичного проверяющего теста относительно произвольных константных неисправностей на выходах элементов не превосходит $n + 3$.

В настоящей работе установлена

Теорема. *Для произвольного полного базиса B при $n \in \mathbb{N}$ имеют место неравенства $2 \leqslant D_B(n) \leqslant 4$.*

Работа выполнена при финансовой поддержке грантов РФФИ № 12-01-00964 и № 10-01-00768.

Список литературы

1. Редькин Н. П. Надежность и диагностика схем. — М.: Изд-во МГУ, 1992.

2. Reddy S. M. Easily testable realization for logic functions // IEEE Trans. Comput. — 1972. — V. 21, № 1. — P. 124–141.

3. Редькин Н. П. О схемах, допускающих короткие тесты // Вестник Моск. ун-та. Серия 1. Матем. Механика. — 1988. — № 2. — С. 17–21.

4. Редькин Н. П. О полных проверяющих тестах для схем из функциональных элементов // Математические вопросы кибернетики. Вып. 2. — М.: Наука, 1989. — С. 198–222.

5. Коваценко С. В. Синтез легкотестируемых схем в базисе Жегалкина для инверсных неисправностей // Вестник Моск. ун-та. Серия 15. Вычислит. матем. и киберн. — 2000. — № 2. — С. 45–47.

6. Редькин Н. П. Единичные проверяющие тесты для схем при инверсных неисправностях элементов // Математические вопросы

кибернетики. Вып. 12. — М.: Физматлит, 2003. — С. 217–230.

7. Бородина Ю. В. О синтезе легкотестируемых схем в случае однотипных константных неисправностей на выходах элементов // Вестник Моск. ун-та. Серия 15. Вычислит. матем. и киберн. — 2008. — № 1. — С. 40–44.

8. Бородина Ю. В. О схемах, допускающих единичные тесты длины 1 при константных неисправностях на выходах элементов // Вестник Моск. ун-та. Серия 1. Матем. Механика. — 2008. — № 5. — С. 49–52.

9. Бородина Ю. В., Бородин П. А. Синтез легкотестируемых схем в базисе Жегалкина при константных неисправностях типа "0" на выходах элементов // Дискретная математика. — 2010. — Т. 22, № 3. — С. 127–133.

10. Коляда С. С. О единичных проверяющих тестах для схем из функциональных элементов // Проблемы теоретической кибернетики. Материалы XVI Международной конференции (Нижний Новгород, 20–25 июня 2011 года). — Нижний Новгород: Издательство Нижегородского университета, 2011. — С. 209–211.

О ТЕСТАХ ОТНОСИТЕЛЬНО СДВИГОВ ПЕРЕМЕННЫХ В БУЛЕВЫХ ФУНКЦИЯХ

Д. С. Романов, Г. В. Антюфеев (Москва)

Пусть $f(x_1, x_2, \ldots, x_n)$ — булева функция, формально зависящая от переменных $x_1, x_2, \ldots, x_n$ (это будет записываться так: $f(\tilde{x}^n) \in P_2^n$), E_2^k — множество всех k-разрядных двоичных наборов. Рассмотрим источник неисправностей U_n^{shifts}, способный действовать на булеву функцию $f(x_1, \ldots, x_n)$ следующим образом. Источником выбираются (произвольным образом) число $k \in \{1, \ldots, n\}$ и набор $\tilde{\gamma} = (\gamma_1, \ldots, \gamma_n) \in E_2^n$, и вместо значения функции $f(\alpha_1, \ldots, \alpha_k, \alpha_{k+1}, \ldots, \alpha_n)$ вычисляется значение $f(\alpha_{k+1}, \ldots, \alpha_n, \gamma_1, \ldots, \gamma_k)$ (то есть функцией неисправности будет функция $f_{k,\bar{\gamma}}(x_1, \ldots, x_n) = f(x_{k+1}, \ldots, x_n, \gamma_1, \ldots, \gamma_k)$). Определим $W_f = \{f_{k,\bar{\gamma}}(x_1, x_2, \ldots, x_n) \mid k \in \{1, 2, \ldots, n\},\ \tilde{\gamma} = (\gamma_1, \ldots, \gamma_n) \in E_2^n\}$. Назовем такой источник неисправностей U_n^{shifts} *источником примитивных сдвигов переменных влево*.

Множество T наборов значений переменных $x_1, x_2, \ldots, x_n$ называется *полным проверяющим (соответственно, диагностическим)*

тестом относительно примитивных сдвигов переменных функции f *влево* тогда и только тогда, когда для любой функции $g \in W_f$ такой, что $g(\tilde{x}^n) \not\equiv f(\tilde{x}^n)$, найдется набор $\tilde{\alpha}$ из T, для которого выполнено неравенство $f(\tilde{\alpha}) \neq g(\tilde{\alpha})$ (соответственно, для любых двух неравных функций g, h из $W_f \cup \{f\}$, найдется набор $\tilde{\alpha}$ из T, для которого выполнено неравенство $g(\tilde{\alpha}) \neq h(\tilde{\alpha})$). Количество различных наборов в тесте T называется его *длиной* и обозначается через $L(T)$ или через $|T|$. Тест минимальной длины называется *минимальным*. Обозначим через $L^{\text{shifts, detect}}(f(\tilde{x}^n))$ (соответственно, через $L^{\text{shifts, diagn}}(f(\tilde{x}^n))$) длину минимального полного проверяющего (соответственно, диагностического) теста относительно примитивных сдвигов переменных функции $f(x_1, x_2, \ldots, x_n)$ влево.

Определим *функции Шеннона длины полного проверяющего и диагностического теста относительно примитивных сдвигов переменных влево*:

$$L^{\text{shifts, detect}}(n) = \max_{f(\bar{x}^n) \in P_2^n} L^{\text{shifts, detect}}(f(\tilde{x}^n)),$$

$$L^{\text{shifts, diagn}}(n) = \max_{f(\bar{x}^n) \in P_2^n} L^{\text{shifts, diagn}}(f(\tilde{x}^n)).$$

Теорема 1. *При* $n \in \mathbb{N}$ *имеет место равенство*

$$L^{\text{shifts, detect}}(n) = 2.$$

Доказательство. Рассмотрим произвольную функцию $f(\tilde{x}^n) \in P_2^n$. Заметим, что если эта функция тождественно равна константе, то никакие примитивные сдвиги переменных влево не обнаруживаются, длина проверяющего теста в этом случае равна нулю. Будем, далее, считать, что у функции $f(\tilde{x}^n)$ есть хотя бы одна существенная переменная. Пусть x_q — существенная переменная с минимальным индексом. Тогда составим множество T из произвольной пары n-разрядных двоичных наборов $\tilde{\beta}' = (\beta_1, \ldots, \beta_{q-1}, 0, \beta_{q+1}, \ldots, \beta_n)$ и $\tilde{\beta}'' = (\beta_1, \ldots, \beta_{q-1}, 1, \beta_{q+1}, \ldots, \beta_n)$, отличающихся лишь значениями переменной x_q и таких, что $f(\tilde{\beta}') \neq f(\tilde{\beta}'')$. Докажем, что T — полный проверяющий тест относительно примитивных сдвигов переменных функции $f(x_1, x_2, \ldots, x_n)$ влево. Поскольку при произвольных $k \in \{1, \ldots, n\}$ и $\tilde{\gamma} = (\gamma_1, \ldots, \gamma_n) \in E_2^n$ функция $f_{k,\tilde{\gamma}}(x_1, \ldots, x_n) = f(x_{k+1}, \ldots, x_n, \gamma_1, \ldots, \gamma_k)$ существенно от переменной x_q не зависит (в силу выбора x_q), то $f_{k,\tilde{\gamma}}(\tilde{\beta}') = f_{k,\tilde{\gamma}}(\tilde{\beta}'')$, и, значит, оба этих значения отличаются от одного из значений $f(\tilde{\beta}')$ и $f(\tilde{\beta}'')$, откуда следует

верхняя оценка $L^{\text{shifts, d}}(n) \leq 2$. Нижняя оценка мгновенно получается из того, что полный проверяющий тест относительно примитивных сдвигов переменных функции $f_0(x_1, x_2, \ldots, x_n) = x_1$ влево не может состоять из одного набора. Теорема 1 доказана.

Теорема 2. *При $n \to \infty$, $n \in \mathbb{N}$ имеет место равенство* $L^{\text{shifts, diagn}}(n) = \Theta(\sqrt{2^n})$.

Доказательство. Верхняя оценка. Положим $k' = \lfloor \frac{n-1}{2} \rfloor$. Легко видеть, что для любых $k \in \{k', k'+1, \ldots, n\}$ набора $\tilde{\gamma} = (\gamma_1, \ldots, \gamma_n) \in E_2^n$ и набора $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_n) \in E_2^n$ значение $f_{k,\tilde{\gamma}}(\tilde{\alpha})$ равно значению $f_{k,\tilde{\gamma}}(\tilde{0}^{k'}, \alpha_{k'+1}, \ldots, \alpha_n)$. Поэтому все эти функции неисправности $f_{k,\tilde{\gamma}}$ попарно отличаются друг от друга (в случае неравенства) на наборах вида $(\tilde{0}^{k'}, \alpha_{k'+1}, \ldots, \alpha_n)$, а число этих наборов есть $O(\sqrt{2^n})$. Количество остальных попарно неравных функций из $W_f \cup \{f\}$ есть $O(\sqrt{2^n})$, поэтому их можно отличить друг от друга и от всех упомянутых ранее функций на $O(\sqrt{2^n})$ наборов. Верхняя оценка доказана.

Нижняя оценка. Рассиотрим (пользуясь идеей из [1], см. также сноску в [1]) функцию

$$h(\tilde{x}^n) = \bigvee_{(\sigma_1, \ldots, \sigma_{k'}) \in E_2^{k'}} x_1^{\sigma_1} x_2^{\sigma_2} \& \ldots \& x_{k'}^{\sigma_{k'}} x_{k'+1}^{\sigma_1} \& \ldots \& x_{2k'}^{\sigma_{k'}} x_{2k'+1} \& \ldots \& x_n.$$

Ясно, что $h(\tilde{x}^n) \not\equiv 0$ и что среди функций из W_h есть тождественный нуль. Замечая, что при $\tilde{\gamma} = (\gamma_1, \ldots, \gamma_{k'}, \tilde{1}^{n-k'})$ функция $h_{k',\tilde{\gamma}}(\tilde{x}^n)$ отличается от тождественного нуля только на наборах вида $(\alpha_1, \ldots, \alpha_{n-k'}, \gamma_1, \ldots, \gamma_{k'})$, делаем вывод, что в любой диагностический тест для функции h должен войти хотя бы один набор такого вида для каждого набора $\tilde{\gamma} = (\gamma_1, \ldots, \gamma_{k'}, \tilde{1}^{n-k'})$, откуда и вытекает нижняя оценка. Теорема 2 доказана.

Работа выполнена при финансовой поддержке грантов РФФИ № 10-01-00768 и № 12-01-00964.

Список литературы

1. Носков В. Н. Диагностические тесты для входов логических устройств // Дискретный анализ. Вып. 26. — Новосибирск: ИМ СО АН СССР, 1974. — С. 72–83.

АСИМПТОТИКА ФУНКЦИИ ШЕННОНА ДЛЯ НАКОПЛЕННОГО ВЕТВЛЕНИЯ СХЕМ ИЗ ФУНКЦИОНАЛЬНЫХ ЭЛЕМЕНТОВ

А. О. Стариков (Москва)

Среди характеристик, оценивающих сложность синтезируемых схем из функциональных элементов (СФЭ), выделяются две основные группы. Первая группа — это характеристики, связанные с размерами схемы, как, например, классическая сложность — количество элементов в схеме [1]. Асимптотика функции Шеннона для количества элементов в схеме в стандартном базисе была найдена О. Б. Лупановым в работе [2]. Вторая группа — «глубинные» характеристики, оценивающие время прохождения сигнала через схему. Асимптотика функции Шеннона для глубины схемы в конечном базисе была найдена О. Б. Лупановым в работе [3], в бесконечном базисе — О. М. Касим-Заде в работе [4].

С физической точки зрения глубина учитывает сумму времен срабатывания логических ячеек вдоль пути от входа до выхода схемы. Однако, кроме ячейки в задержку сигнала схемой вносит вклад и задержка распространения сигнала по проводникам, и с уменьшением норм техпроцесса эта задержка имеет все большую величину [5]. Это дает повод рассмотреть «глубинную» характеристику схемы, учитывающую не только элементы, проходимые сигналом при следовании по пути от входа к выходу, но и элементы, на которые сигнал разветвляется на этом пути. Такая характеристика будет называться накопленным ветвлением схемы.

Дадим необходимые определения. Систему $Б = \{g_1, g_2, \ldots, g_m\}$, где все g_i — функции алгебры логики, будем называть *базисом функциональных элементов*.

Схемой из функциональных элементов над базисом $Б$ будем называть конечный ациклический упорядоченный орграф, в котором:

1) каждому истоку приписана некоторая переменная, причем разным истокам приписаны разные переменные (истоки при этом называются входами схемы, а приписанные им переменные — входными переменными);

2) каждой вершине, в которую входят $k \geq 1$ ребер, приписана функция из базиса $Б$, зависящая от k переменных (вершина с приписанной функцией при этом называется функциональным элементом);

3) некоторые вершины выделены как выходы (истоки также могут являться выходами);

4) индукцией по глубине q вершины ν определяется функция f_ν, реализуемая в данной вершине.

В этой работе рассматриваются СФЭ над стандартным базисом $Б_0 = \{\vee, \&, \neg\}$. Так как эти функции симметричны относительно своих переменных, то ребра, входящие в каждую вершину, можно не упорядочивать.

Будем говорить, что схема реализует систему функций, реализуемых в ее выходах. Схема реализует данную функцию, если она реализует ее хотя бы на одном из выходов.

Назовем *проводом*, исходящим из функционального элемента ν, множество вершин $\{\nu_1, \ldots, \nu_F\}$, в которые из элемента ν идут ребра. *Ветвлением* провода назовем число вершин F в соответствующем ему множестве. Обозначим ветвление провода, исходящего из вершины ν, через $F(\nu)$. Будем считать, что если из ν не выходит ни одного ребра, то $F(\nu) = 1$.

Пусть $P = (\nu_0, \nu_1, \nu_2, \ldots, \nu_n)$ — путь из истока ν_0 (входной вершины) в выходную вершину v_n. Назовем *накопленным ветвлением по пути* P величину

$$F(P) = \sum_{i=0}^{n} F(\nu_i).$$

Назовем *накопленным ветвлением СФЭ* S величину

$$F(S) = \max_{P \text{ "— путь из входа в выход}} F(P).$$

Введем *функцию Шеннона для накопленного ветвления СФЭ* по формуле

$$F(n) = \max_{f \in P_2(n)} \quad \min_{f \text{ реализуется СФЭ } S} \quad F(S).$$

Автором получена следующая оценка функции Шеннона для накопленного ветвления:

Теорема 1. *Для схем из функциональных элементов над базисом* $Б_0 = \{\vee, \&, \neg\}$

$$F(n) = (3 \log_3 2 + 1)n + o(n), \quad (n \to \infty).$$

Кроме того, нижняя оценка функции Шеннона для накопленного ветвления СФЭ существенна:

Теорема 2. *Для почти всех функций из* P_2 *наименьшее накопленное ветвление среди схем из функциональных элементов, реализующих данную функцию, асимптотически совпадает с функцией Шеннона при* $n \to \infty$.

Автор выражает благодарность своему научному руководителю Игорю Викторовичу Кучеренко за постановку задачи и внимание к работе и Валерию Борисовичу Кудрявцеву за ценные советы и замечания.

Список литературы

1. Яблонский С. В. Введение в дискретную математику. — М.: Высшая школа, 2002.

2. Лупанов О. Б. О синтезе некоторых классов управляющих систем // Проблемы кибернетики. Вып. 10. — М.: Физматгиз, 1963. — С. 63–97.

3. Лупанов О. Б. О схемах из функциональных элементов с задержками // Проблемы кибернетики. Вып. 23. — М.: Наука, 1970. — С. 43–81.

4. Касим-Заде О. М. О глубине булевых функций над произвольным бесконечным базисом // Дискретный анализ и исследование операций. Сер. 1. — 2007. — Т. 14, № 1. — С. 45–69.

5. Pillage L. T., Rohrer R. A. Asymptotic waveform evaluation for timing analysis // IEEE Trans. on CAD of Integrated Circuits and Systems. — 1990. — V. 9, № 4. — С. 352–366.

О РАВНОМЕРНОСТИ НЕКОТОРЫХ СИСТЕМ ФУНКЦИЙ МНОГОЗНАЧНОЙ ЛОГИКИ

П. Б. Тарасов (Москва)

В работе рассматривается задача о реализации функций k-значной логики из замкнутых классов формулами в конечных базисах, состоящих из функций, принадлежащих этим же классам. Все необходимые определения можно найти в работах [1–3]

Обозначим через $P_{k,2}$ все функции k-значной логики, принимающие значения 0 и 1, $k \geq 2$. Пусть A — конечная система функций из $P_{k,2}$, Φ — формула над A. Обозначим через $L(\Phi)$ число символов переменных и констант, входящих в формулу Φ (сложность формулы Φ), а через $D(\Phi)$ — глубину формулы Φ. Пусть $f \in [A]$. Положим

$$D_A(f) = \min l(\Phi),\ L_A(f) = \min L(\Phi),$$

где минимум берется по всем формулам Φ над A, реализующим f.

Конечную систему функций A будем называть равномерной, если существуют такие константы c и d, что для любой функции $f \in [A]$ выполнено неравенство

$$D_A(f) \leq c \log L_A(f) + d.$$

В работах [4, 5] доказана равномерность любой конечной полной системы булевых функций (см. также [6]). Позднее, в работе [7] была доказана равномерность всех конечных систем булевых функций, порождающих класс M. В работах [3,8] доказана равномерность всех конечных систем булевых функций. Аналогичный результат получен в работе [9]. Равномерность конечных систем, порождающих некоторые предполные классы в P_k установлена в работах [10, 11], $k \geq 3$.

Пусть $f(x_1, \ldots, x_n)$ — функция из $P_{k,2}$, а $g(x_1, \ldots, x_n)$ — функция из P_2, такие что для любого $\widetilde{\alpha} \in E_2^n$ выполнено равенство $f(\widetilde{\alpha}) = g(\widetilde{\alpha})$. Функцию g будем называть проекцией функции f и обозначать через prf. Пусть A — конечная система функций $P_{k,2}$. Положим $pr(A) = \bigcup\limits_{f \in A} pr(f)$.

Имеет место следующее утверждение.

Теорема. *Всякая конечная система A функций из $P_{k,2}$, такая, что $prA = M$, равномерна, $k \geq 3$.*

Доказательство теоремы опирается на лемму, сформулированную ниже.

Будем говорить, что формула Φ представляется в виде $\Phi_1(\Phi_2)$, если выполнены следующие условия:
1) формулы Φ_1 и Φ_2 нетривиальные;
2) в Φ_2 входят только те переменные, которые входят в Φ;
3) в Φ_1 входят только те переменные, которые входят в Φ, а также выделенная переменная y, причем ровно 1 раз;
4) формула Φ получается из формулы Φ_1 заменой переменной y на формулу Φ_2.

Лемма. *Пусть A — конечная система функций из $P_{k,2}$, такая, что каждая функция из A зависят не более чем от n переменных ($n \geq 1$), а Φ — формула над A, такая, что $L(\Phi) \geq 2(n+1)^2$. Тогда существуют нетривиальные формулы Φ_1, Φ_2 и Φ_3 над A, такие, что Φ представляется в виде $\Phi_1(\Phi_2(\Phi_3))$, и выполняются неравенства*

$$L(\Phi_i) \geq \frac{L(\Phi) + 1}{(n+1)^2}$$

для всех $i \in \{1, 2, 3\}$.

Работа выполнена при финансовой поддержке РФФИ (проект 11–01–00508) и программы фундаментальных исследований ОМН РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения» (проект «Задачи оптимального синтеза управляющих систем»)

Список литературы

1. Яблонский С. В. Введение в дискретную математику. — М.: Высшая школа, 2001.

2. Lau D. Function Algebras on Finite Sets. — Springer-Verlag, 2006.

3. Угольников А. Б. О глубине и полиномиальной эквивалентности формул для замкнутых классов двузначной логики // Математические заметки. — 1987. — Т. 42, вып. 4. — С. 603–612.

4. Яблонский С. В., Козырев В. П. Математические вопросы кибернетики // Информационные материалы. Вып. 32. — М.: Научный совет по комплексной проблеме Кибернетика АН СССР, 1978. — С. 76–94.

5. Spira P. M. On time-hardware complexity tradeoffs for Boolean functions // Proc. 4th Hawai Symposium on System Sciences. — North Hollywood: Western Periodicals Company, 1971. — P. 525–527.

6. Храпченко В. М. О соотношении между сложностью и глубиной формул // Методы дискретного анализа в синтезе управляющих систем. Вып. 32. — Новосибирск: ИМ СО АН СССР, 1978. — С. 76–94.

7. Wegener I. Relating monotone formula size and monotone depth of boolean functions // Information Processing Letters. — 1983. — V. 16. — P. 41–42.

8. Угольников А. Б. О соотношении между глубиной и сложностью формул для замкнутых классов двузначной логики // IV Всесоюзная конференция «Применение методов математической логики»: тезисы докладов. — Таллин, 1986. — С. 184.

9. Ragaz M. E. Parallelizable algebras // Archiv fur mathematische Logik und Grundlagenforschung. — 1986/7. — V. 26. — P. 77–99.

10. Сафин Р. Ф. О глубине и сложности формул в некоторых классах k-значной логики // Вестн. Моск. ун-та. Сер. 1. Математика. Механика. — 2000. — № 6. — С. 65–68.

11. Сафин Р. Ф. О соотношении между глубиной и сложностью формул для предполных классов k-значной логики // Математические вопросы кибернетики. Вып. 13. — М.: Физматлит, 2004. — С. 223–278.

ОБ ОСОБЕННОСТЯХ ОДНОЙ МЕРЫ СЛОЖНОСТИ ЦЕЛОЧИСЛЕННЫХ МАТРИЦ

Е. Н. Трусевич (Москва)

Пусть $U = x_1^{a_{11}} \dots x_q^{a_{1q}}$, $V = x_1^{a_{21}} \dots x_q^{a_{2q}}$ — произвольные мономы и задан моном $R = x_1^{r_1} \dots x_q^{r_q}$, где $0 \le r_i \le \min(a_{1i}, a_{2i})$, $1 \le i \le q$ (отметим, что в отличие от остальных мономов для выражения R может быть выпонено условие $\sum_{i=1}^{q} r_i = 0$, однако будем в дальнейшем называть его мономом). *Композицией* мономов U и V относительно монома R называется [1] моном $x_1^{a_{11}+a_{21}-r_1} \dots x_q^{a_{1q}+a_{2q}-r_q}$, который будем обозначать через $(U, V)_R$.

Последовательность S мономов $X_1, \dots, X_q, X_{q+1}, \dots, X_{q+n}$ называется *схемой композиции для монома* X_{q+n}, если эта последовательность удовлетворяет условиям:

1) для $i = 1, \dots, q$ выполняется равенство $X_i = x_i$;

2) для $i = q+1, \dots, q+n$ найдутся $s = s(i)$ и $t = t(i)$, не превосходящие $i-1$, а также моном R_i, такие что $X_i = (X_s, X_t)_{R_i}$.

Под *сложностью* $l_{sh}(S)$ схемы композиции S понимается число n, т. е. число используемых в схеме S операций композиции.

Схемой композиции для системы мономов $\mathcal{A}$ назовем схему композиции S для некоторого монома из системы, которая содержит в качестве элементов остальные мономы из множества $\mathcal{A}$.

Положим $l_{sh}(\mathcal{A}) = \min l_{sh}(S)$, где минимум берется по всем схемам композиции для системы $\mathcal{A}$. Величину $l_{sh}(\mathcal{A})$ назовем *сложностью системы мономов* $\mathcal{A}$. Система мономов $\mathcal{A}$ полностью определяется матрицей показателей степеней A. Поэтому можно говорить не только о сложности $l_{sh}(\mathcal{A})$ вычисления системы $\mathcal{A}$, но и о *сложности* $l_{sh}(A)$ *матрицы* A, задающей эту систему. Не будем различать эти понятия и будем считать, что $l_{sh}(A) = l_{sh}(\mathcal{A})$.

Понятие схемы композиции можно проинтерпретировать на языке схем из функциональных элементов [2].

Ранее Ю. В. Мерекиным был исследован [3] случай вычисления системы мономов, состоящей из одного монома. Было доказано, что $l_{sh}(x_1^{a_1} \dots x_q^{a_q}) = \lceil \log_2 a \rceil + q - 1$, где $a = \max(a_1 \dots a_q)$.

Утверждение 1 [4]. *Пусть в целочисленной матрице* $A = (a_{ij})$ *размера* 2×2 *с неотрицательными элементами нет нулевых строк и столбцов, а минимальным элементом матрицы* A *является элемент* a_{21}. *Тогда*

$$l_{sh}(A) = \lceil \log_2 a_{22} \rceil + \left\lceil \log_2 \max\left(\frac{a_{11}}{\max(a_{21}, 1)}, \frac{a_{12}}{a_{22}} \right) \right\rceil + \operatorname{sgn} a_{12} + \gamma(A),$$

где $\gamma(A)=1$ *при выполнении условий* $a_{21}=0$, $a_{11}=1$, $0<a_{12}<a_{22}$ *и* $\lceil \log_2 a_{12} \rceil + \left\lceil \log_2 \frac{a_{22}}{a_{12}} \right\rceil = \lceil \log_2 a_{22} \rceil + 1$, *а в остальных случаях* $\gamma(A)=0$.

Сформулированный в утверждении 1 результат приведем к стандартному виду, выражаемому через величину $D(A)$, численно равную максимуму абсолютных величин миноров матрицы A.

Утверждение 2 [4]. *Пусть* $A = (a_{ij})$ — *целочисленная неотрицательная матрица размера* 2×2 *с неотрицательными элементами и* $m = \max(\min(a_{11}, a_{12}, a_{21}, a_{22}), 1)$. *Тогда при* $D(A) \to \infty$ *справедливо соотношение*

$$l_{sh}(A) = \log_2 m + \log_2 D \begin{pmatrix} a_{11}/m & a_{12}/m \\ a_{21}/m & a_{22}/m \end{pmatrix} + O(1).$$

Эти результаты показывают, что для меры l_{sh} сложности целочисленных матриц, в отличие от многих других мер (в частности, мер l и l_2 сложности вычисления систем одночленов, показатели степеней которых задаются исходными матрицами, в моделях, допускающих, соответственно, либо только операции умножения, либо операции умножения и деления, — подробнее см., например, [5]), не выполняется универсальная оценка снизу через величину $\log_2 D(A)$. Дополнительно проиллюстрируем этот факт следующим образом. Пусть $B(p,n)$ — квадратная матрица порядка p, в которой на главной диагонали стоят числа $2n$, а остальные элементы равны n. Обозначим $B_n = B(\lceil \log_2 n \rceil / 2, n)$.

Теорема 1. *При* $n \to \infty$ *справедливы соотношения*

$$l_{sh}(B_n) \sim 2\sqrt{2 \log_2 D(B_n)} \sim 2\sqrt{2 l_2(B_n)}.$$

Действительно, при $p+n \to \infty$, с одной стороны, $l_{sh}(B(p,n)) = \lceil \log_2 n \rceil + 2p - 1$, а с другой, $l_2(B(p,n)) \sim \log_2 D(B(p,n)) \sim p \log_2 n$.

Таким образом, для меры l_{sh} сложности последовательности матриц B_n не выполняется универсальная нижняя оценка из [5]. Более того, величина $l_{sh}(B_n)$ растет по порядку как квадратный корень из сложности $l_2(B_n)$.

Эти факты говорят о значительной «вычислительной силе» операции композиции. Однако оказывается, что ее «сила» в сравнении со стандартными операциями не носит абсолютного характера. Следуя [6], обозначим через $A(t,n)$ множество матриц размера $2t \times 2t$, определяемых следующим образом. Первой строкой матрицы $A(t,n)$ является набор длины $2t$, первая половина разрядов которого равна n, а вторая половина равна нулю. Остальные $2t-1$ строки матрицы

$A(t,n)$ получаются из первой строки последовательным цикличным сдвигом на один разряд вправо.

Теорема 2. *Пусть* $t = o((\log_2 \log_2 n)^{1/2})$ *при* $n \to \infty$. *Тогда*

$$l_{sh}(A(t,n)) \sim \frac{2t}{t+1} \log_2 D((A(t,n)) \sim \frac{2t}{t+1} l_2(A(t,n)).$$

Следовательно, возможностей операции композиции оказывается в этом случае недостаточно даже для того, чтобы понизить асимптотику роста сложности хотя бы до величины универсальной нижней оценки вида $\log_2 D((A(t,n))$.

Еще одним важным отличительным свойством введенной меры сложности является тот факт, что для операции композиции не работают в достаточной мере соображения двойственности.

Определим матрицы $C_1(p)$ и $C_2(p)$ размера $p \times 1$ как векторстолбцы, состоящие, соответственно, из первых p натуральных чисел и из степеней двойки от нулевой до $(p-1)$-й.

Теорема 3. *С одной стороны, сложность реализации матриц* $C_1(p)$ *и* $C_2(p)$ *схемами композиции одинаковая и равна* $p-1$, *в то время как* $l_{sh}(C_1^T(p)) = p - 1 + \lceil \log_2 p \rceil$, $l_{sh}(C_2^T(p)) = 2p - 2$.

Таким образом, приведен пример двух матриц одной сложности, для которых сложность транспонированных к ним матриц отличается асимптотически вдвое.

Список литературы

1. Ширшов А. И. Некоторые алгоритмические проблемы для алгебр Ли // Сиб. матем. журнал. — 1962. — Т. 3. — С. 292–296.

2. Лупанов О. Б. О синтезе некоторых классов управляющих систем // Проблемы кибернетики. Вып. 10. — М.: Физматлит, 1963. — С. 63–97.

3. Мерекин Ю. В. О порождении слов с использованием операции композиции // Дискретн. анализ и исслед. опер. Сер. 1. — 2003. — Т. 10, № 4. — С. 70–78.

4. Трусевич Е. Н. О сложности реализации схемами композиции систем из двух мономов от двух переменных // Материалы VIII молодежной научной школы по дискретной математике и ее приложениям (24–29 октября 2011 г.). Часть 2. — М., 2011. — С. 40–44.

5. Кочергин В. В. О сложности вычисления систем одночленов и систем целочисленных линейных форм // Дискретная математика и ее приложения. Сборник лекций. Выпуск III. — М.: Изд-во механико-математического факультета МГУ, 2007. — С. 3–63.

6. Кочергин В. В. Об одном соотношении двух мер сложности вычисления систем одночленов // Вестник Московского университета. Сер. 1. Математика. Механика. — 2009. — № 4. — С. 8–13.

О СЛОЖНОСТИ РЕАЛИЗАЦИИ ФУНКЦИЙ МНОГОЗНАЧНОЙ ЛОГИКИ ФОРМУЛАМИ СПЕЦИАЛЬНОГО ВИДА

Д. В. Трущин (Москва)

В данной работе рассматривается задача о реализации функций многозначной логики α-формулами. Пусть $k \geq 2$. Обозначим через P_k множество всех функций k-значной логики. Положим $E_k = \{0, 1, \ldots, k-1\}$. Пусть $n \geq 1$, $\mathfrak{A}$ — конечная система функций из P_k. Формулу над $\mathfrak{A}$, не содержащую символов переменных за исключением $x_1, \ldots, x_n$, обозначим через $\Phi(x_1, \ldots, x_n)$. Сложность и глубину формулы Φ обозначим через $L(\Phi)$ и $D(\Phi)$ соответственно. Через $[\mathfrak{A}]$ обозначим замыкание системы $\mathfrak{A}$. Сложность и глубину над системой $\mathfrak{A}$ произвольной функции f из $[\mathfrak{A}]$ обозначим через $L_{\mathfrak{A}}(f)$ и $D_{\mathfrak{A}}(f)$ соответственно. Необходимые определения можно найти в [1, 2].

Известно [3], что для любой полной конечной системы $\mathfrak{A}$ булевых функций и любой булевой функции $f(x_1, \ldots, x_n)$ выполнено соотношение $L_{\mathfrak{A}}(f) \lesssim \frac{2^n}{\log_2 n}$. В работах [4, 5] показано, что для произвольной конечной системы $\mathfrak{A}$ булевых функций и любой функции $f(x_1, \ldots, x_n) \in [\mathfrak{A}]$ справедливы неравенства $L_{\mathfrak{A}}(f) \leq r_1^n$ и $D_{\mathfrak{A}}(f) \leq r_2 n$, где r_1 и r_2 — некоторые константы, зависящие от $\mathfrak{A}$.

Следуя [6], определим индуктивно понятие α–формулы над конечной системой $\mathfrak{A}$ функций алгебры логики. Символ переменной является элементарной α-формулой. Символ нульместной функции из $\mathfrak{A}$ является α-формулой. Выражение вида $u(\Phi)$, где Φ — α-формула над $\mathfrak{A}$, а u — символ одноместной функции из $\mathfrak{A}$, является α-формулой. Наконец, выражение вида $g(\Phi, x_{i_2}, \ldots, x_{i_m})$, где Φ — α-формула над $\mathfrak{A}$, $m \geq 2$, g — символ m-местной функции из $\mathfrak{A}$, а $x_{i_2}, \ldots, x_{i_m} \in X$, также является α-формулой. Отметим, что каждая α-формула является формулой над $\mathfrak{A}$. Множество всех функций, реализуемых α-формулами над $\mathfrak{A}$, будем называть α– пополнением системы $\mathfrak{A}$ и обозначать через $[\mathfrak{A}]_\alpha$. Система $\mathfrak{A} \subseteq P_k$ называется α-полной, если $[\mathfrak{A}]_\alpha = P_k$. Известно [7], что в P_2 не существует конечных α-полных систем. При этом в P_k при $k \geq 3$ конечные α-полные системы существуют [6–8].

Пусть $\mathfrak{A}$ — конечная система функций из P_k, $f \in [\mathfrak{A}]_\alpha$. Положим $D^\alpha_{\mathfrak{A}}(f) = \min D(\Phi)$, $L^\alpha_{\mathfrak{A}}(f) = \min L(\Phi)$, где минимум берется по всем α-формулам Φ над $\mathfrak{A}$, реализующим f. Отметим, что справедливы

неравенства

$$r_1 D^{\alpha}_{\mathfrak{A}}(f) \le L^{\alpha}_{\mathfrak{A}}(f) \le r_2 D^{\alpha}_{\mathfrak{A}}(f),$$

где r_1 и r_2 — положительные константы, зависящие от $\mathfrak{A}$. Формулу Φ назовем минимальной (для функции f), если Φ реализует f, и $D(\Phi) = D^{\alpha}_{\mathfrak{A}}(f)$. Положим $D^{\alpha}_{\mathfrak{A}}(n) = \max D^{\alpha}_{\mathfrak{A}}(F)$, где максимум берется по всем n-местным функциям $F(x_1, \ldots, x_n) \in [\mathfrak{A}]_{\alpha}$.

В работе [9] показано, что для любой конечной системы $\mathfrak{A}$ булевых функций существует многочлен $P(n)$ такой, что $D^{\alpha}_{\mathfrak{A}}(n) \le P(n)$. Из этого результата следует, что в P_2 нет конечных α-полных систем.

Двухместную функцию $g(x, z) \in P_k$ мы будем называть бинарной операцией с правым сокращением, если для любых элементов $b, c \in E_k$ существует, и при том ровно один, элемент $a \in E_k$, такой, что $g(a, b) = c$. Множество всех бинарных операций с правым сокращением из P_k обозначим через $\mathfrak{B}_k$. В работе [10] автором были построены примеры последовательностей функций, имеющие порядок роста глубины 2^n над системой $\mathfrak{B}_3$.

Основным результатом данной работы является следующая теорема, которая может быть доказана с использованием теоремы 1.

Теорема. *Пусть k — простое число, $k \ne 2$. Пусть $n \ge 1$, $f(x_1, \ldots, x_n) \in P_k$. Тогда $f \in [\mathfrak{B}_k]_{\alpha}$ и выполняется неравенство*

$$D^{\alpha}_{\mathfrak{B}_k}(f) \le \frac{2k-1}{k(k-1)} k^n - \frac{k}{k-1}.$$

Следствие. *Пусть k — простое число, $k \ne 2$, $n \ge 1$. Тогда система $\mathfrak{B}_k$ является α-полной, и имеет место неравенство*

$$D^{\alpha}_{\mathfrak{B}_k}(n) \le \frac{2k-1}{k(k-1)} k^n - \frac{k}{k-1}.$$

В заключение приведем нижнюю оценку для функции Шеннона $D^{\alpha}_{\mathfrak{B}_k}(n)$.

Утверждение. *Пусть $k \ge 3$. Имеет место асимптотическое неравенство*

$$D^{\alpha}_{\mathfrak{B}_k}(n) \gtrsim \frac{k^n}{\log_k(n)}.$$

Автор выражает искреннюю признательность проф. А. Б. Угольникову за постановку задачи и обсуждение результатов работы а также проф. Р. М. Колпакову за внимание к работе.

Работа выполнена при финансовой поддержке РФФИ, грант 11–01–00508, и программы фундаментальных исследований Отделения математических наук РАН “Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения” (проект “Задачи оптимального синтеза управляющих систем”).

Список литературы

1. Яблонский С. В. Введение в дискретную математику. — М.: Высшая школа, 2006.

2. Лупанов О. Б. Асимптотичексие оценки сложности управляющих систем. — М.: Изд-во МГУ, 1984.

3. Лупанов О. Б. О сложности реализации функций алгебры логики формулами // Проблемы кибернетики. Вып. 3. — М.: Физматгиз, 1960. — С. 61–80.

4. Угольников А. Б. О глубине формул в неполных базисах // Математические вопросы кибернетики. Вып. 1. — 1988. — С. 242–245.

5. Угольников А. Б. О глубине и сложности формул, реализующих функции из замкнутых классов // Докл. АН СССР. — 1988. — Т. 298, № 6. — С. 1341–1344.

6. Глухов М. М. Об α-замкнутых классах и α-полных системах функций k-значной логики // Дискретн. матем. — 1989. — Т. 1, вып. 1. — С. 16–21.

7. Чернышов А. Л. Условия α-полноты систем функций многозначной логики // Дискретн. матем. — 1992. — Т. 4, вып. 4. — С. 117–130.

8. Шабунин А. Л. Примеры α-полных систем k-значной логики при $k = 3, 4$ // Дискретн. матем. — 2006. — Т. 18, вып. 4. — С. 45–55.

9. Трущин Д. В. О глубине α-пополнений систем булевых функций // Вестн. Моск. ун-та. Матем. Механ. — 2009. — № 2. — С. 72–75.

10. Трущин Д. В. Об оценках глубины α-пополнений систем функций трехзначной логики // Проблемы теоретической кибернетики: Мат-лы XVI Междунар. конф. — Н. Новгород: Изд-во ННГУ, 2011. — С. 484–487.

О РЕАЛИЗАЦИИ НЕДООПРЕДЕЛЕННЫХ ФУНКЦИЙ ФОРМУЛАМИ

А. В. Чашкин (Москва)

Пусть $\mathcal{P}(\mathbb{Z}_m)$ — множество всех непустых подмножеств $\mathbb{Z}_m$. Набор b из $(\mathcal{P}(\mathbb{Z}_m))^n$ назовем недоопределенным m-ичным набором. Набор $k = (k_1, k_2, \ldots, k_m)$ назовем характеристикой набора b, если $\forall i$ число k_i равно количеству i-элементных компонент b. Для набора b с характеристикой $k = (k_1, k_2, \ldots, k_m)$ положим $I(b) = \log_2 \left(\left(\frac{m}{1}\right)^{k_1} \left(\frac{m}{2}\right)^{k_2} \cdots \left(\frac{m}{m}\right)^{k_m} \right)$. Набор $a \in \mathbb{Z}_m^n$ назовем доопределением $b \in (\mathcal{P}(\mathbb{Z}_m))^n$, если $\forall i$ $\alpha_i \in \beta_i$. Множество $A \subseteq \mathbb{Z}_m^n$ назовем доопределением множества B наборов из $(\mathcal{P}(\mathbb{Z}_m))^n$, если для каждого b из B в A найдется элемент a, являющийся его доопределением.

Будем рассматривать сложность вычисления функций из $\{0,1\}^n$ в $\mathcal{P}(\mathbb{Z}_m)$ формулами в базисе из всех двухместных булевых функций, констант $0, 1 \ldots, m-1$ и операций сложения и умножения по модулю m. Функции со значениями в $\mathcal{P}(\mathbb{Z}_m)$ будем называть недоопределенными m-значными функциями. Для недоопределенной m-значной функции f через $I(f)$ обозначим значение введенной выше функции I на векторе значений f. Функцию $h : \{0,1\}^n \to \mathbb{Z}_m$ назовем доопределением недоопределенной m-значной функции f, если вектор значений h является доопределением вектора значений f. Сложностью формулы называется число содержащихся в ней функциональных символов, а сложностью $L(f)$ недоопределенной функции f — сложность самого простого ее доопределения. Ранее реализация недоопределенных функций схемами рассматривалась в [1–3, 5].

Теорема. *Пусть* $\log_2 I(f) \sim n$ *и* $\log_2 m = o(n)$. *Тогда*

$$L(f) \le \frac{I(f)}{\log_2 n}(1 + o(1)).$$

Доказательство. Недоопределенную n-местную функцию f стандартным образом представим таблицей T_f из 2^r столбцов, соответствующих первым r переменным, и 2^{n-r} строк, соответствующих последним $n-r$ переменным. Каждую строку таблицы представим в виде следующих друг за другом наборов b, для каждого из которых, кроме быть может последнего, $I(b) \ge R$ и $I(b') < R$. Множество таких наборов разобьем на классы, поместив в класс P_{ij} наборы, начинающиеся в i-й и заканчивающиеся в j-й позициях.

Известно [3], что для класса P_{ij} существует доопределение, состоящее не более чем из $2^{3r+1}2^R$ наборов длины 2^r, в каждом из

которых первые $i-1$ и последние 2^r-j компонент равны нулю. Поэтому, для множества всех наборов b существует доопределение $H=\{h_i\}$, состоящее не более чем из $2^{5r}2^R$ наборов h_i длины 2^r.

Преобразуем T_f, заменив в ней каждый набор каким-либо его доопределением из H. Преобразованная таблица будет таблицей значений n-местной функции h, являющейся доопределением функции f. Из номеров i тех наборов h_i, которые входят в j-ю строку преобразованной таблицы, составим множество A_j. Каждый набор h_i из H будем рассматривать как вектор значений r-местной функции g_i, зависящей от переменных $x_1,\dots,x_r$. Множество G, состоящее из функций g_i, содержит не более чем $2^{5r}2^R$ элементов и функция h может быть выражена через функции из G следующим образом:

$$h(x_1,\dots,x_n)=\sum_{\sigma=(\sigma_{r+1},\dots,\sigma_n)}\Big(\sum_{g\in A_j}g(x_1,\dots,x_r)\Big)x_{r+1}^{\sigma_{r+1}}\cdot\ldots\cdot x_n^{\sigma_n},\quad(1)$$

где $j=\sum_{i=1}^{n-r}\sigma_{r+i}2^{i-1}$, а суммирование производится по модулю m.

Так как число функций g с $I(g)<R$, не больше чем 2^{n-r}, а для каждой из оставшихся функций $I(g)\ge R$, т. е. их число не превосходит $I(f)/R$, то общее число функций g в (1) не превосходит

$$I(f)\Big/R+2^{n-r}.\quad(2)$$

В (1) поменяем порядок суммирования — сначала вычислим суммы по функциям из G, а затем по элементарным конъюнкциям последних $n-r$ переменных, на которые эти функции умножаются:

$$h(x_1,\dots,x_n)=\sum_{g\in G}g(x_1,\dots,x_r)\Big(\sum_{\sigma_{r+1},\dots,\sigma_n}x_{r+1}^{\sigma_{r+1}}\cdot\ldots\cdot x_n^{\sigma_n}\Big).\quad(3)$$

Здесь в каждой подформуле заключенной в скобки при любых значениях переменных $x_{r+1},\dots,x_n$ не более чем одна конъюнкция может принимать единичное значение. Поэтому в (3) сложения в указанных подформулах можно заменить дизъюнкциями, т. е.

$$h(x_1,\dots,x_n)=\underbrace{\sum_{g\in G}g(x_1,\dots,x_r)}_{A}\underbrace{\Big(\bigvee_{\sigma_{r+1},\dots,\sigma_n}x_{r+1}^{\sigma_{r+1}}\cdot\ldots\cdot x_n^{\sigma_n}\Big)}_{B}.\quad(4)$$

Так как $|G|\le 2^{5r}2^R$ и каждая функция из G является суммой не более чем 2^r элементарных конъюнкций, каждая из которых умножена

на константу из $\mathbb{Z}_m$, то сложность подформул из части A есть

$$\mathcal{O}(r2^r2^{5r}2^R). \tag{5}$$

Часть B состоит не более чем из $2^{5r}2^R$ подформул B_i, реализующих булевы функции $\mathcal{B}_i$, общий вес которых не больше (2). Из [4] следует, что существуют формулы, реализующие функции $\mathcal{B}_i$ со сложностью

$$\mathcal{O}(r2^r2^{5r}2^Rn^{5,62}) + \frac{n\big(I(f)\Big/R + 2^{n-r}\big)}{\log_2 n}(1+o(1)). \tag{6}$$

Очевидно, что $L(f)$ не превосходит суммы величин (5) и (6).

Положим $r = \lceil n - \log_2 I(f) + 2\log_2 n\rceil$, $R = \lfloor \log_2 I(f) - 6r - 7\log_2 n\rfloor$. Тогда, учитывая условие $\log_2 I(f) \sim n$, имеем $R \sim \log_2 I(f) \sim n$, $R + 6r \le \log_2 I(f) - 7\log_2 n$, $n - r \le \log_2 I(f) - 2\log_2 n$. Подставляя эти оценки в (5) и (6), получаем требуемую оценку сложности функции f. Теорема доказана.

Мощностным методом легко показать, что неравенство теоремы асимптотически точное для почти всех рассматриваемых функций.

Работа выполнена при финансовой поддержке РФФИ, проект 11-01-00508.

Список литературы

1. Шоломов Л. А. О функционалах, характеризующих сложность систем недоопределенных булевых функций // Проблемы кибернетики. Вып. 19. — М.: Наука, 1967, с. 123–140.

2. Шоломов Л. А. Информационные свойства функционалов сложности для систем недоопределенных булевых функций // Проблемы кибернетики. Вып. 34. — М.: Наука, 1978, с. 133–150.

3. Чашкин А. В. Вычисление недоопределенных функций // Дискретная математика и ее приложения. Сборник лекций. Вып 6. — М.: ИПМ РАН, 2011, с. 29–40.

4. Чашкин А. В. О сложности реализации булевых функций формулами // Дискретный анализ и исследование операций. 2005. Вып. 2. С. 56–72.

5. Andreev A. E. Complexity of nondetetministic functions // BRICS Report Series, RS-94-2.

СИНТЕЗ НЕЛИНЕЙНЫХ ЦИФРОВЫХ ФИЛЬТРОВ НА ОСНОВЕ СИСТЕМЫ МНОГОЧЛЕНОВ НАД ПОЛЕМ ГАЛУА

С. В. Шалагин (Казань)

Рассмотрен класс нелинейных цифровых фильтров, определенных согласно выражению вида

$$y_k = \sum_{i=1}^{l} a_i f_i(x_{k-i}) + \sum_{j=1}^{m} b_j g_j(y_{k-j}), \qquad (1)$$

где переменные и коэффициенты x_{k-i}, a_i, y_{k-j}, $b_j \in G_n$, $G_n = GF(2^n)$, а функции $f_i(x_{k-i})$ и $g_j(y_{k-j})$ определены в G_n и принимают значения из G_n, $i = \overline{0,l}$, $j = \overline{0,m}$.

Выражение (1) представимо как дискретная детерминированная нелинейная функция от $(l+m+1)$ переменных вида

$$y_k = \psi(x_k, x_{k-1},, x_{k-l}, y_{k-1},, y_{k-m}), \qquad (2)$$

где x_{k-i}, $y_{k-j} \in G_n$, $i = \overline{0,l}$, $j = \overline{0,m}$.

Согласно [1], выражение (2) представимо системой из n полиномиальных функций от $n(l+m+1)$ переменных каждая, определенных над элементами поля $GF(2)$. Примем в качестве меры сложности элементарную схему схему, реализующую произвольную булеву функцию от двух переменных, а в качестве модели вычислений частный случай равнодоступной адресной машины битовые вычисления [2]. На основе вышеизложенного справедливо

Утверждение. *Нижняя оценка временной и оценка емкостной сложности для нелинейных цифровых фильтров вида* (1)*, определенных на основе* (2)*, составляют*

$$T_{NF} =]\log(n(l+m+1))[, \qquad S_{NF} = n^2(l+m+1) - n.$$

Список литературы

1. Шалагин С. В. О представлении нелинейных полиномов над конечным полем распределенной вычислительной системой // Нелинейный мир. — 2009. — № 5. — С. 376–379.

2. Ахо А., Хопкрофт Дж., Ульмани Дж. Построение и анализ вычислительных алгоритмов. — М.: Мир, 1979.

ДВОИЧНОЕ РАЗЛОЖЕНИЕ НЕДООПРЕДЕЛЕННЫХ СИМВОЛОВ

Л. А. Шоломов (Москва)

Задан алфавит $A_0 = \{a_i,\ i \in M\}$, $M = \{0, 1, \ldots, m-1\}$, *основных символов*. Каждому непустому $T \subseteq M$ поставлен в соответствие символ a_T, который называется *недоопределенным*, и *доопределением* которого считается всякий основной символ a_i, $i \in T$. Под *доопределением последовательности* недоопределенных символов понимается любая последовательность, полученная из нее заменой всех символов некоторыми доопределениями. Символ a_M, доопределимый любым основным символом, называется *неопределенным* и обозначается $*$.

Пусть выделена некоторая система $\mathcal{T}$ множеств T и с ней связан *недоопределенный алфавит* $A = \{a_T \mid T \in \mathcal{T}\}$. Задавшись натуральным числом s, припишем каждому символу $a_i \in A_0$ некоторый набор $\mathbf{a}_i \in \{0,1\}^s$, а каждому символу $a_T \in A$ — некоторый набор $\mathbf{a}_T \in \{0,1,*\}^s$. Обозначим через $\mathbf{A}_0$ матрицу, столбцами которой являются наборы (точнее, транспонированные наборы) $\mathbf{a}_i$, $i \in M$, а через $\mathbf{A}$ — матрицу со столбцами $\mathbf{a}_T$, $T \in \mathcal{T}$. Скажем, что пара $(\mathbf{A}_0, \mathbf{A})$ задает *двоичное разложение алфавита* A, если для любых $i \in M$ и $T \in \mathcal{T}$

$$\mathbf{a}_i \textit{ доопределяет } \mathbf{a}_T \iff i \in T.$$

Алфавит, для которого существует двоичное разложение, назовем *разложимым*.

Недоопределенной последовательности $a_{T_1} a_{T_2} \ldots$ соответствует представление $\mathbf{a}_{T_1} \mathbf{a}_{T_2} \ldots$. Его построение и восстановление по нему исходной недоопределенной последовательности использует матрицу $\mathbf{A}$, число столбцов которой может достигать $2^m - 1$. Ниже указано, как задачи представления и восстановления недоопределенных последовательностей можно эффективно решать пользуясь лишь матрицей $\mathbf{A}_0$, содержащей m наборов.

Матрицу $\mathbf{A}_0$ представления (кодирования) алфавита A_0 назовем *допустимой*, если существует такая матрица $\mathbf{A}$, что пара $(\mathbf{A}_0, \mathbf{A})$ задает разложение алфавита A. Для $v = 1, \ldots, s$ через $\mathbf{a}_i(v)$ и $\mathbf{a}_T(v)$ будем обозначать v-ю компоненту наборов $\mathbf{a}_i$ и $\mathbf{a}_T$. Пусть $\mathbf{A}_0$ — некоторое кодирование алфавита A_0. Построим по нему представление $\mathbf{A}'$ алфавита A, положив для $T \in \mathcal{T}$ и $v = 1, \ldots, s$ значение $\mathbf{a}'_T(v)$ равным τ, $\tau \in \{0,1\}$, если $\mathbf{a}_i(v) = \tau$ для всех $i \in T$, и равным $*$, если найдутся $i_1, i_2 \in T$, для которых $\mathbf{a}_{i_1}(v) \neq \mathbf{a}_{i_2}(v)$. Следующая лемма

сводит вопросы существования и построения разложений алфавита к вопросам существования и построения допустимых кодирований.

Лемма 1. *Если кодирование* $\mathbf{A}_0$ *допустимо, то в качестве разложения алфавита* A *может быть взята пара* $(\mathbf{A}_0, \mathbf{A}')$.

Скажем, что система $\mathcal{Z}$ подмножеств множества M образует *дизъюнктивный* (*конъюнктивный*) *базис* системы $\mathcal{T}$, если каждое множество $T \in \mathcal{T}$ может быть получено как объединение (пересечение) некоторых множеств из $\mathcal{Z}$, и образует *обобщенный дизъюнктивный* (*конъюнктивный*) *базис*, если каждое $T \in \mathcal{T}$ может быть образовано посредством объединения (пересечения) каких-либо множеств из $\mathcal{Z}$ либо их дополнений (до M). Кодированию $\mathbf{A}_0$ сопоставим совокупность $\mathcal{Z} = \{Z_1, \ldots, Z_s\}$ подмножеств множества M, где Z_v образовано всеми такими $i \in M$, для которых $\mathbf{a}_i(v) = 1$.

Лемма 2. *Кодирование* $\mathbf{A}_0$ *допустимо тогда и только тогда, когда соответствующая ему система множеств* $\mathcal{Z}$ *образует обобщенный конъюнктивный базис системы* $\mathcal{T}$.

Учитывая очевидный факт существования обобщенного конъюнктивного базиса у произвольной системы $\mathcal{T}$, отсюда получаем следующий результат.

Теорема 1. *Всякий недоопределенный алфавит двоично разложим.*

В [1] рассматривалось другое понятие разложения недоопределенных данных. В отличие от понятия данной работы, оно не обеспечивает возможность разложения произвольного недоопределенного алфавита, но обладает рядом дополнительных полезных свойств.

Длину s наборов, используемых в разложении, назовем *размерностью разложения*. Минимально возможную размерность разложения алфавита A будем называть *размерностью* (*недоопределенного*) *алфавита* A и обозначать $s(A)$. *Задача о размерности алфавита* состоит в том, чтобы по A и числу k узнать, существует ли для алфавита A разложение размерности k.

Теорема 2. *Задача о размерности недоопределенного алфавита NP-полна.*

Этот факт доказывается путем сведения NP-полной задачи MP7 из [2] о базисе системы множеств к задаче о размерности. В связи с трудностью нахождения значения $s(A)$ представляют интерес оценки этой величины.

Теорема 3. *Имеет место оценка*

$$s(A) \leq \min\left(|A_0|, |A|\right),$$

достижимая для любых заданных мощностей $|A_0|$ *и* $|A|$.

Верхняя оценка доказывается путем указания обобщенного конъюнктивного базиса соответствующей мощности. В случае $|A_0| \le |A|$ им является система всех $(m-1)$-элементных подмножеств множества M, в случае $|A_0| > |A|$ — исходная система $\mathcal{T}$. Достижимость оценки подтверждается примерами.

Приведем важный случай, когда размерность существенно ниже гарантируемой теоремой 3. Обозначим через $A_{m,t}$ алфавит, образованный всеми символами, допускающими не более t доопределений. Он соответствует системе $\mathcal{T}_{m,t}$ всех не более чем t-элементных подмножеств множества M.

Теорема 4. *При $t = o(m^{1/2})$ справедливы оценки*

$$\frac{1}{\log_2 3}\, t \log_2 \frac{m}{t} \lesssim s(A_{m,t}) \lesssim \frac{e}{\log_2 e}\,(t+1)^2 \log_2 \frac{m}{t}.$$

Верхняя оценка получается путем построения конъюнктивного базиса для системы $\mathcal{T}_{m,t}$. Система множеств $\mathcal{Z}$ образует конъюнктивный базис для $\mathcal{T}_{m,t}$, если (и только если) для любых $t+1$ различных элементов $i_1, \ldots, i_t, j \in M$, из которых один элемент j отмечен, имеется $Z \in \mathcal{Z}$ такое, что $i_1, \ldots, i_t \in Z$, $j \notin Z$. Система $\mathcal{Z}$ с этим свойством и оценкой мощности, соответствующей верхней оценке теоремы, находится с использованием градиентной процедуры (жадного алгоритма). Нижняя оценка теоремы — мощностная.

Для $t = \mathrm{const}$ оценки теоремы являются точными по порядку.

Работа выполнена при финансовой поддержке ОНИТ РАН по программе фундаментальных исследований.

Список литературы

1. Шоломов Л. А. Декомпозиция недоопределенных данных // Проблемы теоретической кибернетики. Материалы XVI Международной конференции. – Нижний Новгород: Изд. НГУ, 2011. – С. 570–573.

2. Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи. — М.: Мир, 1982.

Секция «Функциональные системы»

О ПОЛНОТЕ СИСТЕМ ФУНКЦИЙ В КЛАССЕ T_1 ДЛЯ КЛАССОВ РАСШИРЕННОЙ СУПЕРПОЗИЦИИ

Я. В. Акулов (Москва)

Э. Пост [1] получил полное описание семейства замкнутых (относительно операции суперпозиции) классов функций двузначной логики (см., например, [2]). Обозначения для замкнутых классов взяты согласно работе [3]. В работе рассматривается задача о реализации булевых функций формулами специального вида. Вводится понятие пополнения систем булевых функций. Устанавливаются критерии полноты в классе функций, сохраняющих единицу, для рассматриваемых функциональных систем. Необходимые определния можно найти в [4].

Пусть F — множество булевых функций, содержащее все селекторные функции и замкнутое относительно операций введения несущественных переменных и переименования переменных (включая отождествление). Будем называть такие множества *инвариантными классами*. Отметим, что данное понятие инвариантного класса отличается от понятия инвариантного класса, введенного С. В. Яблонским [5]. Отметим также, что инвариантный класс в описанном выше смысле является инвариантным классом в терминах, введенных в работе [6].

Пусть F — инвариантный класс булевых функций, $\mathfrak{A}$ — некоторое множество булевых функций. Пару таких множеств $(\mathfrak{A}, F)$ будем называть *типом* булевых функций. Определим понятие *формулы над типом* $U = (\mathfrak{A}, F)$ индуктивно.

1. Выражение $g(x_{i_1}, x_{i_2}, \ldots, x_{i_n})$, где $g \in F$; $x_{i_1}, \ldots, x_{i_n}$ — символы переменных, $n \geq 1$, является формулой над U. Такие формулы будем называть *тривиальными* формулами над U.

2. Пусть $\Phi_1, \Phi_2, \ldots, \Phi_n$ — формулы над U, $n \geq 1$, а $f \in \mathfrak{A}$. Выражение Φ вида $f(\Phi_1, \Phi_2, \ldots, \Phi_n)$ является формулой над U.

Очевидно, что всякая формула над типом U реализует некоторую булеву функцию. Способ реализации булевых функций нетривиальными формулами указанного вида будем называть *операцией*

расширенной суперпозиции.

Пусть $U = (\mathfrak{A}, F)$ — тип булевых функций. *Пополнением* системы $\mathfrak{A}$ относительно класса F назовем множество всех функций, реализуемых нетривиальными формулами над U (обозначение $[\mathfrak{A}]_F$). Отметим, что, если F состоит только из селекторных функций, то $[\mathfrak{A}]_F = [\mathfrak{A}]$. Несложно доказать, что $[\mathfrak{A}]_F = [[\mathfrak{A}]]_F$. Поэтому в дальнейшем будем рассматривать только пополнения замкнутых классов. Пусть A и B — замкнутые классы булевых функций, F — инвариантный класс, такие, что выполняются соотношения $A \subseteq B$, $F \subseteq B$. Будем называть тип (A, F) *полным в классе* B, если $[A]_F = B$. В работе [7] получен критерий полноты в классе P_2. В данной работе приводится критерий полноты в классе T_1.

Обозначим через $\mathfrak{R}(M, T_1)$ множество всех инвариантных классов F, таких, что выполняется хотя бы одно из следующих условий: $x_1 + x_2 + 1 \in F$ или $x_1 \to x_2 \in F$. Обозначим через $\mathfrak{R}(T_0, T_1)$ множество всех инвариантных классов F, таких, что $1 \in F$. Положим $\mathfrak{R}(I^m, T_1) = \mathfrak{R}(T_0, T_1)$, $m = 2, 3, \ldots, \infty$. Обозначим через $\mathfrak{R}(O^m, T_1)$, $m = 2, 3, \ldots, \infty$, множество всех инвариантных классов F, таких, что для любого $n \geq 2$, любого $k \leq m$ и любых k отличных от единичного наборов длины n существует функция $f(x_1, \ldots, x_n)$ из класса F, принимающая на каждом из этих наборов нулевое значение. Обозначим через $\mathfrak{R}(S, T_1)$ множество всех инвариантных классов F, таких, что $1 \in F$. Обозначим через $\mathfrak{R}(L_1, T_1)$ множество всех инвариантных классов F, таких, что для любого $m \geq 1$ существует функция $g(x_1, \ldots, x_m) \in F$ ранга m. Обозначим через $\mathfrak{R}(L_{01}, T_1)$ множество всех инвариантных классов F, таких, что для любого $m \geq 1$ существует функция $g(x_1, \ldots, x_m) \in F$ ранга m, и $\{1\} \in F$. Обозначим через $\mathcal{D}$ множество всех булевых функций, для которых выполнено равенство $f(x_1, \ldots, x_n) = x_1^{\sigma_1} \vee x_2^{\sigma_2} \vee \ldots \vee x_n^{\sigma_n}$, где $\sigma_1, \ldots, \sigma_n \in \{0, 1\}, n \geq 1$. Обозначим через $\mathfrak{R}(K_{01}, T_1)$ множество всех таких инвариантных классов F, таких, что выполняется соотношение $\{1\} \cup (\mathcal{D} \cap T_1) \subseteq F$. Обозначим через $\mathfrak{R}(K_1, T_1)$ множество всех инвариантных классов F, таких, что выполняется соотношение $\mathcal{D} \cap T_1 \subseteq F$. Обозначим через $\mathcal{K}'$ множество всех отличных от константы 0 булевых функций, для которых выполнено равенство

$$f(x_1, \ldots, x_n) = (x_1^{\sigma_1} \& x_2^{\sigma_2} \& \ldots \& x_n^{\sigma_n}) \vee (x_1 \& x_2 \& \ldots \& x_n),$$

где $\sigma_1, \ldots, \sigma_n \in \{0, 1\}, n \geq 1$. Обозначим через $\mathfrak{R}(D_{01}, T_1)$ множество всех таких инвариантных классов F, таких, что выполняется соотношение $\mathcal{K}' \subseteq F$. Положим $\mathfrak{R}(D_1, T_1) = \mathfrak{R}(D_{01}, T_1)$. Обозначим через $\mathfrak{R}(SM, T_1)$ пересечение классов $\mathfrak{R}(M, T_1)$, $\mathfrak{R}(O^2, T_1)$ и $\mathfrak{R}(I^2, T_1)$.

Обозначим через $\mathfrak{R}(M_{01}, T_1)$, $\mathfrak{R}(MI_1^m, T_1)$, $\mathfrak{R}(MO^m, T_1)$ пересечение семейства $\mathfrak{R}(M, T_1)$ с семействами $\mathfrak{R}(T_0, T_1)$, $\mathfrak{R}(I^m, T_1)$, $\mathfrak{R}(T_0, T_1)$ соответственно. Обозначим через $\mathfrak{R}(S_{01}, T_1)$, $\mathfrak{R}(O_0^m, T_1)$, $\mathfrak{R}(MO_0^m, T_1)$ пересечение семейства $\mathfrak{R}(T_0, T_1)$ с семействами $\mathfrak{R}(S, T_1)$, $\mathfrak{R}(O^m, T_1)$, $\mathfrak{R}(MO^m, T_1)$ соответственно. Положим $\mathfrak{R}(I_1^m, T_1) = \mathfrak{R}(I^m, T_1)$ и $\mathfrak{R}(M_1, T_1) = \mathfrak{R}(M, T_1)$.

Теорема. *Пусть A — замкнутый класс, такой, что $A \subseteq T_1$, $A \neq T_1$, $A \neq C_1$. Пусть F — инвариантный класс, такой, что $F \subseteq T_1$. Тогда тип (A, F) является полным в классе T_1 тогда и только тогда, когда $F \in \mathfrak{R}(A, T_1)$.*

Работа выполнена при финансовой поддержке РФФИ (проект 11–01–00508) и программы фундаментальных исследований ОМН РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения» (проект «Задачи оптимального синтеза управляющих систем»)

Список литературы

1. Post E. L. Introduction to a general theory of elementary propositions // Amer. J. Math. — 1921. — V. 43, № 3. — С. 163–185.

2. Яблонский С. В., Гаврилов Г. П., Кудрявцев В. Б. Функции алгебры логики и классы Поста. — М.: Наука, 1966.

3. Угольников А. Б. Классы Поста. — М.: Изд-во ЦПИ при механико-математическом ф-те МГУ, 2008.

4. Яблонский С. В. Введение в дискретную математику. — М.: Высшая школа, 2006.

5. Яблонский С. В. Об одном семействе классов функций алгебры логики, допускающих простую схемную реализацию // Успехи матем. наук. — 1957. — Т. 12. — С. 139–196.

6. Кузнецов Ю. В. О классах булевых функций, инвариантых относительно отождествления переменных // Докл. АН СССР. — 1986. — Т. 290, № 4. — С. 780–785.

7. Акулов Я. В. Критерии полноты для классов расширенной суперпозиции // Мат-лы X Межд. сем. “Дискретная математика и ее приложения” (Москва, МГУ, 1–6 февраля 2010 г.). — М.: Изд-во механико-математического факультета МГУ, 2010. — С. 167–169.

ДИАГОНАЛЬНЫЕ РАНГИ ПОЛУГРУПП

И. В. Барков, И. Б. Кожухов (Москва)

Пусть S — полугруппа. Тогда $S \times S$ является правым диагональным S-полигоном, если S действует на $S \times S$ следующим образом: $(x, y)s = (xs, ys)$. Левый диагональный полигон и биполигон определяются аналогично. Обозначаются соответственно $(S \times S)_S$ и ${}_S(S \times S)$, ${}_S(S \times S)_S$. Множество $S^n = \underbrace{S \times \ldots \times S}_{n}$ очевидным образом так же может быть сделано левым, правым полигоном и биполигоном.

В работе [1] было доказано, что полигоны $(S \times S)_S$, ${}_S(S \times S)$, ${}_S(S \times S)_S$ являются циклическими, если в качестве S выбирать T_X, P_X, B_X где X — бесконечное множество, T_X — моноид преобразований множества X, P_X — моноид частичных преобразований и B_X — моноид всех бинарных отношений на X.

Правым диагональным рангом полугруппы S (обозначается $\mathrm{rdr}S$) назовём наименьшую мощность системы образующих правого диагонального полигона $(S \times S)_S$. Левый диагональный ранг ldr и бидиагональный ранг bdr определяются аналогично. Под $\mathrm{rdr}_n S$ будем понимать правый диагональный ранг полугруппы S порядка n, т.е. наименьшую мощность системы образующих полигона $(S^n)_S$.

Отметим следующие очевидные утверждения:

- $\mathrm{rdr}(A \times B) \leq \max(\mathrm{rdr}A, \mathrm{rdr}B)$;
- $\mathrm{rdr}(S/\rho) \leq \mathrm{rdr}S$ для любой конгруэнции ρ;
- $\mathrm{rdr}(S \cup \{0\}) \leq 3 \cdot \mathrm{rdr}S$;
- $\mathrm{rdr}(S \cup \{1\}) = \infty$ если полугруппа S бесконечна и $1 \notin S$.

Более того, можно доказать следующие утверждения.

Теорема. *Если n нечётно, то* $\mathrm{rdr}_n S \leq (\mathrm{rdr}S)^n$, *а если n чётно, то* $\mathrm{rdr}_n S \leq (\mathrm{rdr}S)^{n-1}$.

Следствие. *Если полигон $(S \times S)_S$ является циклическим, то полигоны $(S^n)_S$ так же являются циклическими для любого $n > 2$.*

Теорема. *Пусть V — линейное пространство над некоторым полем, R — кольцо всех линейных оторбражений $V \to V$, рассматриваемое как полугруппа с умножением, определённым следующим образом: $(vr_1)r_2 = v(r_1 r_2)$. Тогда $rdrR = 1$. Более того, $(a, b)R = R \times R$ тогда и только тогда, когда a, b удовлетворяют условию* $\ker a = \ker b = 0$ *и* $\mathrm{im}a \cap \mathrm{im}b = 0$.

Список литературы

1. Gallagher P., Ruškuc N. Generation of diagonal acts of some semigroups of transformations and relations // Bulletin Australian Mathematical Society. — 2005. — V. 72. — P. 139–146.

ПОЛИНОМИАЛЬНЫЙ АЛГОРИТМ РАСПОЗНАВАНИЯ ФУНКЦИЙ, ИНВАРИАНТНЫХ ОТНОСИТЕЛЬНО ПРЕОБРАЗОВАНИЯ МЁБИУСА

А. В. Бухман (Москва)

В данной заметке предложен полиномиальный алгоритм, который для произвольной булевой функции, заданной полиномом Жегалкина, определяет, является ли эта функция инвариантной относительно преобразования Мёбиуса.

Каждая булева функция $f(x_1, \ldots, x_n)$ может быть задана единственным полиномом Жегалкина [1]. Рассмотрим следующую задачу: требуется построить эффективный алгоритм, который для булевой функции, поданной ему на вход в виде полинома, определял бы, обладает ли эта функция некоторым заданным свойством. При такой постановке проверка большинства свойств, используемых на практике, непосредственно по определению имеет экспоненциальную временную алгоритмическую сложность относительно размера входных данных, то есть размера символьной записи полинома. Поэтому интересным является вопрос о построении полиномиальных алгоритмов. Селезневой С. Н. [2], Горшковым С. П. [3] доказана полиномиальная решаемость задач распознавания ряда свойств для булевых функций.

Мы будем рассматривать следующее свойство: является ли булева функция инвариантной относительно преобразования Мёбиуса. Это свойство находит применение в криптографии [4].

Пусть $E_2 = \{0, 1\}$. *Булевой функцией*, зависящей от n переменных, будем называть любое отображние вида $f : E_2^n \to E_2$.

Будем задавать булевы функции в виде полиномов.

Мономом над переменными $x_1, \ldots, x_n$ называется любое выражение вида $x_{i_i} \ldots x_{i_l}$, где $l \geq 1, 1 \leq i_1, \ldots, i_l \leq n$, все переменные

различны; либо просто 1. *Рангом* монома назовём количество переменных в нём (будем обозначать rk).

Равенство мономов рассматривается с точностью до перестановки сомножителей.

Полиномом называется сумма по модулю 2 конечного числа различных мономов или 0 (можно понимать как сумму нулевого числа мономов). *Длиной* полинома называется число его слагаемых. Длину нулевого полинома будем считать равной 0.

Равенство полиномов рассматривается с точностью до перестановки слагаемых.

Полином Жегалкина функции f будем обозначать P_f.

Преобразованием Мёбиуса функции $f \in P_2^n$ будем называть функцию $g \in P_2^n$ такую, что $g(\alpha) = \bigoplus\limits_{\beta \leq \alpha} f(\beta)$. Будем обозначать $\mu(f) = g$.

Будем говорить, что функция $f \in P_2$ *инвариантна относительно преобразования Мёбиуса*, если $\mu(f) = f$ (см., например, [4]).

Введём обозначение K_α для обозначения монома, соответствующего набору α и равного $x_{i_1} \dots x_{i_s}$, при этом переменная x_{i_j} входит в этот моном тогда и только тогда, когда $\alpha_{i_j} = 1$. Введём естественное упорядочение на множестве мономов от переменных $x_1, \dots, x_n$: $K_\alpha \geq K_\beta$, если $\alpha \geq \beta$.

В качестве алгоритмической модели будем рассматривать RAM. Если в полиноме l слагаемых и n переменных, то положим, что длина его записи равна $N = ln$.

Лемма 1. *Пусть функция $f \in P_2^n$ инвариантна относительно преобразования Мёбиуса. Пусть $K \in P_f$, и набор α удовлетворяет условиям, что $f(\alpha) = 0$, и не существует $\tilde{K} \in P_f$ такого, что $K_\alpha > \tilde{K} > K$. Тогда найдётся слагаемое $K' \in P_f$, такое что $K'K = K_\alpha$.*

Доказательство. Для каждого слагаемого $K \in P_f$ функции f проведём индукцию по рангу набора.

Пусть $|\alpha| = \mathrm{rk}(K) + 1$, тогда $f(\alpha)K(\alpha) = f(\alpha) = 0$. Но при этом $K \in P_{fK}$. Следовательно, найдётся слагаемое $K' \in P_f$(возможно не одно, но их должно быть нечётное число) такое, что $K'K = K_\alpha$.

Шаг индукции.

Пусть верно для ранга $s > \mathrm{rk}(K)$, покажем для ранга $s+1$. Возьмём набор α, такой что $|\alpha| = s + 1$. По предположению индукции каждой точке $\beta < \alpha$ такой, что $K_\beta > K$ соответствует нечётное число мономов K'' таких, что $K''K = K_\beta$. Далее, для разных β со-

ответствующие им K'' различны. Теперь предположим, что нет K' такого, что $K'K = K_\alpha$, получаем, что $K(\alpha) \cdot f(\beta) = 1$, но $f(\beta) = 0$.

Теорема. *Свойство булевой функции быть инвариантной относительно преобразования Мёбиуса можно распознать по её полиному со сложностью $O(N^3)$, где N — длина записи полинома.*

Доказательство. Наборы значений аргументов можно разбить на три группы:

1. Точки, не сравнимые ни с одной конъюнкцией полинома f или меньшие минимальной из них. Эти точки проверять не надо — там функция равна 0, как и ожидается.

2. Точки, лежащие строго выше хотя бы одной конъюнкции полинома. В этих точках функция должна быть равно 0. Просто проверим значение функции во всех этих точках. Для каждой конъюнкции P_f запускаем обход в глубину (вверх по булеву кубу) по нулям функции f. Чтобы функция была инвариантна относительно преобразования Мёбиуса, обход должен завершиться не более, чем за $O(l)$ (l – длина полинома, это из леммы 1) шагов, и на каждом шаге проверяем, что $f = 0$ (со сложностью $O(ln)$) и что текущая вершина не равна ни одному слагаемому полинома. Получаем $O(N^2)$ шагов. Всего конъюнкций l. Поэтому общая сложность $O(lN^2) = O(N^3)$.

3. Точки соответствующие конъюнкциям. Они проверяются за линейное время

Работа выполнена при поддержке РФФИ, грант 12-01-00706-а.

Список литературы.

1. Логачев О. А., Сальников А. А., Ященко В. В. Булевы функции в теории кодирования и криптологии. — М.:МЦНМО: 2004.

2. Селезнева С. Н. О сложности распознавания полноты множества булевых функций, реализованных полиномами Жегалкина // Дискретная математика. — 1997. — Т. 4, вып. 9. — С. 34–41.

3. Горшков С. Н. О сложности распознавания мультиаффинности, биюнктивности, слабой положительности и слабой отрицательности булевой функции. Обозрение прикл. и промышленной матем. Сер. Дискр.матем. — 1997. — 4, вып. 2. — С. 216–237.

4. Pieprzyk J., Zhang X.-M. Computing mobius transforms of boolean functions and characterising coincident boolean functions // Boolean Functions: Cryptography and Applications. France, Rouen: Publications des Universites de Rouen et du Havre, 2007. — P. 135–151.

О СУЩЕСТВОВАНИИ СПЕЦИАЛЬНЫХ ПОРОЖДАЮЩИХ СИСТЕМ В КЛАССАХ МОНОТОННЫХ ФУНКЦИЙ МНОГОЗНАЧНОЙ ЛОГИКИ

О. С. Дудакова (Москва)

Известно, что при $k \leq 7$ все предполные классы в $\mathcal{P}_k$ являются конечно-порожденными [1], а начиная с $k = 8$ существуют предполные классы монотонных функций, не имеющие конечного базиса [2]; полного описания конечно-порожденных предполных классов монотонных функций к настоящему времени не получено. В работах автора [3–6] приводится критерий конечной порожденности для предполных классов функций, монотонных относительно частично упорядоченных множеств ширины два, а также условия существования конечных порождающих систем для ряда других семейств классов монотонных функций. В данной работе продолжены исследования в этом направлении.

Пусть $\preccurlyeq$ — частичный порядок на множестве $E_k = \{1, 2, \ldots, k\}$. Положим $\mathcal{P} = (E_k, \preccurlyeq)$. Будем считать, что множество $\mathcal{P}$ имеет наименьший и наибольший элементы. Через $\mathcal{M}_\mathcal{P}$ будем обозначать класс всех монотонных функций над $\mathcal{P}$ (отметим, что класс $\mathcal{M}_\mathcal{P}$ является предполным [7]).

Функцию $\lambda(x_0, x_1, \ldots, x_k)$ будем называть *функцией выбора*, если $\lambda(i, a_1, \ldots, a_k) = a_i$ для каждого набора $(i, a_1, \ldots, a_k) \in \mathcal{P}^{k+1}$. Легко видеть, что если замкнутый класс функций k-значной логики содержит все константы $1, 2, \ldots, k$ и функцию выбора, то он является конечно-порожденным. Отметим также, что если $\mathcal{P}$ — частично упорядоченное множество, содержащее хотя бы одну цепь длины 2, то $\lambda(x_0, x_1, \ldots, x_k) \notin \mathcal{M}_\mathcal{P}$.

Положим $\mathcal{P}_\lambda = \{(a, b_1, \ldots, b_k) \in \mathcal{P}^{k+1} \mid \text{если } i \preccurlyeq j, \text{ то } b_i \preccurlyeq b_j\}$. Легко видеть, что функция λ монотонна на множестве $\mathcal{P}_\lambda$. Назовем *монотонной функцией выбора* функцию $\nu(x_0, x_1, \ldots, x_k)$ из $\mathcal{M}_\mathcal{P}$, совпадающую на множестве $\mathcal{P}_\lambda$ с функцией $\lambda(x_0, x_1, \ldots, x_k)$. Нетрудно показать, что если класс $\mathcal{M}_\mathcal{P}$ содержит монотонную функцию выбора, то он является конечно-порожденным.

Пусть a_1 и a_2 — элементы множества $\mathcal{P}$, не сравнимые относительно $\preccurlyeq$. Элемент $b \in \mathcal{P}$ называется *верхней гранью* элементов a_1 и a_2, если выполняется неравенство $a_1, a_2 \preccurlyeq b$. Верхняя грань b элементов a_1 и a_2 называется *минимальной верхней гранью* этих элементов, если не существует такой верхней грани c элементов a_1 и a_2, что $c \neq b$ и $c \preccurlyeq b$. Верхняя грань b элементов a_1 и a_2 называется

точной верхней гранью этих элементов ($\sup(a_1, a_2)$), если для любой верхней грани c элементов a_1 и a_2 выполняется неравенство $b \preccurlyeq c$. Аналогичным образом определяется *нижняя, максимальная нижняя* и *точная нижняя грань* элементов a_1 и a_2 (точная нижняя грань обозначается $\inf(a_1, a_2)$). Через $|\mathcal{P}|$ будем обозначать число элементов множества $\mathcal{P}$. Величину $\max|J|$, где максимум берется по всем антицепям J множества $\mathcal{P}$, будем называть *шириной* множества $\mathcal{P}$.

Рассмотрим два семейства частично упорядоченных множеств. Семейство $\mathbb{S}_1$ состоит из всех множеств $\mathcal{P}$, таких, что для любых элементов $a, b \in \mathcal{P}$ в $\mathcal{P}$ существует по крайней мере один из элементов $\sup(a, b)$ и $\inf(a, b)$. Семейство $\mathbb{S}_2$ состоит из всех множеств $\mathcal{P}$, для которых выполняется следующее условие: для любой пары несравнимых элементов a_1 и a_2, не имеющих в $\mathcal{P}$ точной верхней грани, и для любой верхней грани c элементов a_1 и a_2, не сравнимой с некоторой минимальной верхней гранью b этих элементов, в $\mathcal{P}$ существует $\sup(b, c)$. Отметим, что в классе множеств ширины два выполняется равенство $\mathbb{S}_1 = \mathbb{S}_2$, а для множеств большей ширины имеет место строгое включение $\mathbb{S}_1 \subset \mathbb{S}_2$.

Теорема 1 [8]. *Пусть $\mathcal{P}$ — частично упорядоченное множество ширины два. Класс $\mathcal{M}_\mathcal{P}$ содержит монотонную функцию выбора тогда и только тогда, когда $\mathcal{P} \in \mathbb{S}_1$.*

Теорема 2 [9]. *Пусть $\mathcal{P}$ — произвольное частично упорядоченное множество. Если класс $\mathcal{M}_\mathcal{P}$ содержит монотонную функцию выбора, то $\mathcal{P} \in \mathbb{S}_2$.*

Основным результатом данной работы является

Теорема 3. *Пусть $\mathcal{P}$ — частично упорядоченное множество ширины три. Класс $\mathcal{M}_\mathcal{P}$ содержит монотонную функцию выбора тогда и только тогда, когда $\mathcal{P} \in \mathbb{S}_2$.*

Работа выполнена при финансовой поддержке РФФИ, проект № 11-01-00508, и программы фундаментальных исследований Отделения математических наук РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения», проект «Задачи оптимального синтеза управляющих систем».

Список литературы

1. Lau D. Bestimmung der Ordnung maximaler Klassen von Funktionen der k-wertigen Logik // Z. math Log. und Grundl. Math. — 1978. — V. 24. — S. 79–96.

2. Tardos G. A not finitely generated maximal clone of monotone operations // Order. — 1986. — V. 3. — P. 211–218.

3. Дудакова О. С. О классах функций k-значной логики, монотонных относительно множеств ширины два // Вестн. Моск. ун-та.

Серия 1. Математика. Механика. — 2008. — № 1. — С. 31–37.

4. Дудакова О. С. О конечной порожденности замкнутых классов монотонных функций в P_k // Учен. зап. Казан. ун-та. Серия Физ.-матем. науки. — 2009. — Т. 151, кн. 2. — С. 65–71.

5. Дудакова О. С. О конечной порожденности предполных классов монотонных функций девятизначной логики // Мат-лы XVIII Междунар. школы-семинара "Синтез и сложность управляющих систем" (Пенза, 28 сентября – 3 октября 2009 г.). — М.: Изд-во мех.-матем. ф-та МГУ, 2009. — С. 38–41.

6. Дудакова О. С. О классах функций k-значной логики, монотонных относительно множеств ширины три // Мат-лы X Междунар. семинара "Дискретная математика и ее приложения" (Москва, МГУ, 1–6 февраля 2010 г.). — М.: Изд-во мех.-матем. ф-та МГУ, 2010. — С. 178–180.

7. Мартынюк В. В. Исследование некоторых классов в многозначных логиках // Проблемы кибернетики. Вып. 3. — М.: Наука. — 1960. — С. 49–60.

8. Дудакова О. С. О порождающих системах специального вида для предполных классов монотонных функций k-значной логики // Мат-лы XVI Междунар. конф. "Проблемы теоретической кибернетики" (Нижний Новгород, 20–25 июня 2011 г.). — Нижний Новгород: Изд-во Нижегородского гос. ун-та, 2011. — С. 145–147.

9. Дудакова О. С. О существовании порождающих систем специального вида в классах монотонных функций k-значной логики // Мат-лы VIII молодежной научной школы по дискретной математике и ее приложениям (Москва, 24–29 октября 2011 г.). Часть I. — 2011. — С. 27–29.

О СВЯЗЯХ МЕЖДУ ПОЛИГОНАМИ И МУЛЬТИПОЛИГОНАМИ

И. Б. Кожухов, И. А. Лукиных (Москва)

Правым полигоном над полугруппой S (см. [1]) называется множество X, на котором действует полугруппа S, то есть определено отображение $X \times S \to X, (x, s) \mapsto xs$, удовлетворяющее условию $x(ss') = (xs)s'$, при $x \in X, s, s' \in S$. *Левый полигон* определяется

аналогичным образом: $S \times Y \to Y, (ss')y = s(s'y)$. Полигон X (правый или левый) является алгебраической моделью автомата [2], где X — множество состояний, S — множество входных сигналов.

Если S и T — полигоны, то (S,T)-биполигоном называется множество X, являющееся левым полигоном над S и правым полигоном над T, и при этом выполняется условие $(sx)t = s(xt)$ при $x \in X, s \in S, t \in T$. Обозначим через S^{op} полугруппу, антиизоморфную полугруппе S, то есть множество S с операцией $a*b = ba$. Левый полигон X над полугруппой S можно сделать правым полигоном над полугруппой S^{op}, если положить $x * s = sx$ при $x \in X, s \in S$.

Аналогично этому (S,T)-биполигон можно считать правым полигоном над полугруппами S^{op} и T, причём $(xs)t = (xt)s$ при $x \in X, s \in S^{op}, t \in T$. Учитывая вышесказанное, мы можем считать, что все полигоны — правые, а (S,T)-биполигон — это множество, являющееся правым полигоном над S и над T, и действия этих полугрупп перестановочны.

Аналогичным образом, если $\{S_i | i \in I\}$ — семейство полугрупп, то *мультиполигоном* (см.[3]) называется множество X, на котором действуют полугруппы S_i, причём $(xs_i)s_j = (xs_j)s_i$ при $x \in X_j, s_i \in S_i, s_j \in S_j$, где $i \neq j$.

Предложение 1. Любой (S,T)-биполигон X является полигоном над прямым произведением $S \times T$, если положить $x \cdot (s,t) = (xs)t$ при $x \in X, s \in S, t \in T$.

Интересен вопрос о том, верно ли обратное, т. е. всякий ли полигон X над $S \times T$ является (S,T)-биполигоном, другими словами можно ли определить для элементов из X умножения на элементы $s \in S$ и $t \in T$, чтобы выполнялось условие $x \cdot (s,t) = (xs)t$?

Предложение 2. Если S и T — полугруппы с единицей, то всякий полигон над $S \times T$ является (S,T)-биполигоном, причём $x \cdot (s,t) = (xs)t$ при $x \in X, s \in S, t \in T$.

Доказательство. Определим действия полугрупп S и T на X следующим образом: $xs = x \cdot (s,1), xt = x \cdot (1,t)$ при $x \in X, s \in S, t \in T$. Непосредственно проверяется, что X - (S,T)-биполигон. При этом $x \cdot (s,t) = x \cdot ((s,1) \cdot (1,t)) = (x \cdot (s,1)) \cdot (1,t) = (xs)t$.

Заметим, что для доказательства этого утверждения не требуется, чтобы полигон над $S \times T$ был *унитарным* (т.е. $x \cdot (1,1) = x$ при всех $x \in X$).

Если полугруппы S и T не имеют единицы, то полигон над $S \times T$ может не являться (S,T)-биполигоном — соответствующий пример построен в работе [4]. А если полугруппа S имеет единицу, а T — не

имеет? Оказывается и в этом случае существует пример полигона над $S \times T$, не являющегося (S,T)-биполигоном.

Пример. Пусть $S = \{e\} \cup \{(l_i, r_j) | i,j = 1,2\}$ — полугруппа с умножением $es = se = s \quad \forall s \in S$ и $(l_i, r_j) \cdot (l_k, r_m) = (l_i, r_m)$, $T = \{b_1, b_2 | b_i b_j = b_j\}$ — двухэлементная полугруппа правых нулей. Элементы полугруппы $S \times T$ будем записывать в виде $(e, b_i), ((l_i, r_j), b_k)$. Очевидно, $|S \times T| = 10$. Рассмотрим отношение эквивалентности на $S \times T$, у которого один класс состоит из элементов (e, b_1) и (e, b_2), а другие классы одноэлементны. Нетрудно видеть, что ρ — правая конгруэнция на $S \times T$. Положим $X = (S \times T)/\rho$. Очевидно, X — правый $(S \times T)$-полигон. Докажем, что он не является (S,T)-биполигоном.

Предположим, что X — (S,T)-биполигон, и приведём это предположение к противоречию. Элементы из X пронумеруем: $1 = \{(e, b_1), (e, b_2)\}$, $2 = ((l_1, r_1), b_1)$, $3 = ((l_1, r_1), b_2)$, $4 = ((l_1, r_2), b_1)$, $5 = ((l_1, r_2), b_2)$, $6 = ((l_2, r_1), b_1)$, $7 = ((l_2, r_1), b_2)$, $8 = ((l_2, r_2), b_1)$, $9 = ((l_2, r_2), b_2)$. Действия элементов полугруппы $S \times T$ на X запишем в виде отображений:

$$(e, b_1) = \begin{pmatrix} 123456789 \\ 122446688 \end{pmatrix}, \quad (e, b_2) = \begin{pmatrix} 123456789 \\ 133557799 \end{pmatrix},$$

$$((l_1, r_1), b_1) = \begin{pmatrix} 123456789 \\ 222226666 \end{pmatrix}, \quad ((l_1, r_1), b_2) = \begin{pmatrix} 123456789 \\ 333337777 \end{pmatrix},$$

$$((l_1, r_2), b_1) = \begin{pmatrix} 123456789 \\ 444448888 \end{pmatrix}, \quad ((l_1, r_2), b_2) = \begin{pmatrix} 123456789 \\ 555559999 \end{pmatrix},$$

$$((l_2, r_1), b_1) = \begin{pmatrix} 123456789 \\ 622226666 \end{pmatrix}, \quad ((l_2, r_1), b_2) = \begin{pmatrix} 123456789 \\ 733337777 \end{pmatrix},$$

$$((l_2, r_1), b_1) = \begin{pmatrix} 123456789 \\ 844448888 \end{pmatrix}, \quad ((l_2, r_1), b_2) = \begin{pmatrix} 123456789 \\ 955559999 \end{pmatrix}.$$

По предположению X является полигоном над S и над T и $(xs)t = (xt)s = x \cdot (s,t)$ при $s \in S, t \in T$.

Применяя данное равенство к различным элементам полугрупп S и T, убеждаемся в том, что $1b_1 = 1$, $1b_2 = 1$.

Теперь имеем: $1(l_1, r_1) = 1b_1 \cdot (l_1, r_1) = 1((l_1, r_1), b_1) = 2$. В то же время: $1(l_1, r_1) = 1b_2 \cdot (l_1, r_1) = 1((l_1, r_1), b_2) = 3$. Мы получили противоречие.

В заключение докажем, что и в случае нескольких полугрупп $S_1, \ldots, S_n$ могут существовать полигоны над прямым произведением $S_1 \times \ldots \times S_n$, не являющиеся $(S_1 \times \ldots \times S_n)$-мультиполигонами, даже если все полугруппы S_i, кроме одной, имеют единицы.

Действительно, пусть S_1, S_2 — полугруппы из примера, рассмотренного выше, причём S_1 без единицы, S_2 с единицей, X — 9-элементный полигон (из того же примера) над $S_1 \times S_2$, не являющийся (S_1, S_2)-биполигоном. Пусть $S_3, \ldots, S_n$ — произвольные полугруппы с единицами (например, группы). Определим действие на X элементов из $S_1 \times S_2 \times S_3 \times \ldots \times S_n$ следующим образом: $x \cdot (s_1, s_2, \ldots, s_n) = x \cdot (s_1, s_2)$. Нетрудно проверить, что получится $(S_1 \times \ldots \times S_n)$-полигон, не являющийся $(S_1 \times \ldots \times S_n)$-мультиполигоном.

Список литературы

1. Kilp M., Knauer U., Mikhalev A. V. Monoids, acts and categories. — Berlin, N. Y.: W. de Gruyter, 2000.

2. Плоткин Б. И., Гринглаз Л. Я., Гварамия А. А. Элементы алгебраической теории автоматов. — М.: Высшая школа, 1994.

3. Максимовский М. Ю. О биполигонах и мультиполигонах над полугруппами // Матем. заметки. — 2010. — Т. 87, № 6. — 855–866.

4. Kozhukhov I. B., Maksimovskiy M. Yu. On the connections of acts with biacts // 8th Int. Algebraic Conf. in Ukraine. Book of abstracts. — Lugansk, 2011. — P. 262.

О КОЛИЧЕСТВЕ ФУНКЦИЙ, ИНВАРИАНТНЫХ ОТНОСИТЕЛЬНО ПРЕОБРАЗОВАНИЯ МЁБИУСА

А. А. Мазуров (Москва)

Булевы и k-значные функции широко применяются в криптографии и кибернетике. В работах [1] и [2] исследовано преобразование между двумя представлениями булевых функций: в виде вектора значений и в виде полинома Жегалкина. Это преобразование линейно, и оно порождает классы функций, которые являются его

собственными векторами. В этих работах установлены мощности таких классов функций, а также их иерархия и связь функций из них с другими важными свойствами.

В настоящей работе представлено обобщение полученных в [1] и [2] результатов на случай трехзначной логики.

Пусть k — натуральное число, $k \geqslant 2$. Множество всех натуральных чисел от 0 до $k-1$ обозначается через E_k: $E_k = \{0, \ldots, k-1\}$.

Функцией k-значной логики от n переменных называется отображение $f: E_k^n \to E_k$.

Множество всех функций k-значной логики от n переменных обозначается $P_k(n)$. Множество всех функций k-значной логики (от любого количества переменных) обозначается P_k.

Вектором значений функции f, зависящей от переменных $x_1, \ldots, x_n$, называется последовательность значений функции на всех наборах от $(0, \ldots, 0)$ до $(k-1, \ldots, k-1)$ в лексикографическом порядке, т. е. на наборах, обозначающих числа от 0 до $k^n - 1$ в k-ичной системе счисления в порядке возрастания.

Полиномом в k-значной логике называется формула вида

$$f(x_1, \ldots, x_n) = \sum_{\tilde{\alpha} \in E_k^n} c_{\tilde{\alpha}} x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n} \pmod{k},$$

где $x^\alpha = \begin{cases} 1, & \alpha = 0, \\ \underbrace{x \cdot x \cdot \ldots \cdot x}_{\alpha}, & \alpha \neq 0, \end{cases}$ $c_\alpha \in E_k$, $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_n)$.

Числа $c_{\tilde{\alpha}}$ называются *коэффициентами полинома*. Здесь и далее сложение и умножение элементов из E_k (а именно, значений переменых и значений функций, коэффициентов полинома) ведется по модулю k. *Вектором коэффициентов* полинома функции называется последовательность

$$c_{(0,\ldots,0)}, \ldots, c_{(k-1,\ldots,k-1)},$$

где индексы расположены в лексикографическом порядке.

Для любого простого числа k и любой функции $f \in P_k$ существует и единственно представление этой функции в виде полинома с точностью до перестановки слагаемых [3].

Преобразование Мёбиуса – это отображение, переводящее вектор значений функции в вектор коэффициентов соответствующего ей полинома.

Преобразование Мёбиуса – это биективное линейное отображение в пространстве векторов размерности k^n [3, 4].

Функцию $f \in P_k$ назовем *стационарной функцией относительно* μ^p, $p \geqslant 1$, *с константой* m, если $\mu^p(f) = m \cdot f$, где $m \in E_k \backslash \{0\}$.

Стационарным классом (функций n *переменных) с константой* m *относительно* μ^p назовем множество всех стационарных функций k-значной логики (зависящих от n переменных) с константой m относительно μ^p.

Введем следующее обозначение: $Q_m^p(n) = \{f \in P_3(n) \mid \mu^p(f) \equiv m \cdot f\}$.

1. Стационарные относительно μ^4 и μ^2 классы. Эти множества функций были рассмотрены ранее в работе [5]. Был установлен общий вид входящих в эти множества функций, а также найдены мощности этих множеств.

2. Стационарные относительно μ классы. Введем следующее обозначение:

$$R_i(n) = \{f \in P_3(n) : \mu^2(f) + i \cdot \mu(f) = f\}, \quad i = 1, 2.$$

Теорема 1. *Имеют место равенства*

$$|Q_1(n)| = |Q_1(n-1)| \times |R_1(n-1)|,$$

$$|Q_2(n)| = |Q_2(n-1)| \times |R_2(n-1)|.$$

Теорема 2. *Имеют место равенства*

$$|R_1(n)| = |R_1(n-1)| \times |Q_1^4(n-1)|,$$

$$|R_2(n)| = |R_2(n-1)| \times |Q_1^4(n-1)|.$$

Теорема 3. *Имеет место равенство*

$$|R_1(n)| = |R_2(n)| = 3^{\frac{1}{4}(3^n - (-1)^n)}.$$

Теорема 4. *Имеют место равенства*

$$|Q_1(n)| = 3^{\frac{1}{8}(3^n + 6 + (-1)^n)},$$

$$|Q_2(n)| = 3^{\frac{1}{8}(3^n - 2 + (-1)^n)}.$$

Работа выполнена при поддержке РФФИ, грант №12-01-00706-а.

Список литературы

1. Pieprzyk J., Zhang X.-M. Computing möbius transforms of boolean functions and characterising coincident boolean functions // Boolean Functions: Cryptography and Applications. — France, Rouen: Publications des Universités de Rouen et du Havre, 2007. — P. 135–151.

2. Pieprzyk J., Wang H., Zhang X.-M. Möbius-α commutative functions and partially coincident functions // Boolean Functions: Cryptography and Applications. — France, Rouen: Publications des Universités de Rouen et du Havre, 2008. — P. 135–150.

3. Яблонский С. В. Введение в дискретную математику. — М.: Наука, 1986.

4. Логачев О. А., Сальников А. А., Ященко В. В. Булевы функции в кодировании и криптологии. — М.: МЦНМО, 2004.

5. Мазуров А. А. О стационарных классах функций трехзначной логики // Вестник Московского Университета. Вычислительная математика и кибернетика. — 2012. — №. 2.

КРИТЕРИЙ НЕВЫРОЖДЕННОСТИ ПЕРИОДИЧЕСКИХ k-ЗНАЧНЫХ ФУНКЦИЙ В КЛАССЕ ПОЛЯРИЗОВАННЫХ ПОЛИНОМОВ

Н. К. Маркелов (Москва)

В работе рассматриваются функции многозначных логик. Полиномиальные формы являются одним из распространенных способов задания функций многозначных логик. Исследование сложности задания функций многозначных логик в классе полиномиальных форм важно с теоретической и практической точек зрения. Известно, что при простых k функции k-значной логики представимы обычными полиномами по модулю k единственным образом [1]. Исследуются и более общие понятия полиномов — поляризованные и обобщенные полиномы.

В классе поляризованных полиномов для булевых функций найдено точное значение функции Шеннона [2]. В случае $k \geqslant 3$ найдены верхняя [3] и нижняя [4] оценки функции Шеннона.Для поляризованных полиномов при $k \geqslant 3$ нижняя и верхняя оценки расходятся асимптотически.

В настоящей работе рассматривается подход, позволяющий оценить сложность периодических функций $k-$значной логики в классе поляризованных полиномов.

Пусть $k \geqslant 2$, $E_k = \{0, 1, \ldots, k-1\}$. Функция $f(\tilde{x}^n)$ называется *функцией k-значной логики*, если на всяком наборе $\tilde{\alpha} \in E_k^n$ ее значение содержится в E_k. Функцию k-значной логики $f(\tilde{x}^n)$ можно задавать вектором ее значений $\tilde{\alpha}_f^{k^n} = (\alpha_0, \alpha_1, \ldots, \alpha_{k^n-1})$, где координата α_i — это значение функции на наборе, представляющем запись числа i в k-ичной системе счисления.

Поляризованным по вектору поляризации $\sigma = (\sigma_1, \ldots, \sigma_n) \in E_k^n$ *полиномом* назовем выражение вида

$$\sum_{\alpha=(a_1,\ldots,a_n)\in E_k^n} c_f^\sigma(\alpha) \cdot (x_1 + \sigma_1)^{a_1} \cdot \ \ldots \ \cdot (x_n + \sigma_n)^{a_n},$$

в котором $c_f^\sigma(\alpha) \in E_k$ — некоторые коэффициенты.

В [3] показано, что для каждого вектора поляризации $\sigma \in E_k^n$, каждая функция $f(\tilde{x}^n) \in P_k^n$ представима поляризованным по вектору σ полиномом единственным образом. Поляризованный по вектору $\sigma \in E_k^n$ полином функции $f(\tilde{x}^n) \in P_k^n$ будем обозначать $P^\sigma(f)$. Назовем *вектором коэффициентов* поляризованного по вектору поляризации $\sigma \in E_k^n$ полинома функции $f(\tilde{x}^n) \in P_k^n$ вектор значений функции $c_f^\sigma(\tilde{x}^n)$.

Преобразование $W_k : E_k^k \times E_k \to E_k^k$, переводящее вектор функции одной переменной в вектор ее поляризованного полинома описано в [5].

Введем характеристику сложности функций k-значной логики в классе поляризованных полиномов. *Сложностью* $l(P^\sigma)$ *полинома* P^σ, поляризованного по вектору σ, назовем число его слагаемых с ненулевыми коэффициентами. *Сложность функции* k-значной логики f в классе поляризованных полиномов определяется как минимальная по всем поляризациям сложность полинома, реализующего эту функцию:

$$L(f) = \min_{\sigma \in E_k^n} l(P^\sigma).$$

Периодической функцией периода $t < k^n$ будем называть функцию $k-$значной логики, вектор значений $\tilde{\alpha}^{k^n}$ которой обладает следующим свойством: $\alpha_i = \alpha_{i+t} (i = \overline{0, k^n - t})$. *Последовательностью периодических* с периодом $\tilde{p}$ *функций* будем называть последовательность $\{f_n\}$, составленную из периодических функций с одинаковым периодом $\tilde{p}$ от различного количества переменных равного индексу функции в последовательности. Для *последовательности периодических функций* $\{f_n\}$ определим ее *сложность* в клас-

се поляризованных полиномов $L_{\{f_n\}}(n) = L(f_n)$. Последовательности функций $k-$значной логики (вместе с функциями, их составляющими), сложность которых в классе поляризованных полиномов $L_{\{f_n\}}(n) = o(k^n)$, будем называть *вырожденными*.

Пусть период $\tilde{p} \in E_k^T (T > k)$, обозначим $\tilde{p}^{(i)} \in E_k^k$ первые k позиций циклического сдвига периода $\tilde{p}$ на ik позиций влево. (Нетрудно заметить, что если поделить вектор значений периодической функции периода p от n переменных на пятерки компонент и пронумеровать их, начиная с нуля, то $\tilde{p}^{(i)}$ — i-я пятерка, где $i < 5^{n-1}$.)

Введем преобразование $\tilde{\Omega}_T^k : E_k^T \times E_k \to (E_k^T)^T$ вида:

$$\tilde{\Omega}_T^5(\tilde{p}, \sigma) = ((W_k(\tilde{p}^{(0)}, \sigma)[0], W_k(\tilde{p}^{(1)}, \sigma)[0], \ldots, W_k(\tilde{p}^{(T-1)}, \sigma)[0]),$$
$$(W_k(\tilde{p}^{(0)}, \sigma)[1], W_k(\tilde{p}^{(1)}, \sigma)[1], \ldots, W_k(\tilde{p}^{(T-1)}, \sigma)[1]), \ldots,$$
$$(W_k(\tilde{p}^{(0)}, \sigma)[k-1], W_k(\tilde{p}^{(1)}, \sigma)[k-1], \ldots, W_k(\tilde{p}^{(T-1)}, \sigma)[k-1])).$$

Теорема. *Последовательность периодических функций с периодом p невырождена тогда и только тогда, когда $\forall j > 0, \forall \sigma_0, \ldots, \sigma_{j-1}$ все $(\tilde{\Omega}_T^k)^j$ образы p отличны от $(00\ldots0)$.*

При помощи этого подхода были доказаны следующие утверждения:

Следствие 1. *Последовательности периодических функций трехзначной логики с периодами* $1122, 2112, 2211, 1221, 0102, 1020, 0201, 2010$ *являются невырожденными.*

Следствие 2. *Все последовательности периодических функций пятизначной логики с периодами длины* 6 *являются вырожденными.*

Следствие 3. *Все последовательности периодических функций пятизначной логики с периодами длины* 7 *и суммой компонент периода равной нулю по модулю* 5 *являются невырожденными.*

Работа выполнена при финансовой поддержке РФФИ (проект 12-01-00706-а)

Список литературы

1. Яблонский С. В. Введение в дискретную математику. — М.: Высшая школа, 2001.

2. Перязев Н. А. Сложность булевых функций в классе полиномиальных поляризованных форм // Алгебра и логика. — 1995. — Т. 34, вып. 3. — С. 323–326.

3. Селезнева С. Н. О сложности представления функций многозначных логик поляризованными полиномами // Дискретная математика. — 2002. — Т. 14, вып. 2. — С. 48–53.

4. Алексеев В. Б., Вороненко А. А., Селезнева С. Н. О сложности реализации функций k-значной логики поляризованными полиномами // Труды V Международной конференции "Дискретные модели в теории управляющих систем". — М.: МАКС Пресс, 2003. — С. 8–9.

5. Селезнева С. Н., Маркелов Н. К. Быстрый алгоритм построения векторов коэффициентов поляризованных полиномов k-значных функций // Ученые записки Казанского университета Сер. Физико-математические науки, 2009. — Т. 151, вып. 2. — С. 147–153.

ЗАМКНУТЫЕ КЛАССЫ В P_k^*, ОПРЕДЕЛЯЕМЫЕ ЗНАЧЕНИЯМИ ФУНКЦИЙ НА ПАРАЛЛЕЛОГРАММАХ

Д. Г. Мещанинов (Москва)

Пусть k — составное число, имеющее два собственных взаимно простых делителя: $k = d_1 d_2$, $1 < d_1 < k$, $1 < d_2 < k$, $(d_1, d_2) = 1$. В дальнейшем разложение $k = d_1 d_2$ считаем фиксированным, знаком $+$ обозначаем операцию сложения по модулю k.

Для фиксированных векторов $\tilde{\gamma} \in E_k^n$, $\tilde{A} \in E_{d_2}^n \setminus \{\tilde{0}\}$, $\tilde{B} \in E_{d_1}^n \setminus \{\tilde{0}\}$ множество

$$\{\tilde{\gamma},\ \tilde{\gamma} + \tilde{A}d_1,\ \tilde{\gamma} + \tilde{B}d_2,\ \tilde{\gamma} + \tilde{A}d_1 + \tilde{B}d_2\}$$

назовем *параллелограммом с вершиной* $\tilde{\gamma}$ *и сторонами* $\tilde{A}d_1$, $\tilde{B}d_2$. Будем говорить, что *функция* $f(\tilde{x})$ из P_k^* *обладает свойством параллелограмма*, или кратко П-*свойством*, если для всех $\tilde{x}$, $\tilde{A}$, $\tilde{B}$ из E_k^n выполняется равенство

$$f(\tilde{x}) + f(\tilde{x} + \tilde{A}d_1 + \tilde{B}d_2) = f(\tilde{x} + \tilde{A}d_1) + f(\tilde{x} + \tilde{B}d_2).$$

При этом не исключаются $\tilde{A} = \tilde{0}$ и $\tilde{B} = \tilde{0}$.

Если на каждом параллелограмме функция либо не имеет значений $*$, либо имеет не менее трех (т. е. три или четыре) значений $*$, то такая функция обладает П-свойством.

Покажем, как свойства значений на параллелограммах влияют на выразительные способности частичных функций и возможность их доопределения до хорошо изученных отображений, сохраняющих сравнения по обоим модулям d_1, d_2, в частности, до полиномов по модулю k.

Ранее были описаны следующие замкнутые классы.

1. Класс $C^*_{d_1,d_2}$ функций f, обладающих свойством: если $\tilde{\alpha} \equiv \tilde{\beta} \pmod{d_i}$, то либо $f(\tilde{\alpha}) = f(\tilde{\beta}) = *$, либо $f(\tilde{\alpha}) \neq *$, $f(\tilde{\beta}) \neq *$, $f(\tilde{\alpha}) \equiv f(\tilde{\beta}) \pmod{d_i}$, $i = 1, 2$.

2. Класс $C^*(d_1, d_2)$ функций f, удовлетворяющих условию: если $\tilde{\alpha} \equiv \tilde{\beta} \pmod{d_i}$, то либо $f(\tilde{\alpha}) = *$, либо $f(\tilde{\beta}) = *$, либо $f(\tilde{\alpha}) \neq *$, $f(\tilde{\beta}) \neq *$, $f(\tilde{\alpha}) \equiv f(\tilde{\beta}) \pmod{d_i}$, $i = 1, 2$.

Функции этих классов можно доопределить до отображений класса $C(d_1, d_2)$, сохраняющих сравнения по модулям d_1 и d_2, и до полиномов по модулю k (они образуют класс Po); имеют место включения

$$Po \subseteq C(d_1, d_2) \subset C^*_{d_1,d_2} \subset C^*(d_1, d_2).$$

Однако класс $C^*(d_1, d_2)$ характеризуется "большей степенью неопределенности", чем класс $C^*_{d_1,d_2}$, он более удален от классов всюду определенных функций.

Обозначим через $Par(d_1, d_2)$ класс всех функций, обладающих П-свойством.

Теорема 1. *Имеет место равенство*

$$C^*(d_1, d_2) \cap Par(d_1, d_2) = C^*_{d_1,d_2}.$$

Теорема 2. *Если функция f класса $C^*(d_1, d_2)$ имеет на некотором параллелограмме ровно одно значение $*$, то*

$$[C^*_{d_1,d_2} \cup \{f\}] = C^*(d_1, d_2).$$

Введем также подкласс $Par_2(d_1, d_2)$ класса $C^*(d_1, d_2)$, состоящий из всех функций, которые на каждом параллелограмме либо не принимают значение $*$, либо принимают его не менее двух раз.

Теорема 3. *Класс $Par_2(d_1, d_2)$ замкнут и удовлетворяет строгим включениям*

$$C^*_{d_1,d_2} \subset Par_2(d_1, d_2) \subset C^*(d_1, d_2).$$

Теорема 4. *Класс $Par_2(d_1, d_2)$ является предполным в классе $C^*(d_1, d_2)$.*

Таким образом, возможна следующая классификация функций из $C^*(d_1, d_2)$ по наличию параллелограммов с различным числом значений $*$:

если на каждом параллелограмме не менее трех значений $*$ или их нет вообще, то функция принадлежит классу $C^*_{d_1,d_2}$, в частности, таковыми являются всюду определенные и всюду неопределенная функции ("экстремальная степень неопределенности");

если на каждом параллелограмме число значений $*$ равно 0 или не меньше двух, то функция принадлежит классу $Par_2(d_1, d_2)$;

если имеется параллелограмм, на котором функция принимает значение $*$ ровно один раз, то эта функция вместе с элементами класса $C^*_{d_1,d_2}$ порождает весь класс $C^*(d_1, d_2)$, т. е. обладает наибольшей в классе $C^*(d_1, d_2)$ выразительной силой.

О ПОРОЖДАЮЩИХ СИСТЕМАХ НЕКОТОРЫХ ЗАМКНУТЫХ КЛАССОВ МОНОТОННЫХ ФУНКЦИЙ ТРЕХЗНАЧНОЙ ЛОГИКИ

А. В. Михайлович (Москва)

Обозначим через MR множество всех монотонных относительно порядка $0 < 1 < 2$ функций из P_3, принимающих значения только из множества $\{0, 1\}$ и равных нулю на наборах, содержащих хотя бы одну нулевую компоненту. Обозначим через $\widehat{\mathrm{MR}}$ множество всех функций из MR, принимающих нулевое значение на наборах, состоящих из одних единиц, а через MS (соответственно $\widehat{\mathrm{MS}}$) — множество всех симметрических функций из MR (соотв. $\widehat{\mathrm{MR}}$).

В [1, 2] рассмотрены некоторые семейства замкнутых классов, порожденных монотонными симметрическими функциями; для них приведены критерии базируемости и конечной порожденности. В данной работе для классов MR и $\widehat{\mathrm{MR}}$ получено описание всех порождающих систем, состоящих из монотонных симметрических функций. Все необходимые определения можно найти в [1–3].

Пусть $f \in \mathrm{R}$. Будем обозначать через N_f множество всех наборов из E_3^n, на которых функция f принимает значение 1. Число единиц и число двоек в наборе из N_f с наибольшим числом единиц обозначим через e_f и d_f соответственно.

Обозначим через $i_n(x_1,\ldots,x_n)$, $n \geq 1$, функцию из множества MR, принимающую значение 1 на всех наборах из $\{1,2\}^n$. Положим

$$\mathrm{I} = \bigcup_{n\geq 1}\{i_n\},$$

Отметим следующее свойство множества I :

$$\mathrm{I} = [\{i_n\}].$$

Обозначим через $g_i(x_1,\ldots,x_i)$ такую функцию из множества $\widehat{\mathrm{MS}}$, для которой выполняется равенство $e_{g_i} = i-1$. Положим

$$G = \bigcup_{i\geq 1}\{g_i\}.$$

Пусть $n \in \mathbb{N}$, $\widetilde{\alpha} \in \{1,2\}^n$, Определим функцию $f_{\widetilde{\alpha}}(x_1,\ldots,x_n)$ из $\widehat{\mathrm{MR}}$ на наборах из $\{1,2\}^n$ следующим образом. Положим

$$f_{\widetilde{\alpha}}(\widetilde{\beta}) = \begin{cases} 0, \text{ если } \widetilde{\beta} < \widetilde{\alpha}; \\ 1 \text{ в остальных случаях.} \end{cases}$$

Доказательство основных результатов основывается на следующих леммах.

Лемма 1. *Пусть* $n \in \mathbb{N}$, $\widetilde{\alpha} \in \{1,2\}^n$. *Тогда* $f_{\widetilde{\alpha}} \in [\widehat{\mathrm{MS}}]$.

Для доказательства достаточно показать, что если в наборе $\widetilde{\alpha}$ содержится e единиц, то функция $f_{\widetilde{\alpha}}(x_1,\ldots,x_n)$ порождается функцией $g(x_1,\ldots,x_m) \in \widehat{\mathrm{MS}}$, где $m = (n-e)(e+1)$, $e_g = (n-e)e$.

Лемма 2 [1]. *Пусть* $f(x_1,\ldots,x_n), g(x_1,\ldots,x_m) \in \widehat{\mathrm{MS}}$, $n \geq m \geq 1$. *Тогда если* $e_g > e_f$, *то* $f \in [\{g\}]$.

Следствие. *Пусть* $f(x_1,\ldots,x_n) \in \widehat{\mathrm{MS}}$, $\frac{e_f}{d_f} > m$ *для некоторого* $m \in \mathbb{N}$. *Тогда* $g_m \in [\{f\}]$.

Теорема 1. Имеют место следующие равенства:

$$\widehat{\mathrm{MR}} = [\widehat{\mathrm{MS}}]; \quad \mathrm{MR} = [\mathrm{MS}].$$

Для доказательства первого равенства достаточно показать, что для любой функции $f(x_1,\ldots,x_n)$ из $\widehat{\mathrm{MR}}$ существует число t и функции $f_{\widetilde{\alpha}_1},\ldots,f_{\widetilde{\alpha}_t}$, такие, что $f \in [\{f_{\widetilde{\alpha}_1},\ldots,f_{\widetilde{\alpha}_t},g_{n+t}\}]$. Тогда в силу

леммы 1 выполняется равенство $\widehat{\mathrm{MR}} = [\widehat{\mathrm{MS}}]$. Второе получается из первого с использованием соотношений $\mathrm{MR} = \widehat{\mathrm{MR}} \cup \mathrm{I}$ и $\mathrm{MS} = \widehat{\mathrm{MS}} \cup \mathrm{I}$.

Лемма 3. Имеют место следующие равенства:

$$\widehat{\mathrm{MR}} = [G]; \quad \mathrm{MR} = [G \cup i_2].$$

С использованием леммы 3, следствия из леммы 2 и свойства множества I, для множеств $\widehat{\mathrm{MR}}$ и MR получаем описание порождающих систем, состоящих из монотонных симметрических функций.

Теорема 2. Имеют место следующие утверждения.

1. *Пусть* $A \subseteq \widehat{\mathrm{MS}}$. *Равенство* $\widehat{\mathrm{MR}} = [A]$ *выполняется в том и только том случае, когда для любого* $n \in \mathbb{N}$ *существует функция* $f \in A$, *такая, что* $\frac{e_f}{d_f} > n$.

2. *Пусть* $A \subseteq \mathrm{MS}$. *Равенство* $\mathrm{MR} = [A]$ *выполняется в том и только том случае, когда для любого* $n \in \mathbb{N}$ *существует функция* $f \in A$, *такая, что* $\frac{e_f}{d_f} > n$ *и существует* $m \in \mathbb{N}$, *такое, что* $i_m \in A$.

Автор выражает благодарность профессору А. Б. Угольникову за постановку задачи и постоянное внимание к работе.

Работа выполнена при финансовой поддержке РФФИ (проекты № 11–01–00508, № 12–01–31351) и Программы фундаментальных исследований Отделения математических наук РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения» (проект «Задачи оптимального синтеза управляющих систем»).

Список литературы

1. Михайлович А. В. О классах функций трехзначной логики, порожденных монотонными симметрическими функциями // Вестник Моск. ун-та. Сер. 1. Математика. Механика. 2009. — № 1. — С. 33–37.

2. Михайлович А. В. О свойствах замкнутых классов в P_3, порожденных монотонными симметрическими функциями // Материалы VIII Молодежной научной школы по дискретной математике и ее приложениям. Часть II (Москва, 24–29 октября 2011 г.). — Москва: Институт прикладной математики РАН, 2011. — С. 16–19.

3. Яблонский С. В. Введение в дискретную математику. — М.: Высшая школа, 2001.

О ПЕРЕСЕЧЕНИЯХ КЛАССОВ МОНОТОННЫХ ФУНКЦИЙ МНОГОЗНАЧНОЙ ЛОГИКИ

А. С. Нагорный (Москва)

Пусть $k \geq 3$, $E_k = \{0, 1, \ldots, k-1\}$ и P_k — множество всех функций на E_k. Элементы множества P_k будем называть *k-значными функциями* или *функциями k-значной логики.*

Определения суперпозиции k-значных функций, замыкания, замкнутого класса и полноты можно найти в [1].

Замкнутый (относительно суперпозиции) класс H функций k-значной логики назовем *предполным в* P_k, если $H \neq P_k$, но для любой функции $f \in P_k \setminus H$ замыкание множества $H \cup \{f\}$ совпадает с P_k.

Известно [2], что при каждом $k \geq 3$ все классы k-значных функций, монотонных относительно частичных порядков на E_k с наименьшим и наибольшим элементами (т.н. ограниченные порядки), являются функционально замкнутыми и предполными в P_k.

Рассмотрим Θ_k — множество всех линейных порядков на E_k, и $\widehat{\Theta}_k$ — множество всех частичных порядков на E_k, имеющих наименьший и наибольший элементы и таких, что остальные элементы в них попарно несравнимы.

Запись $(b_0, b_1, \ldots, b_{k-1}) \in \Theta_k$ означает, что рассматривается линейный порядок $b_0 < b_1 < \ldots < b_{k-1}$, а запись $\{c, d\} \in \widehat{\Theta}_k$ означает, что рассматривается частичный порядок с наименьшим элементом c, наибольшим элементом d и попарно несравнимыми остальными элементами множества E_k.

Обозначим через $M_{b_0,b_1,\ldots,b_{k-1}}$ множество функций k-значной логики, монотонных относительно порядка $(b_0, b_1, \ldots, b_{k-1}) \in \Theta_k$, а через $M_{\{c,d\}}$ — множество k-значных функций, монотонных относительно порядка $\{c, d\} \in \widehat{\Theta}_k$.

Заметим, что $M_{b_0,b_1,\ldots,b_{k-1}} = M_{b_{k-1},\ldots,b_1,b_0}$ и $M_{\{c,d\}} = M_{\{d,c\}}$, поэтому такие классы в этой работе мы различать не будем.

Легко проверить, что при любом $k \geq 3$ имеется ровно $k!/2$ попарно различных классов первого типа (т. е. вида $M_{b_0,b_1,\ldots,b_{k-1}}$), а при любом $k \geq 4$ — ровно $\binom{k}{2}$ попарно различных классов второго типа (т.е. вида $M_{\{c,d\}}$). Обозначим множество всех классов первого типа через μ^k, а второго типа — через $\widehat{\mu}^k$.

В данной работе будем рассматривать некоторые пересечения классов из множества $\mu^k \cup \widehat{\mu}^k$.

Пусть $A^k = \{0, 1, \ldots, k-1, x\}$ (с точностью до конгруэнтных функций).

Для произвольных $E \subseteq E_k$ и $\tilde{b} = (b_0, b_1, \ldots, b_{k-1}) \in \Theta_k$ обозначим
$I^E_{\max}(\tilde{b}) = \max\limits_{b_i \in E} i, \quad I^E_{\min}(\tilde{b}) = \min\limits_{b_i \in E} i, \quad \Delta^E(\tilde{b}) = I^E_{\max}(\tilde{b}) - I^E_{\min}(\tilde{b})$.

Утверждение 1. *Пусть $p \geq 2$ и $\tilde{b}^j = (b^j_0, b^j_1, \ldots, b^j_{k-1}) \in \Theta_k$ при всех $1 \leq j \leq p$. Тогда $\bigcap\limits_{j=1}^{p} M_{b^j_0, b^j_1, \ldots, b^j_{k-1}} = A^k \iff$ при всех $E \subseteq E_k$ таких, что $1 < |E| < k$, выполнено $\max\limits_{1 \leq j \leq p} \Delta^E(\tilde{b}^j) \geq |E|$.*

Следствие 1. 1. *Для любых классов $K_1, K_2 \in \mu^3$ верно $K_1 \cap K_2 \neq A^3$.* 2. *При всех $r \geq 2$ справедливо*

$$M_{0,1,\ldots,2r} \cap M_{2r-2,2r-4,\ldots,2,0,2r,1,3,\ldots,2r-1} = A^{2r+1}.$$

Следствие 2. *При всех $r \geq 2$*
1) $M_{0,1,\ldots,2r-1} \cap M_{1,3,\ldots,2r-1,0,2,\ldots,2r-4,2r-2} = A^{2r}$;
2) $M_{0,1,\ldots,2r-1} \cap M_{r-1,2r-1,r-2,2r-2,\ldots,1,r+1,0,r} = A^{2r}$.

Следствие 3. *При всех $p > (k-1)!$ справедливо $\bigcap\limits_{j=1}^{p} K_j = A^k$, где все K_j — произвольные попарно различные классы из μ^k.*

Отметим, что при любом $k \geq 3$ в μ^k найдутся $(k-1)!$ попарно различных классов, пересечение которых не равно A^k.

Утверждение 2. *Для любых классов $K_1 \in \widehat{\mu}^k$ и $K_2 \in \mu^k \cup \widehat{\mu}^k$ верно $K_1 \cap K_2 \neq A^k$.*

При всех $s, t \in E_k$ положим

$$\overline{s,t} = \begin{cases} s, s+1, \ldots, t, & \text{если } s \leq t; \\ s, s-1, \ldots, t, & \text{иначе.} \end{cases}$$

Рассмотрим вопрос о необходимых и достаточных условиях вложения пересечений классов из множества $\mu^k \cup \widehat{\mu}^k$ в класс $M_{\overline{0,k-1}}$ обычных монотонных k-значных функций.

Заметим, что все пересечения классов, равные A^k (в частности, все указанные в формулировках утверждения 1 и следствий из него), целиком содержатся в классе $M_{\overline{0,k-1}}$. Имеются и другие примеры вложения пересечений классов из $\mu^k \cup \widehat{\mu}^k$ в класс $M_{\overline{0,k-1}}$.

Утверждение 3. *Для любого l, удовлетворяющего неравенствам $0 < l < k-2$, справедливо вложение*

$$M_{\overline{k-1,l+1},\,\overline{0,l}} \cap M_{\overline{0,l},\,\overline{k-1,l+1}} \subseteq M_{\overline{0,k-1}}.$$

Пусть $Shift(b_0, b_1, \ldots, b_{k-1})$ — множество всех линейных порядков $(c_0, c_1, \ldots, c_{k-1})$, которые получаются из $(b_0, b_1, \ldots, b_{k-1}) \in \Theta_k$ некоторым циклическим сдвигом, т.е. $c_i = b_{i+s \pmod k}$ при некотором $s \in E_k$ и всех $i \in E_k$. Далее всюду считаем, что $k \geq 4$.

Утверждение 4. *$M_{\{0,k-1\}} \cap M_{b_0,b_1,\ldots,b_{k-1}} \subseteq M_{\overline{0,k-1}}$ тогда и только тогда, когда*
$(b_0, b_1, \ldots, b_{k-1}) \in Shift(0, 1, \ldots, k-1) \cup Shift(k-1, \ldots, 1, 0)$.

Утверждение 5. *Пусть $0 < l < k-1$.*
$M_{\{0,l\}} \cap M_{b_0,b_1,\ldots,b_{k-1}} \subseteq M_{\overline{0,k-1}}$ тогда и только тогда, когда
$(b_0, b_1, \ldots, b_{k-1}) \in \{(\overline{k-1,l},\ \overline{0,l-1}),\ (\overline{l-1,0},\ \overline{l,k-1})\}$.

Утверждение 6. *Пусть $c, d \in E_k \setminus \{0, k-1\}$, $c \neq d$. Тогда для всех классов $K \in \mu^k$ выполняется $M_{\{c,d\}} \cap K \not\subseteq M_{\overline{0,k-1}}$.*

Положим

$$p_0(k) = \begin{cases} 2, & \text{если } k = 4; \\ 3, & \text{если } k = 5; \\ \left[\frac{k-1}{2}\right], & \text{если } k \geq 6. \end{cases}$$

Утверждение 7. *При всех $k \geq 4$ и при всех $K_0 \in \mu^k$*

1) *при $2 \leq p \leq p_0(k)$ для любых классов $K_1, K_2, \ldots, K_p \in \widehat{\mu}^k$ верно*

$$\bigcap_{j=1}^{p} K_j \not\subseteq K_0;$$

2) *при $p > p_0(k)$ найдутся классы $K_1, K_2, \ldots, K_p \in \widehat{\mu}^k$ такие, что*

$$\bigcap_{j=1}^{p} K_j \subseteq K_0.$$

В заключение автор выражает благодарность А. А. Вороненко за постановку задачи и С. С. Марченкову за ценные замечания.

Список литературы

1. Яблонский С. В. Введение в дискретную математику. — М.: Наука, 1986.

2. Мартынюк В. В. Исследование некоторых классов функций в многозначных логиках // Проблемы кибернетики. — 1960. — Вып. 3. — С. 49–60.

О ПОЛНОТЕ СИСТЕМ МОНОТОННЫХ ОДНОМЕСТНЫХ ФУНКЦИЙ В P_k

Д. Ю. Панин (Москва)

Рассматривается задача о полноте систем одноместных функций многозначной логики, монотонных относительно частичного порядка специального вида. Подобные вопросы возникают при изучении свойств предполных классов монотонных функций, не имеющих конечных порождающих систем [3–6]. В работе получен критерий полноты для рассматриваемой функциональной системы (см. также [7, 8]).

Все необходимые определения можно найти в [1, 2]. Пусть P — некоторое множество, а $\leq$ — частичный порядок на P. Пусть $\alpha, \beta \in P$. Если для этих элементов выполняется по крайней мере одно из соотношений $\alpha \leq \beta$, $\beta \leq \alpha$, то эти элементы называются *сравнимыми*, в противном случае — *несравнимыми*.

Будем обозначать через $M^P_{\leq x}$ множество всех одноместных функций $f(x)$, определенных на множестве P, принимающих значения из P, монотонных относительно частичного порядка $\leq$, и таких, что $f(\delta) \leq \delta$ для всех $\delta \in P$. Рассматривается задача реализации функций из $M^P_{\leq x}$ формулами.

Пусть $n \geq 1$. Положим $Q_k = \{0, a_1, a'_1, \ldots, a_k, a'_k\}$, где $0 \leq k \leq n$. Положим $Q = Q_n$, $a_0 = a'_0 = 0$, Множество $\Delta_i = \{a_i\} \cup \{a'_i\}$, где $0 \leq i \leq n$, будем называть *i-ым слоем*.

Введем на элементах множества Q отношение частичного порядка $\leq$ следующим образом:

1) $\varepsilon_i \leq \varepsilon_j$ для всех $\varepsilon_i, \varepsilon_j$, таких, что $\varepsilon_i \in \Delta_i, \varepsilon_j \in \Delta_j$, $0 \leq i < j \leq n$,

2) $\varepsilon \leq \varepsilon$ для всех $\varepsilon \in Q$.

Пусть $\varepsilon \in Q \setminus \{0\}$. Через $c(\varepsilon)$ будем обозначать элемент, несравнимый с элементом ε.

Цепью длины m, $1 \leq m \leq n+1$, будем называть последовательность элементов $b_0, b_1, b_2, \ldots, b_{m-1} \in Q$, таких, что для всех $i = 0, \ldots, m-1$ элемент b_i принадлежит множеству Δ_i). Через $\mathcal{C}_m$ будем обозначать множество всех цепей длины m.

Положим $F = M^Q_{\leq x}$. Пусть $\varepsilon \in Q$, а f — произвольная функция из множества F. Будем говорить, что функция f сохраняет элемент ε, если $f(\varepsilon) = \varepsilon$.

Пусть $\Omega \subseteq Q$. Положим $S_\Omega = \{f \in F \mid f(\delta) = \delta$ для всех $\delta \in \Omega\}$. В частности, $S_{\{a_n\}}$ — множество всех функций из F, сохраняющих

элемент a_n. Пусть $f \in F$. Будем говорить, что функция f сохраняет множество Ω, если $f \in S_\Omega$. Пусть $f \in F$, $Q' \subseteq Q$. Положим $f(Q') = \{f(\delta) \mid \delta \in Q'\}$.

Будем обозначать через D_1 множество всех функций g из F, для которых найдутся номер k, $2 \leq k \leq n$, и цепь Ω длины $k-1$, такие, что выполнены следующие условия: $g \in S_\Omega$, $g(\Delta_k) = \Delta_{k-1}$.

Пусть $\Omega = (\omega_0, \ldots, \omega_k)$ – цепь длины $k+1$, где $0 \leq k \leq n$. Определим функцию φ_Ω:

$$\varphi_\Omega(\delta) = \begin{cases} \delta, & \text{если } \delta \in \Delta_i, \text{ где } k+1 \leq i \leq n; \\ w_i, & \text{если } \delta = w_i, \text{ где } 0 \leq i \leq k; \\ w_{i-1}, & \text{если } \delta = c(w_i), \text{ где } 1 \leq i \leq k. \end{cases}$$

Определим множество D_2 следующим образом. Положим

$$D_2 = \bigcup_{k=0}^{n} \bigcup_{\Omega \in \mathcal{C}_{k+1}} \{\varphi_\Omega\}.$$

В работе [8] получен критерий полноты для систем функций из множества F.

Теорема 1. *Пусть $D \subseteq F$. Система D является полной в F тогда и только тогда, когда $D_1 \cup D_2 \subseteq D$.*

Будем обозначать элемент a'_n через $1'$. Положим $Q^1 = Q \setminus \{1'\}$, $F^1 = M^{Q^1}_{\leq x}$.

Пусть $f \in F$. Через $f|_{Q^1}$ будем обозначать функцию $g : Q^1 \to Q^1$, такую, что для любого элемента δ из Q^1 выполняется равенство $g(\delta) = f(\delta)$.

Положим $\mathcal{A} = (D_1 \cup D_2) \cap S_{\{1'\}}$. Определим множество K следующим образом:

$$K = \bigcup_{f \in \mathcal{A}} \{f|_{Q^1}\}.$$

Имеет место следующий критерий полноты для систем функций из множества F^1.

Теорема 2. *Пусть $D \subseteq F^1$. Система D является полной в F^1 тогда и только тогда, когда $K \subseteq D$.*

Доказательство теоремы 2 опирается на теорему 1 и следующие леммы.

Лемма 1. *Пусть $f_1, f_2 \in F^1$, а g — функция из K, такая, что $g(x) = f_1(f_2(x))$. Тогда $g = f_1$ или $g = f_2$.*

Лемма 2. *Пусть f — произвольная функция из F, такая, что $f(1') = 1'$, а Φ — формула над $D_1 \cup D_2$, реализующая функцию f. Тогда существует формула Φ' над K, реализующая функцию $f|_{Q^1}$.*

Работа выполнена при финансовой поддержке РФФИ (проект 11–01–00508) и программы фундаментальных исследований ОМН РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения» (проект «Задачи оптимального синтеза управляющих систем»)

Список литературы

1. Яблонский С. В. Введение в дискретную математику. — М.: Высшая школа, 2008.

2. Яблонский С. В. Функциональные построения в k-значной логике // Труды математического института АН СССР. — 1958. — Т. 51. — С. 5–142.

3. Tardos G. A not finitely generated maximal clone of monotone operations // Order. — 1986. — V. 3. — P. 211–218.

4. Lau D. Function algebras on finite sets: a basic course on many-valued logic and clone theory. — Springer Monographs in Mathematics. Berlin: Springer, 2006.

5. Дудакова О. С. О конечной порожденности предполных классов монотонных функций многозначной логики // Математические вопросы кибернетики. Вып. 17. — М.: Физматлит, 2008. — С. 13–104.

6. Дудакова О. С. О классах функций k-значной логики, монотонных относительно множеств ширины два // Вестник Московского университета. Математика. Механика. — 2008. Вып. 1. — С. 31–37.

7. Панин Д. Ю. О порождении одноместных монотонных функций многозначной логики // Вестник Московского университета. Математика. Механика. — 2010. Вып. 6. — С. 52–55.

8. Панин Д. Ю. О некоторых свойствах одноместных монотонных функций многозначной логики // Проблемы теоретической кибернетики. Материалы XVI Международной конференеции (Нижний Новгород, 20–25 июня 2011 г.). — 2011. — С. 349–352

О НЕКОТОРЫХ СВОЙСТВАХ ОПЕРАЦИИ СУПЕРПОЗИЦИИ СПЕЦИАЛЬНОГО ВИДА

Д. К. Подолько (Москва)

Известно [1], что множество всех замкнутых классов функций k-значной логики континуально при $k \geq 3$. Поэтому в ряде работ рассматривались некоторые усиления операции замыкания, позволяющие получать семейства замкнутых классов счетной или конечной мощности (см., например, [2–4]).

Настоящая работа относится к данному направлению исследований. Функции k- значной логики кодируются и рассматриваются как векторы функций алгебры логики, а операция замыкания ведется не только относительно операций суперпозиции и введения фиктивной переменной, но и относительно специальной операции двоичной суперпозиции. Все необходимые определения и обозначения см. в [5].

Пусть $k = 2^m$, $m \geq 2$ и $E_k = \{0, 1, \ldots, k-1\}$. Обозначим через P_k множество всех функций k-значной логики. Каждое число из E_k можно записать в двоичной системе счисления. Таким образом строится биекция между числами α из E_k и двоичными векторами $< \alpha_1, \alpha_2, \ldots, \alpha_m >$ из $\{0,1\}^m$ (обозначение $\widehat{\alpha}$).

Далее, переменной x, которая принимает значения из E_k, поставим в соответствие вектор-переменную $< x_1, x_2, \ldots, x_m >$, где $x_1, \ldots, x_m$ являются переменными, принимающими значения из множества $\{0,1\}$, таким образом, что каждому значению α переменной x ставится в соответствие значение $< \alpha_1, \alpha_2, \ldots, \alpha_m >$ вектор-переменной $< x_1, x_2, \ldots, x_m >$ (обозначение $\widehat{x}$).

Аналогичным образом любой n-местной функции многозначной логики $F^{(n)}(x^1, x^2, \ldots, x^n)$ можно взаимно-однозначно сопоставить вектор-функцию $< f_1, f_2, \ldots, f_m >$, где f_i — p-местные функции из P_2 для $i = 1, \ldots, m$, где $p = n \cdot m$. Они зависят от переменных $x_1^1, \ldots, x_m^n$. Будем обозначать $\widehat{F} =< f_1, f_2, \ldots, f_m >$ или расширенно $\widehat{F}^{(n)}(\widehat{x}^1, \widehat{x}^2, \ldots, \widehat{x}^n) =< f_1, f_2, \ldots, f_m > (\widehat{x}^1, \widehat{x}^2, \ldots, \widehat{x}^n)$. Такие представления называются *двоичным представлением числа α, переменной x* и *функции F* соответственно.

Пусть $\mathcal{A}$ — некоторое подмножество множества P_k. Определим понятие формул и вектор-формул над $\mathcal{A}$.

1) Если x^i — переменная, то x_j^i — *формула* над $\mathcal{A}$, $j = 1, 2, \ldots, m$. Такие формулы называются *тривиальными*.

2) Если $< f_1^{(n \cdot m)}, \ldots, f_m^{(n \cdot m)} > (\widehat{x}^1, \ldots, \widehat{x}^n)$ — двоичное представление некоторой функции $F^{(n)}(x^1, \ldots, x^n)$ из $\mathcal{A}$ для $n \geq 1$, а

$\varphi_1,\ \varphi_2,\ \ldots,\ \varphi_{n\cdot m}$ — формулы над $\mathcal{A}$, то формулы φ'_i, имеющие вид $f_i^{(n\cdot m)}(\varphi_1, \varphi_2, \ldots, \varphi_{n\cdot m})$, являются *формулами* над $\mathcal{A},\ i = 1, 2, \ldots, m$. При этом формула Φ, имеющая вид

$$< f_1^{(n\cdot m)}(\varphi_1, \varphi_2, \ldots, \varphi_{n\cdot m}), \ldots, f_m^{(n\cdot m)}(\varphi_1, \varphi_2, \ldots, \varphi_{n\cdot m}) >,$$

является *вектор-формулой* над $\mathcal{A}$.

Если множество тривиальных подформул формулы φ содержит только формулы из множества $\{x_{j_1}^{i_1}, \ldots, x_{j_p}^{i_p}\}$, где $1 \le j_q \le m$ для $q = 1, \ldots, p$, то будем обозначать формулу φ через $\varphi(x_{j_1}^{i_1}, \ldots, x_{j_p}^{i_p})$ и говорить, что формула φ зависит от переменных $x_{j_1}^{i_1}, \ldots, x_{j_p}^{i_p}$. В свою очередь, вектор-формулу Φ, в которую входят символы переменных $x^1, \ldots, x^n$ и только они, будем обозначать через $\Phi(\widehat{x}^1, \ldots, \widehat{x}^n)$.

Определим значение формулы $\varphi(x_{j_1}^{i_1}, \ldots, x_{j_p}^{i_p})$ на произвольном наборе $(\alpha_{j_1}^{i_1}, \ldots, \alpha_{j_p}^{i_p})$ из $\{0,1\}^p$ и вектор-формулы $\Phi(\widehat{x}^1, \ldots, \widehat{x}^n)$ на наборе $(\widehat{\alpha}^1, \ldots, \widehat{\alpha}^n)$ для каждого вектора $(\alpha^1, \ldots, \alpha^n)$ из E_k^n.

1) Если формула $\varphi(x_j^i)$ имеет вид $x_j^i,\ 1 \le j \le m$, то $\varphi(\alpha_j^i) = \alpha_j^i$.

2) Если формула $\varphi(x_{j_1}^{i_1}, \ldots, x_{j_p}^{i_p})$ имеет вид

$$f_r^{(n\cdot m)}\Big(\varphi_1\big(x_{j_1}^{i_1}, \ldots, x_{j_p}^{i_p}\big), \ldots, \varphi_{n\cdot m}\big(x_{j_1}^{i_1}, \ldots, x_{j_p}^{i_p}\big)\Big),$$

где $1 \le r \le m$, а φ_q являются формулами над $\mathcal{A}$, зависящими от переменных $x_{j_1}^{i_1}, \ldots, x_{j_p}^{i_p}$ для всех $q = 1, 2, \ldots, n\cdot m$, то значение $\varphi(\alpha_{j_1}^{i_1}, \ldots, \alpha_{j_p}^{i_p})$ равно

$$f_r^{(n\cdot m)}\Big(\varphi_1\big(\alpha_{j_1}^{i_1}, \ldots, \alpha_{j_p}^{i_p}\big), \ldots, \varphi_{n\cdot m}\big(\alpha_{j_1}^{i_1}, \ldots, \alpha_{j_p}^{i_p}\big)\Big).$$

3) Если вектор-формула $\Phi(\widehat{x}^1, \ldots, \widehat{x}^n)$ имеет вид

$$< \varphi_1(x_{j_1}^{i_1}, \ldots, x_{j_p}^{i_p}), \ldots, \varphi_m(x_{j_1}^{i_1}, \ldots, x_{j_p}^{i_p}) >,$$

где φ_r — формулы над $\mathcal{A},\ r = 1, \ldots, m$, то

$$\Phi(\widehat{\alpha}^1, \ldots, \widehat{\alpha}^n) =< \varphi_1(\alpha_{j_1}^{i_1}, \ldots, \alpha_{j_p}^{i_p}), \ldots, \varphi_m(\alpha_{j_1}^{i_1}, \ldots, \alpha_{j_p}^{i_p}) >,$$

где $\widehat{\alpha}^i =< \alpha_1^i, \ldots, \alpha_m^i >$ для $i = 1, 2, \ldots, n$.

Таким образом, каждой вектор-формуле $\Phi(\widehat{x}^1, \ldots, \widehat{x}^n)$ над $\mathcal{A}$ сопоставляется двоичное представление $\widehat{F}(\widehat{x}^1, \ldots, \widehat{x}^n)$ некоторой функции $F(x^1, \ldots, x^n)$ из P_k. Будем говорить, что F получена при помощи *операции двоичной суперпозиции* из функций системы $\mathcal{A}$.

Замыканием множества $\mathcal{A}$ относительно двоичной суперпозиции (обозначение $[\mathcal{A}]_\Sigma$) называются все функции из P_k, которые могут быть получены из функций системы $\mathcal{A}$ применением операций введения несущественной переменной и двоичной суперпозиции.

Класс $\mathcal{A}$ называется *замкнутым относительно двоичной суперпозиции*, если $\mathcal{A} = [\mathcal{A}]_\Sigma$.

Обозначим через $\widehat{P_{k,2}}$ множество всех функций P_k, принимающих не более двух значений. Известно (см., например, [6]), что множество всех замкнутых классов функций из $\widehat{P_{k,2}}$ континуально. Но в рамках рассматриваемой операции замыкания имеет место утверждение.

Теорема. *Множество всех классов функций из $\widehat{P_{k,2}}$, замкнутых относительно операции двоичной суперпозиции, счетно.*

Работа выполнена при финансовой поддержке РФФИ (проект 11–01–00508) и программы фундаментальных исследований ОМН РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения» (проект «Задачи оптимального синтеза управляющих систем»).

Список литературы

1. Янов Ю. И., Мучник А. А. О существовании k-значных замкнутых классов, не имеющих конечного базиса // Докл. АН СССР. — 1959. — Т. 127, 1. — С. 44–46.

2. Тарасова О. С. Классы функций k-значной логики, замкнутые относительно операций суперпозиции и перестановок // Математические вопросы кибернетики. Вып. 13. — М.: Физматлит, 2004. — С. 59–112.

3. Марченков С. С. S-классификация функций многозначной логики // Дискретная математика. — 1997. — Т. 9, вып. 3. — С. 125–152.

4. Нгуен Ван Хоа. О семействах замкнутых классов k-значной логики, сохраняемых всеми автоморфизмами // Дискретная математика. — 1993. — Т. 5, вып. 4. — С. 87–108.

5. Яблонский С. В. Введение в дискретную математику. — М.: Высшая школа, 2001.

6. Lau D. Function algebras on finite sets. — New York: Springer, 2006.

НИЖНЯЯ ОЦЕНКА СЛОЖНОСТИ НАХОЖДЕНИЯ ПОЛИНОМОВ БУЛЕВЫХ ФУНКЦИЙ В КЛАССЕ СХЕМ С РАЗДЕЛЕННЫМИ ПЕРЕМЕННЫМИ

С. Н. Селезнева (Москва)

В настоящей заметке доказывается точная нижняя оценка сложности нахождения коэффициентов полинома булевой функции в классе схем с разделенными переменными.

Пусть $B = \{0, 1\}$. Множество B^n, $n \geq 1$, назовем *n-мерным булевым кубом*. На кубе B^n введем частичный порядок: если $\alpha = (a_1, \ldots, a_n) \in B^n$ и $\beta = (b_1, \ldots, b_n) \in B^n$, то $\alpha \leq \beta$ при $a_1 \leq b_1$, $\ldots$, $a_n \leq b_n$. *Весом* $|\alpha|$ набора $\alpha = (a_1, \ldots, a_n) \in B^n$ назовем число единиц в нем. *Тенью* набора $\alpha = (a_1, \ldots, a_n) \in B^n$ назовем множество $S(\alpha) = \{\beta \in B^n \mid \beta \leq \alpha, |\beta| = |\alpha| - 1\}$.

Функция $f(x_1, \ldots, x_n)$ называется *булевой*, если $f : B^n \to B$, где $n = 0, 1, 2, \ldots$. Множество всех булевых функций, зависящих от переменных $x_1, \ldots, x_n$, обозначим как P_2^n.

Каждая булева функция $f(x_1, \ldots, x_n) \in P_2^n$ задается *полиномом* (по модулю 2), или *алгебраической нормальной формой* (АНФ), т. е. формулой вида $f(x_1, \ldots, x_n) = \sum\limits_{\sigma=(s_1,\ldots,s_n)\in B^n} c_f(\sigma) \cdot x_1^{s_1} \cdot \ldots \cdot x_n^{s_n}$, где $c_f(\sigma) \in B$, $\sigma \in B^n$, – коэффициенты, а $x_i^{s_i}$ — степени, т.е. $x_i^1 = x_i$, $x_i^0 = 1$, и сложение и умножение рассматривается по модулю 2.

В качестве алгоритмической модели рассмотрим схемы из функциональных элементов (СФЭ) в некотором базисе. *Сложностью* $L(S)$ СФЭ S назовем число функциональных элементов в ней.

СФЭ S с входами $x_1, \ldots, x_n$ и выходами $y_1, \ldots, y_m$ называется *схемой с разделенными переменными* (СФЭРП), если для любых i и j ориентированный путь от входа x_i к выходу y_j существует только в том случае, когда реализующаяся на выходе y_j функция *существенно* зависит от переменной x_i.

Известен быстрый алгоритм построения по вектору значений булевой функции $f(x_1, \ldots, x_n)$ ее полинома, описанный Гавриловым Г. П., Сапоженко А. А. в 1977 г. в [1]. Он реализуется СФЭ с разделенными переменными со сложностью $n \cdot 2^{n-1}$.

В настоящей работе мы докажем нижнюю оценку сложности в классе схем с разделенными переменными нахождения по вектору значений булевой функции коэффициентов ее полинома и покажем, что алгоритм из [1] является оптимальным в этом классе схем.

Определение. Обозначим как Π_n любую такую СФЭ с 2^n входами $u(\alpha)$, $\alpha \in B^n$, и 2^n выходами $v(\sigma)$, $\sigma \in B^n$, что если на входах $u(\alpha)$

появляются значения $f(\alpha)$ произвольной функции $f(x_1, \ldots, x_n) \in P_2^n$, то на выходах $u(\sigma)$ выдаются значения $c_f(\sigma)$ коэффициентов ее полинома.

Известно [2], как выражаются коэффициенты полинома булевой функции через ее значения.

Теорема 1 [2]. *Для каждой булевой функции $f(x_1, \ldots, x_n) \in P_2^n$ каждый коэффициент $c_f(\sigma)$, $\sigma \in B^n$, ее полинома может быть найден по формуле* $c_f(\sigma) = \sum\limits_{\tau \leq \sigma} f(\tau)$.

Следствие 1.1. *В СФЭ Π_n на ее выходах v реализуется система LP_n булевых функций ее входов u, где* $LP_n = \left\{ \sum\limits_{\tau \leq \sigma} u(\tau) \mid \sigma \in B^n \right\}$.

Сначала докажем нижнюю оценку сложности СФЭРП Π_n в базисе $B_{L_0} = \{\oplus\}$ из одного элемента сложения по модулю 2.

Теорема 2. *В базисе $B_{L_0} = \{\oplus\}$ сложность СФЭРП Π_n не меньше $n \cdot 2^{n-1}$.*

Доказательство. Пусть нам задана какая-то СФЭРП Π_n.

Доказажем индукцией по весу набора σ, что в СФЭРП Π_n для каждого набора $\sigma \in B^n$ можно найти не менее $|\sigma|$ элементов, причем так, что для разных наборов σ и τ соответствующие им элементы не пересекаются.

Базис индукции: $|\sigma| = 1$. Рассмотрим в СФЭРП Π_n куст, растущий из выхода $v(\sigma)$. На выходе $v(\sigma)$ реализуется функция $f(0, \ldots, 0) \oplus f(\sigma)$, поэтому этот куст содержит хотя бы один элемент. Припишем выходному элементу этого куста пометку σ. Ясно, что если $\sigma \neq \tau$, $|\sigma| = |\tau| = 1$, то пометки σ и τ будут приписаны разным элементам в силу свойства схемы быть с разделенными переменными. Положим $\Pi_n^1 = \Pi_n$.

Индуктивный переход от $k-1$ к k, $2 \leq k \leq n$.

Рассмотрим СФЭРП Π_n^{k-1} с входами $u(\alpha)$, $|\alpha| \geq k-2$. Преобразуем ее: подадим на все входы $u(\beta)$, $|\beta| = k-2$, значение 0 и удалим из схемы все элементы, хотя бы на один вход которых пришел 0. Рассмотрим теперь выходы $v(\tau)$, $|\tau| = k-1$. На каждом из них реализуется тождественная функция своего единственного (в силу разделенности переменных схемы) входа. Если на пути от входа к выходу есть элементы, удалим их также.

Обозначим полученную СФЭРП с входами $u(\alpha)$, $|\alpha| \geq k-1$, как Π_n^k. Заметим, что по построению в СФЭРП Π_n^k нет элементов с пометками.

Пусть $|\sigma| = k$. Рассмотрим в СФЭРП Π_n^k куст, растущий из выхода $v(\sigma)$. На выходе $v(\sigma)$ реализуется функция $u(\sigma) \oplus \sum\limits_{\tau \in S(\sigma)} u(\tau)$, поэтому этот куст содержит не менее k элементов (в силу существенности всех переменных этой функции). Припишем всем таким элементам пометку σ.

Если $\sigma_1 \neq \sigma_2, |\sigma_1| = |\sigma_2| = k$, то пометки σ_1 и σ_2 будут приписаны разным элементам. В самом деле, пусть какой-то элемент s получил хотя бы две пометки, σ_1 и $\sigma_2, \sigma_1 \neq \sigma_2$. Рассмотрим куст, растущий из элемента s. Если он содержит только один вход, то его без ущерба для схемы можно удалить. Пусть он содержит хотя бы два входа $u(\tau_1)$ и $u(\tau_2)$, $\tau_1 \neq \tau_2$. Тогда, т.к. $|\,(\{\sigma_1\} \cup S(\sigma_1)) \cap (\{\sigma_2\} \cup S(\sigma_2))\,| \leq 1$, например, не верно, что $\tau_1 \leq \sigma_2$.

Тогда, с одной стороны, найдется ориентированный путь от входа $u(\tau_1)$ к элементу s. А с другой стороны, найдется ориентированный путь от элемента s к выходу $v(\sigma_2)$. Получаем противоречие с разделенностью переменных схемы.

Следовательно, $L(\Pi_n) \geq \sum\limits_{k=1}^{n} \sum\limits_{\sigma \in B_k^n} k = \sum\limits_{k=1}^{n} k \cdot C_n^k = n \cdot 2^{n-1}$.

Следствие 2.1. *В базисе* $B_{L_0} = \{\oplus\}$ *минимальная сложность СФЭРП* Π_n *равна* $n \cdot 2^{n-1}$.

Следствие 2.2. *В базисе* $B = \{\&, \vee, \neg\}$ *минимальная сложность СФЭРП* Π_n *лежит в пределах от* $3n \cdot 2^{n-1}$ *до* $4n \cdot 2^{n-1}$.

Работа поддержана РФФИ, гранты 10-01-00768-а, 12-01-00706-а.

Список литературы

1. Гаврилов Г.П., Сапоженко А.А. Сборник задач по дискретной математике. — М.: Наука, 1977.

2. Логачев О.А., Сальников А.А., Ященко В.В. Булевы функции в теории кодировании и криптологии. — М.: МЦНМО, 2004.

УНИВЕРСАЛЬНЫЕ МНОЖЕСТВА ОБОБЩЕННЫХ ФОРМУЛ

Л. Н. Сысоева (Москва)

В работе рассматривается задача о реализации булевых функций обобщенными α-формулами. Вводится понятие универсального множества обобщенных α-формул для заданного множества булевых функций. Показывается, что для каждого $n \geq 2$ для множества

$T_{01}(n)$ всех булевых функций от переменных $x_1, x_2, \ldots, x_n$, сохраняющих константы 0 и 1, существуют универсальные множества.

Понятие *α-формул*, т. е. таких формул, в которых любая подформула содержит не более одной нетривиальной главной подформулы, было введено в работе [3]. В работах [3–5] показано наличие конечных α-полных систем в P_k при $k \geq 3$ и отсутствие их в P_2, где через P_k обозначается множество всех функций k-значной логики, $k \geq 2$. В работах [6, 7] свойства α-формул изучены с точки зрения теории сложности.

Обобщенной α-формулой называется α-формула над некоторым множеством автоматных функций со специальным образом сопоставленной ей функцией алгебры логики. Рассматриваются автоматные функции, которые в каждом состоянии реализуют некоторую булеву функцию. Пусть $\Phi(x_1, x_2, \ldots, x_n)$ — α-формула над некоторым множеством автоматных функций, $\alpha_1, \alpha_2, \ldots, \alpha_{2^n}$ — последовательность всех двоичных наборов длины n, в которой наборы подаются на формулу Φ, $n \geq 1$. Таким образом, задается последовательность $\Phi(\alpha_1), \Phi(\alpha_2), \ldots, \Phi(\alpha_{2^n})$ значений формулы Φ на всех двоичных наборах длины n. Формуле Φ сопоставляется функция $f(x_1, x_2, \ldots, x_n)$ алгебры логики, такая, что выполнены равенства $f(\alpha_i) = \Phi(\alpha_i)$ для всех $i = 1, \ldots, 2^n$.

Пусть A — некоторое множество булевых функций. Множество $\mathfrak{A}$ обобщенных α-формул называется *универсальным* для A, если для любой булевой функции $f(x_1, x_2, \ldots, x_n)$ из A существует обобщенная α-формула Φ из множества $\mathfrak{A}$ и последовательность всех двоичных наборов длины n, такие, что формула Φ при такой последовательности подаваемых наборов реализует функцию f, $n \geq 1$.

Пусть V — конечный автомат с двумя входами и одним выходом, такой, что $\{q_1, q_2\}$ — множество его состояний, в состоянии q_1 автомат реализует функцию $x_1 \& x_2$, в состоянии q_2 — функцию $x_1 \vee x_2$ и автомат в момент времени t переходит из состояния q_i в состояние q_j тогда и только тогда, когда входные символы в этот момент времени совпадают, $i \neq j$. Обозначим через G_1 и G_2 автоматные функции, реализуемые инициальными автоматами V_{q_1} и V_{q_2} соответственно.

Обозначим через $\mathcal{A}_n$ семейство всех множеств следующего вида $\{\Phi_1(x_1, x_2, \ldots, x_n), \Phi_2(x_1, x_2, \ldots, x_n)\}$, где Φ_i — обобщенная α-формула над $\{G_i\}$, в которую каждая переменная входит ровно один раз, $i = 1, 2$.

Теорема. *Каждое множество обобщенных α-формул из семейства $\mathcal{A}_n$ является универсальным для множества $T_{01}(n)$, $n \geq 2$.*

Следует отметить, что для любой булевой функции f, не принад-

лежащей множеству $T_{01}(n)$, не существует обобщенной α-формулы из семейства $\mathcal{A}_n$, реализующей эту функцию, $n \geq 2$.

В заключение автор выражает искреннюю признательность А. Б. Угольникову за постановку задачи и обсуждение результатов работы.

Список литературы

1. Яблонский С. В. Введение в дискретную математику. — М.: Высшая школа, 2006.

2. Конспект лекций О. Б. Лупанова по курсу "Введение в математическую логику". — М.: Изд-во ЦПИ при механико-математическом факультете МГУ имени М. В. Ломоносова, 2007.

3. Глухов М. М. Об α-замкнутых классах и α-полных системах функций k-значной логики // Дискретная математика. — 1989. — Т. 1, вып. 1. — С. 16–21.

4. Чернышов А. Л. Условия α-полноты систем функций многозначной логики // Дискретная математика. — 1992. — Т. 4, вып. 4. — С. 117–130.

5. Шабунин А. Л. Примеры α-полных систем k-значной логики при $k = 3, 4$ // Дискретная математика. — 2006. — Т. 18, вып. 4. — С. 45–55.

6. Трущин Д. В. О глубине α-пополнения систем булевых функций // Вестник Московского университета. Сер. 1. Математика. Механика. — 2009. — вып. 2. — С. 72–75.

7. Трущин Д. В. Об оценках глубины α-пополнений систем функций трехзначной логики // Проблемы теоретической кибернетики: Мат-лы XVI международной конф. — Н. Новгород: Изд-во НН-ГУ, 2011. — С. 484–487.

ПОЗИЦИОННО-ОПТИМАЛЬНЫЕ СТРАТЕГИИ ПОИСКА ОБЛАСТИ НАИБОЛЬШИХ ЗНАЧЕНИЙ ФУНКЦИИ (МНОГОМЕРНЫЙ СЛУЧАЙ)

В. П. Тарасова (Москва)

Задачи детерминированного многошагового минимаксного поиска возникли сравнительно недавно [1].

Областью наибольших значений (ОНЗ) функции называется такая область, значение функции в которой больше, чем вне этой

области. В настоящей работе, с применением метода моделирования стратегии противника [2], строятся позиционно-оптимальные стратегии поиска области наибольших значений функции, определенной в некоторой области m-мерного эвклидова пространства, когда $m \geq 2$. Задачи оптимального одномерного поиска области наибольших (наименьших) значений для различных классов многоэкстремальных функций были решены в [2, 3].

Общая постановка задачи. Рассматривается множество вещественных функций определенных в некоторой области Ω m-мерного эвклидова пространства. Из этого множества функций выделяется класс L таких функций, каждая из которых имеет область наибольших значений Δ. Области Δ, Ω являются m-мерными кубами с ребрами параллельными осям координат. Задана длина ребра Δ, одинаковая для всех функций класса L. Требуется путем получения информации о значениях произвольной функции f из L в n точках области Ω и с учетом свойств, общих для всех функций класса, приближенно, то есть с некоторой точностью, зависящей от n, найти ОНЗ функции f. Число n фиксируется заранее.

Поиск осуществляется n-ходовыми стратегиями, принадлежащими некоторому множеству $\mathfrak{A}$ и определяющими последовательный выбор точек из области Ω.

Результатом стратегии поиска будет наименьшая по объему (площади, длине) область, содержащая ОНЗ функции f и названная областью локализации. Эффективностью применяемых n-ходовых стратегий является объем области локализации. Оптимальность стратегий во всех работах [1-4] понимается в минимаксном смысле, т. е. оптимальной для класса функций будет такая стратегия поиска, которая гарантирует наилучший результат, при любых допустимых значениях функций из заданного класса.

Задача состоит в том, чтобы найти оптимальную стратегию поиска области наибольших значений для функций класса L.

Игровое представление задачи. Сформулированную задачу можно представить в виде задачи нахождения оптимальной стратегией первого игрока в антагонистической многоходовой (позиционной) игре $J = \langle \mathfrak{A}, \mathfrak{B}, X, Y, M; \delta, \delta_i, \leq \rangle$, где $\mathfrak{A}$ — множество n-ходовых чистых стратегий первого игрока, определяющих последовательный выбор точек (ходов первого игрока) из множества Ω, $\mathfrak{B}$ — множество n-ходовых чистых стратегий второго игрока, являющихся функциями класса L, $(\mathfrak{B} = L)$ и определяющих соответствующие значения (ответные ходы второго игрока) функции f из L, $\mathfrak{A} \times \mathfrak{B}$ множество ситуаций (A, B), $A \in \mathfrak{A}$, $B \in \mathfrak{B}$, X, Y — множества ходов первого и второго игроков соответственно, $M = R$ — множество

вещественных чисел, $\leq$ — естественный порядок на множестве R, δ — функция выигрыша первого игрока, $\delta: \mathfrak{A} \times \mathfrak{B} \to R$, $\delta_n(A, f)$ — выигрыш вычислителя равный, по определению, объему (длине, площади) области локализации Δ функции f, получаемой после n ходов (окончании партии) при применении стратегии A из $\mathfrak{A}$ и стратегии f из L, δ_i — функция оценки позиции (выигрыша вычислителя после каждого хода), для подсчета значений которой используются свойства функции класса L.

Каждая A из $\mathfrak{A}$ есть функция $a_{i+1} = A(a_1, b_1, \ldots, a_i, b_i)$, определенная на конечных последовательностях вида $(a_1, b_1, \ldots, a_i, b_i)$, где $(a_1, \ldots, a_i) \subset X$, $(b_1, \ldots, b_i) \subset Y$. Каждая B из $\mathfrak{B}$ есть функция $b_{i+1} = B(a_1, b_1, \ldots, a_i, b_i, a_{i+1})$, определенная на конечных последовательностях вида $(a_1, b_1, \ldots, a_i, b_i, a_{i+1})$, $\ldots$, где $(a_1, \ldots, a_i, a_{i+1}) \subset X$, $(b_1, \ldots, b_i) \subset Y$.

При этом последовательности $(a_1, b_1, \ldots, a_i, b_i)$, $(a_1, b_1, \ldots, a_i, b_i, a_{i+1})$ называются *позициями*, а множества X, Y — *множествами ходов* первого и второго игроков соответственно. Считаем, что первый ход делает первый игрок $a_1 = A(\varnothing)$, затем второй игрок делает ход $b_1 = B(a_1)$ и так далее, чередуясь.

Последовательность ходов $(a_1, b_1, \ldots, a_n, b_n)$, определяемую ситуацией (A, B) назовем *партией*, ее отрезок $(a_1, b_1, \ldots, a_i, b_i)$ назовем *позицией после i-го хода* и обозначим через (A_i, B_i). Равенство ситуаций $(A, B) = (C, D)$ в многоходовых играх будем понимать как равенство соответствующих им партий, то есть из $(A, B) = (C, D)$, $(A, B) = (a_1, b_1, \ldots)$, $(C, D) = (c_1, d_1, \ldots)$ следует $a_1 = c_1$, $b_1 = d_1, \ldots$ и обратно. Если фигурирующая в определении многоходовой игры функция A (соответственно B) является вычислимой, то соответствующая ей стратегия A (соответственно B) называется алгоритмом. Далее, последовательность (позиция) $(a_1, b_1, \ldots, a_i, b_i)$, $a_k \in X$, $b_k \in Y$, $k = 1, \ldots, i$ называется *допустимой*, если существуют такие стратегии $A \in \mathfrak{A}$, $B \in \mathfrak{B}$, что $(A_i, B_i) = (a_1, b_1, \ldots, a_i, b_i)$.

Позиционно-оптимальные стратегии. Оптимальной для позиции будет такая оптимальная стратегия, для которой эта позиция является начальной. Стратегия первого игрока называется позиционно-оптимальной, если она оптимальна для любой допустимой позиции, при любой стратегии второго игрока.

В [3] построены оптимальные (минимаксные) и позиционно-оптимальные n-шаговые стратегии поиска отрезка наибольших значений для одномерных функций. В определении стратегий участвуют известные числа Фибоначчи.

В настоящей работе строятся позиционно-оптимальные многоходовые стратегии поиска m-мерной области наибольших значений для класса T функций, определение которого получается из определения класса L, если положить $m \geq 2$. Оптимальные минимаксные стратегии для этого класса функций сформулированы в [4].

Также как и в [4], исходная многомерная задача, при достаточном числе n, сводится к композиции m одномерных задач. В результате совместных решений этих задач, приближенно или точно определяются границы области наибольших значений функции.

Задача решается в два этапа: начальный этап заканчивается, когда найдена хотя бы одна прямая, содержащая хотя бы одну точку из ОНЗ функции; на конечном этапе решаются одномерные задачи с применением позиционно- оптимальных стратегий поиска отрезка наибольших значений из работ [2, 3].

Стратегия A из $\mathfrak{A}$ называется *походово-оптимальной*, если для любого i она оптимальна для позиции (A_i, B_i) на один ход с функцией выигрыша первого игрока δ_{i+1}.

Теорема. *На начальном этапе все позиционно-оптимальные стратегии являются походово-оптимальными.*

Список литературы

1. Kiefer J. Sequential minimax search for a maximum // Proc. Amer. Math. Soc. — 1953. — № 3. — P. 502–505.

2. Тарасова В. П. Метод стратегии противника в задачах оптимального поиска. — Изд-во МГУ, 1988.

3. Тарасова В. П. Оптимальные алгоритмы поиска отрезка наибольших значений для некоторого класса функций // ЖВМиМФ. — 1981. — Т. 21, № 5. — С. 1108–1115.

4. Тарасова В. П. Оптимальный поиск экстремальной области функции // Материалы XVI Международной конференции “Проблемы теоретической кибернетики”. — Нижний Новгород, 2011. — С. 465–469.

О ТРАНСЛЯЦИИ ФОРМУЛ ЛОГИКИ ЛИНЕЙНОГО ВРЕМЕНИ В ФОРМУЛЫ ЛОГИКИ ВЕТВЯЩЕГОСЯ ВРЕМЕНИ

Р. В. Хелемендик (Москва)

Логика линейного времени (ллв, Linear Time Logic, LTL) является расширением логики высказываний (лв), в которой наряду с

классическими связками добавлены следующие временны́е: $\bigcirc$ (в следующий момент), U (до тех пор, пока) и другие, выражаемые через вышеуказанные. Логика ветвящегося времени (лвв, Computational Tree Logic, CTL) также является расширением логики высказываний, в которой по сравнению с ллв перед каждой временно́й связкой (и только перед ней) стоит квантор $\forall$, либо $\exists$. Сравнение выразительных возможностей LTL и CTL (вместе с введением объединяющей их логики CTL*) проведено в [1]. Вопросы сведе́ния задачи распознавания выполнимости формул ллв и лвв к распознаванию выполнимости формул лв рассмотрены в [2–3]. В настоящей работе построена прямая трансляция произвольной формулы ллв в формулу лвв с обоснованием равносильности этих формул в смысле выполнимости и достижения совпадения в этом случае их моделей. Похожая задача для других модальных логик рассматривалась в работе [4].

Определения формул ллв (*ллв-формул*) и формул лвв (*лвв-формул*), модели, истинности формулы в модели вводятся ниже для обеих логик единообразно и в обобщенной семантике [2, 3, 5].

Каждая пропозициональная переменная p_i есть ллв-формула и лвв-формула; если φ и ψ ллв-формулы (лвв-формулы), то $\neg\varphi$, $(\varphi\wedge\psi)$, $(\varphi\vee\psi)$ тоже являются ллв-формулами (лвв-формулами); если φ и ψ ллв-формулы, то $\bigcirc\varphi$, $(\varphi\ U\ \psi)$, $(\varphi\ \sqcap\ \psi)$ тоже являются ллв-формулами; если φ и ψ лвв-формулы, то $\forall\bigcirc\varphi$, $\exists\bigcirc\varphi$, $\forall(\varphi\ U\ \psi)$, $\exists(\varphi\ U\ \psi)$, $\forall(\varphi\ \sqcap\ \psi)$, $\exists(\varphi\ \sqcap\ \psi)$ тоже являются лвв-формулами.

Ллв-формулу θ обозначим через θ^{LTL}, лвв-формулу θ — через θ^{CTL}.

Моделью в лвв будем называть пару $M=\langle\Gamma, L\rangle$, где Γ — связный ориентированный граф с выделенной вершиной u_0, каждая вершина которого имеет не более одного сына, а L — функция означивания, сопоставляющая каждой вершине множество пропозициональных переменных. *Моделью в ллв* называется такая модель в лвв, для которой в её графе Γ каждая вершиная имеет не более одного сына. *Полным путём* в графе называется бесконечный путь или цепь, последняя вершина которой не имеет сыновей.

Истинность формулы θ в вершине u_i модели M будем обозначать через $M, u_i \models \theta$ и определим индуктивно.

Если $\theta = p$, то $M, u_i \models \theta \rightleftharpoons p \in L(u_i)$. Если $\theta = \neg\varphi$, то $M, u_i \models \theta \rightleftharpoons M, u_i \not\models \varphi$ (неверно $M, u_i \models \varphi$). Если $\theta = (\varphi \wedge \psi)$ $[\theta = (\varphi \vee \psi)]$, то $M, u_i \models \theta \rightleftharpoons M, u_i \models \varphi$ и [или] $M, u_i \models \psi$. Если $\theta^{LTL} = \bigcirc\varphi$ $[\theta^{CTL} = \forall\bigcirc\varphi]$, то $M, u_i \models \theta^{LTL}$ $[M, u_i \models \theta^{CTL}]$ $\rightleftharpoons M, u_j \models \varphi^{LTL}$ $[M, u_j \models \varphi^{CTL}]$ для [каждого] сына u_j вершины

u_i, либо вершина u_i не имеет сына [сыновей]. Если $\theta^{CTL} = \exists\bigcirc\varphi$, то $M, u_i \models \theta^{CTL} \rightleftharpoons$ существует сын u_j вершины u_i, для которого верно $M, u_j \models \varphi^{CTL}$. Если $\theta^{LTL} = (\varphi\ U\ \psi)$ $[\theta^{CTL} = \forall(\varphi\ U\ \psi)]$, то $M, u_i \models \theta^{LTL}$ $[M, u_i \models \theta^{CTL}] \rightleftharpoons$ для [каждого] полного пути с началом в вершине u_i существует вершина u_j, для которой верно $M, u_j \models \psi^{LTL}$ $[M, u_j \models \psi^{CTL}]$, а в каждой вершине u_k этого пути, предшествующей u_j, верно $M, u_k \models \varphi^{LTL}$ $[M, u_k \models \varphi^{CTL}]$. Если $\theta^{CTL} = \exists(\varphi\ U\ \psi)$, то $M, u_i \models \theta^{CTL} \rightleftharpoons$ для некоторого полного пути с началом в вершине u_i существует вершина u_j, для которой верно $M, u_j \models \psi^{CTL}$, а в каждой вершине u_k этого пути, предшествующей u_j, верно $M, u_k \models \varphi^{CTL}$. Если $\theta^{LTL} = (\varphi \sqcap \psi)$ $[\theta^{CTL} = \forall(\varphi \sqcap \psi)]$, то $M, u_i \models \theta^{LTL}$ $[M, u_i \models \theta^{CTL}] \rightleftharpoons$ для [каждого] полного пути с началом в вершине u_i и всякой его вершины u_j, для которой верно $M, u_j \models \psi^{LTL}$ $[M, u_j \models \psi^{CTL}]$, существует вершина u_k этого пути, предшествующая u_j, для которой верно $M, u_k \models \varphi^{LTL}$ $[M, u_k \models \varphi^{CTL}]$. Если $\theta^{CTL} = \exists(\varphi \sqcap \psi)$, то $M, u_i \models \theta^{CTL} \rightleftharpoons$ существует такой полный путь с началом в вершине u_i, что у всякой его вершины u_j, для которой верно $M, u_j \models \psi^{CTL}$, существует вершина u_k этого пути, предшествующая u_j, для которой верно $M, u_k \models \varphi^{CTL}$.

Формула θ *истинна в модели* M, если она истинна в выделенной вершине u_0 этой модели. Формула θ *выполнима*, если она истинна в некоторой модели (имеет модель).

Формула θ *общезначима*, если она истинна в каждой модели.

Трансляцию формулы θ^{LTL} в формулу θ^{CTL} обозначим через $Tr(\theta^{LTL}) = \theta^{CTL}$ и определим индукцией по строению формулы θ^{LTL}:

$Tr(p) = p$, $Tr(\neg p) = \neg p$, $Tr(\neg\neg\varphi) = Tr(\varphi)$;

$Tr(\varphi \wedge \psi) = (Tr(\varphi) \wedge Tr(\psi))$, $Tr(\varphi \vee \psi) = (Tr(\varphi) \vee Tr(\psi))$;

$Tr\neg(\varphi \wedge \psi) = (Tr(\neg\varphi) \vee Tr(\neg\psi))$, $Tr\neg(\varphi \vee \psi) = (Tr(\neg\varphi) \wedge Tr(\neg\psi))$;

$Tr(\bigcirc\varphi^{LTL}) = \forall\bigcirc Tr(\varphi)$; $Tr(\neg\bigcirc\varphi^{LTL}) = (\forall\bigcirc Tr(\neg\varphi) \wedge \exists\bigcirc(p_1 \vee \neg p_1))$;

$Tr(\neg(\varphi\ U\ \psi)^{LTL}) = Tr((\neg\varphi \sqcap \psi)^{LTL})$, $Tr(\neg(\varphi \sqcap \psi)^{LTL}) = Tr((\neg\varphi\ U\ \psi)^{LTL})$;

$Tr((\varphi\ U\ \psi)^{LTL}) = (Tr(\psi) \vee ((Tr(\varphi) \wedge \forall\bigcirc\forall(Tr(\varphi)\ U\ Tr(\psi))) \wedge \exists\bigcirc(p_1 \vee \neg p_1)))$;

$Tr((\varphi \sqcap \psi)^{LTL}) = (Tr(\neg\psi) \wedge (Tr(\varphi) \vee \forall\bigcirc\forall(Tr(\varphi) \sqcap Tr(\psi))))$.

Теорема. *Если формула* θ^{LTL} $[\theta^{CTL}]$ *выполнима, то она имеет*

такую модель M, *что формула* θ^{CTL} $[\theta^{LTL}]$ *выполнима и истинна в модели* M.

Доказательство теоремы проводится с использованием методов работы [5].

Работа выполнена при финансовой поддержке программы фундаментальных исследований ОМН РАН "Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения".

Список литературы

1. Emerson E. A, Halpern J. Y. "Sometimes" and "Not Never" revisited: on branching versus linear time temporal logic // JACM. — V. 33, № 1. — P. 151–178.

2. Хелемендик Р. В. О сведении задачи распознавания выполнимости формул логики линейного времени к распознаванию выполнимости формул логики высказываний // Проблемы теоретической кибернетики. Материалы XVI Международной конференции (Нижний Новгород, 20–25 июня 2011г.). — Нижний Новгород: Изд-во Нижегородского госуниверситета, 2011. — С. 523–526.

3. Хелемендик Р. В. О сведении задачи распознавания выполнимости формул логики ветвящегося времени к распознаванию выполнимости формул логики высказываний // Сборник трудов XVII Международной школы-семинара "Синтез и сложность управляющих систем" имени академика О. Б. Лупанова (Новосибирск, 27 октября – 1 ноября 2008г.). — М.: Изд-во механико-математического факультета МГУ, 2008. — С. 177–180.

4. Шилов Н. В. О квазидетерминированной логике процессов // Математическая теория программирования // Советско-болгарский сборник научных трудов. — Новосибирск: ВЦ СО АН СССР, 1985. — С. 65–81.

5. Хелемендик Р. В. Алгоритм распознавания выполнимости формул логики ветвящегося времени и эффективный алгоритм построения выводов общезначимых формул из аксиом // Мат. вопросы кибернетики. Вып. 15. — М.: Физматлит, 2006. — С. 217–266.

Секция «Комбинаторный анализ»

НЕСУЩЕСТВОВАНИЕ АНАЛОГА ТЕОРЕМЫ КРАСКАЛА — КАТОНЫ ДЛЯ ЗАДАЧИ МИНИМИЗАЦИИ ДВУСТОРОННЕЙ ТЕНИ

М. А. Башов (Москва)

Пусть $\mathcal{F}$ — семейство k-элементных подмножеств $[n] = \{1, 2, \ldots, n\}$, то есть $\mathcal{F} \subseteq \binom{[n]}{k}$. *Нижней тенью* $\Delta\mathcal{F}$ называется семейство таких $(k-1)$-множеств A, что существует $B \in \mathcal{F}$, $A \subset B$. Аналогично, *верхней тенью* $\nabla\mathcal{F}$ называется семейство таких $(k+1)$-множеств A, что существует $B \in \mathcal{F}$, $A \supset B$. *Двусторонней тенью* $\overline{\Delta}\mathcal{F}$ называется объединение семейств $\Delta\mathcal{F}$ и $\nabla\mathcal{F}$.

Множество $\mathcal{F} \subseteq \binom{[n]}{k}$ называется *минимальным по нижней тени* (*верхней тени, двусторонней тени*), если $|\Delta\mathcal{F}| \leqslant |\Delta\mathcal{G}|$ (соответственно $|\nabla\mathcal{F}| \leqslant |\nabla\mathcal{G}|$, $|\overline{\Delta}\mathcal{F}| \leqslant |\overline{\Delta}\mathcal{G}|$) для любого $\mathcal{G} \subseteq \binom{[n]}{k}$ такого, что $|\mathcal{G}| = |\mathcal{F}|$.

Краскал [1] и Катона [2] описали решения задачи минимизации односторонней тени:

Теорема (Краскал, Катона). *Левые лексикографические отрезки* $\binom{[n]}{k}$ *являются минимальными семействами по нижней тени.*

Простое доказательство теоремы Краскала — Катоны можно найти в [3]. Клементс и Линдстрём [4] доказали аналогичный результат для задачи минимизации односторонней тени в произвольном декартовом произведении цепей. Аналоги теоремы Краскала — Катоны доказаны также для декартова произведения звёзд и других частично упорядоченных множеств [5].

В данной работе рассматривается задача минимизации двусторонней тени в булевом кубе.

Назовём линейный порядок на $\binom{[n]}{k}$ *минимизирующим*, если все его начальные отрезки являются минимальными по двусторонней тени. В [6] доказано, что в $\binom{[n]}{3}$ не существует минимизирующего порядка при $n \geqslant 8$.

Определим на $\binom{[n]}{k}$ частичный порядок. Пусть A и B — элементы $\binom{[n]}{k}$, $A = \{a_1, a_2, \ldots, a_k\}$, $B = \{b_1, b_2, \ldots, b_k\}$, и элементы A и B упорядочены по возрастанию, то есть $a_1 < a_2 < \ldots < a_k$, $b_1 < b_2 < \ldots < b_k$. Множество A *предшествует* множеству B ($A \sqsubseteq B$), если $a_i \leqslant b_i$ для всех $i = 1, 2, \ldots, k$. Через $\mathcal{I}(A)$ обозначим минимальный по включению идеал, содержащий A, то есть семейство $\{B \in \binom{[n]}{k} \mid B \sqsubseteq A\}$.

Утверждение 1 [6]. *Если* $\mathcal{F} \subseteq \binom{[n]}{k}$ *— идеал, то* $|\bigvee\mathcal{F}| = \sum\limits_{A\in\mathcal{F}} s(A)$, *где* $s(A) = s_l(A) + s_u(A)$, $s_l(A) = \min([n] \setminus A) - 1$, $s_u(A) = n - \max A$.

Пусть $A = \{1, 2, \ldots, m, a_{m+1}, \ldots, a_{k-1}, a_k\} \in \binom{[n]}{k}$, $a_{m+1} > m + 1$. Обозначим $A^0 = \{2, 3, \ldots, m + 1, a_{m+1}, \ldots, a_{k-1}, n\}$. Также положим $\widehat{\mathcal{I}}(A^0) = \{B \in \binom{[n]}{k}, B^0 = A^0\}$. Пусть $p = \min(\{q : a_q > q + 1\} \cup \{k\})$. Частично упорядоченное множество $(\widehat{\mathcal{I}}(A^0), \sqsubseteq)$ содержит наименьшую точку $\{1, 2, \ldots, p-1, a_p, \ldots, a_{k-1}, a_{k-1}+1\}$. Обозначим эту наименьшую точку через A^1.

Пусть $4 \leqslant k \leqslant \frac{n}{2}$. Предположим, что на $\binom{[n]}{k}$ можно определить минимизирующий двустороннюю тень линейный порядок $<_{min}$. Из свойств оператора сдвига [3] следует, что, не ограничивая общности, можно считать, что начальные отрезки этого порядка являются идеалами, то есть из $A \sqsubseteq B$ следует $A <_{min} B$.

Утверждение 2. *Пусть* $<_{min}$ *— минимизирующий порядок, и выполнено* $A <_{min} B <_{min} C$ *и* $A^0 = C^0$. *Тогда* $A^0 = B^0 = C^0$.

Таким образом, семейства $\widehat{\mathcal{I}}(A^0)$ являются отрезками минимизирующего порядка.

Утверждение 3. *Пусть* $<_{min}$ *— минимизирующий порядок, для всех* $C^0 \sqsubseteq A^0$ *выполнено* $C^0 <_{min} B^0$, *для всех* $C^0 \sqsubseteq B^0$ *выполнено* $C^0 <_{min} A^0$, *и* $s(A^1) < s(B^1)$. *Тогда* $A^0 <_{min} B^0$.

Утверждение 4. *Пусть* $<_{min}$ *— минимизирующий порядок, для всех* $C^0 \sqsubseteq A^0$ *выполнено* $C^0 <_{min} B^0$, *для всех* $C^0 \sqsubseteq B^0$ *выполнено* $C^0 <_{min} A^0$, $s(A^1) = s(B^1)$, $\max\{s_l(A^1), s_u(A^1)\} > \max\{s_l(B^1), s_u(B^1)\}$. *Тогда* $A^0 <_{min} B^0$.

Поскольку наименьшая в смысле частичного порядка $\sqsubseteq$ точка $\binom{[n]}{k}$ принадлежит $\mathcal{C}_1(n, k) = \widehat{\mathcal{I}}(\{2, 3, \ldots, k, n\})$, а наименьшая точка $\binom{[n]}{k} \setminus \mathcal{C}_1(n, k)$ принадлежит $\widehat{\mathcal{I}}(\{2, 3, \ldots, k-1, k+1, n\})$, то семейства $\mathcal{C}_1(n, k)$ и $\widehat{\mathcal{C}}_1(n, k) = \mathcal{C}_1(n, k) \cup \widehat{\mathcal{I}}(\{2, 3, \ldots, k-1, k+1, n\})$ являются

начальными отрезками $<_{min}$. Семейство $\binom{[n]}{k} \setminus \widehat{\mathcal{C}}_1(n,k)$ содержит две минимальные точки. В случае $n \neq 2k$ порядок этих точек определён однозначно по утверждению 4.

Пусть $n > 2k$. Рассмотрим начальный отрезок $\mathcal{L}$ порядка $<_{min}$ длины $|\mathcal{I}(\{2,3,\ldots,k-1,k+2,n\})| = 1+k(n-k)+(k-1)(2n-2k-3)$. Этот отрезок состоит из идеала $\mathcal{I}(\{2,3,\ldots,k-2,k,k+1,n\}$ и $n-2k$ множеств из семейства $\widehat{\mathcal{I}}(\{2,3,\ldots,k-3,k,k+1,k+2,n)$. Подсчитывая размер тени отрезка согласно утверждению 1, получаем, что $|\sum\mathcal{L}| = |\sum\mathcal{I}(\{2,3,\ldots,k-1,k+2,n\})|+(n-2k)(k-3)$, что противоречит определению минимизирующего порядка.

Теорема 1. *При $4 \leqslant k < \frac{n}{2}$ никакой линейный порядок на $\binom{[n]}{k}$ не является минимизирующим.*

Теперь рассмотрим случай $n = 2k$, $k \geqslant 5$. Обозначим

$$\mathcal{F} = \mathcal{I}(\{3,4,\ldots,k+1,n\}) \cup \mathcal{I}(\{2,3,\ldots,k-2,k,k+2,n\}).$$

В силу симметрии можно, не ограничивая общности, считать, что $\{2,3,\ldots,k-1,k+2,n\} >_{min} \{2,3,\ldots,k-2,k,k+1,n\}$. По утверждениям 3 и 4 начальный отрезок $\mathcal{L}$ порядка $<_{min}$ длины $|\mathcal{F}|$ состоит из идеалов $\mathcal{I}(\{3,4,\ldots,k+1,n\})$, $\mathcal{I}(\{2,3,\ldots,k-1,k+3,n\})$ и множества $\{1,2,\ldots,k-2,k+4,k+5\}$. Подсчёт размера тени даёт $|\sum\mathcal{L}| = |\sum\mathcal{F}| + k - 4$, что противоречит определению минимизирующего порядка.

Теорема 2. *При $5 \leqslant k = \frac{n}{2}$ никакой линейный порядок на $\binom{[n]}{k}$ не является минимизирующим.*

Непосредственной проверкой установлено, что в $\binom{[8]}{4}$ и $\binom{[7]}{3}$ также не существует минимизирующих линейных порядков, а в $\binom{[6]}{3}$ такой порядок существует.

Работа выполнена при финансовой поддержке РФФИ (проект 10-01-00768-а).

Список литературы

1. Kruskal J. The number of simplices in a complex // Mathematical Optimization Techniques. — Berkeley, Los Angeles: Uni. of California Press, 1963. — P. 251–278.

2. Katona G. O. H. A theorem of finite sets // Proceedings of Tihany Conference. — 1966. — P. 187–207.

3. Ahlswede R., Aydinian H., Khachatrian L. H. More about shifting techniques // European J. Combin. — 2003. — № 24 (5). — P. 551–556.

4. Clements G. F., Lindström B. A generalization of a combinatorial theorem of Macaulay // J. Comb. Theory. — 1969. — № 7. — P. 230–238.

5. Bezrukov S. L., Leck U. Macaulay posets // Electron. J. Combin. — 2004. — Dynamic Survey DS12.

6. Башов М. А. Минимизация двусторонней тени в единичном кубе // Дискретная математика. — 2011. — Т. 23, № 4. — С. 115–132.

ОБ ЭФФЕКТИВНОМ ПОИСКЕ БУКВЕННЫХ СОСТАВОВ В ФРАГМЕНТАХ ДВУМЕРНЫХ СЛОВ

Д. Белаззогу (Париж, Франция), Р. М. Колпаков (Москва), М. Раффино (Париж, Франция)

Под двумерным словом размера $m \times n$ над алфавитом Σ формально понимается составленная из символов алфавита Σ прямоугольная матрица с m строками и n столбцами. Подматрица данной матрицы, образованная пересечением произвольного числа идущих подряд строк с произвольным числом идущих подряд столбцов, называется прямоугольным фрагментом двумерного слова. Прямоугольный фрагмент двумерного слова называется квадратным, если его высота равна его ширине. Без ограничения общности мы полагаем, что $m \leq n$. Под буквенным составом фрагмента двумерного слова понимается множество всех различных символов, содержащихся в данном фрагменте. Если множество A является буквенным составом некоторого фрагмента двумерного слова, то данный фрагмент называется ареалом для A. Прямоугольный ареал для буквенного состава A называется максимальным, если любой прямоугольный фрагмент большего размера, содержащий данный ареал, имеет буквенный состав, отличный от A. Аналогичным образом, квадратный ареал для буквенного состава A называется максимальным, если любой квадратный фрагмент большего размера, содержащий данный ареал, имеет буквенный состав, отличный от A. В данной работе рассматривается задача эффективного поиска всевозможных буквенных составов для прямоугольных и квадратных фрагментов произвольного заданного двумерного слова. Аналогичная задача эффективного поиска всевозможных буквенных составов для фрагментов одномерных слов рассматривалась в [1–3].

В данной работе получены следующие результаты. Пусть w — произвольное двумерное слово размера $m \times n$ над алфавитом Σ размера σ. Обозначим через L_r (L_s) число максимальных прямоугольных (квадратных) ареалов в слове w.

Теорема 1. *Все буквенные составы для прямоугольных фрагментов слова w могут быть вычислены за время $O(nm^2\sigma+L_r\log\sigma)$.*

Теорема 2. *Все буквенные составы для квадратных фрагментов слова w могут быть вычислены за время $O(nm\sigma+L_s\log\sigma)$.*

Работа выполнена при финансовой поддержке РФФИ (проект 11-01-00508).

Список литературы

1. Amir A., Apostolico A., Landau G. M., and Satta G. Efficient text fingerprinting via parikh mapping // Journal of Discrete Algorithms. — 2003. — V. 1, № 5–6. — P. 409–421.

2. Chi-Yuan Chan, Hung-I Yu, Wing-Kai Hon, and Biing-Feng Wang. Faster query algorithms for the text fingerprinting problem // Information and Computation. — 2011. — V. 209, № 7. — P. 1057–1069.

3. Kolpakov R., Raffinot M. New algorithms for text fingerprinting // Journal of Discrete Algorithms. — 2008. — V. 6, № 2. — P. 243–255.

СТАТИСТИКИ НА VP-МОНОТОННЫХ ПЕРЕСТАНОВКАХ

Л. Н. Бондаренко (Пенза), М. Л. Шарапова (Москва)

В [1, 2] на симметрической группе S_n перестановок $\sigma{=}\sigma_1\dots\sigma_n$, где σ — слово над алфавитом $[n]{=}\{1,\dots,n\}$, рассматривались следующие статистики: $\mathrm{rise}(\sigma){=}\#\{i : 1\le i\le n,\ \sigma_i{>}\sigma_{i-1},\ \sigma_0{=}0\}$; $\mathrm{imal}(\sigma){=}\mathrm{card}\{\gamma_1,\dots,\gamma_n\}$, где $\gamma_1{=}0$, $\gamma_i{=}\#\{j : 1\le j\le i{-}1,\ \sigma_j{<}\sigma_i\}$, $i\ge 2$; $\mathrm{inv}(\sigma){=}\#\{(i,j) : 1\le i{<}j\le n,\ \sigma_i{>}\sigma_j\}$; $\mathrm{maj}(\sigma){=}\sum_{i=1}^{n} i$, $\sigma_i{>}\sigma_{i+1}$; $\mathrm{fix}(\sigma){=}\#\{i : 1\le i\le n,\ \sigma_i{=}i\}$; $\mathrm{lec}(\sigma){=}\sum_{i=1}^{n}\mathrm{inv}(\kappa_i)$; $\mathrm{pix}(\sigma){=}|p\,|$.

В записи двух последних статистик используется представление $\sigma{=}p\kappa_1\dots\kappa_m$, где крюки $\kappa_1,\dots,\kappa_m$ находятся рекурсивно: κ_m — суффикс слова σ вида $\sigma_s{>}\sigma_{s+1}{<}\dots{<}\sigma_n$, крюк κ_{m-1} определяется аналогично для слова $\sigma_1\dots\sigma_{s-1}$ и т. д.; p — префикс слова σ, не являющийся крюком, а $|p\,|$ — его длина.

Биекция $\mathrm{vp} : \sigma\mapsto\tau$, отображает $\sigma{\in}S_n$ на слово $\tau{=}\tau_1\dots\tau_n$, $\tau{\in}T_n$ по правилу $\tau{=}\sigma\oplus\nu$, где $\tau_i{=}\sigma_i{+}\nu_i(\mathrm{mod}\ n)$, $\nu_i{=}n{-}i{+}1$, $i{=}1,\dots,n$, а τ_i — наименьший положительный вычет, и индуцирует следующие статистики [3]: $\mathrm{ivp}(\sigma){=}n^{-1}\sum_{i=1}^{n}\tau_i$; $\mathrm{exc}(\sigma){=}\#\{i : 1\le i\le n,\ \sigma_i\ge i\}$; $\mathrm{var}(\sigma){=}\mathrm{card}\{\tau_1,\dots,\tau_n\}$, причем $\mathrm{ivp}(\sigma){+}\mathrm{exc}(\sigma){=}n{+}1$.

Вид производящего многочлена $\sum_{\sigma\in S_n} t^{\mathrm{stat}(\sigma)}$ определяет класс статистики stat. Так, stat называется эйлеровой (E-статистикой), если ее производящий многочлен эйлеров, т. е. задается рекуррентным соотношением $A_0(t)=1,\ A_n(t)=ntA_{n-1}(t)+t(1-t)A'_{n-1}(t),\ n\geq 1$. Например, lec (с многочленом $t^{-1}A_n(t)$), rise, imal, ivp, а также exc являются E-статистиками [1–3].

При производящем многочлене $B_n(q)=[n]_q!$, $[n]_q=(1-q)^{-1}(1-q^n)$ stat называется статистикой Мак-Магона (M-статистикой). Например, inv и maj являются M-статистиками [1].

stat назовем D-статистикой, если ее производящий многочлен, который связан с задачей о встречах, определяется рекуррентной формулой $D_0(t)=1,\ D_n(t)=nD_{n-1}(t)+(t-1)^n,\ n\geq 1$ [4]. Например, fix и pix являются D-статистиками [2].

Определение 1. *Слово $\tau\in T_n$ называется монотонным, если все его последовательные символы образуют неубывающую последовательность, а $\sigma=\mathrm{vp}^{-1}(\tau)$, $\sigma\in S_n$, называется* vp-*монотонной перестановкой (множество этих перестановок* $\mathrm{mon}(S_n)$ *задается биекцией* $\mathrm{vp}:\mathrm{mon}(S_n)\to\mathrm{mon}(T_n)$ [5]).

Лемма 1. а) *Если $\sigma\in\mathrm{mon}(S_n)$ и $\sigma=\xi n\eta$, то префикс ξ и суффикс η являются монотонно возрастающими словами.*

б) *Множество* $\mathrm{mon}(S_n)$ *изоморфно булевой решетке ранга* $n-1$.

Доказательство. а) Фиксация в слове $\sigma=\xi n\eta$ положения символа n и равенство $\tau=\sigma\oplus\nu$, где $\tau\in\mathrm{mon}(T_n)$, легко приводит к требуемому.

б) Если $\sigma\in\mathrm{mon}(S_n)$ и $\sigma=\xi n\eta$, то биекция $\varphi:\sigma\mapsto\{\xi\}$, $\{\xi\}\subseteq[n-1]$ определяет искомый изоморфизм. При этом $\{\eta\}\subseteq[n-1]-\{\xi\}$, ранг перестановки $\sigma\in\mathrm{mon}(S_n)$ как элемента решетки равен $|\xi\,|$, а ранговопроизводящая функция решетки $\mathrm{mon}(S_n)$ имеет вид $(1+t)^{n-1}$.

Естественно возникает задача определения вида производящих многочленов $\sum_{\sigma\in\mathrm{mon}(S_n)} t^{\mathrm{stat}(\sigma)}$ для рассмотренных выше статистик.

Для статистики rise, в силу леммы 1, результат тривиален: имеется одна перестановка $\sigma\in\mathrm{mon}(S_n)$, для которой $\mathrm{rise}(\sigma)=n$, а для остальных $2^{n-1}-1$ таких перестановок $\mathrm{rise}(\sigma)=n-1$.

Теорема 1. а) $\mathrm{ivp}(\sigma)=1+\mathrm{lec}(\sigma)$, *и для статистик* ivp, exc *производящий многочлен* $\widetilde{A}_n^{(1)}(t)=t(1+t)^{n-1}$. б) *Для статистики* imal *производящий многочлен* $\widetilde{A}_n^{(2)}(t)=t^n((1+t^{-1/2})^n+(1-t^{-1/2})^n)/2$.

Доказательство. а) По лемме 1 для $\sigma\in\mathrm{mon}(S_n)$ как элемента решетки ранга k находится равенство $\mathrm{exc}(\sigma)=k+1$. Так как $\sigma\in\mathrm{mon}(S_n)$ имеет не более одного крюка, то также имеем $\mathrm{exc}(\sigma)+\mathrm{lec}(\sigma)=n$.

б) С помощью леммы 1 соотношение для многочлена $\widetilde{A}_n^{(2)}(t)$ устанавливается методом математической индукции.

Теорема 2. а) *Для статистики* maj *производящий многочлен* $\widetilde{B}_n^{(1)}(t)=t(1+t)^{n-1}-t^n+1$. б) *Для статистики* inv *производящий многочлен* $\widetilde{B}_n^{(2)}(t)=H_{n-1}(t,t)$, *а* $H_n(t,q)$ — *многочлен Роджерса—Сеге* [6], *определяемый формулой* $H_n(t,q)=\sum_{k=0}^{n}\begin{bmatrix}n\\k\end{bmatrix}_q t^k$, *где* $\begin{bmatrix}n\\k\end{bmatrix}_q=\frac{[n]_q}{[k]_q[n-k]_q}$ — *многочлен Гаусса. Многочлен* $H_n(t,q)$ *находится также с помощью следующего рекуррентного соотношения* [6] $H_0(t,q)=1$, $H_1(t,q)=1+t$, $H_{n+1}(t,q)=(1+t)H_n(t,q)-(1-q^n)tH_{n-1}(t,q)$.

Доказательство. а) По лемме 1 для $\sigma\in\mathrm{mon}(S_n)$ как элемента решетки ранга k вычисляется $\mathrm{maj}(\sigma)=k+2$, если $k\le n-2$, и $\mathrm{maj}(\sigma)=1$, если $k=n-1$. б) Для всех $\sigma\in\mathrm{mon}(S_n)$ как элементов решетки ранга k методом математической индукции находится многочлен $\begin{bmatrix}n\\k\end{bmatrix}_t t^k$.

Теорема 3. а) *Для статистики* fix *имеем производящий многочлен* $\widetilde{D}_n^{(1)}(t)=t^n+(2-t)^{-1}(2^{n-1}-t^{n-1})$. б) *Для статистики* pix *производящий многочлен* $\widetilde{D}_n^{(2)}(t)=(1+t)^{n-1}-(1-t)t^{n-1}$.

Доказательство. а) Соотношение для многочлена $\widetilde{D}_n^{(1)}(t)$ устанавливается методом математической индукции с помощью леммы 1. б) По лемме 1 для $\sigma\in\mathrm{mon}(S_n)$ как элемента решетки ранга k вычисляется $\mathrm{pix}(\sigma)=k$, если $k\le n-2$, и $\mathrm{pix}(\sigma)=n$, если $k=n-1$.

Теорема 4. *Для статистики* var *имеем производящий многочлен* $\widetilde{C}_n(t)=((1+t)^n-(1-t)^n)/2$.

Доказательство. Соотношение для многочлена $\widetilde{C}_n(t)$ устанавливается методом математической индукции с помощью леммы 1.

Отметим, что для статистики var на группе перестановок S_n в отличие от множества $\mathrm{mon}(S_n)$ явного выражения для производящего многочлена до сих пор не найдено.

В заключение запишем также следующие простые связи между полученными производящими многочленами: $\widetilde{B}_n^{(1)}(t)-\widetilde{A}_n^{(1)}(t)=1-t^n$, $\widetilde{C}_{2m+1}(t)=t^{-(2m+1)}\widetilde{A}_{2m+1}^{(2)}(t^2)$, $\widetilde{C}_{2m}(t)+t^{-2m}\widetilde{A}_{2m}^{(2)}(t^2)=(1+t)^{2m}$.

Работа выполнена при финансовой поддержке первого автора грантом РФФИ (проект 11-01-00212а).

Список литературы

1. Фоата Д. Распределения типа Эйлера и Макмагона на группе перестановок // Проблемы комбинаторного анализа. — М.: Мир,

1980. — С. 120–141.

2. Foata D., Han G. Fix-Mahonian calculus III; a quadruple distribution // Monatshefte für Mathematik. — 2008. — 154. — P. 177–197.

3. Бондаренко Л. Н., Шарапова М. Л. Два типа r-перестановок и r-многочлены Эйлера // Материалы X Международного семинара "Дискретная математика и ее приложения" (Москва, МГУ, 1–6 февраля 2010 г.). — М.: Изд-во механико-математического факультета МГУ, 2010. — С. 217–220.

4. Риордан Дж. Введение в комбинаторный анализ. — М.: Изд-во иностр. литер., 1963.

5. Бондаренко Л. Н., Шарапова М. Л. Параметрические комбинаторные задачи и методы их исследования // Известия высших учебных заведений. Поволжский регион. Физико-математические науки. — 2010. — № 4. — С. 50–63.

6. Эндрюс Г. Теория разбиений. — М.: Наука, 1982.

СТАТИСТИКИ НА ГРУППЕ ПЕРЕСТАНОВОК И ПЕРМАНЕНТЫ

Л. Н. Бондаренко (Пенза), М. Л. Шарапова (Москва)

В [1, 2] на симметрической группе S_n перестановок $\sigma{=}\sigma_1\dots\sigma_n$, где σ — слово над алфавитом $\{1,\dots,n\}$, рассматривалась биекция $\mathrm{vp}: S_n \to W_n$, отображающая $\sigma{\in}S_n$ при фиксированном ключе $\kappa{=}\kappa_1\dots\kappa_n$, $\kappa{\in}S_n$ на слово $\omega{=}\omega_1\dots\omega_n$, $\omega{\in}W_n$ по правилу $\omega{=}\sigma\oplus\kappa$, где $\omega_i{=}\sigma_i{+}\kappa_i(\mathrm{mod}\ n)$, $i{=}1,\dots,n$, а ω_i — наименьший положительный вычет, и индуцируемые ей статистики: $\mathrm{ivp}(\sigma,\kappa){=}n^{-1}\sum_{i=1}^{n}\omega_i$; $\mathrm{exc}(\sigma,\kappa){=}\#\{i: 1\le i\le n,\ \sigma_i{+}\kappa_i{>}n\}$ (для простоты записи ссылка на ключ $\kappa{=}\nu$, где $\nu{=}\nu_1\dots\nu_n$, $\nu_i{=}n{-}i{+}1$, $i{=}1,\dots,n$, будет опускаться).

В [1] показано, что по терминологии работы [3] ivp и exc — эйлеровы статистики, т. е. $A_n(t){=}\sum_{\sigma\in S_n} t^{\mathrm{ivp}(\sigma,\kappa)}{=}\sum_{\sigma\in S_n} t^{\mathrm{exc}(\sigma,\kappa)}$ — многочлен Эйлера, который определяется рекуррентным соотношением $A_0(t){=}1$, $A_n(t){=}ntA_{n-1}(t){+}t(1{-}t)A'_{n-1}(t)$, $n\ge 1$, причем этот многочлен также вычисляется через перманент $A_n(t) = \mathrm{per}\,C(t,\kappa)$, где матрица $C(t,\kappa)$ получается соответствующей перестановкой строк циркулянта $C(t){=}(c_{ij}(t))_{i,j=1}^{n}$, порожденного последовательно циклически сдвигаемым на позицию вправо вектором $\left(t^{1/n}, t^{2/n},\dots,t\right)$, а перманент $\mathrm{per}\,C(t){=}\sum_{\sigma\in S_n} c_{1\sigma_1}(t)\dots c_{n\sigma_n}(t)$.

По определению статистика $\mathrm{exc}(\sigma)=\#\{i : 1 \le i \le n,\, \sigma_i \ge i\}$ и $A_n(t) = \operatorname{per} T(t)$, где $T(t)=(t_{ij}(t))_{i,j=1}^{n}$, $t_{ij}(t)=t$ при $i \le j$ и $t_{ij}(t)=1$ при $i > j$, причем матрица $T(t,\kappa)$ получается из $T(t)$ соответствующей перестановкой строк. Это дает комбинаторное доказательство следующего утверждения.

Лемма 1. *При всех* $\kappa^{(1)}, \kappa^{(2)} \in S_n$ $\operatorname{per} C(t,\kappa^{(1)}) = \operatorname{per} T(t,\kappa^{(2)})$.

По аналогии с [3] введем обозначения: $\mathrm{iivp}(\sigma,\kappa)=\mathrm{ivp}(\sigma^{-1},\kappa)$ и $\mathrm{iexc}(\sigma,\kappa)=\mathrm{exc}(\sigma^{-1},\kappa)$. Тогда для этих статистик в лемме 1 получим матрицы $C^*(t,\kappa^{(1)})$ и $T^*(t,\kappa^{(2)})$, где "*" означает транспонирование.

Полагая $\mathrm{qun}(\sigma,\kappa)=\#\{i : 1 \le i \le n,\, \omega_i=1\}$, имеем $\mathrm{qun}(\sigma)=\mathrm{fix}(\sigma)$, где $\mathrm{fix}(\sigma)=\#\{i : 1 \le i \le n,\, \sigma_i=i\}$ использована в [4], а производящий многочлен $D_n(t)$ для $\mathrm{fix}(\sigma)$ связан с задачей о встречах [5] и задается соотношением $D_0(t)=1$, $D_n(t)=nD_{n-1}(t)+(t-1)^n$, $n \ge 1$, причем $D_n(t) = \operatorname{per} F(t,\kappa)$, а $F(t,\kappa)$ получается соответствующей перестановкой строк матрицы $F(t)=(f_{ij}(t))_{i,j=1}^{n}$, $f_{ii}(t)=t$ и $f_{ij}(t)=1$, $i \ne j$.

Отметим, что несложные вычисления приводят к соотношениям: $\det C(t)=t(1-t)^{n-1}$, $\det T(t)=t(t-1)^{n-1}$, $\det F(t)=(t+n-1)(t-1)^{n-1}$.

В [3, 4] рассматривались многомерные распределения ряда статистик и соответствующие им аналитические выражения.

Так как производящие многочлены статистик ivp, exc, iivp, iexc, qun описываются с помощью перманентов, то естественно возникает задача нахождения перманентов, задающих совместные распределения этих статистик.

Симметрия эйлерова распределения $\{A_{n,k}/n!\}_{k=1}^{n}$, отвечающая равенству $A_n(t)=t^{n+1}A_n(t^{-1})$, приводит к следующему понятию.

Определение 1. *Эйлеровы статистики* stat_1 *и* stat_2 *назовем зависимыми при фиксированном* $n \ge 1$, *если* $\forall \sigma \in S_n$ $\mathrm{stat}_1=\mathrm{stat}_2$ *или* $\mathrm{stat}_1+\mathrm{stat}_2=n+1$, *и, соответственно, независимыми, если при фиксированном* $n \ge 3$ *это условие нарушается.*

В частности, $\mathrm{ivp}(\sigma,\kappa)$ и $\mathrm{exc}(\sigma,\kappa)$ зависимы при любом $\kappa \in S_n$, так как $\mathrm{ivp}(\sigma,\kappa)+\mathrm{exc}(\sigma,\kappa)=n+1$ [1, 2], а независимость статистик stat_1 и stat_2 означает, что производящий многочлен двух переменных, описывающий их совместное распределение, имеет более n одночленов.

Лемма 2. а) *Статистики* $\mathrm{ivp}(\sigma,\kappa^{(1)})$ *и* $\mathrm{exc}(\sigma,\kappa^{(2)})$ *независимы при* $\kappa^{(1)} \ne \kappa^{(2)}$. б) *Статистики* $\mathrm{ivp}(\sigma,\kappa)$ *и* $\mathrm{iivp}(\sigma,\kappa)$, *а также* $\mathrm{exc}(\sigma,\kappa)$ *и* $\mathrm{iexc}(\sigma,\kappa)$ *зависимы только в следующих двух случаях:* 1) *ключ* $\kappa \in S_n$ *является циклическим сдвигом единичной перестановки* $\varepsilon=1 \ldots n$; 2) *ключ* $\nu^{(m)} \in S_n$ *является циклическим сдвигом слова* $\nu \in S_n$ *влево на* m *символов, а* $n=2m-1$.

Доказательство. Первая часть утверждения следует из независимости функций $\mathrm{ivp}(\sigma,\kappa^{(1)})$ и $\mathrm{ivp}(\sigma,\kappa^{(2)})$ при $\kappa^{(1)}\neq\kappa^{(2)}$ и зависимости $\mathrm{ivp}(\sigma,\kappa)$ и $\mathrm{exc}(\sigma,\kappa)$ при любом $\kappa\in S_n$, а вторая доказывается рассмотрением слов $\omega=\sigma\oplus\kappa$.

Из приведенных результатов следует утверждение.

Лемма 3. *Производящий многочлен распределения на группе* S_n $P(t,\kappa^{(1)};\, s,\kappa^{(2)};\, z,\kappa^{(3)};\, u,\kappa^{(4)};\, v,\kappa^{(5)})$ *пятимерного вектора* $(\mathrm{ivp}(\sigma,\kappa^{(1)}),\ \mathrm{iivp}(\sigma,\kappa^{(2)}),\ \mathrm{qun}(\sigma,\kappa^{(3)}),\ \mathrm{exc}(\sigma,\kappa^{(4)}),\ \mathrm{iexc}(\sigma,\kappa^{(5)}))$ *есть* $\sum_{\sigma\in S_n} t^{\mathrm{ivp}(\sigma,\kappa^{(1)})}s^{\mathrm{iivp}(\sigma,\kappa^{(2)})}z^{\mathrm{qun}(\sigma,\kappa^{(3)})}u^{\mathrm{exc}(\sigma,\kappa^{(4)})}v^{\mathrm{iexc}(\sigma,\kappa^{(5)})}$ *и равен перманенту матрицы* $H=H(t,\kappa^{(1)};\, s,\kappa^{(2)};\, z,\kappa^{(3)};\, u,\kappa^{(4)};\, v,\kappa^{(5)})$, *где* $H=C(t,\kappa^{(1)})\circ C^*(s,\kappa^{(2)})\circ F(z,\kappa^{(3)})\circ T(u,\kappa^{(4)})\circ T^*(v,\kappa^{(5)})$, *а произведение матриц понимается как произведение Адамара– Шура, т. е. поэлементное умножение матриц.*

Производящие многочлены маргинальных распределений получаются из перманента леммы 3 приравниванием соответствующих переменных единице, а также верны следующие утверждения.

Теорема 1. *Пусть* $\kappa^{(1)}=\kappa^{(2)}=\kappa^{(3)}=\nu$ *и* $\kappa^{(4)}=\kappa^{(5)}=\nu^{(1)}$. *Тогда* $P(t;\, s;\, z;\, u,\nu^{(1)};\, v,\nu^{(1)})=\mathrm{per}\,(C(t)\circ C^*(s)\circ F(z)\circ T(u,\nu^{(1)})\circ T^*(v,\nu^{(1)}))$, *и все маргинальные двумерные распределения, отвечающие эйлеровым статистикам, имеют одинаковые производящие многочлены.*

Доказательство проводится с использованием лемм, а статистика $\mathrm{exc}(\sigma,\nu^{(1)})=1+\#\{i:\,1\le i\le n-1,\ \sigma_i>i\}$ отличается на единицу от аналогичной статистики в [4].

Теорема 2. *Пусть* $\kappa^{(1)}=\kappa^{(2)}=\kappa^{(3)}=\nu^{(k)}$ *и* $\kappa^{(4)}=\kappa^{(5)}=\nu^{(k+1)}$, $k=0,\dots,n-1$. *Тогда* $P(t,\nu^{(k)};\, s,\nu^{(k)};\, z,\nu^{(k)};\, u,\nu^{(k+1)};\, v,\nu^{(k+1)})$ *равен* $P(t,\nu^{(k+m)};\, s,\nu^{(k+m)};\, z,\nu^{(k+m)};\, u,\nu^{(k+m+1)};\, v,\nu^{(k+m+1)})$ *при* $n=2m$ *и совпадает с* $P(u,\nu^{(n-k)};\, v,\nu^{(n-k)};\, z,\nu^{(n-k)};\, t,\nu^{(n-k+1)};\, s,\nu^{(n-k+1)})$ *при* $n=2m-1$.

Доказательство опирается на лемму 3 и свойства слов $\omega=\sigma\oplus\kappa$.

Отметим, что с учетом леммы 1 можно матрицы C и C^* в лемме 3 заменить на T и T^* (или T и T^* — на C и C^*), но тогда формулировки леммы 3 и теорем 1, 2 должны быть несколько модифицированы.

Работа выполнена при финансовой поддержке первого автора грантом РФФИ (проект 11-01-00212а).

Список литературы

1. Бондаренко Л. Н. О статистиках Эйлера на группе перестановок // Материалы IX Международного семинара "Дискретная математика и ее приложения", посвященного 75-летию со дня рождения

академика О. Б. Лупанова (Москва, МГУ, 18–23 июня 2007 г.) — М.: Изд-во механико-математического факультета МГУ, 2007. — С. 206–208.

2. Бондаренко Л. Н., Шарапова М. Л. Два типа r-перестановок и r-многочлены Эйлера // Материалы X Международного семинара "Дискретная математика и ее приложения" (Москва, МГУ, 1–6 февраля 2010 г.) — М.: Изд-во механико-математического факультета МГУ, 2010. — С. 217–220.

3. Фоата Д. Распределения типа Эйлера и Макмагона на группе перестановок // Проблемы комбинаторного анализа: сб. статей. — М.: Мир, 1980. — С. 120–141.

4. Foata D., Han G. Fix-Mahonian calculus III; a quadruple distribution // Monatshefte für Mathematik. — 2008. — 154. — P. 177–197.

5. Риордан Дж. Введение в комбинаторный анализ. — М.: Изд-во иностр. литер., 1963.

ИНВЕСТИЦИОННАЯ БУЛЕВА ЗАДАЧА С КРИТЕРИЯМИ ВАЛЬДА И СЭВИДЖА В УСЛОВИЯХ НЕОПРЕДЕЛЕННОСТИ

В. А. Емеличев, В. В. Коротков (Минск)

Рассматривается бикритериальный дискретный вариант управления инвестициями, основанный на портфельной теории Марковица [1], с двумя упорядоченными критериями — максиминным критерием эффективности Вальда [2]

$$e(x,E)=\min_{i\in N_m}\sum_{j\in N_n}e_{ij}x_j\to\max_{x\in X} \tag{1}$$

и минимаксным критерием риска Сэвиджа [3]

$$r(x,R)=\max_{i\in N_m}\sum_{j\in N_n}r_{ij}x_j\to\min_{x\in X}. \tag{2}$$

$N_n=\{1,2,\dots,n\}$ — альтернативные инвестиционные проекты (активы); N_m — возможные состояния рынка; $x=(x_1,x_2,\dots,x_n)^T\in$

$X \subseteq \{0,1\}^n$ — инвестиционный портфель, где $x_j = 1$, если инвестиционный проект $j \in N_n$ реализуется, и $x_j = 0$ в противном случае; e_{ij} — ожидаемая оценка эффективности (чистый доход) проекта $j \in N_n$ в случае, когда рынок находится в состоянии $i \in N_m$; r_{ij} — мера риска, которому подвергается инвестор, выбирая проект $j \in N_n$ при i-м состоянии рынка. Таким образом, исходной информацией задачи являются две матрицы — матрица эффективности $E = [e_{ij}] \in \mathbf{R}^{m\times n}$ и матрица рисков $R = [r_{ij}] \in \mathbf{R}^{m\times n}$.

Под бикритериальной инвестиционной задачей $Z^m(E,R)$ с упорядоченными критериями Вальда и Сэвиджа будем понимать задачу поиска множества оптимальных портфелей $L^m(E,R)$ задачи

$$r(x,R) \to \min_{x\in L^m(E)},$$

где $L^m(E)$ — множество оптимальных портфелей задачи (1). Тем самым, $L^m(E,R)$ — множество лексикографически оптимальных портфелей задачи (1)–(2).

Высокая степень неопределенности и некорректности исходной информации, возникающие в связи с использованием статистических и экспериментальных оценок эффективности и риска инвестиционных проектов (см., например, [4]) вызывает необходимость выявления предельного уровня изменений начальных данных задачи, сохраняющих лексикографическую оптимальность выбранного портфеля. Такой подход приводит к ключевому понятию радиуса устойчивости портфеля $x^0 \in L^m(E,R)$, под которым, следуя [5], будем понимать число $\rho^m(x^0,E,R) = \sup\ \Xi$, если $\Xi \neq \emptyset$, и $\rho^m(x^0,E,R) = 0$, если $\Xi = \emptyset$, где

$$\Xi = \{\varepsilon > 0 :\ \forall (E',R') \in \Omega(\varepsilon) \quad (x^0 \in L^s(E+E', R+R'))\},$$

$$\Omega(\varepsilon) = \{(E',R') \in \mathbf{R}^{m\times n} \times \mathbf{R}^{m\times n} :\ \|E'\| < \varepsilon\ \&\ \|R'\| < \varepsilon\}.$$

Под нормой $\|A\|$ любой матрицы $A = [a_{ij}] \in \mathbf{R}^{m\times n}$ понимаем число $\sum\limits_{i\in N_m}\sum\limits_{j\in N_n} |a_{ij}|$.

Теорема. *Для радиуса устойчивости $\rho^m(x^0,E,R)$ любого лексикографически оптимального портфеля $x^0 \in L^m(E,R)$ бикритериальной задачи $Z^m(E,R)$, $m \geq 1$, справедливы следующие достижимые оценки*

$$\varphi \leq \rho^m(x^0,E,R) \leq 2\varphi,$$

где

$$\varphi = \min_{x \in X \setminus \{x^0\}} \max_{i \in N_m} \min_{k \in N_m} \Big(\sum_{j \in N_n} e_{kj} x^0 - \sum_{j \in N_n} e_{ij} x \Big).$$

Следствие. *При* $x^0 \in L^1(E, R)$ *справедлива формула*

$$\rho^1(x^0, E, R) = \varphi.$$

Случай, когда $m = 1$ (критерии (1) и (2) — линейные), можно интерпретировать, как ситуацию, при которой состояние рынка не вызывает сомнений.

Другой вариант устойчивости векторной инвестиционной булевой задачи с упорядоченными критериями Сэвиджа рассмотрен в [6].

Работа выполнена при финансовой поддержке Белорусского республиканского фонда фундаментальных исследований (проект Ф11К–095).

Список литературы

1. Markowitz H. M. Portfolio selection: efficient diversification of investments. — Oxford: Blackwell Publ., 1991.

2. Wald A. Statistical decision functions. — New York: John Wiley, 1950.

3. Savage L. J. The foundations of statistics. — New York: Dover Publ., 1972.

4. Виленский П. Л., Лившиц В. Н., Смоляк С. А. Оценка эффективности инвестиционных проектов: теория и практика. — М.: Дело, 2008.

5. Емеличев В. А., Коротков В. В. Оценки радиуса устойчивости лексикографического оптимума векторной булевой задачи с критериями рисков Сэвиджа // Дискретный анализ и исследования операций. — 2011. — Т. 18, № 2. — С. 41–50.

6. Емеличев В. А., Коротков В. В. Анализ чувствительности векторной инвестиционной булевой задачи с упорядоченными критериями рисков Сэвиджа // Материалы XVI Международной конференции «Проблемы теоретической кибернетики» (20–25 июня 2011 г.). — Нижний Новгород: Изд-во Нижегородского госуниверситета, 2011. — С. 159–162.

К ОПТИМИЗАЦИИ НА РАЗМЕЩЕНИЯХ

О. А. Емец, А. О. Емец (Полтава)

Определенный класс задач комбинаторной оптимизации игрового типа на размещениях [1] порождает задачу минимизации линейной функции на множестве размещений, когда сумма элементов размещения — единица [2]:

$$\sum_{j=1}^{k} c_j x_j \to \min; \tag{1}$$

$$x = (x_1, ..., x_k) \in E^k_{\eta\nu}(G); \tag{2}$$

$$\sum_{j=1}^{k} x_j = 1, \tag{3}$$

где $G = \{g_1, ..., g_\eta\}$ — известное мультимножество, c_j, $g_j \in R^1$, $E^k_{\eta\nu}(G)$ — общее множество k-размещений [3].

Для ее решения предлагается использовать методологию метода ветвей и границ (МВГ).

Рассмотрим способ ветвления множества допустимых решений на подмножества в МВГ. Упорядочим коэффициенты целевой функции согласно неравенств:

$$c_{\alpha_1} \geq c_{\alpha_2} \geq ... \geq c_{\alpha_l} \geq 0 > c_{\alpha_{l+1}} \geq ... \geq c_{\alpha_k}, \tag{4}$$

а элементы мультимножества G считаем, без ограничения общности рассуждений, пронумерованными так, что выполняются соотношения:

$$g_1 \leq g_2 \leq ... \leq g_k \leq g_{k+1} \leq ... \leq g_\eta. \tag{5}$$

Ветвления предлагается делать "в глубину", определяя одну за одной переменные в векторе $x \in E^k_{\eta\nu}$ в порядке номеров $\alpha_1, \alpha_2, ..., \alpha_{l-1}, \alpha_l$, а потом $\alpha_k, \alpha_{k-1}, ..., \alpha_{l+2}, \alpha_{l+1}$, где порядок определяется условиями (4), придавая значения переменным с номерами $\alpha_1, \alpha_2, ..., \alpha_l$ последовательно $g_1, g_2, ...$, а переменным с номерами $\alpha_k, \alpha_{k-1}, ..., \alpha_{l+1}$ — последовательно значения $g_\eta, g_{\eta-1}, ...$ Если дальнейшее ветвление "в глубину" не возможно (множество пустое или одноэлементное), происходит возврат на предыдущий уровень дерева ветвлений с присвоением ранее определенной переменной следующего в изложенном порядке значения.

Рассмотрим способ оценивания допустимых подмножеств решений в МВГ. Пусть при описанном способе ветвления при образовании подмножества Q множества допустимых решений задачи (1)–(3) уже определились переменные $x_{\beta_1}, x_{\beta_2}, ..., x_{\beta_t}$. Очевидно, что в силу (4) имеем:

$$c_{\beta_1} \geq c_{\beta_2} \geq ... \geq c_{\beta_t}. \tag{6}$$

Переменные, которые остались неопределенными, обозначим $\tilde{x}_1$, ..., $\tilde{x}_\tau$, где $t+\tau = k$. Нумерацию этих неопределенных переменных, не нарушая общности рассуждений, осуществим так, чтобы выполнялись следующие соотношения для коэффициентов $\tilde{c}_j$ целевой функции при переменных $\tilde{x}_j$ $\forall j \in J_\tau$:

$$\tilde{c}_1 \geq \tilde{c}_2 \geq \tilde{c}_\lambda \geq 0 > \tilde{c}_{\lambda+1} \geq ... \geq \tilde{c}_\tau. \tag{7}$$

Значения t переменных

$$x_{\beta_1} = g_{i_1}, ..., x_{\beta_t} = g_{i_t}, \tag{8}$$

которые определены согласно описанных правил ветвления при образовании подмножества Q, объединим в мультимножество $G_B = \{g_{i_1}, ..., g_{i_t}\}$. Тогда значения неопределенных переменных могут выбираться из мультимножества $\tilde{G}$, которое является разностью муль- тимножеств G и G_B: $\tilde{G} = G - G_B = \{\tilde{g}_1, ..., \tilde{g}_\chi\}$, где $\chi + t = \eta$. Пусть элементы $\tilde{G}$ пронумерованы так, что

$$\tilde{g}_1 \leq \tilde{g}_2 \leq ... \leq \tilde{g}_\chi. \tag{9}$$

Суммируя слагаемые целевой функции значениями переменных $x_{\beta_1}, ..., x_{\beta_t}$, определенные в (8), получим такое выражение:

$$\nu = \sum_{p=1}^{t} c_{\beta_p} g_{i_p}. \tag{10}$$

Как известно, число ξ в задаче минимизации функций $F(x)$ на множестве $x \in D$ в МВГ является оценкой подмножества $D_i \subset D$, если $\xi \leq F(x)$ $\forall x \in D_i$.

Теорема 1. *Оценкой ξ подмножества Q, определяемого условием* (8), *множества допустимых решений задачи* (1)–(3) *является величина*

$$\xi = \nu + c^*, \tag{11}$$

где ν вычисляется по формуле (10), *а*

$$c^* = \sum_{j=1}^{\lambda} \tilde{c}_j \tilde{g}_j + \sum_{j=1}^{\tau-\lambda} \tilde{c}_{\lambda+j} \tilde{g}_{\chi-\tau+\lambda+j} \qquad (12)$$

при условиях (7), (9).

Обозначим подмножество Q допустимых решений в МВГ для задачи (1)–(3) так:

$$D_{i_1\dots i_r}^{\beta_1\dots\beta_r} = \{x = (x_1, \dots, x_k) \in R^k | x_{\beta_j} = g_{i_j} \ \forall j \in J_r,$$

$$\forall r \in J_n, (\beta_1, \dots, \beta_r) \in E_k^r(J_k); (i_1, \dots, i_r) \in E_\eta^r(J_\eta)\},$$

где $E_k^r(J_k)$ обозначает [3] множество r-размещений без повторений из множества $J_k = \{1, 2, \dots, k\}$; β_j, i_j удовлетворяют (6), (8) при условии $r = t$. Оценку ξ этого множества, определенную по формулам (10)–(12) при условиях (6), (7), (9) обозначим $\xi_{i_1\dots i_r}^{\beta_1\dots\beta_r}$. Имеет место теорема.

Теорема 2. *Между оценками подмножеств*

$$D_{i_1\dots i_r}^{\beta_1\dots\beta_r} \quad и \quad D_{i_1\dots i_r\dots i_{r+\chi}}^{\beta_1\dots\beta_r\dots\beta_{r+\chi}}$$

справедливо соотношение: $\xi_{i_1\dots i_r}^{\beta_1\dots\beta_r} \le \xi_{i_1\dots i_{r+\chi}}^{\beta_1\dots\beta_{r+\chi}}$, *где* $r + \chi \le k$, $\forall r \in J_{k-1}$ $\forall \chi \in J_{k-1}^0 = J_{k-1} \cup \{0\}$, $(\beta_1, \dots, \beta_q) \in E_k^q(J_k)$; $q \in \{r; r + \chi\}$, $(i_1, \dots, i_q) \in E_\eta^q(J_\eta)$; *величины* $i_j \in J_\eta$ *и* $\beta_1, \dots, \beta_{r+\chi}$ *удовлетворяют условиям* (6), (8).

Доказано еще одно свойство оценки допустимых пожмножеств в МВГ, позволяющее улучшать отсечения.

В докладе приводятся доказательства этих теорем.

Список литературы

1. Емец О. А., Ольховская Е. В. Итерационный метод решения комбинаторных задач игрового типа на размещениях // Проблемы управления и информатики. — 2011. — № 3. — С. 69–78.

2. Емець О. О., Емець Ол-ра О. Розв'язування задач комбінаторноі оптимізації на нечітких множинах. Монографія. — Полтава: ПУЕТ, 2011.

3. Стоян Ю. Г., Емец О. О. Теория и методы евклидовой комбинаторной оптимизации. — К.: н-т системн. досліджень освіти, 1993.

КОМБИНАТОРНАЯ ЗАДАЧА НАХОЖДЕНИЯ МАКСИМАЛЬНОГО ПОТОКА

О. А. Емец, Е. М. Емец, Ю. Ф. Олексийчук (Полтава)

В работе рассматривается комбинаторная задача нахождения максимального потока и методы ее решения. Рассматриваемая задача является обобщением задачи нахождения максимального потока и позволяет расширить класс моделируемых задач.

Постановка задачи. Пусть транспортная сеть [1] задана графом $\Gamma = (V, U)$ с множеством вершин $V = \{v_1, v_2, \ldots, v_{|V|}\}$ и множеством дуг U. Дугу из вершины v_i у вершину v_j будем обозначать u_{ij}. Пропускная способность дуги u_{ij} равна $b_{ij} \geq 0$. Источник будем обозначать v_s, сток — v_t.

Потоком называют функцию $w : U \to R$ со следующими свойствами:

1. Значение функции w на дуге u_{ij} не может превышать пропускную способность дуги, то есть $w(u_{ij}) \leq b_{ij}$.

2. Сохранение баланса во всех вершинах, кроме стока и источника, то есть $\sum_{u_{iz} \in U} w(u_{iz}) = \sum_{u_{zj} \in U} w(u_{zj})$ $\forall z$, $z \neq s$, $z \neq t$.

Величиною потока $|w|$ будем называть суму значений функции w по исходящим из источника дугам: $\sum_{u_{si} \in U} w(u_{si}) = |w|$.

В задаче нахождения максимального потока наложим дополнительные ограничения. Пусть поток по дугам $u_{ij} \in U' \subseteq U$ может принимать значения, которые не превышают число $x_{ij} = g_l \in G$, то есть $w(u_{ij}) \leq x_{ij}$, где $G = \{g_1, g_2, ..., g_\eta\}$ — заданное мультимножество; причем вектор из x_{ij} является k-размещением из η элементов мультимножества G, то есть $x = (x_{i_1 j_1}, x_{i_2 j_2}, ..., x_{i_k j_k}) \in E^k_{\eta n}(G)$, где n — количество элементов основы [2].

Назовем эту задачу комбинаторной задачей нахождения максимального потока. Рассматриваемая задача впервые была поставлена в [3] и до этого не рассматривалась.

Математическая модель задачи. Пусть поток по дуге u_{ij}, равен y_{ij}, то есть $y_{ij} = w(u_{ij})$. Задача состоит в отыскании максимального значения функции f и соответственных значений x_{ij}, y_{ij}:

$$f = \sum_{u_{jt} \in U} y_{jt} \to \max, \tag{1}$$

при выполнении условий: сохранение баланса в вершинах

$$\sum_{u_{iz}\in U} y_{iz} = \sum_{u_{zj}\in U} y_{zj}, z \neq t, z \neq s, \tag{2}$$

ограничения на пропускную способность дуг

$$0 \leq y_{ij} \leq b_{ij} \quad \forall u_{ij} \in U, \tag{3}$$

и при дополнительных комбинаторных ограничениях

$$y_{ij} \leq x_{ij} \quad \forall u_{ij} \in U, \tag{4}$$

$$x = (x_{i_1 j_1}, x_{i_2 j_2}, \ldots, x_{i_k j_k}) \in E^k_{\eta n}(G). \tag{5}$$

Задача (1)–(5) является частным случаем линейной задачи евклидовой частично комбинаторной оптимизации на размещениях [2].

Методы решения. Известны методы решения евклидовых комбинаторных задач на размещениях (см. например, [2–5]), которые применимы для решения комбинаторной задачи нахождения максимального потока [3]. Справедлива теорема.

Теорема. *Комбинаторная задача нахождения максимального потока является NP-трудной.*

Учитывая NP-трудность задачи, актуальной является разработка приближенных методов. В [6] предложен "жадный" алгоритм для решения задачи. Идея метода состоит в том, что на каждом этапе находится самый короткий путь из источника в сток (если таких путей несколько, то выбирается путь с максимальной пропускной способностью без учета комбинаторных ограничений). Затем x_{ij} с найденного пути принимают значения, которые максимизируют допустимый поток по этому пути. После этого находится остаточная сеть и т. д. Справедливо такое утверждение.

Теорема. *Время работы жадного алгоритма для комбинаторной задачи нахождения максимального потока* $T(n) = O(|U|n|w^*|)$, *где* $|U|$ *— количество дуг в графе,* n *—количество разных элементов в мультимножестве* G, $|w^*|$ *— искомая величина максимального потока.*

Рассмотрим применение метода ветвей и границ для решения задачи. Пронумеруем дуги, на которые наложены комбинаторные ограничения: u_1, u_2, …, u_k. Как начальное рекордное значение можно взять решение, полученное некоторым приближенным методом, например жадным алгоритмом. Начальным етапом будем считать

классическую задачу нахождения максимального потока (без комбинаторных ограничений), начальной оценкой — ее решение.

Ветвление делается так: для u_i полагаем x_i равным всем доступным значениям из G (по порядку). Оценкой будет решение классической задачи с пропускними способностями $b^*_{ij} = \min(b_{ij}, x_{ij})$. Если оценка больше рекордного значения, продолжаем ветвление, иначе — отсекаем вершину (очевидно, что добавление дополнительных ограничений не может увеличить максимальный поток). Изменяя $i = 1, 2, \ldots, k$ и используя поиск в глубину находим решение задачи.

Список литературы

1. Форд Л. Р., Фалкерсон Д. Р. Потоки в сетях. — М.: Мир, 1966.

2. Стоян Ю. Г., Емец О. О. Теория и методы евклидовой комбинаторной оптимизации. — К.: СДО, 1993. — 188 с.

3. Емець О. О., Емець Е. М., Олексійчук Ю. Ф. Знаходження максимального потоку в мережі з додатковими комбінаторними обмеженнями // Таврический вестник информатики и математики. — 2011. — № 1. — С. 43–50.

4. Емец О. А., Емец Е. М., Олексийчук Ю. Ф. Прямой метод отсечений для задач комбинаторной оптимизации с дополнительными ограничениями // Кибернетика и системный анализ. — 2011. — № 6. — С. 116–124.

5. Барболина Т. Н., Емец О. А. Полностью целочисельный метод отсечения для решения линейных условных задач оптимизации на размещениях // Журн. вычисл. математики и матем. физики. — 2005. — Т. 45, № 2. — С. 254–261.

6. Емец О. А., Емец Е. М., Олексийчук Ю. Ф. Методы решения задачи нахождения максимального потока с дополнительными комбинаторными ограничениями // Материалы 3-й международной конференции "Математическое моделирование, оптимизация и информационные технологии" (Кишинев, 19–23 марта 2012 г.). — Кишинев: Эврика, 2012. — С. 333–337.

H-ПЕРИМЕТР И L-ОКРУЖЕНИЕ МАТРОИДА

А. Н. Исаченко, Я. А. Исаченко (Минск)

Аксиоматизация матроида может проводиться на основе различных понятий: независимого множества, базиса, цикла, функции ранга, остовного множества, оператора замыкания, плоскости, гиперплоскости, циклического множества. Учитывая двойственные соотношения, матроид можно определить также в терминах конезависимых множеств, кобазисов, коциклов и т. д. Свойства указанных понятий матроида приведены в работах [1–3].

В настоящем сообщении вводятся два новых двойственных понятия для матроида (H-периметр и L-окружение) и приводится аксиоматизация матроида на их основе. Даются определения, соответствующих этим понятиям оракулов, и результаты о полиномиальной сводимости к ним других оракулов.

Пусть (S, F) матроид на множестве S с семейством независимых множеств F. H-периметром матроида (S, F) назовем функцию $\gamma_H : 2^S \to \{0, ..., |S|\}$ со значениями $\gamma_H(A) = \max\{|C| : C \subseteq A, C - \text{цикл}\}$, если A зависимое множество, и $\gamma(A) = 0$, если $A \in F$.

Теорема 1. (*Аксиомы H-периметра*). *Функция $\gamma_H : 2^S \to \{0, ..., |S|\}$ является функцией H-периметра некоторого матроида (S, F) тогда и только тогда, когда для нее выполняются условия:*

H1) *если $\gamma_H(X) > 0$, то существует множество $Y \subseteq X$, для которого $\gamma_H(X) = \gamma_H(Y) = |Y|$;*

H2) *если $X \supseteq Y$, то $\gamma_H(X) \geq \gamma_H(Y)$;*

H3) *если $\gamma_H(X) = |X|$, то $\gamma_H(X \backslash x) = 0$ для любого $x \in X$;*

H4) *если $\gamma_H(X) = |X|$, $\gamma_H(Y) = |Y|$, $X \neq Y$, $x \in X \cap Y$, то $\gamma_H((X \cup Y) \backslash x) > 0$.*

Доказательство. Необходимость. Пусть (S, F) матроид и функция $\gamma_H : 2^S \to \{0, ..., |S|\}$ является его H-периметром. Выполнение условия H1) следует непосредственно из определения функции γ_H. Рассмотрим условие H2). Предположим, что $X \supseteq Y$. Пусть C – цикл матроида (S, F), причем $C \subseteq Y$ и $\gamma_H(Y) = |C|$. Получим $X \supseteq Y \supseteq C$, следовательно, $\gamma_H(X) \geq |C| = \gamma_H(Y)$.

Равенство $\gamma_H(X) = |X|$ означает, что X является циклом матроида (S, F). Следовательно, $X \backslash x \in F$ для любого $x \in X$, что влечет $\gamma_H(X \backslash x) = 0$.

Если $\gamma_H(X) = |X|$, $\gamma_H(Y) = |Y|$, то X и Y являются циклами матроида (S, F). Следовательно, по аксиомам циклов при

$X \neq Y$, $x \in X \cap Y$, существует цикл C такой, что $C \subseteq (X \cup Y)\backslash x$. То есть $\gamma_H((X \cup Y)\backslash x) \geq |C| > 0$.

Достаточность. Пусть S – конечное множество, а $\gamma_H : 2^S \to \to \{0, ..., |S|\}$ функция, удовлетворяющая условиям H1)–H4). Определим семейство подмножеств $\vartheta = \{X | X \in 2^S,\ \gamma_H(X) = |X|\}$ множества S. Пусть $X \in \vartheta$. Возьмем любое непустое собственное подмножество Y множества X и предположим, что $Y \in \vartheta$. Тогда $\gamma_H(Y) = |Y|$ и $Y \subseteq X\backslash x$ для некоторого $x \in X$. По условию H2) получим $\gamma_H(X\backslash x) \geq \gamma_H(Y) = |Y| > 0$, что противоречит условию H3). Таким образом,

C1) если X, Y различные подмножества из ϑ, то Y не является подмножеством X.

Выполнение условия H4) означает, что

C2) если $X, Y \in \vartheta$ и $x \in X \cap Y$, то существует $Z \in \vartheta$ такое, что $Z \subseteq (X \cup Y)\backslash x$.

Условия C1), C2) являются аксиомами циклов матроида. Следовательно, ϑ является множеством циклов некоторого матроида (S, F), что и доказывает достаточность.

L-окружением матроида (S, F) назовем функцию $\varphi_L : 2^S \to \to \{1, ..., |S|, \infty\}$, задаваемую равенствами $\varphi_L(A) = \min\{|L| : A \subseteq L,\ L$ — гиперплоскость$\}$, если ранг A меньше ранга S, и $\varphi_L(A) = \infty$, в противном случае. По аналогии с теоремой 1, на основании аксиом гиперплоскостей получим справедливость следующего утверждения.

Теорема 2. *Функция $\varphi_L : 2^S \to \{1, ..., |S|, \infty\}$ является L-окружением некоторого матроида (S, F) тогда и только тогда, когда для нее выполняются условия:*

L1) *если $\varphi_L(X) < \infty$, то существует множество $Y \supseteq X$, для которого $\varphi_L(X) = \varphi_L(Y) = |Y|$;*

L2) *если $X \supseteq Y$, то $\varphi_L(X) \leq \varphi_L(Y)$;*

L3) *если $\varphi_L(X) = |X| < \infty$, то $\varphi_L(X \cup x) = \infty$ для любого $x \in S\backslash X$;*

L4) *если $\varphi_L(X) = |X|$, $\varphi_L(Y) = |Y|$, $X \neq Y$, $x \in X \cup Y$, то $\varphi_L((X \cap Y) \cup x) < \infty$.*

Определим функцию L-периметра матроида (S, F) как функцию $\gamma_L : 2^S \to \{0, ..., |S|\}$ со значениями $\gamma_L(A) = \min\{|C| : C \subseteq A,\ C$ — цикл$\}$, если A зависимое множество, и $\gamma_L(A) = 0$, если $A \in F$. Аксиомы L-периметра получим, заменив в теореме 1 знак нестрогого неравенства на противоположный знак нестрогого неравенства в условии H2).

H-окружением матроида назовем функцию $\varphi_H : 2^S \to \{1, ..., |S|, \infty\}$, определяемую равенствами $\varphi_H(A) = \max\{|H| : A \subseteq H,\ H$ — гиперплоскость$\}$, если ранг A меньше ранга S, и $\varphi(A) = \infty$, в противном случае. Заменяя в теореме 2, в условии L2), нестрогое неравенство на противоположное нестрогое неравенство, получим аксиомы функции φ_H.

H-периметр, L-периметр, H-окружение и L-окружение двойственного к (S, F) матроида (S, F^*) назовем соответственно H-кориметром, L-кориметром, H-коокружением, L-коокружением и обозначим γ_H^*, γ_L^*, φ_H^*, φ_L^*. Получим для любого $X \notin F$

$\gamma_H(X) = |S| - \varphi_L^*(S \setminus X)$, $\gamma_L(X) = |S| - \varphi_H^*(S \setminus X)$,

если $\rho(X) < \rho(S)$, то

$\varphi_H(X) = |S| - \gamma_L^*(S \setminus X)$, $\varphi_L(X) = |S| - \gamma_H^*(S \setminus X)$.

Для каждого из приведенных понятий можно определить соответствующий оракул u как инъективное отображение $W_u : (2^S, \mu(S)) \to E(u)$. Здесь $\mu(S)$ — совокупность всех матроидов на множестве S, $E(u) = \{0, ..., |S|\}$ для H-периметра, H-кориметра, L-периметра, L-кориметра, $E(u) = \{1, ..., |S|, \infty\}$ для H-окружения, H-коокружения, L-окружения, L-коокружения. Для оракулов, приведенных в работах [2,3], имеет место следующая теорема.

Теорема 3. *Оракулы "независимое", "конезависимое", "базис", "кобазис", "цикл", "коцикл", "ранг", "коранг", "остовное", "коостовное", "замыкание", "козамыкание", "плоскость", "коплоскость", "гиперплоскость", "когиперплоскость", "циклическое", "коциклическое" полиномиально сводимы к оракулу "H-периметр" и оракулу "L-окружение".*

Список литературы

1. Welch D. J. Matroid Theory. — London: Academic Press., 1976.

2. Исаченко А. Н. Полиномиальная сводимость матроидных оракулов // Известия АН БССР. Сер. физ.-мат. наук. — 1984. — Вып. 6. — С. 33–36.

3. Исаченко А. Н., Ревякин А. М. О сводимости матроидных оракулов // Вестник МГАДА. Сер.: Философские, социальные и естественные науки. — 2011. — Вып. 3. — С. 117–127.

БАЗОВО УПОРЯДОЧЕННЫЕ МАТРОИДЫ

А. Н. Исаченко (Минск), А. М. Ревякин (Москва)

Используются терминология и обозначения работ [1–5]. Пусть $P(S)$ — множество всех подмножеств конечного множества S. Система $\mathcal{I} \subseteq P(S)$ подмножеств из S называется матроидом $M = (S, \mathcal{I})$, а множества из $\mathcal{I}$ — независимыми, если выполняются следующие условия: (i1) $\varnothing \in \mathcal{I}$; (i2) если $A \subseteq B$ и $B \in \mathcal{I}$, то $A \in \mathcal{I}$; (i3) если $A, B \in \mathcal{I}$ и $|A| > |B|$, то найдется $a \in A \setminus B$ такое, что $B \cup \{a\} \in \mathcal{I}$.

Максимальное по включению множество в $\mathcal{I}$ называется базой матроида M.

Пара $M = (S, \mathcal{B})$, где $\mathcal{B}$ – семейство подмножеств (баз) из S, образует матроид, если: (b1) никакое собственное подмножество базы не является базой; (b2) если $B_1, B_2 \in \mathcal{B}$ и $x \in B_1$, то $(B_1 \setminus \{x\}) \bigcup \{y\} \in \mathcal{B}$ для некоторого $y \in B_2$. При этом подмножество $A \in \mathcal{I}(M)$, если найдется $B \in \mathcal{B}$ такое, что $A \subseteq B$.

Матроид M на множестве S называется базово упорядоченным, если для любых двух баз B_1, B_2 матроида M существует такая биекция $\pi : B_1 \to B_2$, что для любого $x \in B_1$ как $(B_1 \setminus \{x\}) \cup \{\pi(x)\}$, так и $(B_2 \setminus \{\pi(x)\}) \cup \{x\}$ являются базами матроида M. Скажем, что матроид M является строго базово упорядоченным, если для любых двух баз B_1, B_2 матроида M существует такая биекция $\pi : B_1 \to B_2$, что для всех подмножеств $A \subseteq B_1$ множество $(B_1 \setminus A) \cup \pi(A)$ является базой матроида M. Легко показать, что для любого такого π множество $(B_2 \setminus \pi(A)) \cup A$ также является базой матроида M. Очевидно, что если M является строго базово упорядоченным, то он — базово упорядоченный. Но обратное утверждение неверно.

Приведём ряд результатов для базово упорядоченных и строго базово упорядоченных матроидов.

Класс базово упорядоченных и класс строго базово упорядоченных матроидов замкнуты относительно объединения, взятия миноров и перехода к двойственным матроидам.

Трансверсальные матроиды и гаммоиды [6–8] являются строго базово упорядоченными матроидами.

Циклический матроид $M(K_4)$ полного графа K_4 является базово упорядоченным.

Матроид M на 9-элементном множестве называется папповым, если он изоморфен конфигурации Паппа. Очевидно, матроид Дезарга является регулярным. Если в матроиде Паппа одну прямую

заменить тремя тривиальными прямыми, то получим так называемый непаппов матроид, который не представим ни над каким полем. Непаппов матроид [1] является базово упорядоченным матроидом, но не является гаммоидом.

Нетрудно проверить, что матроид Фано не является базово упорядоченным.

Пусть M — матроид на множестве S, $x \in S$ и $y \notin S$. Последовательным расширением матроида M на x, y называется матроид $sM(x,y)$ на множестве $S \bigcup y$, базами которого являются множества вида $B \bigcup y$, если B – база матроида M, или $B \bigcup x$, если B — база матроида M и $x \notin B$. Аналогично, параллельным расширением матроида M называется матроид $pM(x,y)$ на множестве $S \bigcup y$, базами которого являются базы матроида M или множества вида $(B \backslash x) \bigcup y$, если $x \in B$, где B — база матроида M. Можно доказать, что $(sM(x,y))^* = pM^*(x,y)$. Последовательно-параллельным расширением матроида M называется матроид N, который может быть получен из M с помощью серии последовательных и параллельных расширений.

Последовательно-параллельным расширением гаммоида (соответственно, базово упорядовенного матроида) является гаммоид (соответственно, базово упорядоченный матроид).

Последовательно-параллельным матроидом называется матроид, который может быть получен с помощью последовательных и параллельных расширений из одноэлементного матроида. Последовательно-параллельный матроид всегда является циклическим матроидом некоторого планарного графа. Таким образом, последовательно-параллельный матроид не более, чем циклический матроид некоторой последовательно-параллельной сети. Поэтому для графа, определяющего сеть, и циклического матроида этого графа используется одно и то же название последовательно-параллельная сеть [1].

Дается новое доказательство эквивалентности ряда утверждений для бинарных матроидов.

Теорема. *Пусть M — бинарный матроид. Тогда эквивалетны утверждения* : 1) M — *гаммоид*; 2) M —*базово упорядоченный матроид*; 3) M — *последовательно-параллельная сеть*; 4) M *не содержит в качестве минора циклического матроида $M(K_4)$ полного графа K_4. Более того, каждый бинарный базов о упорядоченный матроид является строго базово упорядоченным.*

Пусть A — множество всех базово упорядоченных матроидов, B — матроиды, представимые над полем действительных чисел,

C — строго базово упорядоченные матроиды, D — гаммоиды, E — строгие гаммоиды, F — трансверсальные матроиды и G — фундаментальные трансверсальные матроиды. Тогда: $D \subset C \bigcap B \subset A \bigcap B$, $C \subset A$, $B \backslash A \neq \emptyset$ [7]; циклический матроид $M(K_4)$ полного графа на 4 вершинах принадлежит множествам $A \backslash C$ и $A \backslash B$; $E \bigcup F \subset D$, $G \subset E \bigcap F$; циклический матроид $M(K_{3,2}) \in E \backslash F$; M — строгий гаммоид [6] тогда и только тогда, когда двойственный ему M^* является трансверсальным матроидом.

В сообщении также обсуждаются вопросы сводимости матроидных оракулов [9].

Список литературы

1. Welsh D. J. A. Matroid theory. — London: Acad. Press, 1976.
2. Recski A. Matroid theory and its applications in electric network theory and in statics. — Budapest: Akad. Kiado, 1989.
3. Oxley J. G. Matroid theory. — N.Y.: Oxford University Press, 1992 и 2006.
4. Revyakin A. M. Matroids // J. Math. Sci. — 2002. — V. 108, № 1. — С. 71–130.
5. Ревякин А. М. Матроиды: криптоморфные системы аксиом и жесткость ферм // Вестник МГАДА. Серия "Философские, социальные и естественные науки". Вып. 5. — М.: МГАДА, 2010. — С. 96–106.
6. Ingleton A. W., Piff M. J. Gammoids and transversal matroids // J. Combin. Theory. — 1973. — B15, № 1. — P. 51–68.
7. Ingleton A. W. Transversal matroids and related structures // Higher Combinatorics. — Dordrecht, Boston, 1977. — С. 117–131.
8. Mason J. H. Matroids as the study of geometrical configurations // Higher Combinatorics. — Dordrecht, Boston, 1977. — С. 133–176.
9. Исаченко А. Н., Ревякин А. М. О сводимости матроидных оракулов // Вестник МГАДА. Сер. "Философские, социальные и естественные науки". — 2011. — Вып. 3. — С. 117–127.

ЭКВИВАЛЕНТНОСТЬ ПРАВИЛ МЭЗОНА ДЛЯ ПЕРЕДАТОЧНОЙ ФУНКЦИИ В ГРАФЕ СИГНАЛЬНЫХ ПОТОКОВ ОСНОВНОЙ ФОРМУЛЕ МЕТОДА ТРАНСФЕР-МАТРИЦЫ

Л. М. Коганов (Москва)

1. Графы сигнальных потоков (сигнальные графы) интенсивно используются как адекватные математические модели в теории автоматического регулирования [1, гл. 2, с. 90–157], теоретической электротехнике [2, гл. 2, разд. 2.5, с. 41, Приложения Б и В на с. 161–164], теории свёрточных кодов [3, с. 230–234, 238–244, 277–290] и в ряде других областей точного знания [4, с. 155–169, 188–198]. При этом основополагающими правилами для расчёта передаточной функции (коротко — передачи) между двумя узлами (вершинами, состояниями) сигнального графа: отдельно в виде *определителя графа* — для знаменателя, и отдельно для алгебраического дополнения (минора с точностью до знака), соответствующего двум выделенным полюсам, являются *правила Мэзона* (Мейсона в другой транскрипции) [5, гл.4, с. 117–122, 125–126; 2, с. 141, 161–162].

Мы показываем, что граф переходов, построенный по нагруженной матрице смежностей (weighted adjacency matrix), может трактоваться как сигнальный граф. Это же касается стандартно и однозначно объемлющего этот граф двухполюсника [6, 7]. А передача между полюсами является естественным обобщением производящей функции путей по перечисляющему параметру — длине пути (числу пройденных дуг с учётом кратности). Передача, напомним, есть сумма произведений нагрузок вдоль всех путей.

На это обстоятельство, но без дальнейших приложений в *перечислительной комбинаторике*, было, по-видимому, впервые указано Эндрю Витерби (Andrew Viterbi) в [8, p. 755]. Там в первом абзаце второй колонки справа Витерби прямо пишет: "Now we may evaluate the generating function of all path merging with all zeros at the j-th node level simply by evaluating the generating functions of all the weights of the output sequences of the finite-state machine". И, далее, в подстрочном примечании добавляет, что: "Alternatively, this can be regarded as a transfer-function of the diagram as a signal flow graph". (Мы намеренно даём извлечение из этой ставшей в теории свёрточных кодов классической работы без перевода — Л. К.).

Автору на это обстоятельство впервые указал Л. Н. Бондаренко (кафедра дискретной математики Пензенского ГУ) в дискуссиях

по докладам автора [7, 9]. При этом Л. Н. Бондаренко сразу отметил многообразие возможностей упрощения по Мэзону с помощью стандартных операций [5, гл.4] исходного графа переходов и объемлющего двухполюсника. Затем автором [9], была добавлена достаточно унифицирующая *операция слияния когерентных состояний*, резко упрощающая исходный граф, либо, шире, объемлющий стандартный двухполюсник.

2. В настоящей работе мы показываем, что правила Мэзона в совокупности доставляют центральную формулу теории трансферматрицы [10, часть I, разд. 4.7, теорема 4.7.2, формула (34)]. Доказательство основано на ряде известных фактов из теории определителей [11, разд. 34 на с. 53], [12, (любое издание, начиная с 11-го), задачи № 330 и № 227] и понятии полуразбиения, введенного на конечном множестве [13]. Полуразбиение (разбиение на блоки непустого подмножества вершин-узлов) совместимо (compatible) с графом, если орграфы, индуцированные на блоках полуразбиения, суть все без исключения *простые несамопересекающиеся контуры графа*, приходящиеся в точности по одному на каждый блок. Одно из правил Мэзона — для числителя — естественно интерпретируется при разрыве одного из контуров при удалении дуги, соединяющей полюсы. Правила знаков для чётностей индуцированных подстановок в случаях обоих правил Мэзона стандартны с учётом разложения цикла в прямое произведение транспозиций, число которых на единицу меньше длины цикла.

3. Отметим в заключение, что понятие полуразбиения, правда, с исключительно двухэлементными блоками, находит кроме вышеуказанного, применение в комбинаторике свободных конечнопорождённых групп, связанной с некоммутативным обобщением [14] так называемой *циклической леммы* [15].

Автор благодарит Л. Н. Бондаренко за стимулирующую, проясняющую суть дела переписку. Именно в письме автора к Л. Н. Бондаренко от 25.04.2010 были проведены рассуждения, доставляющие вышеуказанную эквивалентность.

Список литературы

1. Тракселл Дж. Синтез систем автоматического регулирования. — М.: Машгиз, 1959.

2. Абрахамс Дж., Каверли Дж. Анализ электрических цепей методом графов. — М.: Мир, 1967.

3. Витерби А. Д., Омура Дж. К. Принципы цифровой связи и кодирования. — М.: Радио и связь, 1982.

4. Волькенштейн М. В. Физика ферментов. — М.: Наука, 1967.

5. Мэзон С., Циммерман Г. Электронные цепи, сигналы и системы. — М.: ИЛ, 1963.

6. Коганов Л. М. Передаточная функция в перечислительной комбинаторике (часть I). // Вестник Московского городского педагогического университета. Сер. “Информатика и информатизация образования”. — 2008. — № 1 (12). — С. 30–39.

7. Коганов Л. М. Развитие метода трансфер-матрицы в перечислительной комбинаторике // Дискретные модели в теории управляющих систем: VIII Международная конференция (Москва, 6–9 апреля 2009 г.). Труды. — М: Издательский отдел факультета ВМиК МГУ им. М. В. Ломоносова; МАКС Пресс, 2009. — с. 130–131.

8. Viterbi A. J. Convolutional codes and their performance in communication systems // IEEE Transactions on communications technology. — 1971. — V. COM-19, № 5. — P. 751–772.

9. Коганов Л. М. Развитие метода трансфер-матрицы в перечислительной комбинаторике. III: Операция слияния когерентных состояний // Материалы X Международного семинара “Дискретная математика и её приложения” (Москва, МГУ, 1–6 февраля 2010). — С. 236–239.

10. Стенли Р. Перечислительная комбинаторика (часть I-я). — М.: Мир, 1990.

11. Нетто Е. Начала теории определителей. — Одесса: Mathesis, 1912.

12. Фаддеев Д. К., Соминский И. С. Задачи по высшей алгебре. — СПб: Лань, 2001 г.

13. Коганов Л. М. Использование одного комбинаторного тождества при перечислении комбинаций, инвариантных относительно подстановки // Časopis pro pěstováni matematiky. — 1987. — V. 12, № 1. — P. 58–65.

14. Armstrong C., Mingo J. A., Speicher R., Wilson J. C. H. The noncommutative cycle lemma // J. Combin. Theory. Series A. — 2010. — A117. — P. 1158–1166.

15. Dershowitz N., Zaks S. The cycle lemma and some applications // European J. of Combinatorics. — 1990. — V. 11, № 1. — P. 35–40.

ПРОИЗВОДЯЩИЕ ФУНКЦИИ В ЗАДАЧЕ О РАНЦЕ

В. К. Леонтьев (Москва)

Рассмотрим стандартную задачу о ранце с булевыми переменными

$$\begin{aligned} &\sum_{j=1}^{n} c_j x_j \to \max, \\ &\sum_{j=1}^{n} a_j x_j \le b, \\ &x_j \in \{0,1\}. \end{aligned} \tag{1}$$

Мы предполагаем, что все параметры задачи — натуральные числа. Целочисленный многогранник задачи (1) — это множество $V_b(a_1,\ldots,a_n)$ $(0,1)$-решений следующего неравенства

$$\sum_{j=1}^{n} a_j x_j \le b. \tag{2}$$

С множеством $V_b(a_1,\ldots,a_n)$ свяжем следующую производящую функцию

$$P_b(z_1,\ldots,z_n) = \sum_{\substack{\{x_1,\ldots,x_n\} \\ \sum_{j=1}^{n} a_j x_j \le b}} z_1^{a_1 x_1}\ldots z_n^{a_n x_n}.$$

Лемма 1. *Справедлива формула*

$$\sum_{r=0}^{\infty} P_r(z_1,\ldots,z_n)u^r = \frac{(1+(z_1u)^{a_1})\ldots(1+(z_nu)^{a_n})}{1-u}\,.$$

Через V_b мы обозначим число $(0,1)$-решений неравенства (2).

Следствие 1. *Имеет место формула*

$$V_b = \frac{1}{2\pi i}\oint\limits_{|u|=\rho} \frac{(1+u^{a_1})\ldots(1+u^{a_n})}{u^{b+1}(1-u)}\,du,$$

где $\rho < 1$.

Следующая производящая функция характеризует распределение значений функционала

$$f(x_1, \ldots, x_n) = \sum_{j=1}^{n} c_j x_j$$

на многограннике $V_b(a_1, \ldots, a_n)$:

$$F_b(z_1, \ldots, z_n) = \sum_{\sum_{j=1}^{n} a_j x_j \le b} z_1^{c_1 x_1} \ldots z_n^{c_n x_n}.$$

Лемма 2. *Справедлива формула*

$$\sum_{r=0}^{\infty} F_r(z_1, \ldots, z_n) u^r = \frac{(1 + z_1^{c_1} u^{a_1})(1 + z_2^{c_2} u^{a_2}) \ldots (1 + z_n^{c_n} u^{a_n})}{1 - u}.$$

Пусть $\Phi_b(z) = F_b(z, \ldots, z)$.

Следствие 2. *Имеет место формула*

$$\Phi_b(z) = \frac{1}{2\pi i} \oint\limits_{|u|=\rho} \frac{(1 + z^{c_1} u^{a_1}) \ldots (1 + z^{c_n} u^{a_n})}{u^{b+1}(1 - u)}\, du,$$

где $\rho < 1$.

Ясно, что $\Phi_b(1) = V_b$ — объем многогранника (2).

Для полинома $\Phi_b(z)$ справедливо представление

$$\Phi_b(z) = \sum_{k=0}^{\infty} A_k z^k,$$

где A_k — число точек многогранника $V_b(a_1, \ldots, a_n)$, имеющих значения целевой функции $f(x_1, \ldots, x_n)$ равное k. Ясно, что

$$\max_{V_b} f(x_1, \ldots, x_n) = \max_k \{k : A_k \ge 1\}.$$

Если рассмотреть равномерное распределение на множестве $V_b(a_1, \ldots, a_n)$ и производящую функцию $P(z)$ распределения значений f, то ясно, что

$$P(z) = \frac{\Phi_b(z)}{\Phi_b(1)}.$$

Для "среднего" значения $\bar{f}(V_b)$ целевой функции $f(x_1, \ldots, x_n)$ на $V_b(a_1, \ldots, a_n)$ справедливо следующее выражение.

Лемма 3. *Имеет место формула*

$$\bar{f}(V_b) = \sum_{k=1}^{n} c_k \left(1 - \frac{V_k(b)}{V_b}\right),$$

где $V_k(b)$ — это объем проекции $V_b(a_1, \ldots, a_n)$, т. е. число $(0,1)$-решений неравенства

$$\sum_{j \neq k} a_j x_j \leq b.$$

Следствие 3. *Справедливо неравенство*

$$\max f(x_1, \ldots x_n) \geq \sum_{k=1}^{n} c_k - \sum_{k=1}^{n} c_k \frac{V_k(b)}{V_b}.$$

Работа выполнена при финансовой поддержке РФФИ, проект 11–01–00398.

Список литературы

1. Сигал И. Х., Иванова А. П. Введение в прикладное дискретное программирование — М.: Физматлит, 2002.

2. Кузюрин Н. Н., Фомин С. В. Эффективные алгоритмы и сложность вычислений — М.: МФТИ, 2007.

ПРОСТЫЕ РЕШЕТОЧНЫЕ МАТРИЦЫ НАД ДИСТРИБУТИВНЫМИ РЕШЕТКАМИ

В. Е. Маренич (Москва)

Пусть $(P, \wedge, \vee, \leq)$ — дистрибутивная решетка с нулем $\widetilde{0}$ и единицей $\widetilde{1}$. Матрица A называется *простой* над решеткой P, если она не обратима и из равенства $A = BC$, где $B, C \in P^{n \times n}$, следует, что B или C — обратимая матрица.

В работах [3], [4] установлены факты: доказано, что не существует простых матриц порядка 2; доказано существование простых матриц над конечными дистрибутивными решетками; найдены условия существования простых $n \times n$ матриц, где $n \geq 3$; рассмотрены свойства простых матриц.

Рассмотрим простые матрицы над решетками, которые не обязательно конечны.

Простые матрицы над цепями. Пусть $(P, \wedge, \vee, \leq)$ — цепь с нулем $\widetilde{0}$ и единицей $\widetilde{1}$.

Теорема 1. *Если простая матрица $A \in P^{n\times n}$, то справедливо одно из следующих утверждений.*

i) Матрица A вполне неразложимая.

ii) Матрица A перестановочно эквивалентна блочной матрице,

$$\begin{pmatrix} B_{11} & 0_{t\times s} \\ 0_{s\times t} & E_{s\times s} \end{pmatrix} = B_{11} \oplus E_{s\times s},$$

где B_{11} — вполне неразложимая простая $t \times t$ матрица, числа $1 \leq s,\ t \leq n-1$, $s+t=n$.

Теорема 2. *Пусть $1 \leq\ t \leq n$. Если простая матрица $B \in P^{t\times t}$, то прямая сумма $B \oplus E_{(n-t)\times(n-t)}$ — простая $n \times n$ матрица.*

Теорема 3. *Каждая строка и каждый столбец простой матрицы $A \in P^{n\times n}$ содержит нуль $\widetilde{0}$ и единицу $\widetilde{1}$.*

Теорема 4. *Справедливы утверждения.*

i) Каждая матрица вида

$$\begin{pmatrix} \widetilde{0} & * & * \\ * & \widetilde{0} & * \\ * & * & \widetilde{0} \end{pmatrix}, \tag{1}$$

где на помеченных местах расположены элементы не равные нулю так, что каждая строка и каждый столбец матрицы (1) *содержит единицу $\widetilde{1}$, является простой.*

ii) Каждая простая 3×3 матрица подстановочно эквивалентна одной из матриц вида (1).

Следствие 1. *Перманенты простых матриц над цепями могут принимать любые ненулевые значения.*

Простые матрицы над прямым произведением решеток. Пусть решетка $(L, \wedge, \vee, \leq)$ есть прямое произведение дистрибутивных решеток $(P_z, \vee, \wedge, \leq)$ с нулем $\widetilde{0}$ и единицей $\widetilde{1}$, где индекс $z \in I$.

Теорема 5. *Пусть матрица $A \in P^{n\times n}$. Следующие утверждения равносильны.*

i) Матрица A является простой над решеткой P.

ii) Существует индекс $w \in I$ такой, что проекция $pr_w(A)$ является простой матрицей над решеткой P_w, а для любого индекса

$u \neq w$ проекция $pr_u(A)$ является обратимой матрицей над решеткой P_u.

Простые матрицы над булеаном. Пусть U — непустое множество, $\widetilde{0} = \emptyset$, $\widetilde{1} = U$. Булеан $Bul(U)$ есть прямое произведение двухэлементных цепей,

$$Bul(U) \cong \times \prod_{z \in U} [\emptyset, \{z\}]_{\subseteq},$$

где $[\emptyset, \{z\}]_{\subseteq}$ — двухэлементная цепь.

Теорема 6. *Пусть число $n \geq 3$. Тогда простыми $n \times n$ матрицами над булеаном $Bul(U)$ являются только матрицы вида*

$$\{u\}B + \sum_{z \in U - \{u\}} \{z\}M(\pi_z), \quad (1)$$

где элемент $u \in U$, B — некоторая простая матрица размера $n \times n$, $M(\pi_z)$ — некоторая подстановочная матрица размера $n \times n$ над двухэлементной решеткой $\{\widetilde{0}, \widetilde{1}\}$.

Следствие 1. *Каждая простая матрица над булеаном есть линейная комбинация подстановочных матриц.*

Следствие 2. *Перманент каждой простой матрицы над булеаном $Bul(U)$ равен единице $\widetilde{1} = U$.*

Пример 1. Пусть U — непустое множество, элемент $u \in U$. Матрица

$$A = \begin{pmatrix} U - \{u\} & \{u\} & \{u\} \\ \{u\} & U - \{u\} & \{u\} \\ \{u\} & \{u\} & U - \{u\} \end{pmatrix}$$

— простая матрица над булеаном $Bul(U)$. Матрица A не содержит нулей и единиц булеана $Bul(U)$.

Простые матрицы над булевыми решетками. Пусть $(P, \wedge, \vee, \leq)$ — булева решетка с нулем $\widetilde{0}$ и единицей $\widetilde{1}$. Обозначим $Lbul(A)$ конечную булеву подрешетку решетки P, порожденную элементами матрицы $A \in P^{n \times n}$.

Теорема 7. *Пусть матрица $A \in P^{n \times n}$. Следующие утверждения равносильны.*

i) Матрица A проста над решеткой P.

ii) Матрица A проста над любой конечной булевой подрешеткой Q решетки P, содержащей подрешетку $Lbul(A)$.

Следствие 1. *Перманент каждой простой матрицы над булевой решеткой P равен единице $\widetilde{1}$.*

Рассмотрим матрицы $SM(n)$, $SM(x,n)$, $n \geq 3$, где x — атом решетки P,

$$SM(n) = \begin{pmatrix} \widetilde{0} & \dots & \widetilde{0} & \widetilde{1} & \widetilde{1} \\ \widetilde{0} & \dots & \widetilde{1} & \widetilde{0} & \widetilde{1} \\ \dots & \dots & \dots & & \\ \widetilde{1} & \dots & \widetilde{0} & \widetilde{0} & \widetilde{1} \\ \widetilde{1} & \dots & \widetilde{1} & \widetilde{1} & \widetilde{0} \end{pmatrix},$$

$$SM(x,n) = \begin{pmatrix} \bar{x} & \dots & \widetilde{0} & x & x \\ \widetilde{0} & \dots & x & \widetilde{0} & x \\ \dots & \dots & \dots & & \\ x & \dots & \widetilde{0} & \bar{x} & x \\ x & \dots & x & x & \bar{x} \end{pmatrix}.$$

Если $n \geq 3$, то $SM(x,n)$ — простая матрица над решеткой P.

Теорема 8. *Пусть булева решетка P содержит хотя бы один атом. Тогда над решеткой P существуют простые $n \times n$ матрицы, для всех $n \geq 3$.*

Список литературы

1. Kim K. X. Boolean matrix theory and applications — New York: Marcel Dekker, 1982.

2. Сачков В. Н., Тараканов В. Е. Комбинаторика неотрицательных матриц. — Москва: научное издательство "ТВП", 2000.

3. Маренич В. Е. Простые матрицы над дистрибутивными решётками // Фундаментальная и прикладная математика. — 2008. — Т. 14, № 7. — с. 157–173.

4. Marenich V. E. Prime lattice matrices over distributive lattices // Journal of mathematical Sciences. — 2010. — V. 164, № 2. — P. 260–271.

ТЕОРЕМА ФРОБЕНИУСА ДЛЯ ПОЛУГРУППЫ МАТРИЦ НАД ДИСТРИБУТИВНОЙ РЕШЕТКОЙ

Е. Е. Маренич (Москва)

Пусть $(P, \wedge, \vee, \leq)$ — дистрибутивная решетка с нулем $\widetilde{0}$ и единицей $\widetilde{1}$, $P^{n\times n}$ — множество всех $n \times n$ матриц над решеткой P.

Сложение и умножение матриц над решеткой P определяются как обычно: вместо операции умножения используются операция пересечения $\wedge$, а вместо операции сложения используются операция объединения $\vee$.

Полугруппа $\langle A\rangle = \{A, A^2, A^3, \ldots\}$, порожденная матрицей $A \in P^{n\times n}$ конечна, так как фактическое вычисление степеней матрицы $A \in P^{n\times n}$ производится над конечной решеткой $L = Lattice(A)$. По теореме Фробениуса для полугрупп, существует индекс $ind(A)$ и период $peri(A)$ матрицы A.

По теореме Фробениуса, множество

$$Gr(A) = \{A^{ind(A)}, A^{ind(A)+1}, \ldots, A^{ind(A)+peri(A)-1}\} =$$

$$= A^{ind(A)}\{E_{n\times n}, A, A^2, \ldots, A^{peri(A)-1}\}$$

— мультипликативная циклическая группа порядка $peri(A)$ с единицей A^m, где $peri(A)|m$, $\quad ind(A) \le m < ind(A) + peri(A)$. Матрица A^m — идемпотент. Образующим элементом группы $Gr(A)$ является матрица A^p, где $p \equiv 1(\mathrm{mod} peri(A))$, $ind(A) \le p < ind(A) + peri(A)$.

Обозначим $E_{n\times n}$ единичную $n\times n$ матрицу. Подстановочная матрица $M(\pi) = (\,m(\pi)_{ij})$ порядка n определяется подстановкой $\pi \in S_n$,

$$m(\pi)_{ij} = \begin{cases} \widetilde{1},\ j = \pi(i) \\ \widetilde{0},\ j \ne \pi(i), \end{cases} \qquad i, j = 1, \ldots, n.$$

Известна следующая теорема 1 и следствие 1.

Теорема 1. *Пусть решетка $P = \{\widetilde{0}, \widetilde{1}\}$, матрица $A \in P^{n\times n}$, $t = ind(A)$, $s = rank_c(A^t)$. Тогда существуют матрицы $B \in P^{n\times s}$ и $C \in P^{s\times n}$, существует подстановочная матрица $M(\pi) \in P^{s\times s}$ такая, что $Gr(A) = B\{E_{n\times n}, M(\pi), \ldots, M(\pi^{peri(A)-1})\}C$, $A^{t+j} = BM(\pi^j)C$, $j \in N_0$. Кроме того, $C = [E_{s\times s}, D]M(\sigma)$, где матрица $D \in P^{s\times(n-s)}$ и подстановочная матрица $M(\sigma) \in P^{n\times n}$.*

Следствие 1. *Пусть решетка $P = \{\widetilde{0}, \widetilde{1}\}$, матрица $A \in P^{n\times n}$. Если столбцовый ранг матрицы A равен числу n, то существует подстановочная матрица $M(\pi) \in P^{n\times n}$ такая, что*

$$Gr(A) = A^{ind(A)}\{E_{n\times n}, M(\pi), \ldots, M(\pi^{peri(A)-1})\}. \qquad (1)$$

Равенство (1) может выполняться и для матриц A, не удовлетворяющих условиям следствия 1.

Теорема 2. *Пусть матрица* $A \in P^{n\times n}$, $A^t \geq A^{t-1}M(\sigma)$ *для некоторого целого* $t \geq 1$ *и некоторой подстановочной матрицы* $M(\sigma)$. *Тогда существует подстановочная матрица* $M(\pi) \in P^{n\times n}$ *такая, что*

$$Gr(A) = A^{ind(A)}\{E_{n\times n}, M(\pi), M(\pi^2), \ldots, M(\pi^{peri(A)-1})\}, \qquad (2)$$

$$A^{ind(A)+j} = A^{ind(A)}M(\pi^j), \quad j \geq 0.$$

Следствие 2. *Для всех целых* $j \geq ind(A)$,

$$Gr(A) = A^j\{E_{n\times n}, M(\pi), M(\pi^2), \ldots, M(\pi^{peri(A)-1})\}.$$

Следствие 3. *Справедливы утверждения.*

i) Период матрицы A *равен наименьшему натуральному числу* l *такому, что* $A^{ind(A)} = A^{ind(A)}M(\pi^l)$. *В частности, период матрицы* A *не превосходит порядка подстановки* π.

ii) Справедливо неравенство $peri(A) \leq \min\{m!, l!\}$, *где* m — *число различных строк,* l — *число различных столбцов матрицы* $A^{ind(A)}$.

iii) Если столбцы матрицы $A^{ind(A)}$ *попарно различны, то множество* $\{E_{n\times n}, M(\pi), M(\pi^2), \ldots, M(\pi^{peri(A)-1})\}$ — *циклическая группа.*

Теорема 3. *Пусть матрица* $A \in P^{n\times n}$, $A^t \geq M(\sigma)A^{t-1}$ *для некоторого целого* $t \geq 1$ *и некоторой подстановочной матрицы* $M(\sigma)$. *Тогда существует подстановочная матрица* $M(\pi)$ *такая, что*

$$Gr(A) = \{E_{n\times n}, M(\pi), M(\pi^2), \ldots, M(\pi^{peri(A)-1})\}A^{ind(A)}, \qquad (3)$$

$$A^{ind(A)+j} = M(\pi^j)A^{ind(A)}, \quad j \geq 0.$$

Пример 1. Пусть $P = [0;1]$ — нечеткая решетка. Для нечеткой матрицы

$$A = \begin{pmatrix} 0 & 0,1 & 1 \\ 0,3 & 0 & 1 \\ 0 & 1 & 0,2 \end{pmatrix}$$

имеем:

$$Gr(A) = \{A^5, A^6\},$$

$$A^4 = \begin{pmatrix} 0,2 & 1 & 0,3 \\ 0,3 & 1 & 0,3 \\ 0,3 & 0,3 & 1 \end{pmatrix}, \quad A^5 = \begin{pmatrix} 0,3 & 0,3 & 1 \\ 0,3 & 0,3 & 1 \\ 0,3 & 1 & 0,3 \end{pmatrix},$$

$$A^6 = \begin{pmatrix} 0,3 & 1 & 0,3 \\ 0,3 & 1 & 0,3 \\ 0,3 & 0,3 & 1 \end{pmatrix}, \quad A^5 > A^4 M(\sigma), \quad M(\sigma) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Поэтому $Gr(A) = A^{ind(A)}\{E_{n\times n}, M(\sigma)\}$, кроме того, множество $\{E_{n\times n}, M(\sigma)\}$ — группа. Заметим, что матрицу A^6 нельзя получить перестановкой строк матрицы A^5.

Матрица $A \in P^{n\times n}$ называется *матрицей Холла*, если $A \geq M(\tau)$ для некоторой подстановочной матрицы $M(\tau) \in P^{n\times n}$.

Следствие 1. *Пусть матрица Холла $A \in P^{n\times n}$. Тогда существуют подстановочные матрицы $M(\pi), M(\sigma) \in P^{n\times n}$ такие, что*

$$Gr(A) = A^{ind(A)}\{E_{n\times n}, M(\pi), M(\pi^2), \ldots, M(\pi^{peri(A)-1})\} =$$

$$= A^{ind(A)}\{E_{n\times n}, M(\sigma), M(\sigma^2), \ldots, M(\sigma^{peri(A)-1})\}A^{ind(A)},$$

$$A^{ind(A)+j} = A^{ind(A)}M(\pi^j) = M(\sigma^j)A^{ind(A)}, \quad j \geq 0.$$

Для матриц A, для которых справедливо равенство (2) или (3), существуют более простой, чем алгоритм Кима, алгоритм вычисления периода.

Список литературы

1. Kim K. X. Boolean matrix theory and applications — New York: Marcel Dekker, 1982.

КООРДИНАТИЗАЦИЯ МАТРОИДОВ

А. М. Ревякин (Москва)

Рассматриваются проблемы, связанные с линейной представимостью матроидов [1–3]. Использованы терминология и обозначения работ [4–5].

Матроид M на множестве S называется представимым над полем F, если существует линейное пространство V над полем F и отображение $\phi : S \longrightarrow V$, при котором $A \subseteq S$ независимо в M тогда и только тогда, когда $\phi|_A$ взаимно однозначно и $\phi(A)$ — линейно независимое множество векторов в V. Проблему координатизации матроидов можно сформулировать в следующем виде: "для каждого подмножества Q множества неотрицательных простых чисел Z найти матроиды, которые линейно представимы над всеми полями

с характеристиками из Q и не представимы ни над каким полем характеристики p, если $p \notin Q$".

Обозначим множество всех характеристик полей над которыми представим матроид M через $\mathrm{Char}(M)$. Пусть $GF(q)$ — конечное поле характеристики q. Матроид, представимый над полем GF(2) (GF(3)), называют бинарным (соответственно, тернарным). Матроиды, представимые над каждым полем, называют унимодулярными (или регулярными). Татт доказал, что если $p \neq 2$ и $\{2, p\} \subseteq \mathrm{Char}(M)$, то $\mathrm{Char}(M) = Z$. Поэтому представляют интерес вопросы представимости небинарных матроидов. Матроид M называется почти регулярным, если он представим над каждым полем, кроме поля GF(2).

Матроид Фано Φ представим над полем $GF(2)$ и не представим ни над каким другим полем характеристики, отличной от 2. Матроид Φ^-, получаемый из Φ заменой одной прямой на три тривиальные прямые, является почти регулярным. Матроид M на 10-элементном множестве называется дезарговым, если он изоморфен конфигурации Дезарга. Очевидно, матроид Дезарга является регулярным. Если в матроиде Дезарга одну прямую заменить тремя тривиальными прямыми, то получим так называемый "не-дезаргов" матроид, который не представим ни над каким полем. Матроид Вамоса [3–4] также не представим ни над каким полем.

Пусть G — граф с множествами вершин V и ребер E. Тогда семейство всех циклов (разрезов) графа G является множеством всех циклов (соответственно, разрезов) некоторого матроида $M(G)$ на E, называемого циклическим матроидом (соответственно, матроидом разрезов) графа G. Матроид M называют графическим (кографическим), если существует граф G, циклический матроид (соответственно, матроид разрезов) которого изоморфен M. Графические и кографические матроиды являются унимодулярными. Лазарсона построил матроиды M_p, у которых $\mathrm{Char}(M) = \{p\}$. Брилавский и Кэлли построили матроид с $\mathrm{Char}(M) = \{1103, 2089\}$. Неизвестно, существуют ли другие матроиды M с $\mathrm{Char}(M) = \{p, q\}$, где $p \neq q$ и $p, q \neq 2$.

Представимые матроиды на конечных множествах удобно описывать с помощью матриц. Пусть M — матроид на конечном множестве S , представимый над полем F, $|S| = n$ и $\phi : S \longrightarrow V$ — его координатизация над полем F. Тогда $(k \times n)$-матрица A с коэффициентами из поля F, столбцами которой являются векторы $\phi(p)$, где $p \in S$, называется матрицей координатизации матроида M над полем F.

Пусть матрица

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & -1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & -1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & -1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & -1 \end{pmatrix}$$

является матрицей представления матроида R_{10} над полем рациональных чисел. Матроид R_{10} называют матроидом Сеймура [6]. Матроид, двойственный к матроиду Сеймура R_{10}, совпадает с R_{10}. Все миноры R_{10} являются либо графическими, либо кографическими. Однако, сам матроид R_{10} таковым не является. Исключение произвольного элемента из матроида Сеймура ведет к образованию матроида, изоморфного циклическому матроиду полного двудольного графа Куратовского $K_{3,3}$. Кроме того, R_{10} является унимодулярным.

Пусть A — множество всех матроидов, B — графические, C — кографические, D — регулярные, E — бинарные, F — тернарные и G — планарные матроиды. Тогда $D = E \bigcap F$, $B, C \subseteq D$, $G = B \bigcap C$, $R_{10} \in D$, $R_{10} \notin B \bigcup C$, $\Phi \in E \backslash F$, $U_{4,2} \in F \backslash D$, $M(K_{3,3}), M(K_5) \in B \backslash C$, $M^*(K_{3,3}), M^*(K_5) \in C \backslash B$, где $M(K_{3,3})$ и $M(K_5)$ — циклические матроиды графов Куратовского $K_{3,3}$ и K_5, а $M^*(K_{3,3})$ и $M^*(K_5)$ — их матроиды разрезов.

Доказано, что если матроид представим над $GF(p)$ для каждого нечетного простого p, то он представим над полем рациональных чисел. Матрица с рациональными коэффициентами называется двоичной, если все ее миноры равны 0 или $\pm 2^i$, где i — некоторое целое. Матроид, обладающий двоичной матрицей представления над полем рациональных чисел, называется двоичным матроидом. $\sqrt[6]{1}$-матрицей называется матрица с комплексными коэффициентами, все ненулевые миноры которой равны корням шестой степени из единицы. $\sqrt[6]{1}$-матроидом называется матроид, который можно представить столбцами $\sqrt[6]{1}$-матрицы. Установлено, что матроид M является почти регулярным тогда и только тогда, когда M является одновремено двоичным и $\sqrt[6]{1}$-матроидом (или M представим над полями $GF(3)$, $GF(4)$ и $GF(5)$).

Пусть S — n-элементное множество, k — некоторое целое такое, что $1 \leq k \leq n$, и $I = \{A \subseteq S : |A| \leq k\}$. Матроид (S, I) называют однородным и обозначают через $U_{k,n}$. Известно, что однородный матроид $U_{k,n}$ представим над $\mathrm{GF}(q)$ тогда и только тогда, когда

$n \leq N$ и если либо $k = 3, N = q+1$ и $q-$нечетное, либо $k = 3, N = q+2$ и $q-$четное, либо $k = 4, N = 5$ и $q \leq 3$, либо $k = 4, N = q+1$ и $q \geq 4$, либо $k = 5, N = 6$ и $q \leq 4$ или $k = 5, N = q+1$ и $q \geq 5$. Задача нахождения полей над которыми представим однородный матроид $U_{k,n}$ для любых k, n, является открытой проблемой.

Доказано, что если M — тернарный матроид, то для M справедливо одно из утверждений: M представим только над полем характеристики три, M — регулярный или M — почти регулярный матроид.

Список литературы

1. Welsh D. J. A. Matroid theory. — London: Acad. Press, 1976.

2. Recski A. Matroid theory and its applications in electric network theory and in statics. — Budapest: Akad. Kiado, 1989.

3. Oxley J. G. Matroid theory. — N.Y.: Oxford University Press, 1992 и 2006.

4. Ревякин А. М. Координатизация и представимость матроидов // Комбинатор. анализ. Вып. 8. — М.: МГУ, 1989. — С. 6–37.

5. Revyakin A. M. On some classes of linear representable matroids // Formal Power Series and Algebraic Combinatorics: 12 International Conference. Proceedings. FPSAC'oo, Moscow, Russia. June, 2000. — Berlin, N.Y.: Springer, 2000. — С. 564–574.

6. Seymour P. D. Matroid representation over $GF(3)$ // J. Combin. Theory. — 1979. — B26, № 2. — С. 159–173.

О ЧИСЛЕ МНОЖЕСТВ, СВОБОДНЫХ ОТ НУЛЯ, В ГРУППАХ ПРОСТОГО ПОРЯДКА

В. Г. Саргсян (Москва)

Пусть $\mathbf{Z}_p$ — группа вычетов по простому модулю p. Подмножество $A \subseteq \mathbf{Z}_p$ называется *свободным от нуля*, если уравнение $a + b + c = 0$ не имеет решения в множестве A. Семейство всех подмножеств, свободных от нуля, в группе $\mathbf{Z}_p$, обозначим через $S(p)$. Целью настоящей работы является получение оценки числа $|S(p)|$.

Теорема 1. *Пусть p — простое число. Тогда существует положительная константа C, такая, что*

$$2^{\lfloor (p-2)/3 \rfloor}(p-1)(1+O(2^{-Cp})) \le |S(p)| \le 2^{p/3+\kappa(p)},$$

где $\kappa(p)/p \to 0$ при $p \to \infty$.

Для всякого $A \subseteq \mathbf{Z}_p$ и любого целого числа d положим $d \star A = \{da : a \in A\}$ и назовем его *растяжением* множества A. Обозначим через $\chi_A(x)$ характеристическую функцию множества A. Определим $(\chi_A * \chi_A)(x)$ — количество наборов $(x_1, x_2) \in A^2$ таких, что $x = x_1 + x_2$. Положим $A+A = \{x_1+x_2 : x_1, x_2 \in A\}$, $-A = \{p-x : x \in A\}$ и $S_h(A) = \{x \in \mathbf{Z}_p : (\chi_A * \chi_A)(x) \ge h\}$, где $h > 0$.

Теорема 2 [1]. *Пусть A — подмножество последовательных элементов группы $\boldsymbol{Z}_p$ и $|A| < p/3+1$. Тогда*

$$|\{d \star B : B \subseteq A, d \in \boldsymbol{Z}_p\}| = 2^{|A|}(1-2^{-|A\setminus(-A)|-1})(p-1) + O(2^{5|A|/6}p^2).$$

Лемма 1 [2]. *Пусть A — непустое подмножество группы $\boldsymbol{Z}_p$ и $h \le |A|$. Тогда $|S_h(A)| \ge \min(p, 2|A|) - 2(hp)^{1/2}$.*

Пусть L — натуральное число. Для каждого $y \in \{0, \dots, p-1\}$ определим разбиение $\mathbf{R}_{y,L}$ группы $\mathbf{Z}_p$ на интервалы вида

$$J_i^y = \{(iL+1+y), \dots, ((i+1)L+y)\}, 0 \le i \le \lfloor p/L \rfloor - 1.$$

Все интервалы J_i^y разбиения $\mathbf{R}_{y,L}$ имеют длину L, а множество $J_y = \mathbf{Z}_p \setminus \bigcup_i J_i^y$ имеет мощность $p - L\lfloor p/L \rfloor < L$. Множество $A \subseteq \mathbf{Z}_p$ называется L- *гранулированным* (см. [2]), если для некоторого целого числа d и некоторого разбиения $\mathbf{R}_{y,L}$ растяжение $d \star A$ является объединением нескольких интервалов J_i^y разбиения $\mathbf{R}_{y,L}$ (отличных от J_y). Обозначим множество L-гранулированных подмножеств группы $\mathbf{Z}_p$ через $\mathbf{G}_L(\mathbf{Z}_p)$.

Лемма 2. *Справедливо неравенство $|\boldsymbol{G}_L(\boldsymbol{Z}_p)| \le p2^{p/L}$.*

Лемма 3 [2]. *Пусть $A \subseteq \boldsymbol{Z}_p$ — подмножество мощности αp, $\varepsilon_1, \varepsilon_2, \varepsilon_3$ — положительные действительные и L — натуральное числа, а p — простое число, такое, что выполняется неравенство*

$$p > (4L)^{256\alpha^2\varepsilon_1^{-4}\varepsilon_2^{-2}\varepsilon_3^{-1}}. \tag{1}$$

Тогда существует $A' \subseteq \boldsymbol{Z}_p$ со следующими свойствами:

(i) A' является L-гранулированным;

(ii) $|A \setminus A'| \le \varepsilon_1 p$;

(iii) множество $A+A$ *содержит все элементы* $x \in \boldsymbol{Z}_p$*, для которых* $(\chi_{A'} * \chi_{A'})(x) \ge \varepsilon_2 p$*, за исключением не более* $\varepsilon_3 p$ *элементов.*

Доказательство теоремы 1. В [3] доказано, что существует арифметическая прогрессия, свободная от нуля, мощности $\lfloor (p-2)/3 \rfloor + 1$ с разностью 1, в Z_p. Отсюда и из теоремы 2 получим, что

$$2^{\lfloor (p-2)/3 \rfloor}(p-1)(1+O(2^{-Cp})) \le |S(p)|,$$

где C –положительная константа.

Пусть s — удовлетворяет условию $3es \le 2^s$. Рассмотрим разбиение множества $\mathbf{S}(p)$ на две части:

$$\mathbf{S}(p) = \mathbf{S}'_s(p) \cup \mathbf{S}''_s(p),$$

где

$$\mathbf{S}'_s(p) = \{A \in \mathbf{S}(p) : |A| < p/3s\},\ \ \mathbf{S}''_s(p) = \{A \in \mathbf{S}(p) : |A| \ge p/3s\}.$$

Очевидно, что $|S(p)| = |\mathbf{S}'_s(p)| + |\mathbf{S}''_s(p)|$. Нетрудно заметить, что $\left|\mathbf{S}'_s(p)\right| \le 2^{p/3}$. Теперь оценим сверху $|\mathbf{S}''_s(p)|$. Пусть $A \in \mathbf{S}''_s(p)$ и p — простое число, такое, что выполняется условие (1). Тогда по лемме 3 существует подмножество A', обладающее свойствами $(i) - (iii)$. Оценим $|\mathbf{S}''_s(p)|$ путем подсчета количество пар (A', A).

Пусть $A' \in \mathbf{G}_L(\mathbf{Z}_p)$ — выбрано. Рассмотрим два случая: $|A'| \ge p/3$ и $|A'| < p/3$.

В первом случае в силу утверждения (iii) леммы 3 имеем

$$|S_{\varepsilon_2 p}(A') \setminus (A+A)| \le \varepsilon_3 p.$$

Так как A — множество, свободное от нуля, что то же самое, что $(A+A) \cap (-A) = \emptyset$, получим, что

$$|A| \le p - |S_{\varepsilon_2 p}(A')| + \varepsilon_3 p.$$

В силу леммы 1 имеем

$$|S_{\varepsilon_2 p}(A')| \ge \min(p, 2|A'|) - 2(\varepsilon_2 p^2)^{1/2}.$$

При условии $|A'| \ge p/3$, получаем

$$|S_{\varepsilon_2 p}(A')| \ge 2p/3 - 2{\varepsilon_2}^{1/2} p.$$

Отсюда следует, что число способов выбора A при заданом A' мощности, превышающей $p/3$, не превосходит

$$2^{p/3+(2\varepsilon_2{}^{1/2}+\varepsilon_3)p}.$$

Если $|A'| < p/3$, то в силу утверждения (ii) леммы 3 имеем

$$|A \setminus A'| \le \varepsilon_1 p.$$

Отсюда следует, что

$$|A| \le |A'| + \varepsilon_1 p.$$

Итак, число способов выбора A при заданом A' мощности, не превышающей $p/3$, не превосходит

$$2^{p/3+\varepsilon_1 p}.$$

В силу леммы 2 с применением леммы 3 с параметрами $L = 1 + \lfloor 1/\varepsilon \rfloor$ и $\varepsilon_1 = \varepsilon_3 = \varepsilon_2^{1/2} = \varepsilon$, получим, что

$$|\mathbf{S}_s''(p)| \le 2^{p/3+c\varepsilon p}.$$

Отсюда следует, что

$$|S(p)| \le 2^{p/3} + 2^{p/3+c\varepsilon p} = 2^{p/3+c\varepsilon p}.$$

Легко показать, что можно взять $\varepsilon = O(\log\log p)^{2/3}(\log p)^{-1/9})$.

Работа выполнена при поддержке РФФИ (проект 10–01–00768-а).

Список литературы

1. Lev V. F., Schoen T. Cameron—Erdos modulo a prime // Finite Fields Appl. — 2002. — V. 8, № 1. — P. 108–119.

2. Green B., Ruzsa I. Counting sum-sets and sum-free sets modulo a prime // Studia Sci. Math. Hungarica. — 2004. — V. 41. — P. 285–293.

3. Bajnok B. On the maximum size of a (k, l)-sum-free subset of an abelia group // International Journal of Number Theory. — 2009. — V. 5, № 6. — P. 953–971.

О ПОДОБИИ МАТРИЦЫ ВТОРОГО ПОРЯДКА И ТРАНСПОНИРОВАННОЙ К НЕЙ МАТРИЦЫ НАД КОЛЬЦОМ ЦЕЛЫХ ЧИСЕЛ

С. В. Сидоров (Нижний Новгород)

В [1] исследовалась задача о подобии матриц второго порядка над кольцом целых чисел как обобщение классической задачи о подобии матриц над полем рациональных чисел.

Квадратные матрицы A и B порядка n называются *подобными над полем рациональных чисел*, если существует такая матрица $X \in \mathbf{Q}^{n\times n}$, что $AX = XB$ и $\det X \neq 0$

Квадратные матрицы A и B порядка n называются *подобными над кольцом целых чисел*, если существует такая матрица $X \in \mathbf{Z}^{n\times n}$, что $AX = XB$ и $\det X \in \{1, -1\}$

Хорошо известно, что над полем рациональных чисел матрицы A и $A^\top$ подобны. Над кольцом целых чисел этот факт, вообще говоря, не имеет места. Здесь будем рассматривать матрицы второго порядка, все собственные числа которых целые.

В статье [1] доказано, что множество матриц второго порядка с характеристическим многочленом вида $d(x) = (x-\alpha)(x-\beta)$ разбивается на счетное число классов подобия, если $\alpha = \beta$, и на конечное число классов, если $\alpha \neq \beta$. В первом случае каноническими матрицами являются матрицы вида $\begin{pmatrix} \alpha & k \\ 0 & \alpha \end{pmatrix}$, где $k \geq 0$. Во втором случае канонические матрицы - это матрицы вида $\begin{pmatrix} \alpha & k \\ 0 & \beta \end{pmatrix}$, где $0 \leq k \leq \left\lfloor \frac{\beta-\alpha}{2} \right\rfloor$. Следующая теорема показывает, при каких условиях такие матрицы подобны своим транспонированным матрицам.

Теорема. *Пусть* $A = \begin{pmatrix} \alpha & k \\ 0 & \beta \end{pmatrix}$ *и* $A^\top = \begin{pmatrix} \alpha & 0 \\ k & \beta \end{pmatrix}$.

1) *Если* $\alpha = \beta$, *то* A *и* $A^\top$ *подобны над* $\mathbf{Z}$.

2) *Если* $\alpha \neq \beta$, *то* A *и* $A^\top$ *подобны над* $\mathbf{Z}$ *тогда и только тогда, когда либо* $\frac{k^2+d^2}{d(\beta-\alpha)}$, *либо* $\frac{k^2-d^2}{d(\beta-\alpha)}$ *является целым числом, где* $d = НОД(\beta-\alpha, k)$.

Доказательство. Случай $k = 0$ очевиден, поэтому далее предполагаем, что $k \neq 0$. Если $\alpha = \beta$, то $AS = SA^\top$, где $S = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, поэтому A и $A^\top$ подобны над $\mathbf{Z}$. Теперь рассмотрим случай, когда

$\alpha \neq \beta$. Если $T = \begin{pmatrix} t_1 & t_2 \\ t_3 & t_4 \end{pmatrix}$ — целочисленная матрица, удовлетворяющая условию $AT = TA^\top$, то $\alpha t_1 + kt_3 = \alpha t_1 + kt_2$, $\alpha t_2 + kt_4 = \beta t_2$, $\beta t_3 = \alpha t_3 + kt_4$. Следовательно, $t_2 = t_3$ и $t_4 = \frac{(\beta-\alpha)t_2}{k}$. Обозначим $t_1 = x$, $d = \text{НОД}(\beta - \alpha, k)$, $t = \frac{k}{d}$, $s = \frac{\beta-\alpha}{d}$, $y = \frac{t_2}{t}$. Далее, $t_4 \in \mathbf{Z}$ только в том случае, когда $y \in \mathbf{Z}$. Следовательно, матрица T имеет вид $T = \begin{pmatrix} x & yt \\ yt & ys \end{pmatrix}$. Поскольку $\det T$ должен быть равен 1 или -1, то имеет место уравнение $\det T = y(xs - yt^2) = \pm 1$. Данное уравнение имеет решение в целых числах, если $y = \pm 1$ и $xs \pm t^2 = \pm 1$, откуда получаем $x = \frac{\pm t^2 \pm 1}{s} = \frac{\pm k^2 \pm d^2}{d(\beta-\alpha)}$. Поскольку x должен быть целым числом, получаем доказываемое.

Список литературы

1. Шевченко В. Н., Сидоров С. В. О подобии матриц второго порядка над кольцом целых чисел // Известия вузов. Математика. — 2006. — № 4. — С. 57–64.

Секция «Теория графов»

ГРАФ МНОГОГРАННИКА ЗАДАЧИ РАЗБИЕНИЕ НА ТРЕУГОЛЬНИКИ

А. И. Антонов, В. А. Бондаренко (Ярославль)

Рассмотрим задачу следующего вида. Задан полный граф G с множеством вершин $N_n = \{1, \ldots, n\}$, где $n = 3k$, для каждого ребра (t, s) $(t < s)$ которого задана его длина c_{ts}. Требуется множество вершин N_n разбить на k троек так, чтобы сумма периметров соответствующих треугольников была минимальной.

Сужением этой задачи служит известная NP-полная задача «Разбиение на треугольники» [1].

Определим многогранник рассматриваемой задачи. С этой целью в пространстве R^m, где m равно количеству ребер графа G, т. е. $m = n(n-1)/2$, для каждого разбиения δ на треугольники рассмотрим его характеристический вектор $x = x(\delta)$. Пусть X — множество всех таких x. Многогранником M нашей задачи служит выпуклая оболочка $\mathrm{conv}X$. Очевидно, что X — множество вершин многогранника M. Множество его ребер описывает следующая

Теорема 1. *Вершины x_1 и x_2 $(x_i = x(\delta_i))$ многогранника M будут смежны в том и только том случае, когда множество вершин исходного графа G, получающееся после отбрасывания общих для δ_1 и δ_2 троек, нельзя разбить на два подмножества, каждое из которых распадается на тройки для δ_1 и для δ_2.*

Для доказательства теоремы 1 можно воспользоваться следующим простым утверждением: x_1 и x_2 не смежны в том и только том случае, когда существует $x \in X$, $x \neq x_1$, $x \neq x_2$, для которого выполняется неравенство $x \leq x_1 + x_2$.

С помощью теоремы 1 удается получить экспоненциальную нижнюю оценку кликового числа графа многогранника M.

Теорема 2. *Максимальное количество p попарно смежных вершин многогранника M удовлетворяет неравенству*

$$p(X) \geq 2^{\sqrt{k}/2-2}. \tag{1}$$

Доказательство. Предположим сначала, что $k = (2r+1)^2$, где r натурально. Вершины исходного графа G, где $n = 3(2r+1)^2$, обозначим следующим образом:

$$u(i,j), v(i,j), w(i,j),$$

где $i, j = 0, 1, \ldots, 2r$.

Пусть I — множество вида:

$$I = \{i_0, i_1, \ldots, i_r\}, \tag{2}$$

где $0 = i_0 < i_1 < \cdots < i_r \leq 2r$ и при любом $s = 1, \ldots, r$ величина i_s принимает одно из двух значений: $2s-1$ и $2s$. Рассмотрим набор троек вершин исходного графа:

$$\{u(i_s, i_{t+1}), v(i_s, i_t), w(i_t, i_s)\} \qquad s, t = 0, 1, \ldots, r, \tag{3}$$

считая, что $i_{r+1} = i_0 = 0$. Дополним набор (3) тройками вида

$$\{u(i,j), v(i,j), w(i,j)\}, \qquad (i,j) \notin I \times I; \tag{4}$$

получим разбиение множества вершин исходного графа G на k троек.

Обозначим через Y множество характеристических векторов всех подграфов, определяемых разбиениями описанного вида, $Y \subset X$. Каждое разбиение однозначно определяется соответствующим множеством I, следовательно,

$$|Y| = 2^r. \tag{5}$$

Покажем, что точки множества Y являются попарно смежными вершинами многогранника $\mathrm{conv}X$.

Пусть $x_1, x_2 \in Y, x_1 \neq x_2$. Обозначим через I_{x_1} и I_{x_2} множества вида (2), определяющие по указанному выше правилу наборы троек соответственно для x_1 и x_2:

$$I_{x_1} = \{i_0, i_1, \ldots, i_r\}, \qquad I_{x_2} = \{i'_0, i'_1, \ldots, i'_r\}.$$

Пусть $i \in I_{x_1}$ и $i \notin I_{x_2}$; такой номер, очевидно, найдется. Обозначим через Q наименьшее по включению подмножество вершин исходного графа G, которое распадается на тройки из δ_1 и из δ_2 и которое содержит вершину $v(i,0)$. Вершина $v(i,0)$ входит в тройку вида (3) из δ_1 и вида (4) из δ_2. Поэтому $u(i,i_1) \in Q, v(i,i_1) \in Q$ и,

по индукции, $u(i,j), v(i,j) \in Q$ для всех $j \in I_{x_1}$. Отсюда вытекает, что $w(j,i) \in Q$, если $j \in I_{x_1}$, и, следовательно, $v(j,i) \in Q$. Последнее включение дает возможность повторить предыдущие рассуждения, взяв в качестве начальной вершину $v(j,i)$ вместо $v(i,0)$. В результате получим, что если номера i,j из I_{x_1}, и хотя бы один из них не входит в I_{x_2}, то $v(i,j) \in Q$.

Рассмотрим теперь номер s, $0 \leq s \leq r-1$, для которого $i_s = i'_s$, $i_{s+1} \notin I_{x_2}$, $i'_{s+1} \in I_{x_1}$; из свойств множеств I_{x_1} и I_{x_2} следует существование такого s. Из доказанного выше вытекает, что $v(0,i_{s+1}) \in Q$, поэтому $u(0,i_{s+1}) \in Q$ и $v(0,i_s) = v(0,i'_s) \in Q$. Отсюда следуют включения $u(0,i'_{s+1}) \in Q$, $v(0,i'_{s+1}) \in Q$, $w(0,i'_{s+1}) \in Q$ и, наконец, $v(i'_{s+1},0) \in Q$. Вновь используя рассуждения предыдущего абзаца, приходим к выводу о том, что $v(i,j) \in Q$, если i,j из I_{x_2} и хотя бы один из номеров i и j не входит в I_{x_1}.

Обозначим через $v(i,j)$ вершину исходного графа, которая входит в разные тройки из δ_1 и δ_2. Последнее означает, что оба номера i и j принадлежат хотя бы одному из множеств I_{x_1} или I_{x_2}. Если i и j одновременно входят лишь в одно из указанных множеств, то непосредственно из установленного ранее следует включение $v(i,j) \in Q$. Если же $i,j \in I_{x_1}$ и $i,j \in I_{x_2}$, то для некоторых s и t выполняются равенства $i_s = i'_s = i$ и $i_t = i'_t = j$, причем $i_{t+1} \neq i'_{t+1}$, так как по предположению $v(i,j)$ входит в разные тройки из δ_1 и δ_2, которые имеют, очевидно, вид (3). Поэтому $i_{t+1} \notin I_{x_2}$ и $v(i_s,i_{t+1}) \in Q$. Следовательно, $u(i_s,i_{t+1}) \in Q$ и, наконец, $v(i_s,i_t) = v(i,j) \in Q$. Таким образом, Q представляет собой такое подмножество вершин исходного графа G, которое получается отбрасыванием вершин общих для δ_1 и δ_2 треугольников. С учетом минимальности множества Q из теоремы 1 следует смежность x_1 и x_2.

Для получения оценки (1) при произвольном k остается воспользоваться равенством (5) и монотонностью $p(X_{3k})$.

Работа выполнена при поддержке гранта Правительства РФ по постановлению № 220, договор № 11.G34.31.0053.

Список литературы

1. Гэри Д., Джонсон Д. Вычислительные машины и труднорешаемые задачи. — М.: Мир, 1982.

ПЕРЕЧИСЛЕНИЕ ПОМЕЧЕННЫХ ЭЙЛЕРОВЫХ КАКТУСОВ

В. А. Воблый (Москва)

Кактусом называется связный граф, в котором нет ребер, лежащих более чем на одном простом цикле [1, с. 93]. Все блоки кактуса — ребра или простые циклы (многоугольники) [2]. Форд и Уленбек перечислили помеченные кактусы с заданным распределением числа вершин по многоугольникам [2]. Эйлеров граф — это связный граф, все вершины которого имеют четную степень [1, с. 22].

Теорема. *Пусть D_n — число помеченных эйлеровых кактусов с n вершинами. При $n \geq 3$ верна формула*

$$D_n = (n-1)! \sum_{k=1}^{[\frac{n-1}{2}]} \frac{n^{k-1}}{k! 2^k} \binom{n-k-2}{k-1}.$$

Доказательство. Мостом связного графа называется его ребро, после удаления которого граф становится несвязным [3, с. 41].

Эйлеровы графы являются графами без мостов. Действительно, множество ребер эйлерова графа можно разбить на простые циклы [3, теорема 7.1]. В то же время мост графа не принадлежит ни одному его простому циклу [3, теорема 3.2]. Таким образом, у эйлеровых кактусов все блоки являются простыми циклами.

Пусть C_n — число помеченных связных графов с n вершинами, а B_n — число помеченных блоков с n вершинами. Рассмотрим производящие функции

$$C(z) = \sum_{n=1}^{\infty} C_n \frac{z^n}{n!}, \; B(z) = \sum_{n=3}^{\infty} B_n \frac{z^n}{n!}.$$

В работах [4, 5] автором получено соотношение

$$C_n = \frac{(n-1)!}{n} [z^{n-1}] \exp(nB'(z)).$$

Обозначая через $\bar{B}(z)$ экспоненциальную производящую функцию для числа блоков помеченных эйлеровых кактусов, получим

$$D_n = \frac{(n-1)!}{n} [z^{n-1}] \exp(n\bar{B}'(z)).$$

Так как число циклов с n помеченными вершинами равно $(n-1)!/2$, имеем

$$\bar{B}(z) = \sum_{n=3}^{\infty} \frac{1}{2}(n-1)!\frac{z^n}{n!} = -\frac{1}{2}\ln(1-z) - \frac{z}{2} - \frac{z^2}{4},$$

$$\bar{B}'(z) = \frac{1}{2(1-z)} - \frac{z}{2} - \frac{1}{2} = \frac{z^2}{2(1-z)}.$$

$$D_n = \frac{(n-1)!}{n}[z^{-1}] \exp\left(\frac{nz^2}{2(1-z)}\right) z^{-n}.$$

Разлагая экспоненту в степенной ряд, найдем

$$D_n = \frac{(n-1)!}{n}[z^{-1}]\left(z^{-n} + \sum_{k=1}^{\infty} \frac{n^k z^{2k-n}}{k!2^k(1-z)^k}\right).$$

С помощью известного ряда [6, с. 141]

$$(1-z)^{-k} = \sum_{m=0}^{\infty} \binom{m+k-1}{k-1} z^m$$

получим

$$D_n = (n-1)![z^{-1}] \sum_{k=1}^{\infty} \frac{n^{k-1}}{k!2^k} \sum_{m=0}^{\infty} \binom{m+k-1}{k-1} z^{2k+m-n} =$$

$$= (n-1)! \sum_{k=1}^{\infty} \frac{n^{k-1}}{k!2^k} \binom{n-k-2}{k-1}.$$

Учитывая, что биномиальный коэффициент обращается в ноль при $n-k-2 < k-1$, т. е. при $2k > n-1$, завершим доказательство теоремы.

Список литературы

1. Харари Ф., Палмер Э. Перечисление графов. — М.: Мир, 1977.

2. Ford G. W., Uhlenbeck G. E. Combinatorial problems in theory graphs. III. — Proc. Nat. Acad. Sci. USA. — 1956. — V. 42. — P. 529–535.

3. Харари Ф. Теория графов. — М.: Мир, 1973.

4. Воблый В. А. О перечислении помеченных связных графов по числу точек сочленения // Дискретная математика. — 2008. —Т. 20, вып. 1. — С. 14–23.

5. Воблый В. А. Об одной формуле для числа помеченных связных графов // Дискретный анализ и исследование операций (в печати).

6. Риордан Дж. Комбинаторные тождества. — М.: Наука, 1982.

О ГРАФАХ ДЕЗА, ЯВЛЯЮЩИХСЯ ГРАФАМИ КЭЛИ

С. В. Горяинов, Л. В. Шалагинов (Челябинск)

В данной работе рассматривается метод получения графов Деза из групп, предложенный в статье [1], в приложении к группам небольшого порядка. А именно, для этих групп найдены все неизоморфные графы Кэли, являющиеся графами Деза.

Все графы, рассматриваемые в данной статье конечны, неориентированы, без петель и кратных ребер.

Графом Деза с параметрами (v, k, b, a), где $b \geq a$, называется граф на v вершинах, степень каждой вершины которого равна k, и любые две вершины имеют a или b общих соседей.

Точным графом Деза называется граф Деза диаметра 2, не являющийся сильно регулярным.

Пусть G — группа и $D \subset G$. Определим D^{-1} как множество $\{d^{-1} : d \in D\}$. Пусть Γ — граф, множество вершин которого — все элементы группы G, и вершины u и v смежны тогда и только тогда, когда $v^{-1}u \in D$. Если единица группы G не содержится в D и $D^{-1} = D$, то Γ называется графом Кэли группы G по системе образующих D и обозначается $Cay(G, D)$.

Подмножества элементов D и D' группы G называются *изоморфными*, если найдется $\alpha \in Aut(G)$, что $\alpha(D) = D'$. Если подмножества D и D' изоморфны, то изоморфны и графы $Cay(G, D)$ и $Cay(G, D')$.

Определим DD^{-1} как мультимножество $\{dd'^{-1} : d, d' \in D\}$ (в DD^{-1} могут быть повторяющиеся элементы). Для подмножеств A и B множества элементов G и целых чисел a и b будем писать $DD^{-1} = aA + bB$, если в DD^{-1} содержится a копий каждого элемента из A и b копий каждого элемента из B.

Теорема 1 [1]. *Пусть D подмножество элементов группы G, такое что*

1) $|G| = v$ *и* $|D| = k$;

2) $DD^{-1} = aA + bB + ke$, *где* A, B *и* $\{e\}$ — *разбиение* G.

Тогда $Cay(G, D)$ — *граф Деза с параметрами* (v, k, b, a).

Для поиска графов была написана программа. На первом этапе для каждой группы перебирались все подмножества их элементов, являющиеся системами образующих графов Кэли. На втором этапе отбирались системы, удовлетворяющие условию теоремы 1, из которых получаются точные графы Деза. То есть были найдены все наборы параметров графов Деза, являющихся графами Кэли соответствующих групп. Для каждого набора был составлен список графов Кэли. На третьем этапе из этого списка отбирались все неизоморфные графы.

В дальнейшем преставляет интерес теоретическое обобщение свойств графов Деза, являющихся графами Кэли, и изучение графов, получающихся из известных классов групп. Так как неизоморфные графы получаются только из неизоморфных систем образующих, то одним из дальнейших направлений работы является изучение групп автоморфизмов групп.

Работа выполнена при финансовой поддержке гранта Президента РФ для молодых ученых (проект МК-938.2011.1).

Список литературы

1. Erickson M., Fernando S., Haemers W. H., Hardy D., Hemmeter J. Deza graphs: a generalization of strongly regular graphs // J. Comb. Designs. — 1999. — V. 7. — P. 359–405.

О НЕЗАВИСИМЫХ МНОЖЕСТВАХ В УНИЦИКЛИЧЕСКИХ ГРАФАХ

А. Б. Дайняк (Москва)

В терминологии и обозначениях мы следуем книгам [1] и [2] соответственно.

В данной заметке приводятся точные оценки количества максимальных по включению независимых множеств (далее, *м. н. м.*) в унициклических графах.

Висячим будем называть ребро графа, инцидентное висячей вершине. Имеют место следующие верхние оценки количества м. н. м. в

унициклических графах. Первая теорема касается графов с фиксированным числом вершин и обхватом. Аналогичная задача для «обычных» н. м. была рассмотрена в [4].

Теорема 1. *Пусть G — унициклический граф на n ($n \geq 9$) вершинах с обхватом g, имеющий максимальное количество м. н. м. среди графов с тем же числом вершин и обхватом. Тогда:*

При $g = 3$ и нечетных n граф G получается присоединением $\frac{n-3}{2}$ листьев к одной из вершин C_3 и последующим подразбиением каждого из висячих ребер.

При $g = 3$ и четных n граф G получается присоединением $\frac{n-8}{2}$ листьев к одной из вершин C_3, подразбиением каждого из висячих ребер и добавлением пятивершинной цепи к вершине максимальной степени в полученном графе.

При $g = 4$ и четных n граф G получается присоединением t и $\left(\frac{n-4}{2} - t\right)$ листьев к паре соседних вершин C_4 и последующим подразбиением каждого из висячих ребер. Число t может быть любым в диапазоне от 0 до $\left\lfloor \frac{n-4}{4} \right\rfloor$.

При $g \geq 4$ и нечетных $(n-g)$ граф G получается присоединением 1 и $\frac{n-g-1}{2}$ листьев к паре соседних вершин C_g и последующим подразбиением каждого из висячих ребер, инцидентных вершине максимальной степени.

При $g \geq 4$ и четных $(n-g)$ граф G получается присоединением $\frac{n-g}{2}$ листьев к одной из вершин C_g и последующим подразбиением каждого из висячих ребер.

Вторая из доказанных нами теорем касается унициклических графов с фиксированным числом вершин и диаметром. Аналог этой теоремы для обычных н. м. доказан в [3].

Теорема 2. *Пусть G — унициклический граф диаметра d ($d \geq 8$) на n вершинах, имеющий максимальное количество м. н. м. среди графов с тем же числом вершин и диаметром. Тогда:*

При $(n-d)$ нечетном, граф G получается присоединением к одной из вершин C_3 $\frac{n-d-1}{2}$ листьев, и последующим $(d-2)$–кратным подразбиением одного из висячих ребер и однократным подразбиением остальных висячих ребер в полученном графе.

При $(n-d)$ четном, G изоморфен следующему графу. Подразобьем у звезды $K_{\frac{n-d}{2}}$ однократно все лучи, кроме одного, а один луч подразобьем $(d-2)$–кратно, а бывший центр звезды затем соединим с любой из вершин C_3.

Перейдем к нижним оценкам. Пусть $G = (V, E)$ — произволь-

ный граф. Очевидно, отношение $R = \{(u, v) \subseteq V^2 \mid N(u) = N(v)\}$ является отношением эквивалентности на множестве V. Обозначим через $V_1, \ldots, V_q$ классы эквивалентности по отношению R. Назовем *сжатием* графа G граф $s(G)$, в котором $V(s(G)) = \{V_1, \ldots, V_q\}$ и $E(s(G)) = \{V_iV_j \mid \exists u, v\colon (u \in V_i \wedge v \in V_j \wedge uv \in E(G)\}$. Неформально, граф $s(G)$ получается из G заменой каждого множества V_i на любого из своих представителей.

Теорема 3. *Пусть G — граф обхвата g, имеющий минимальное число м. н. м. среди графов с тем же числом вершин и обхватом, и пусть $4 < g < |G|$. Тогда $s(G) \simeq G''_g$, где G''_g — граф, получаемый добавлением к C_g висячей вершины.*

Если G — граф, имеющий минимальное число м. н. м. среди графов с обхватом 4, то G — полный двудольный.

Если G — граф, имеющий минимальное число м. н. м. среди графов с обхватом 3, то $s(G)$ изоморфен одному из следующих трех графов: K_3, K_3 с добавленным листом, K_3 с добавленными к двум различным вершинам листьями.

Работа выполнена при поддержке гранта Президента РФ МК-3429.2010.1 и гранта РФФИ № 10-01-00768а.

Список литературы

1. Емеличев В. А., Мельников О. И., Сарванов В. И., Тышкевич Р. И. Лекции по теории графов. — М.: Книжный дом «Либроком», 2009.

2. Diestel R. Graph Theory. Fourth Edition. — Springer-Verlag, 2010.

3. Li S., Zhu Zh. The number of independent sets in unicyclic graphs with a given diameter // Discrete Appl. Math. — 2009. — V. 7, № 157. — P. 1387–1395.

4. Pedersen A. S., Vestergaard P. D. The Number of Independent Sets in Unicyclic Graphs // Discrete Appl. Math. — 2005. — V. 3, № 152. — P. 246–256.

ГИПОТЕЗА ЛОЗИНА ДЛЯ ПОДКЛАССОВ КЛАССА ГРАФОВ БЕЗ $K_{1,3}$

В. А. Замараев (Нижний Новгород)

В работе рассматриваются обыкновенные графы, вершины которых помечены натуральными числами. Если X — множество графов, то через X_n обозначается подмножество n-вершинных графов

из X. Множество графов называется *наследственным* классом, если оно замкнуто относительно изоморфизма и удаления вершины. Наследственный класс может быть задан множеством запрещенных порожденных подграфов. Пусть $\mathcal{M}$ — множество графов, тогда через $Free(\mathcal{M})$ принято обозначать множество всех графов, не содержащих порожденных подграфов, изоморфных графам из $\mathcal{M}$. Общеизвестно, что множество графов $\mathbf{X}$ является наследственным классом тогда и только тогда, когда $\mathbf{X} = Free(\mathcal{M})$ для некоторого $\mathcal{M}$.

В [1] В. Е. Алексеев доказал, что для любого бесконечного наследственного класса $\mathbf{X}$ обыкновенных графов, отличного от класса всех графов, справедливо следующее соотношение:

$$\log_2 |\mathbf{X}_n| = \left(1 - \frac{1}{k(\mathbf{X})}\right) \frac{n^2}{2} + o(n^2). \qquad (1)$$

где $k(\mathbf{X})$ — натуральное число, называемое *индексом* класса $\mathbf{X}$. Множество классов с определенным значением индекса называется *слоем*. Видно, что соотношение (1) не дает асимптотической оценки функции $\log_2 |\mathbf{X}_n|$ для классов из *унитарного* слоя, то есть слоя с индексом, равным 1. Вместе с тем, этому слою принадлежат многие важные с практической и теоретической точек зрения классы, например, леса, планарные графы, реберные графы, интервальные графы, кографы, хордальные двудольные графы и др.

Для исследования асимптотического поведения функции $\log_2 |\mathbf{X}_n|$ для классов из унитарного слоя В. Е. Алексеев ввел понятие равновеликости [2]. Множества графов X и Y называются *равновеликими*, если существуют положительные константы c_1, c_2, n_0 такие, что $|Y_n|^{c_1} \leq |X_n| \leq |Y_n|^{c_2}$ для всех $n > n_0$. Множество X называется *не более чем факториальным*, если существуют положительные константы c, n_0 такие, что $|X_n| \leq n^{cn}$ для всех $n > n_0$ и *факториальным*, если существуют положительные константы c_1, c_2, n_0 такие, что $n^{c_1 n} \leq |X_n| \leq n^{c_2 n}$ для всех $n > n_0$. *Сверхфакториальным* называют множество графов X такое, что для любых положительных c и n_0 существует $n > n_0$, при котором $|X_n| > n^{cn}$. Нетрудно видеть, что равновеликость является отношением эквивалентности. Классы эквивалентности по отношению равновеликости на множестве наследственных классов графов называются *ярусами*.

В [3] Э. Шайнерман и Дж. Зито выделили четыре самых нижних яруса унитарного слоя: *константный*, *полиномиальный*, *экспоненциальный* и *факториальный*. Для этих ярусов $\log_2 |X_n|$ по порядку совпадает с $1, \log n, n$ и $n \log n$ соответственно. Авторы [3] также показали, что для наследственных классов никаких промежуточных

типов поведения не существует. Независимо, такой же результат был получен В. Е. Алексеевым [2]. Более того, для первых трех ярусов В. Е. Алексеев получил структурные описания и в каждом из четырех нашел все минимальные элементы. Позже аналогичные результаты были получены Дж. Балогхом, Б. Болоба́шем и Д. Вайнрайхом [4].

Факториальный ярус существенно богаче предыдущих трех, а классы из этого яруса имеют более разнообразную структуру. Значимость факториального яруса заключается в том, что он содержит многие классы, представляющие большой интерес с теоретической и практической точек зрения. При этом, факториальный ярус до сих пор не имеет какой-либо полной структурной характеризации. В качестве одного из шагов на пути к получению такой характеризации в [5] была предложена следующая гипотеза.

Гипотеза Лозина: Наследственный класс $\mathbf{X}$ не более чем факториальный тогда и только тогда, когда каждый из классов $\mathbf{X} \cap \mathbf{B}$, $\mathbf{X} \cap \widetilde{\mathbf{B}}$ и $\mathbf{X} \cap \mathbf{S}$ не более чем факториальный.

Здесь $\mathbf{B}$ — класс двудольных графов, $\widetilde{\mathbf{B}}$ — класс дополнительных к двудольным (кодвудольных) графов и $\mathbf{S}$ — класс расщепляемых графов, т. е. графов, множество вершин которых можно разбить на клику и независимое множество.

Истинность этой гипотезы и знание всех факториальных подклассов класса двудольных, кодвудольных и расщепляемых графов может оказать существенную помощь при ответе на вопрос, является ли заданный наследственный класс $\mathbf{X}$ факториальным.

Основным результатом настоящей работы является следующая теорема, одним из следствий которой является справедливость гипотезы Лозина для наследственных подклассов класса $\mathbf{K} = Free(K_{1,3})$, где $K_{1,p}$ — звезда с p листьями.

Теорема 1. *Пусть $\mathcal{M}$ — некоторое множество графов. Класс $Free(\mathcal{M}) \cap \mathbf{K}$ — не более чем факториальный класс тогда и только тогда, когда $Free(\mathcal{M}) \cap \widetilde{\mathbf{B}}$ — не более чем факториальный.*

Следствие (гипотеза Лозина для подклассов класса $\mathbf{K}$). *Пусть $\mathcal{M}$ — некоторое множество графов. Класс $\mathbf{X} = Free(\mathcal{M}) \cap \mathbf{K}$ не более чем факториальный тогда и только тогда, когда каждый из классов $\mathbf{X} \cap \mathbf{B}$, $\mathbf{X} \cap \widetilde{\mathbf{B}}$ и $\mathbf{X} \cap \mathbf{S}$ не более чем факториальный.*

Помимо этого следствия теорема 1 в совокупности с результатом из [6] позволяет охарактеризовать почти все факториальные классы с двумя запрещенными графами, один из которых $K_{1,3}$.

Обозначим через $\Phi_{p,q}$ граф, получаемый из двух звезд $K_{1,p}$ и $K_{1,q}$ соединением их центральных вершин простым путем длины 2, через

$T_{1,2,3}$ — граф, получаемый из звезды $K_{1,3}$ одиночным подразбиением одного из её ребер и двойным подразбиением другого её ребра. Через P_7, как обычно, обозначается семивершинный путь.

Теорема. *Если G не является порожденным подграфом какого-либо из графов $\overline{T_{1,2,3}}, \overline{\Phi_{p,q} + K_1}$ или $\overline{P_7}$, то класс $Free(K_{1,3}, G)$ — сверхфакториальный. Если G — порожденный подграф графа $\overline{T_{1,2,3}}$ или $\overline{\Phi_{p,q} + K_1}$ для некоторых натуральных p, q, то $Free(K_{1,3}, G)$ — не более чем факториальный.*

Работа выполнена при финансовой поддержке РФФИ (проекты 11-01-00107-а и 12-01-00749-а), ФЦП «Научные и научно-педагогические кадры инновационной России на 2009–2012 гг.» (ГК 16.740.11.0310) и лаборатории алгоритмов и технологий анализа сетевых структур НИУ ВШЭ, грант правительства РФ дог. 11.G34.31.0057.

Список литературы

1. Алексеев В. Е. Область значений энтропии наследственных классов графов // Дискретная математика. — 1992. — Т. 4, вып. 2. — С. 148–157.

2. Алексеев В. Е. О нижних ярусах решётки наследственных классов графов // Дискретный анализ и исследование операций. — 1997. — Т. 4. — С. 3–12.

3. Scheinerman E. R., Zito J. On the size of hereditary classes of graphs // Journal of Combinatorial Theory. Series B. — 1994. — V. 61. — P. 16–39.

4. Balogh J., Bollobás B., Weinreich D. The speed of hereditary properties of graphs // Journal of Combinatorial Theor. Series B. — 2000. — V. 79. — P. 131–156.

5. Lozin V. V., Mayhill C., Zamaraev V. A note on the speed of hereditary graph properties // The Electronic Journal of Combinatorics. — 2011. — V. 18, № 1.

6. Lozin V. V., Mayhill C., Zamaraev V. Locally bounded coverings and factorial properties of graphs // European Journal of Combinatorics. — 2012. — V. 33, № 4. — P. 534–543.

СИММЕТРИЧЕСКИЕ ЛИНЕЙНЫЕ ПРОСТРАНСТВА ДВУДОЛЬНЫХ ГРАФОВ

Д. В. Захарова (Нижний Новгород)

В работе продолжается начатое в [1, 2] исследование симметрических линейных простанств графов. Симметрической разностью графов $G_1 = (V, E_1)$ и $G_2 = (V, E_2)$ называется граф $G1 \oplus G2 = (V, (E_1 - E_2) \cup (E_2 - E_1))$. Множество графов с фиксированным множеством вершин называется симметрическим линейным пространством графов (СЛПГ), если оно замкнуто относительно симметрической разности и перестановок вершин. В [2] описаны все СЛПГ, их существует не более 14 при любом количестве вершин. Здесь рассматриваются симметрические линейные пространства двудольных графов (СЛПДГ). СЛПДГ — это множество двудольных графов с фиксированными долями, замкнутое относительно симметрической разности и перестановок вершин внутри каждой доли. Отметим, что СЛПДГ, вообще говоря, не является СЛПГ. Основной результат настоящей работы состоит в том, что при любых размерах долей имеется не более 12 СЛПДГ. Каждое из них является одним из следующих множеств графов:

D1 — все двудольные графы;

D2 — двудольные графы с четным числом ребер;

D3 — двудольные графы, у которых степени всех вершин имеют одинаковую четность;

D4 — двудольные графы, у которых степени всех вершин имеют одинаковую четность, совпадающую с четностью числа ребер;

D5 — двудольные графы, у которых степени вершин одной доли имеют одинаковую четность (два пространства);

D6 — двудольные графы, у которых вершины одной доли имеют четные степени (два пространства);

D7 — двудольные графы с четными степенями всех вершин;

D8 $=$ **D2** $\cap$ **D3** — двудольные графы с четными числом ребер и с вершинами одинаковой четности;

D9 $=$ **D2** $\cap$ **D8** — полный двудольный граф и дизъюнктные объединения двух полных двудольных (граф с одной пустой долей считается полным двудольным);

D10 — полный двудольный и пустой графы.

Замкнутость всех этих множеств относительно симметрической разности легко проверяется.

Теорема. *Если* $\boldsymbol{X}$ *— СЛПДГ, то* $\boldsymbol{X}$ *совпадает с одним из множеств* **D1**–**D10**.

Работа выполнена при финансовой поддержке РФФИ (проект 12-01-00749).

Список литературы

1. Алексеев В. Е., Захарова Д. В. О симметрических пространствах графов // Дискретный анализ и исследование операций. Серия 1. — 2007. — Т. 14, вып. 1. — С. 21–26.

2. Захарова Д. В. Симметрические линейные прстранства графов // Дискретная математика. — 2011. — Т. 23, вып. 2. — С. 104–107.

ИЗБЫТОЧНОСТЬ КОНСТРУКТИВНЫХ ОПИСАНИЙ ГАМИЛЬТОНОВЫХ ПЛАНАРНЫХ ГРАФОВ

М. А. Иорданский (Нижний Новгород)

Рассматриваются обыкновенные непомеченные, конечные, неориентированные графы. Используется *конструктор* графов, включающий вместе с каждым графом его изоморфные копии. К графам конструктора применяется бинарная *операция склейки*, при выполнении которой производится отождествление изоморфных подграфов $G_1' \subseteq G_1$ и $G_2' \subseteq G_2$ графов-операндов G_1 и G_2. Граф $\tilde{G}$, изоморфный подграфам G_1' и G_2', называется *подграфом склейки*.

Конструктивные описания графов задаются суперпозициями операций склейки. В качестве исходных графов-операндов выбираются элементарные графы, обладающие заданным свойством. Для сохранения этого свойства у результирующих графов на операции склейки накладывается система ограничений H, включающая в себя в общем случае ограничения на вид отождествляемых подграфов, их выбор в графах-операндах и способ отождествления [1].

Операции склейки сохраняют отсутствие кратных ребер если каждой паре вершин не смежных в подграфе склейки $\tilde{G}$ соответствуют несмежные вершины хотя бы в одном из графов-операндов. Такие операции обозначаются как $\prec H \succ$-склейки.

Операции H_g-склейки сохраняют свойство гамильтоновости, если $|V(\tilde{G})| = \min\{|V(G_1)|, |V(G_2)|\}$ либо $|V(\tilde{G})| = 2$ и эти две вершины являются смежными в гамильтоновых циклах графов-операндов G_1 и G_2 [1].

Операции H_p-склейки сохраняют свойство планарности, если множества $V(G_1')$ и $V(G_2')$ принадлежат одной грани соответственно в плоских укладках графов G_1 и G_2 и пары отождествляемых вершин выбираются в соответствии с порядком круговых обходов этих граней [2].

Операции, сохраняющие характеристические свойства обыкновенных гамильтоновых планарных графов, обозначаются как операции $\prec H_{gp} \succ$-склейки.

Возможность такого единообразного формулирования условий наследования различных характеристических свойств графов основывается на избыточности, вносимой в задание информации о графах при их конструктивных описаниях. При этом один и тот же граф может быть реализован суперпозициями, обладающими различной избыточностью.

В работе получены оценки избыточности конструктивных описаний обыкновенных гамильтоновых планарных графов для функции шенноновского типа. Исходными графами являются циклы $C_n, n \geq 3$, а отождествляемыми подграфами выбираются цепи L_2 или цепи L_n, $n = \min\{|V(G_1)|, |V(G_2)|\}$, принадлежащие гамильтоновым циклам графов-операндов, либо, при $|V(G_1)| = |V(G_2)|$, гамильтоновы циклы графов-операндов.

Для подсчета величины $I_s(G)$ — избыточности суперпозиции s операций $\prec H_{gp} \succ$-склейки, реализующей граф G, используется формула

$$I_s(G) = \frac{\sum_{i=1}^{q} |E(\tilde{G}_i)|}{|E(G)|},$$

где $\tilde{G}_i$ — подграф склейки i-й операции; q — общее число операций $\prec H_{gp} \succ$-склейки в суперпозиции s.

Пусть $\Im_n$ — множество n-вершинных обыкновенных гамильтоновых планарных графов; S — множество всех суперпозиций операций $\prec H_{gp} \succ$-склейки, реализующих граф $G \in \Im_n$ с использованием подграфов склейки $\tilde{G} \in \{L_2, L_3, L_4, C_4, L_5, C_5, ...\}$. Введем следующие обозначения

$$\min_{s \in S} I_s(G) = I(G), \ \max_{G \in \Im_n} I(G) = I(\Im_n).$$

Теорема. *При* $n \geq 3$

$$1 - \frac{1}{n-2} \leq I(\Im_n) \leq 1.$$

Доказательство. Оценка сверху. Любой обыкновенный планарный гамильтонов граф G, не изоморфный C_n, можно построить с помощью суперпозиции s, для которой величина соответствующей избыточности $I_s(G) \leq 1$. Если граф G, $|E(G)| = m$ внешнепланарный, то для его построения достаточно выполнить $m - n$ раз операцию $\prec H_{gp} \succ$-склейки по подграфу $\tilde{G} \cong L_2$. В противном случае граф G можно рассматривать как результат склейки по C_n двух внешнепланарных графов. В любом случае, число ребер, включенных во все подграфы склейки, не превосходит общего числа ребер графа. В силу произвольности графа G получаем при этом $I(\Im_n) \leq 1$.

Оценка снизу. Рассмотрим произвольную плоскую укладку графа G. Разобьем множество $E(G)$ на два непересекающихся подмножества. В первое подмножество отнесем ребра, принадлежащие внешней грани. Обозначим их число через m_0. Во второе подмножество — внутренние ребра, не принадлежащие внешней грани; их число равно $m - m_0$. При построении плоского графа G из простых циклов $C_n, n \geq 3$ по подграфам склейки $\tilde{G} \in \{L_2, L_3, L_4, C_4, L_5, C_5, \ldots\}$ число ребер в подграфе склейки каждой операции не меньше числа появляющихся при этом внутренних ребер. Таким образом, при любом порядке сборки графа G справедливо соотношение

$$I(G) \geq \frac{m - m_0}{m} = 1 - \frac{m_0}{m}.$$

Поскольку $m_0 \geq 3$, а $m \leq 3n - 6$, то

$$\max_{G \in \Im_n} I(G) \geq 1 - \frac{1}{n-2}.$$

Следствие. *При* $n \to \infty$.

$$I(\Im_n) \to 1.$$

Список литературы

1. Иорданский М. А. Конструктивные описания графов // Дискретный анализ и исследование операций. — 1996. — Т. 3, № 4. — С. 35–63.

2. Иорданский М. А. Конструктивные описания гамильтоновых графов // Вестник Нижегородского университета им. Н. И. Лобачевского. — 2012. – № 3 (1). — С. 137–140.

АСИМПТОТИЧЕСКАЯ ФОРМУЛА ДЛЯ ЧИСЛА ЭЙЛЕРОВЫХ ОРИЕНТАЦИЙ В ГРАФАХ С БОЛЬШОЙ АЛГЕБРАИЧЕСКОЙ СВЯЗНОСТЬЮ

М. И. Исаев (Москва)

Эйлеровой ориентацией графа G называется ориентация его ребер такая, что для любой вершины количество входящих ребер и выходящих ребер одинаково. Пусть $EO(G)$ — число различных Эйлеровых ориентаций. Легко видеть, что $EO(G) = 0$, если степень хотя бы одной вершины G нечетная. Регулярным турниром называется Эйлерова ориентация полного графа K_n.

Неориентированный граф без петель и кратных ребер называется простым.

Известно, что [5]:

1. Задача о точном подсчете числа Эйлеровых ориентаций простого графа G является полной для класса $\#P$. Другими словами, данная задача является трудной с точки зрения теории сложности.

2. Данную задачу можно свести к подсчету числа полных паросочетаний такого класса двудольных графов, для которых это может быть сделано приближенно с большой вероятностью за полиномиальное время.

Даже для полного графа K_n точное выражение числа эйлеровых ориентаций неизвестно, и только асимптотическая формула была получена [6]: при нечетных $n \to \infty$

$$EO(K_n) = \left(\frac{2^{n+1}}{\pi n}\right)^{(n-1)/2} n^{1/2} e^{-1/2} \left(1 + O(n^{-1/2+\varepsilon})\right) \qquad (1)$$

для любого $\varepsilon > 0$.

В настоящей работе обобщен подход [6]. Получена асимптотическая формула для числа Эйлеровых ориентаций в простых графах с большой алгебраической связностью. Данный результат детально представлен ниже, см. теорему 1.

Для простого графа G можно определить следующую $n \times n$ матрицу:

$$Q_{jk} = \begin{cases} -1, & \{v_j, v_k\} \in EG, \\ d_j, & j = k, \\ 0, & \text{в остальных случаях,} \end{cases}$$

где $n = |VG|$, d_j обозначает степень вершины $v_j \in VG$. Матрица $Q = Q(G)$ называется матрицей Лапласа графа G. Собственные значения $\lambda_1 \le \lambda_2 \le \ldots \le \lambda_n$ матрицы Q являются неотрицательными

вещественными числами, причем количество нулевых собственных значений совпадает с количеством компонент связности, в частности, $\lambda_1 = 0$. Число λ_2 называется алгебраической связностью графа G. (Для дополнительной информации о спектральных свойствах матрицы Лапласа см., например, [3, 7].)

По теореме Кирхгофа (матричная теорема о деревьях), см. [4],

$$t(G) = \frac{1}{n}\lambda_2\lambda_3\cdots\lambda_n, \tag{2}$$

где $t(G)$ обозначает число остовных деревьев графа G.

Теорема 1. *Пусть G — простой граф с n вершинами $v_1, \ldots, v_n$, имеющими четную степень, причем алгебраическая связность графа $\lambda_2(G) \geq \gamma n$ для некоторого $\gamma > 0$. Тогда*

$$EO(G) = (1 + \delta(G)) \left(2^{|EG| + \frac{n-1}{2}} \pi^{-\frac{n-1}{2}} \frac{1}{\sqrt{t(G)}} \prod_{(v_j, v_k) \in EG} P_{jk} \right),$$

где d_j — степень вершины v_j, $t(G)$ — число остовных деревьев G,

$$P_{jk} = 1 - \frac{1}{4(d_j+1)^2} - \frac{1}{2(d_j+1)(d_k+1)} - \frac{1}{4(d_k+1)^2},$$

и для любого $\varepsilon > 0$

$$|\delta(G)| \leq C n^{-1/2+\varepsilon},$$

где константа $C > 0$ зависит только от γ и ε.

Замечание 1. Используя (2), число $t(G)$ может быть выражено с помощью главного минора матрицы Лапласа Q.

Замечание 2. Для полного графа $\lambda_2(K_n) = n$, $EK_n = \frac{n(n-1)}{2}$, $t(K_n) = n^{n-2}$,

$$\prod_{\{v_j, v_k\} \in EK_n} P_{jk} = \left(1 - \frac{1}{4n^2} - \frac{1}{2n^2} - \frac{1}{4n^2}\right)^{\frac{n(n-1)}{2}} =$$

$$= \left(e^{\ln\left(1 - \frac{1}{n^2}\right)}\right)^{\frac{n(n-1)}{2}} = e^{-1/2} + O(n^{-1}).$$

Результат теоремы 1 в этом случае сводится к (1).

Работа выполнена под руководством С. П. Тарасова при частичной поддержке гранта РФФИ 11-01-00398а.

Список литературы

1. Isaev M. Asymptotic behaviour of the number of Eulerian circuits // Electronic Journal of Combinatorics. — 2011. — V. 18 (1). — P. 219. — e-print arXiv: 1104.3046.

2. Isaev M. Asymptotic behaviour of the number of Eulerian orientations of graphs // e-print arXiv:1110.2598.

3. Fiedler M. Algebraic connectivity of graphs // Czech. Math. J. — 1973. — V. 23 (98). — P. 298–305.

4. Kirchhoff G. Über die Auflösung der Gleichungen, auf welche man bei der Untersuchung der linearen Verteilung galvanischer Ströme geführt wird // Ann. Phys. Chem. — 1847. — 72. — P. 497–508.

5. Mihail M., Winkler P. On the number of Eulerian orientations of a graph // Algorithmica. — 1996. — V. 16. — P. 402–414.

6. McKay B. The asymptotic numbers of regular tournaments, eulirian digraphs and eulirian oriented graphs // Combinatorica. — 1990. — V. 10. — P. 367–377.

7. Mohar B. The Laplacian spectrum of graphs // Graph Theory, Combinatorics, and Applications. — Wiley, 1991. — V. 2. — P. 871–898.

ОБ ОДНОМ АЛГОРИТМЕ РЕШЕНИЯ ЗАДАЧИ МИНИМАЛЬНОГО K-РАЗРЕЗА

И. В. Козлов (Долгопрудный)

Пусть задан граф $G(V, E) : |V| = n, |E| = m$ (V — множество вершин графа, E — множество ребер) и натуральное число k. Задача минимального k-разреза *(min k-cut)* заключается в поиске разбиения V на k непересекающихся подмножеств $V = \{V_1, \ldots, V_k\}$ такого, чтобы число ребер между подмножествами было минимальным.

Объединение всех ребер между подмножествами будем называть *k-разрезом*. Количество ребер в объединении будем называть величиной разреза.

В случае $k = 2$, 2-разрез будем называть просто разрезом. Соответственно, в этом случае задача минимального k-разреза является

обычной задачей минимального разреза *(min cut)*. В случае $k = 2$, разрез, разделяющий в графе G вершины s и t, будем называть $s-t$ разрезом.

Рассматриваемая задача является расширением классической задачи поиска минимального разреза в графе на случай нескольких ($k > 2$) компонент связности. Поэтому многие методы ее решения являются модифицированными методами решения задачи *min cut*. В свою очередь, задача *min cut* является обобщением задачи поиска минимального разреза в сети *(min s-t cut)*, которая является двойственной к задаче поиска максимального потока.

В работе [1] показано, что задача *min k-cut* при фиксированном k разрешима за полиномиальное время $O(n^{k^2})$. В работе [2], в свою очередь, показано, что задача *min k-cut* не принадлежит классу сложности FPT и, следовательно, если справедлива гипотеза теории параметрической сложности, то у всех точных алгоритмов, решающих данную задачу, параметр k должен входить в показатель степени. Поэтому возникает необходимость поиска различных приближенных алгоритмов.

В работе Сарана и Вазирани [3] были предложены несколько жадных алгоритмов приближенного решения задачи *min k-cut*. В частности, в [3] была предложена схема разделения SPLIT, позволяющая получить $(2 - \frac{2}{k})$-приближенное решение задачи. Напомним схему SPLIT, поскольку она будет далее использоваться в работе.

1. Найти минимальный разрез в графе, увеличивающий число компонент связности, с помощью вспомогательной процедуры.

2. Удалить ребра, принадлежащие найденному разрезу.

3. Повторять шаги 1,2, пока в графе не окажется k компонент связности.

В процессе работы алгоритма минимальный разрез в графе вычисляется $k-1$ раз, поэтому результат работы представим в виде объединения $k-1$ минимального разреза, а трудоемкость алгоритма SPLIT составляет $O(kF)$, где F — время, за которое решается задача *min cut*.

В работе [4] в рамках схемы SPLIT в качестве внутренней процедуры поиска минимального разреза использовался алгоритм Хао-Орлина из работы [5]. В настоящей работе в качестве внутренней процедуры предлагается использовать вероятностный алгоритм Каргера из работы [6]. Этот алгоритм является рекордным по скорости вероятностным алгоритмом типа Лас-Вегас для решения задачи *min cut*.

Совмещая результаты, полученные в работах [4] и [6], получаем

следующую теорему.

Теорема. *Алгоритм SPLIT, использующий в качестве внутренней процедуры поиска минимального разреза вероятностный алгоритм Каргера, находит* $(2 - \frac{2}{k})$*-приближенное решение задачи min k-cut за время* $\tilde{O}(knc^{3/2})$*, где* c *— величина минимального разреза в графе, а* $\tilde{O}(f) = O(f \cdot poly \log n)$.

По имеющимся у автора сведениям, рассмотренный вариант обладает минимальной трудоемкостью среди всех известных алгоритмов, находящих 2-приближенное решение задачи *min k-cut*. Алгоритм допускает обобщение на случай взвешенных графов [6], и его в принципе можно дерандомизировать.

Работа выполнена при поддержке гранта РФФИ 11-01-00398.

Список литературы

1. Goldschmidt O., Hochbaum D. Polynomial algorithm for the k-cut problem // Proceedings of the 29th Annual Symposium on Foundations of Computer Science. — 1988. — P. 444–451.

2. Downey R. Cutting up is hard to do: the parametrized complexity of k-cut and related problems // Electronic Notes in Theoretical Computer Science. — 2003. — V. 78. — P. 205–218.

3. Saran H. Vazirani V. Finding k-cuts within twice the optimal // Proceedings of the 32th Annual Symposium on Foundations of Computer Science. — 1991. — P. 743–751.

4. Козлов И. В. Оценка трудоемкости одного алгоритма решения задачи минимального k-разреза // Труды 54-й научной конференции МФТИ. Управление и прикладная математика. — 2011. — С. 59–60.

5. Hao J. Orlin J. A faster algorithm for finding the minimum cut in a directed graph // Journal of Algorithms. — 1994. — V. 17, № 3. — P. 424–446.

6. Karger D. Random sampling in cut, flow and network design problems // Mathematics of Operations Research. — 1999. — V. 24, № 2. — P. 383–413.

КОНЕЧНЫЕ ПОЛЯ И 1-ХРОМАТИЧЕСКОЕ ЧИСЛО ОРИЕНТИРУЕМЫХ ДВУМЕРНЫХ ПОВЕРХНОСТЕЙ

В. П. Коржик (Черновцы)

Всегда интересно увидеть неожиданную связь между двумя, на первый взгляд совершенно различными, математическими объектами. Конечные поля (поля Галуа) были впервые рассмотрены при исследовании условий, при выполнении которых корни алгебраического уравнения с одним неизвестным можно выразить через коэффициенты с помощью арифметических операций и радикалов. Граф 1-*вложен* в двумерную поверхность, если он нарисован на этой поверхности так, что каждое его ребро пересекается не более чем с одним другим ребром. 1-*хроматическим* числом $\chi_1(S)$ поверхности S называется максимальное хроматическое число графов, которые 1-вкладываются в эту поверхность. Ниже мы показываем непосредственную связь между существованием бесконечного числа конечных полей и возможностью определить с точностью до единицы 1-хроматическое число бесконечного числа ориентируемых поверхностей.

Обозначим через S_p ориентируемую поверхность рода $p \geq 0$. Рингель [1] получил верхнюю границу

$$\chi_1(S_p) \leq R(S_p) = \left\lfloor \frac{9 + \sqrt{64p + 17}}{2} \right\rfloor$$

для каждой ориентируемой поверхности S_p, отличной от сферы, и

$$\chi_1(S_p) \leq \left\lfloor \frac{13 + \sqrt{144p + 25}}{3} \right\rfloor \leq R(S_p),$$

когда $\chi_1(S_p)$ чётное. Рингель выдвинул гипотезу, что эта верхняя граница является точной для всех ориентируемых поверхностей (за исключением, быть может, нескольких поверхностей малого рода). Всё, что известно в литературе относительно 1-хроматического числа ориентируемых поверхностей, это следующее: Рингель [1] показал, что эта верхняя граница является точной для $p = 1, 89$; автор [2] доказал, что

$$R(S_p) - 10 \leq \chi_1(S_p) \tag{1}$$

для каждого $p \geq 0$. Заметим, что сейчас намного больше известно относительно 1-хроматического числа неориентируемых поверхностей: в [3] было найдено точное значение 1-хроматического числа для

примерно 7/12 всех неориентируемых поверхностей и было найдено с точностью до единицы 1-хроматическое число каждой неориентируемой поверхности достаточно большого рода.

Для целого $\ell \geq 0$, ориентируемой ℓ-последовательностью называется такая последовательность $S^{(1)}, S^{(2)}, S^{(3)}, \ldots$ ориентируемых поверхностей, что $R(S^{(i)}) - \ell \leq \chi_1(S^{(i)})$ для $i = 1, 2, \ldots$. Чтобы получить нижнюю границу (1), автор, используя сложные конструкции графов токов, построил ориентируемые 3-последовательности. До настоящего времени не удалось построить ориентируемых ℓ-последовательностей для $\ell \leq 2$.

Известно, что конечное поле $F(n)$ порядка $n > 1$ существует (и есть единственным, с точностью до изоморфизма) тогда и только тогда, когда $n = p^r$, где p — простое число, r — положительное целое число. Для $p \neq 2$, имеем или $p \equiv 1 \pmod 4$ (в этом случае $p^r \equiv 1 \pmod 4$ для каждого $r \geq 1$), или $p \equiv 3 \pmod 4$ (в этом случае $p^{2r} \equiv 1 \pmod 4$ для каждого $r \geq 1$). Таким образом, существует бесконечно много конечных полей $F(n)$, $n \equiv 1 \pmod 4$. Поле имеет две бинарные операции: $+$ (сложение) и умножение. Для каждого конечного поля $F(n)$ существует элемент ε (называемый первообразным корнем этого поля) такой, что элементы $1, \varepsilon, \varepsilon^2, \varepsilon^3 \ldots, \varepsilon^{n-2}$ есть все ненулевые элементы этого поля.

Теорема. *Если существует конечное поле $F(n)$ порядка $n = 4m + 1$, где m — целое число, $m \geq 3$, то*

$$8m + 2 \leq \chi_1(S_{4m^2-m+1}) \leq 8m + 3 = R(S_{4m^2-m+1}).$$

Схема доказательства. Рассмотрим полный граф K_n, множеством вершин которого есть множество всех элементов поля $F(n)$. Пусть ε — первообразный корень этого поля. Для каждого $x \in F(n)$, обозначим через $H(x)$ $(n-1)$-угольную грань, границей которой есть цикл $x + 1, x + \varepsilon, x + \varepsilon^2, x + \varepsilon^3, \ldots, x + \varepsilon^{n-2}$ графа K_n. Эти n $(n-1)$-угольных граней есть все грани такого вложения графа K_n в ориентируемую поверхность рода $1 - n + \frac{n(n-1)}{4}$, каждые две грани которого имеют общее ребро. Для каждой грани этого вложения, добавим новую вершину в середину этой грани и соединим эту новую вершину ребрами со всеми вершинами этой грани и со всеми новыми добавленными вершинами в смежных гранях. Получим 1-вложение графа K_{2n} без 1-фактора. Добавляя $\lfloor \frac{n}{2} \rfloor + 1$ ручек, можно вложить все рёбра этого 1-фактора. Получаем 1-вложение графа $K_{2n} = K_{8n+2}$ в ориентируемую поверхность рода $4m^2 - m + 1$, что

и завершает доказательство теоремы.

Полное доказательство этой теоремы приведено в [4].

Список литературы

1. Ringel G. A nine color theorem for the torus and the Klein bottle // The Theory and Applications of Graphs. — New York: Wiley, 1981. — P. 507–515.

2. Korzhik V. A tighter bounding interval for the one-chromatic number of a surface // Discrete Math. — 1997. — V. 169. — P. 95–120.

3. Korzhik V. On the 1-chromatic number of nonorientable surfaces with large genus //Journal of Combin. Theory Ser. B. — 2012. — V. 102. — P. 283–328.

4. Korzhik V. Finite fields and the 1-chromatic number of orientable surfaces // Journal of Graph Theory. — 2010. — V. 63. — P. 179–184.

СПЕКТР ХРОМАТИЧЕСКИХ ЧИСЕЛ СПИНАЛЬНЫХ КВАДРАНГУЛЯЦИЙ ЗАМКНУТОЙ ПОВЕРХНОСТИ

С. А. Лавренченко (Москва)

Квадрангуляцией сферы с g ручками S_g с конечным, неориентированным, без петель и кратных ребер графом G называется 2-клеточная укладка $G \hookrightarrow S_g$, у которой каждый регион ограничен циклом длины 4 графа G. *Хроматическое число* графа G, а также любой квадрангуляции с этим графом, обозначается $\chi(G)$ и определяется как минимальное число цветов, достаточное для раскраски вершин у G так, чтобы никакая пара смежных вершин не была бы раскрашена одинаково. *Число Бетти* (первое) связного графа G выражается формулой $\beta(G) = |E(G)| - |V(G)| + 1$, где $|V(G)|$ и $|E(G)|$ — мощности множеств вершин и ребер у G (соответственно). *Двойное сплетение* графа G есть граф, обозначаемый $G[:]$, с множеством вершин $V(G[:]) = V(G') \cup V(G'')$, где G' и G'' — две непересекающиеся копии графа G, и с множеством ребер $E(G[:]) = E(G') \cup E(G'')$ плюс ребра, соединяющие каждую вершину $v' \in V(G')$ с каждой вершиной в G'', смежной соответствующей вершине $v'' \in V(G'')$ (но не с самой v''). Следующая лемма доказана в [1].

Лемма 1. *Для любого нетривиального связного графа G существует квадрангуляция $G[:] \hookrightarrow S_{\beta(G)}$.*

Любая квадрангуляция вида $G[:] \hookrightarrow S_{\beta(G)}$ называется *спинальной квадрангуляцией рода $g = \beta(G)$ с позвоночником G*. По лемме 1

род спинальной квадрангуляции равен числу Бетти позвоночника. Следующая лемма — очевидное, но полезное наблюдение.

Лемма 2. $\chi(G[:]) = \chi(G)$.

Следствие 3. *Для любого нетривиального дерева T любая укладка $T[:] \hookrightarrow S_0$ есть бихроматическая квадрангуляция сферы.*

В этой заметке устанавливается следующий квадратичный аналог известного результата [2] о триангуляциях (цитируемого в учебнике Уайта [3]) и доказывается полнота полученного спектра хроматических чисел при фиксированном роде. Через $\beta(K_n) = \frac{1}{2}(n-1)(n-2)$ обозначается число Бетти полного графа K_n на n вершинах.

Теорема 4. *Для любых целых чисел $g \geq 0$ и $n \geq 2$ таких, что $g \geq \beta(K_n)$, существует спинальная квадрангуляция поверхности S_g с хроматическим числом n.*

Доказательство. По леммам 1 и 2 в качестве позвоночника достаточно взять любой граф G с $\beta(G) = g$ и $\chi(G) = n$. Чтобы построить такой позвоночник, берем K_n. Если $\beta(K_n) = g$, позвоночник готов. Если же $\beta(K_n) < g$, берем лестничный граф с $g - \beta(K_n)$ независимыми циклами и отождествляем одну из его вершин с какой-нибудь вершиной у K_n. Теорема доказана.

Ниже показывается, что полученный спектр хроматических чисел $\{n\}$ полон при любом фиксированном роде $g \geq 0$.

Утверждение 5. *Для любого связного графа G имеем*

$$(2\chi(G) - 3)^2 \leq 1 + 8\beta(G). \tag{1}$$

Доказательство. Индукция по числу вершин у G. Заметим, что неравенство (1) справедливо для $G = K_1$ и K_2. Предположим, что (1) справедливо для любого связного графа с $\leq n$ вершинами, и пусть G — связный граф с $n+1$ вершиной ($n \geq 2$). Обозначим через H граф, получаемый из G удалением одной вершины v такой, что H остается связным. Тогда, очевидно,

$$\beta(G) = \beta(H) + \deg_G(v) - 1, \tag{2}$$

где $\deg_G(v)$ обозначает степень вершины v в G.

Случай 1. $\chi(G) = \chi(H)$. Тогда по предположению индукции имеем $(2\chi(G) - 3)^2 = (2\chi(H) - 3)^2 \leq 1 + 8\beta(H) \leq 1 + 8\beta(G)$.

Случай 2. $\chi(G) = \chi(H) + 1$. Тогда $\deg_G(v) \geq \chi(H)$ и в силу (2) $\beta(G) \geq \beta(H) + \chi(H) - 1$, и поэтому $(2\chi(G) - 3)^2 = (2\chi(H) - 3)^2 + 8\chi(H) - 8 \leq 1 + 8\beta(H) + 8\chi(H) - 8 \leq 1 + 8\beta(G)$. Утверждение доказано.

Род любой спинальной квадрангуляции с позвоночником G равен $g = \beta(G)$ по лемме 1, а хроматическое число равно $n = \chi(G)$ по лемме 2. С учетом этих равенств неравенство $g \geq \beta(K_n) = \frac{1}{2}(n-1)(n-2)$ в условии теоремы 4 путем стандартных алгебраических преобразований приводится к неравенству (1) и, значит, на самом деле не является ограничительным в классе спинальных квадрангуляций.

Попутно получаются следующие оценки на хроматическое число произвольного связного графа, где нижняя оценка получена в [4]. (Обе оценки достигаются на полных графах.)

Следствие 6. *Для любого связного графа G имеем*

$$\frac{|V(G)|^2}{|V(G)|^2 - 2|E(G)|} \leq \chi(G) \leq \frac{3 + \sqrt{9 - 8|V(G)| + 8|E(G)|}}{2}.$$

В заключение дадим толкование термина «спинальная квадрангуляция». *Топологический d-мерный полиэдр* $|K|$ есть топологическая криволинейная реализация $K \hookrightarrow \mathbf{R}^n$ абстрактного конечного симплициального комплекса K размерности $d \leq n-1$. Обозначим через $N^n = N^n(|K|)$ замкнутую регулярную окрестность у $|K|$, а через $\beta_k(|K|)$ — k-е число Бетти у $|K|$. Стандартная композиция изоморфизмов, $\tilde{H}_k(\partial N^n; \mathbf{Q}) \cong \tilde{H}_k(N^n; \mathbf{Q}) \oplus \tilde{H}_k(\mathbf{R}^n - N^n; \mathbf{Q}) \cong \tilde{H}_k(|K|; \mathbf{Q}) \oplus H_{n-k-1}(|K|; \mathbf{Q})$, в которой первый изоморфизм из точной последовательности Майера-Вьеториса, а второй обеспечивается двойственностью Александера, приводит к следующей формуле:

$$\beta_k(\partial N^n(|K|)) = \beta_k(|K|) + \beta_{n-k-1}(|K|), \tag{3}$$

где $0 \leq k \leq n-1$. При $n = 3$ граница ∂N^3 — несвязное объединение топологических сфер с ручками. Обозначим общее число ручек через $\sharp\mathrm{hand}\,\partial N^3$. При $n = 3$ и $k = 1$ формула (3) сводится к такой: $\sharp\mathrm{hand}\,\partial N^3(|K|) = \beta_1(|K|)$ для любого 1- или 2-мерного полиэдра $|K|$ в $\mathbf{R}^3$. Более конкретно, для любого связного вложенного в $\mathbf{R}^3$ графа G имеем $\sharp\mathrm{hand}\,\partial N^3(G) = \beta(G)$. Тело $N^3(G)$ известно в топологии как *тело с ручками*, причем G называется его *позвоночником*. Таким образом, *род тела с ручками с позвоночником G равен числу Бетти позвоночника G*. Теперь лемму 1 можно перефразировать так: *двойное сплетение графа G квадрангулирует границу любого тела с ручками с позвоночником G*. Таким образом, граф G естественно называть позвоночником любой квадрангуляции $G[:] \hookrightarrow S_{\beta(G)}$, а саму квадрангуляцию спинальной.

Список литературы

1. White A. T. On the genus of the composition of two graphs // Pacific j. math. — 1972. — V. 41, № 1. — P. 275–279.

2. Harary F., Lawrencenko S., Korzhik V. Realizing the chromatic numbers of triangulations of surfaces // Discrete math. — 1993. — V. 122, № 1–3. — P. 197–204.

3. White A. T. Graphs of groups on surfaces: interactions and models. — Amsterdam: North-Holland, 2001.

4. Myers B. R., Liu R. A lower bound on the chromatic number of a graph // Networks. — 1971. — V. 1, № 3. — P. 273–277.

О РЕБЕРНОЙ РАСКРАСКЕ ДВУДОЛЬНОГО ГРАФА

А. М. Магомедов (Махачкала)

Максимальную степень вершины графа будем обозначать через Δ, количество вершин — через n. Определим рёберную Δ-раскраску графа $G = (X, Y, E)$ как сюръекцию $E \to \{1, \ldots, \Delta\}$. Рёберную Δ-раскраску графа G будем называть *интервальной*, если в любой вершине v графа цвета инцидентных рёбер образуют набор из $d_G v$ последовательных целых положительных чисел.

Двудольный граф $G = (X, Y, E)$ называется (α, β)–*бирегулярным*, если степень каждой вершины множества X равна α, а степень каждой вершины множества Y равна β.

Известно, например, что любой $(\Delta, 2)$–бирегулярный граф обладает интервальной Δ–раскраской при чётном Δ и интервальной $(\Delta + 1)$–раскраской — при нечётном Δ. С привлечением компьютерных вычислений в [1] доказано, что каждый двудольный граф с $n \leq 14$ интервально-раскрашиваем. В [2] установлена NP-полнота задачи об интервальной раскрашиваемости двудольного графа.

Двудольные графы, не допускающие интервальной раскраски, построены С. В. Севастьяновым, M. Malafiejcki, A. Hertz, D. de Werra и P. Erdős. Отметим, что ни один из них не является бирегулярным.

В [3] установлена NP-полнота задачи об интервальной 6-раскрашиваемости $(6, 3)$-бирегулярного графа. Построим $(6, 3)$–бирегулярный граф $G = (X, Y, E)$ с $n = 33$: $X = \{x_1, \ldots, x_{11}\}$, $Y = \{y_1, \ldots, y_{22}\}$, множество рёбер E представим списками смежности вершин множества X:

$x_1(y_1, y_2, y_3, y_4, y_5, y_6)$, $x_2(y_1, y_2, y_3, y_4, y_7, y_8)$,

$x_3(y_5, y_6, y_7, y_8, y_9, y_{10})$, $x_4(y_1, y_2, y_3, y_4, y_{11}, y_{12})$,
$x_5(y_9, y_{10}, y_{11}, y_{12}, y_{13}, y_{14})$, $x_6(y_5, y_6, y_{13}, y_{14}, y_{15}, y_{16})$,
$x_7(y_7, y_8, y_{16}, y_{17}, y_{21}, y_{22})$, $x_8(y_9, y_{10}, y_{15}, y_{17}, y_{19}, y_{20})$,
$x_9(y_{11}, y_{12}, y_{15}, y_{18}, y_{21}, y_{22})$, $x_{10}(y_{13}, y_{14}, y_{16}, y_{18}, y_{19}, y_{20})$,
$x_{11}(y_{17}, y_{18}, y_{19}, y_{20}, y_{21}, y_{22})$.

Утверждение. *Бирегулярный граф $G = (X, Y, E)$ не допускает интервальной 6-раскраски.*

Перейдем к интервальной Δ-раскраске двудольного мультиграфа. Набор параллельных рёбер будем называть *пучком*. Интервальную раскраску мультиграфа будем называть *интервальной в пучке*, если цвета рёбер пучка различны и образуют интервал.

Задача о раскраске двудольного мультиграфа. Условие: Задан двудольный мультиграф $G = (X, Y, E)$, где $X = \{x_1, x_2\}$, $d_G x_1 = d_G x_2 = \Delta$, $d_G y \leq \lceil \Delta/2 \rceil$ для каждой вершины $y \in Y$.

Вопрос: Существует ли интервальная Δ-раскраска мультиграфа G, интервальная в каждом пучке?

Теорема. *Задача о раскраске двудольного мультиграфа NP-полна.*

Напомним [4], что если $\min\{|X|, |Y|\} \leq 3$, то для любого *простого* двудольного графа $G = (X, Y, E)$ рёберная интервальная раскраска существует.

Работа выполнена при финансовой поддержке госзадания (проект 1.1923.2011).

Список литературы

1. Giaro K. Compact task scheduling on dedicated processors with no waiting period (in Polish). PhD thesis. — Technical University of Gdansk, IETI Faculty. Gdansk, 1999.

2. Севастьянов С. В. Об интервальной раскрашиваемости рёбер двудольного графа // Методы дискретного анализа. — 1990. — Т. 50. — С. 61–72.

3. Asratian A. S., Casselgren C. J. Some results on interval edge colorings of (α, β)-biregular bipartite graphs // Department of Mathematics, Linkoping University S–581 83, Sweden, 2007.

4. Giaro K., Kubale M., Malafiejcki M. On the deficiency of bipartite graphs // Discrete Applied Mathematics. — Gdansk, 1999. — V. 94. — P. 193–203.

РАСШИРЯЮЩИЕ ОПЕРАТОРЫ ПРИМЕНИТЕЛЬНО К ЗАДАЧЕ О НЕЗАВИСИМОМ МНОЖЕСТВЕ

Д. С. Малышев (Нижний Новгород)

К настоящему времени накоплено огромное количество фактов о полиномиальной разрешимости и о NP-полноте тех или иных задач при самых различных ограничениях. Достаточно напомнить, что поисковая машина компании Google выдает примерно 13000000 результатов поиска по запросу «NP-completeness» и примерно 400000 результатов поиска по запросу «polynomial-time solvability». Направляющие мотивы к получению новых сведений такого рода могут быть самими разнообразными, но можно выделить два наиболее распространенных:

1. Поиск более широких «простых» классов, объемлющих ранее известные.

2. Поиск NP-полных сужений для известных «сложных» случаев.

Вместе с тем, при рассмотрении целых семейств классов индивидуальных входных данных той или иной массовой задачи можно ставить проблемы более общего характера, чем анализ сложности для конкретного класса. В частности, можно поставить целью выявление пределов, до которых возможны расширения полиномиальной сложности и сужения с «противоположным» сложностным статусом. Другой целью может быть выявление «универсальных» (т. е. пригодных для многих семейств входных данных) расширяющих (сужающих) преобразований, сохраняющих полиномиальную разрешимость (NP-полноту). В настоящей публикации формулируются два таких преобразования применительно к задаче о независимом множестве в семействе наследственных классов графов.

Класс графов $\mathcal{X}$ называется *наследственным*, если он замкнут относительно изоморфизма и удаления вершин. Любой наследственный класс (и только наследственный класс) графов $\mathcal{X}$ может быть задан множеством своих запрещенных порожденных подграфов $\mathcal{S}$. В этом случае принята запись $\mathcal{X} = \mathcal{F}ree(\mathcal{S})$. Совокупность наследственных классов графов является достаточно представительным континуальным семейством и включает такие известные подсемейства, как множества монотонных и минорно замкнутых классов графов.

Пусть П — какая-нибудь NP-полная задача на графах. Наследственный класс графов с полиномиально разрешимой задачей П будем далее называть П-*простым*. Все известные автору результаты работ по выявлению новых случаев эффективной разрешимости задач на графах используют в значительной мере специфику

старых, более узких случаев. Вместе с тем (как уже было отмечено ранее), хотелось бы иметь «универсальные» обобщения такого рода. Именно, предлагается рассматривать такие преобразования $f : \mathcal{S} \longrightarrow \mathcal{S}'$ (функции одного или многих (неизвестных) аргументов — графов из части $\mathcal{S}$), что $\mathcal{F}ree(\mathcal{S}) \subset \mathcal{F}ree(\mathcal{S}')$ и из П-простоты класса $\mathcal{F}ree(\mathcal{S})$ следовала бы П-простота класса $\mathcal{F}ree(\mathcal{S}')$. Такого рода преобразования мы будем называть П-*расширяющими операторами.*

Полезность понятия расширяющего оператора состоит в том, что конкретные операторы такого рода позволяют конструктивно («регулярным образом») порождать новые П-простые случае. Например, если $\mathcal{F}ree(\mathcal{S})$ — конкретный П-простой класс, а f — расширяющий оператор, для которого $\mathcal{S}$ входит в область его определения, то $\mathcal{F}ree(f(\mathcal{S})), \mathcal{F}ree(f(f(\mathcal{S}))), \mathcal{F}ree(f(f(f(\mathcal{S}))))$ — монотонно возрастающая бесконечная цепь (по отношению включения) из П-простых классов. Заметим, что такие трансформации могут быть особенно полезными, когда известно сразу несколько расширяющих операторов (поскольку можно рассматривать действия их суперпозиций). Заметим также, что понятие расширяющего оператора может быть применено к любой задаче на графах, а не только к задаче о независимом множестве.

В настоящей работе рассматривается случай, когда П — задача о независимом множестве (далее задача НМ, т. е. задача определения в обыкновенном графе множества попарно несмежных вершин наибольшей мощности) и когда $\mathcal{S} = \{P_5, C_5, G\}$. Интерес к наследственным подклассам $\mathcal{F}ree(\{P_5, C_5\})$ не случаен. Так, среди всех связных графов G с пятью вершинами случай простого пути является единственным, для которого статус задачи НМ в классе $Free(\{G\})$ остается открытым вопросом [1]. Там же доказано, что для любого графа G с не более чем 5 вершинами, отличного от P_5 и C_5, задача НМ полиномиально разрешима в классе графов $\mathcal{F}ree(\{P_5, G\})$. Вопрос для класса $\mathcal{F}ree(\{P_5, C_5\})$ пока остается открытым.

Далее будут указаны два конкретных НМ-расширяющих оператора. Под *суммой* $G_1 \oplus G_2$ понимается объединение графов G_1 и G_2 с непересекающимися множествами вершин. Под *произведением* $G_1 \circ G_2$ графов G_1 и G_2 понимается граф $(V(G_1) \cup V(G_2), E(G_1) \cup E(G_2) \cup V(G_1) \times V(G_2))$. В работах [2] и [3] соответственно доказаны следующие утверждения.

Теорема 1. *Преобразование* $\{P_5, C_5, G\} \longrightarrow \{P_5, C_5, G \circ K_1\}$ *является НМ-расширяющим оператором.*

Теорема 2. *Для любого* p *преобразование* $\{P_5, C_5, G\} \longrightarrow$

$\{P_5, C_5, G \circ O_2, G \oplus K_{1,p}\}$ *является НМ-расширяющим оператором.*

Работа выполнена при поддержке РФФИ (проект № 11-01-00107-а), при поддержке ФЦП «Научные и научно-педагогические кадры инновационной России на 2009-2013» (ГК № 16.740.11.0310) и лаборатории алгоритмов и технологий анализа сетевых структур НИУ-ВШЭ, грант Правительства РФ, дог. № 11.G34.31.0057,

Список литературы

1. Mosca R. Some observations on maximum weight stable sets in certain P // European Journal of Operational Research. — 2008. — V. 184, №3. — P. 849–859.

2. Малышев Д. С. Полиномиальная разрешимость задачи о независимом множестве для графов без порожденных простого пути и простого цикла с пятью вершинами и обобщения порогового графа // Дискретный анализ и исследование операций. — (Направлено в журнал.)

3. Малышев Д. С. Расширяющие операторы для задачи о независимом множестве // Дискретный анализ и исследование операций. — (Направлено в журнал.)

СТРУКТУРНЫЕ И СЛОЖНОСТНЫЕ ХАРАКТЕРИСТИКИ КЁНИГОВЫХ ГРАФОВ ОТНОСИТЕЛЬНО 3-ПУТЕЙ

Д. Б. Мокеев (Нижний Новгород)

Пусть $\mathbf{X}$ — множество графов. $\mathbf{X}$-*упаковкой* графа G называется множество его непересекающихся порожденных подграфов, каждый из которых изоморфен какому-нибудь графу из $\mathbf{X}$. Наибольшее число подграфов в $\mathbf{X}$-упаковке графа G будем обозначать через $pack(\mathbf{X}; G)$. $\mathbf{X}$-*покрытием* графа G называется множество вершин, после удаления которых получается граф, не содержащий порожденных подграфов, принадлежащих $\mathbf{X}$. Наименьшее число вершин в $\mathbf{X}$-покрытии графа G будем обозначать через $cover(\mathbf{X}; G)$. В случае, когда $\mathbf{X}$ состоит из единственного графа H, будем говорить просто об H-покрытии и H-упаковке. В частности, K_2- упаковки — это паросочетания, а K_2-покрытия известны как вершинные покрытия.

Очевидно, всегда выполняется неравенство $pack(\mathbf{X}; G) \leq \leq cover(\mathbf{X}; G)$. Теорема Кёнига утверждает, что для двудольных графов имеет место равенство $pack(P_2; G) = cover(P_2; G)$. Верно и в

известном смысле обратное утверждение: если это равенство выполняется для графа G и любого его порожденного подграфа, то этот граф — двудольный.

Граф G будем называть *кёниговым* графом относительно множества $\mathbf{X}$, если для любого его порожденного подграфа H выполняется равенство $pack(\mathbf{X}; H) = cover(\mathbf{X}; H)$. Класс всех кёниговых графов относительно $\mathbf{X}$ обозначим через $\mathbf{K}(\mathbf{X})$.

Класс $\mathbf{K}(\mathbf{X})$ при любом $\mathbf{X}$ является наследственным и, следовательно, может быть описан множеством минимальных запрещенных (порожденных) подграфов. Для P_2 такую характеризацию дает теорема Кёнига вместе с известным критерием двудольности. Кроме этой классической теоремы нам известен еще только один результат такого рода для обыкновенных графов — в работе [1] описаны все запрещенные подграфы для класса $\mathbf{K}(\mathbf{C})$, где $\mathbf{C}$ — множество всех простых циклов.

Цель настоящей работы — охарактеризовать и дать алгоритм распознавания графов класса $\mathbf{K}(P_3)$. Применяется "конструктивный" подход к описанию этого класса: показано, как можно построить любой граф из этого класса с помощью операций подразбиения ребер и замены вершин кликами. На этом подходе построен полиномиальный алгоритм распознавания кёниговых относительно 3-пути графов.

Далее вместо $pack(P_3; G)$ и $cover(P_3; G)$ пишем просто $pack(G)$ и $cover(G)$, под покрытием и упаковкой подразумеваем P_3-покрытие и P_3-упаковку, а под кёниговым графом — кёнигов граф относительно P_3.

Заметим, что граф кёнигов тогда и только тогда, когда каждая его компонента связности — кёнигов граф. Поэтому мы будем рассматривать только связные графы.

Операция замены вершины x t-кликой состоит в том, что эта вершина удаляется из графа, к нему добавляются t новых вершин, все они попарно соединяются между собой и каждая из них соединяется ребром с каждой вершиной, с которой была смежна x. Граф, получаемый из графа G заменой некоторых его вершин степени 1 и 2 кликами (возможно, разного размера), назовем расширением графа G, а клики, на которые были заменены вершины, будем называть секциями. Каждая вершина, не подвергавшаяся замене, считается отдельной секцией.

Лемма. *Каждое наименьшее покрытие любого расширения любого графа состоит из целых секций.*

Связные графы из класса $\mathbf{K}(P_3)$ удобно разделить на две категории: расширенные циклы и все остальные графы, их будем называть

ординарными.

Пусть H — мультиграф без петель. Каждое цикловое ребро (ребро, принадлежащее какому-нибудь циклу) этого мультиграфа подразобьем двумя вершинами. Эти вершины будем называть новыми. Заменим каждую новую вершину и каждую вершину степени 1 или 2, не принадлежащую циклу, какой-нибудь кликой. Полученный таким образом граф будем называть 2-расширением исходного мультиграфа.

Теорема 1. *Любой ординарный кёнигов граф является 2-расширением некоторого мультиграфа, отличного от простого цикла.*

Для расширений циклов справедлива следующая теорема.

Теорема 2. *Расширение цикла C_n является кёниговым графом тогда и только тогда, когда не существует трёх секций из двух и более вершин, расстояние между которыми равно k_1, k_2, k_3 соответственно, где $k_1 \equiv k_2 \equiv k_3 \equiv 1(mod 3)$ и $k_1 \geq 4, k_2 \geq 4, k_3 \geq 4$.*

Назовём две вершины x и y подобными, если они смежны и если любая другая вершина, смежная с x смежна и с y.

Из представленного "конструктивного" описания кёниговых графов непосредственно следует алгоритм распознавания таких графов:

G — связный граф. $\forall v \in V(G)\ w(v) = 1$

while $\exists (x, y) \in E(G), x$ и y подобны *do* $\{\ w(x) = w(x) + w(y)$, удалить вершину y. Полученный граф обозначим $G_0.\}$

if $\exists v \in V(G_0), w(v) > 1$ & $deg(v) > 2$ *then* Граф G не кёнигов. Конец.

if $\forall v \in V(G_0) w(v) = 2$ *then* см. п. 6 **else** см. п. 7

if $\exists v_1, v_2, v_3, d(v_1, v_2) = k_1, d(v_2, v_3) = k_2, d(v_3, v_1) = k_3$, где $k_1 \equiv k_2 \equiv k_3 \equiv 1(mod 3)$ и $k_1 \geq 4, k_2 \geq 4, k_3 \geq 4$ *then* Граф G не кёнигов. Конец. **else** Граф G кёнигов. Конец.

$\forall v \in V(G_0) deg'(v) = deg(v), g(v) = -1$

if G_0 — дерево *then* Граф G кёнигов *else* Разобьём G_0 на блоки.

$B_1, B_2, ..., B_k$ — блоки G_0, состоящие из 3 и более вершин

$for\ i = 1\ to\ k\ do$

$\{$

Выберем в B_i вершины $v_0, v_1, v_2, ..., v_{n-1}$, составляющие цикл, где $deg'(v_0) \geq 3$

$\forall i = 1...n-1\ g(v_i) = i\ mod\ 3$

if n не делится на 3 *then* Граф G не кёнигов. Конец.

if $\exists v \in B_i, g(v) = 0$ & $w(v) > 1$ *then* Граф G не кёнигов. Конец.

if $\exists v \in B_i, g(v) > 0$ & $deg'(v) > 2$ *then* Граф G не кёнигов. Конец.

Повторить для каждого цикла блока B_i
}
Граф G кёнигов. Конец.

Теорема 3. *Трудоёмкость представленного алгоритма — $O(nm)$, где n — число вершин графа, а m — число его рёбер.*

Работа выполнена при финансовой поддержке РФФИ (проекты 11-01-00107-а и 12-01-00749-а), ФЦП Научные и научно-педагогические кадры инновационной России на 2009–2012 гг. (номер ГК 16.740.11.0310), при поддержке лаборатории алгоритмов и технологий анализа сетевых структур НИУ ВШЭ, грант Правительства РФ (дог. 11.G34.31.0057)

Список литературы

1. Ding G., Xu Z., Zang W. Packing cycles in graphs. II // Journal of Combinatorial Theory. Ser. B. — 2003. — V. 87. — P. 244–253.

СВОЙСТВА ГРАФОВ МИНИМАЛЬНЫХ БАЗИСОВ ПРОЕКТИВНОЙ ПЛОСКОСТИ И ТОРА

В. И. Петренюк, А. Я. Петренюк (Кировоград)

Проверим: 1) гипотезу о покрытии каждого графа из минимального базиса множества миноров непроективних графов двумя графами, гомеоморфными одному из графов множества $\{K_5, K_{3,3}\}$, 2) гипотезу о покрытии каждого графа из минимального базиса множества миноров нетороидальных графов парой или тройкой графов, гомеоморфных, либо графу K_5, либо графу $K_{3,3}$. Понятия минимальных базисов множества миноров непроективных графов и множества миноров нетороидальных графов введены с целью уменьшения объёма информации. Все остальные элементы множества минимальных относительно операций сжатия или удаления рёбер непроективних графов (т. е. миноров для проективной плоскости), приведены в [1, 1с]. Отметим, что минимальный базис множества минимальных непроективных графов приведен в [1а, 1в, 3, 5], а специфические преобразования графов, описанные в [4], вносят частичный порядок и заключаются в следующих действиях: 1) удалении висячих рёбер и изолированых вершин, 2) сжатии в точку ребер с концевими вершинами (по меньшей мере одной) степени 2 или концевые вершины степени не менее 3; 3) Замене звезды с тремя лучами на простой

цикл длины 3 на концевых вершинах лучей; 4) Подразбиение новой вершиной ребра с концевыми вершинами степени 3 и замена каждой звезды с центрами в концевых вершинах на треугольники с общей новой вершиной. Идея этих преобразований и преобразований по расщеплению вершин, приведенных в [1а, 1в, 3] и названых $Y\triangle$-преобразованиями, заключается в таких манипуляциях над вершинами степени 3, некоторыми рёбрами или гранями заданого графа, которые минимизируют число граней и не приводять к замене эйлеровой характеристики графа. В [3] введено понятие минимального базиса множества минимальных непроэктивных графов и доказана полнота списка из 12-ти графов, а также предложен метод релятивных компонент с целью построения минимальных графов G эйлерового рода $\gamma(G)$ для замкнутой поверхности S рода $\gamma(S)$, где $\gamma(G) = \gamma(S) + 1$.

Теорема 1. *Имеют место следующие соотношения:*

1. *Множество рёбер каждого графа минимального базиса проективной плоскости покрывается объединением множеств рёбер пары графов гомеоморфных одному из графов* $\{K_5, K_{3,3}\}$, *причём один из них может не иметь одного ребра.*

2. *Удаление произвольного ребра* (a, b) *из произвольного базисного графа* G *проективной плоскости приводит к тому, что один из двух графов покрытия содержит множество точек* $\{a, b\}$ *с числом достижимости на проективной плоскости равным* 2.

Доказательство имеет конструктивный характер. Примером может служить покрытие базисного графа A_2 парой графов $(K_5, K_5 \backslash (a, b))$.

Теорема 2. *Имеют место следующие соотношения:*

1. *Множество рёбер каждого графа минимального базиса тора покрывается объединением множеств рёбер пары, тройки или четвёрки графов гомеоморфных одному из графов* $\{K_5, K_{3,3}\}$, *причём не более трёх из них могут не иметь одного ребра.*

2. *Удаление произвольного ребра* (a, b) *из произвольного базисного графа* G *тора приводит к тому, что один из двух графов покрытия содержит множество точек* $\{a, b\}$ *с числом достижимости на торе, равным* 2.

Доказательство носит конструктивный характер.

Список литературы

1. Archdeacon D. A Kuratowski theorem for the projective plane // J. Graph Theory. — 1981. — V. 5, № 3. — P. 243–246.

1a. Bodendiek R., Schumacher H., Wagner K. Die Minimalbasis der Menge aller nicht in die projektive Ebene einbettbaren Graphen // J.

Reine Angew. Math.. — 1981. — V. 327. — P. 119–142.

1b. Bodendiek R., Schumacher H., Wagner K. Uber Relationen auf Graphenmengen // Abh. Math. Sem. Univ. Hamburg. — 1981. — V. 51. — P. 232–243.

1c. Bodendiek R., Schumacher H., Wagner K. Zur Minimalstruktur dernicht in die projektive Ebene einbettbaren Graphen // J. Reine Angew. Math. — 1981. — V. 321. — P. 99–112.

2. Bodendiek R., Schumacher H., Wagner K. Uber Graphen auf Flachen und Spindelchen // Graphs in research and teaching. — Kiel, 1985. — P. 18–47.

3. Bodendiek R., Schumacher H., Wagner K. A characterization of the minimal basis of the torus // Combinatorica. — 1986. — V. 6, № 3. — P. 245–260.

4. Epifanov G.V. Reduction of a plane graph to an edge by star-triangle transformations // Dokl. Akad. Nauk SSSR. — 1966. — V. 166. — P. 19–22.

5. Truemper K. On the delta-wye reduction for planar graphs // J. Graph Theory. — 1989. — V. 13, № 2. — P. 141–148.

ПЕРЕЧИСЛЕНИЕ НЕИЗОМОРФНЫХ КУБИЧЕСКИХ РАЗЛОЖЕНИЙ ГРАФА K_{10}

Д. А. Петренюк (Киев), А. Я. Петренюк (Кировоград)

Кубическим разложением графа K_n будем называть разложение этого графа на регулярные компоненты степени 3 (кубические подграфы). Рассмотрим условия существования разложений графа K_n на регулярные компоненты степени $k > 2$. Первое необходимое условие существования разложений графа K_n на компоненты, каждая из которых является регулярным графом степени $k > 2$, следует из того, что из каждой вершины графа выходит число ребер, кратное числу k, и имеет вид:

$$n = 1 \pmod{k}. \tag{1}$$

Еще одно необходимое условие разложения графа K_n на регулярные подграфы степени $k > 2$ заключается в равенстве суммарного количества ребер всех компонент разложения порядку графа. Количество ребер регулярного графа порядка m степени k равно $km/2$. Количество ребер графа K_n определяется выражением $n(n-1)/2$.

Типом разложения назовем вектор $a = a_4, a_5, a_6, ..., a_n$, где a_i – количество компонент порядка i в разложении. Тогда условие существования разложения примет вид:

$$\sum (ki/2)a_i = n(n-1)/2. \tag{2}$$

В случае $k = 3$ имеем разложение графа K_n на кубические компоненты, то есть кубическое разложение. Условие (2) для кубического разложения выглядит так:

$$\sum (3i/2)a_i = n(n-1)/2. \tag{3}$$

Так как количество ребер кубического графа порядка i определяется выражением $3i/2$ и является целым числом, такой граф существует лишь в случае, когда i – четное число, $i \geq 4$. Тогда уравнение (3) можно записать так:

$$2a_4 + 3a_6 + 3a_8 + ... + (n/2)a_n = n(n-1)/6. \tag{4}$$

При $n = 4$ существует лишь одно разложение графа K_n на кубические компоненты. Следующее n, удовлетворяющее условию (1), это $n = 7$. Единственный возможный тип разложения графа K_7 это $a = \{2, 1\}$. Изучение случая $n = 10$ было начато [1], где были опубликованы 14 возможных типов разложения графа K_10 на кубические компоненты, являющиеся решениями уравнения (4) для $n = 10$. Была поставлена задача перечисления всех неизоморфных разложений для каждого типа. В данной работе приводится решение этой задачи для трех типов разложения: 3, 3, 0, 0; 5, 0, 0, 1; 1, 3, 1, 0. Для типа 3, 3, 0, 0 была найдена лишь одна реализация, компоненты которой представлены ниже:

2-3 2-4 2-7 3-4 3-7 4-7; 4-8 4-9 4-10 8-9 8-10 9-10; 5-6 5-7 5-10 6-7 6-10 7-10; 1-2 1-3 1-4 2-5 2-6 3-5 3-6 4-5 4-6; 1-5 1-6 1-7 5-8 5-9 6-8 6-9 7-8 7-9; 1-8 1-9 1-10 8-2 8-3 9-2 9-3 10-2 10-3.

Для типа 5, 0, 0, 1 также получена лишь одна реализация:

1-5 1-8 1-10 5-8 5-10 8-10; 1-6 1-7 1-9 6-7 6-9 7-9; 2-3 2-9 2-10 3-9 3-10 9-10; 2-4 2-7 2-8 4-7 4-8 7-8; 3-4 3-5 3-6 4-5 4-6 5-6; 1-2 1-3 1-4 2-5 2-6 3-7 3-8 4-9 4-10 5-7 5-9 6-8 6-10 7-10 8-9.

Для типа 1, 3, 1, 0 получены четыре неизоморфных разложения:

1. 4-8 4-9 4-10 8-9 8-10 9-10; 1-5 1-6 1-7 5-2 5-9 6-2 6-9 7-2 7-9; 1-8 1-9 1-10 8-2 8-3 9-2 9-3 10-2 10-3; 3-4 3-7 3-6 4-7 4-5 7-10 6-10 6-5 10-5; 1-2 1-3 1-4 2-3 2-4 3-5 4-6 5-7 5-8 6-7 6-8 7-8.

2. 4-8 4-9 4-10 8-9 8-10 9-10; 1-5 1-6 1-7 5-9 5-10 6-9 6-10 7-9 7-10; 1-8 1-9 1-10 8-2 8-3 9-2 9-3 10-2 10-3; 2-4 2-6 2-7 4-6 4-3 6-5 7-5 7-3 5-3; 1-2 1-3 1-4 2-3 2-5 3-6 4-5 4-7 5-8 6-7 6-8 7-8.

3. 4-6 4-9 4-10 6-9 6-10 9-10; 1-5 1-6 1-7 5-6 5-9 6-2 7-2 7-9 2-9; 1-8 1-9 1-10 8-9 8-7 9-3 10-3 10-7 3-7; 2-8 2-10 2-4 8-10 8-3 10-5 4-5 4-3 5-3; 1-2 1-3 1-4 2-3 2-5 3-6 4-7 4-8 5-7 5-8 6-7 6-8.

4. 4-8 4-9 4-10 8-9 8-10 9-10; 1-5 1-6 1-7 5-9 5-10 6-9 6-10 7-9 7-10; 1-8 1-9 1-10 8-2 8-3 9-2 9-3 10-2 10-3; 2-3 2-4 2-7 3-4 3-6 4-5 7-5 7-6 5-6; 1-2 1-3 1-4 2-5 2-6 3-5 3-7 4-6 4-7 5-8 6-8 7-8.

Список литературы

1. Petrenjuk A. J. Decomposing K_{10} into cubic graphs of order 6 // Bull. Inst. Combin. Appl. — 1994. — V. 12. — P. 9–14.

ДЛИННЫЕ ЦИКЛЫ В СИЛЬНО СВЯЗНЫХ ТУРНИРАХ ПОРЯДКА N И ДИАМЕТРА D

С. В. Савченко (Черноголовка)

По определению, *турнир* является ориентацией ребер полного графа. Известная теорема Муна [1] утверждает, что сильно связный турнир T порядка n обладает свойством вершинной панцикличности: для любого $\ell = 3, ..., n$ каждая вершина в T содержится в цикле длины ℓ. Одним из многочисленных следствий этой теоремы является оценка снизу $c_\ell(T) \geq n - \ell + 1$ для числа $c_\ell(T)$ циклов длины ℓ в T, где $3 \leq \ell \leq n$. По теореме Лас-Верньяса [2] равенство $c_\ell(T) = n - \ell + 1$ при некотором $\ell = 4, ..., n-1$ однозначно определяет T : он должен быть изоморфен единственному (опять, с точностью до изоморфизма) сильно связному турниру $T_{n-1,n}$ порядка n и диаметра $n-1$. Этот турнир нетрудно описать: если $v_0, v_1, ..., v_{n-2}, v_{n-1}$ — (единственный) путь из v_0 в v_{n-1} длины $n-1$, то $v_j \to v_i$ при любом $j > i+1$. Если же мы изменим ориентацию каждой дуги в $v_0, v_1, ..., v_{n-2}, v_{n-1}$ на противоположную, то получим транзитивный турнир TT_n порядка n, который, как легко видеть, вообще не имеет никаких циклов.

В настоящей работе приведенные выше (классические) теоремы уточняются в классе $\mathcal{T}_{d,n}$ всех сильно связных турниров порядка n

и диаметра d. Подробное доказательство сформулированных ниже результатов можно найти в [3].

Для турнира T с вершинами $v_0, ..., v_m$ и $m+1$ турниров $T_0, ..., T_m$ мы определим *композицию* $T(T_0, ..., T_m)$ как турнир, полученный из T при помощи замены его вершин $v_0, ..., v_m$ и бинарного соотношения $\to$ между ними на турниры $T_0, ..., T_m$ и бинарное соотношение $\Rightarrow$ между ними соответственно, где $T_i \Rightarrow T_j$ означает, что каждая вершина в T_i доминирует любую вершину в T_j. Обозначим через $\lfloor \frac{n-d+1}{2} \rfloor$ наибольшее целое число, меньшее или равное $\frac{n-d+1}{2}$, а через $\lceil \frac{n-d+1}{2} \rceil$ наименьшее целое число, большее или равное $\frac{n-d+1}{2}$, и при $n > d \geq 3$ положим

$$T_{d,n} = T_{d,d+1}(TT_{\lfloor \frac{n-d+1}{2} \rfloor}, v_1, ..., v_{d-1}, TT_{\lceil \frac{n-d+1}{2} \rceil}).$$

Гипотеза. *Для любого сильно связного турнира T порядка $n \geq 4$, чей диаметр не превосходит $d \geq 3$, справедливо неравенство $c_\ell(T) \geq c_\ell(T_{d,n})$ при каждом $\ell = 3, ..., n$. Кроме того, если $d \geq \frac{n+3}{2}$, то равенство $c_\ell(T) = c_\ell(T_{d,n})$ при некотором $\ell = n-d+3, ..., d$ означает, что T изоморфен $T_{d,n}$ или его обратному $T_{d,n}^-$.*

Нетрудно проверить, что $T_{d,n}$ содержит ровно один гамильтонов цикл. Следовательно, при $\ell = n$ теорема Муна влечет первое утверждение гипотезы 1. Оно также справедливо при $\ell = 3$. Однако, в дальнейшем мы в основном будем рассматривать случай, когда ℓ достаточно близко к n.

По определению, вершина v *разделяет* T, если подтурнир $T - v$ порядка $n-1$ не является сильно связным. Легко проверить, что множество разделяющих вершин турнира $T_{d,n}$ состоит из $v_1, ..., v_{d-1}$. Как известно, свойство наличия ровно одного гамильтонова цикла наследуется всеми сильно связными подтурнирами. Следовательно, $T_{d,n}$ имеет ровно $n-d+1$ циклов длины $n-1$. Нетрудно показать, что при $n > d \geq 3$ каждый турнир $T \in \mathcal{T}_{d,n}$ допускает не более чем $d-1$ разделяющих вершин. Поэтому теорема Муна позволяет утверждать, что неравенство гипотезы 1 также справедливо при $\ell = n-1$.

Что касается второго ее утверждения, то при $d = n-1$ оно эквивалентно теореме Лас-Верньяса. Наше доказательство по индукции для $d = n-2$ занимает в [3] три страницы. Случай $d \leq n-3$ представляется достаточно трудным. Для читателя, который попробует доказать гипотезу 1 в общем случае, мы приводим значения вели-

чины $c_\ell(T_{d,n})$ при $d \geq \frac{n+3}{2}$ и $\ell = n-d+3, ..., d$:

$$c_\ell(T_{d,n}) = d - \ell + 2^{\lceil \frac{n-d+1}{2} \rceil} + 2^{\lfloor \frac{n-d+1}{2} \rfloor} - 2.$$

Пусть теперь T — сильно связный турнир порядка n и диаметра 2. Простейшим примером такого турнира является ориентированный цикл $\vec{K}_3$ длины 3. Нетрудно показать, что если v — разделяющая вершина в T, то $T = \vec{K}_3(v, T_1, T_2)$, где каждый из турниров T_1 и T_2 является сильно связным и или содержит ровно одну вершину или имеет диаметр два. По теореме Муна-Буша [4] турнир $T - v$ (напомним, что он имеет структуру $T_1 \Rightarrow T_2$) содержит хотя бы β^{n-3} гамильтоновых путей, где $\beta = 5^{\frac{1}{3}}$. Поскольку $T_2 \Rightarrow v \Rightarrow T_1$, то любой гамильтонов путь в $T - v$ продолжается до гамильтонова цикла в самом T. Поэтому T содержит β^{n-3} гамильтоновых циклов. С другой стороны, по теореме Томассена-Буша [4] каждый 2-связный турнир порядка n имеет по крайней мере $\beta^{\frac{n}{32}-1}$ гамильтоновых циклов. Таким образом, для случая $h = 0$ мы получили доказательство следующей теоремы.

Теорема. *Для каждого $h = 0, ..., n-3$ сильно связный турнир T порядка n и диаметра 2 имеет по крайней мере*

$$\min\{\beta^{\frac{n-h}{32}-1}, \beta^{\frac{2}{3}(n-h-1)-c(h)-h}\}$$

циклов длины $n-h$, где $\beta = 5^{\frac{1}{3}}$ и $c(h) = (h+1)(h+4)/2$.

Как видим, при любом фиксированном $h \geq 0$ минимум $c_{n-h}(T)$ в классе $\mathcal{T}_{2,n}$ растет экспоненциально быстро по n. Заметим, что если $2h \leq n-d+1$, то $c_{n-h}(T_{d,n}) = \binom{n-d+1}{h}$. Поэтому при данных $d \geq 3$ и $h \geq 0$ минимум $c_{n-h}(T)$ в классе $\mathcal{T}_{d,n}$ является $O(n^h)$. Таким образом, случаи $d \geq 3$ и $d = 2$ отличаются друг от друга достаточно существенно.

Список литературы

1. Moon J. W. Topics on Tournaments. — New York: Holt, Rinehart and Winston, 1968.

2. Las Vergnas M. Sur le nombre de circuits dans un tournoi fortement connexe // Cahiers Centre Études Recherche Opér. — 1975. — V. 17. — P. 261–265.

3. Savchenko S. V. Non-critical vertices and long circuits in strong tournaments of order n and diameter d // Journal of Graph Theory. — DOI 10.1002/jgt.20615.

4. Busch A. H. A note on the number of hamiltonian paths in strong tournaments // Electronic Journal of Combinatorics. — 2006. — V. 13, № 3.

НЕКОТОРЫЕ ТИПЫ ГРАФОВ, ДОПУСКАЮЩИЕ ДИСТАНЦИОННУЮ МАГИЧЕСКУЮ РАЗМЕТКУ

М. Ф. Семенюта (Кировоград), Ж. Т. Черноусова (Киев)

Для нужд радиотрансляции возникла необходимость введения разметок графов, связанных с расстоянием между вершинами. В связи с этим, М. Миллер и др. в работе [1] предложили 1-вершинно магическую вершинную разметку, названную авторами [2] дистанционной магической. В настоящее время значительные успехи достигнуты в решении задачи существования дистанционной магической разметки для графа $G[\overline{K_n}]$, где G — r-регулярный граф, $\overline{K_n}$ — безреберный n-вершинный граф [1–4]. В [1–4] представлены условия существования дистанционной магической разметки для графов $mC_p[\overline{K_n}], mK_p[\overline{K_n}]$. Мы получили результаты по графам $P_m[P_n], P_m[C_n]$ и mC_4, отображенные в теоремах 1–3.

Теорема 1. *Граф $P_m[P_n]$ допускает дистанционную магическую разметку:* 1) *для $m = 1$ только при $n = 1$ или $n = 3$;* 2) *для $m = 3$ только при $n = 1$. При $m = 2$ и $n \geq 1$, а также при $m > 3$ и $n = 1, n = 2, n \geq 4$ граф $P_m[P_n]$ не является дистанционным магическим.*

Доказательство. Если $m = 1$, то граф $P_1[P_n] = P_n$ является дистанционным магическим [1] только при $n = 1$ или $n = 3$. Если $n = 1$, аналогично, граф $P_m[P_1] = P_m$ является дистанционным магическим только при $m = 1$ или $m = 3$. Для $m \geq 2, n = 2$ и $m = 3, n = 3$ в графе $P_m[P_n]$ найдутся две вершины u и v такие, что $|N(u) \cap N(v)| = deg(u) - 1 = deg(v) - 1$, где $N(u), N(v)$ — множества смежности вершин u и v соответственно. Согласно [1] граф $P_m[P_n]$ не будет дистанционным магическим. Рассмотрим случай $m = 2, n = 3$. Пусть $V(P_2) = \{x_1, x_2\}$ и $V(P_3) = \{y_1, y_2, y_3\}$, тогда $V(P_2[P_3]) = \{(x_1, y_1), (x_1, y_2), (x_1, y_3), (x_2, y_{1)}, (x_2, y_2), (x_2, y_3)\}$. Предположим, что граф $P_2[P_3]$ имеет дистанционную магическую разметку f, тогда получим $2f((x_1, y_2)) + 2f((x_2, y_2)) = 21$. Выполнение этого равенства невозможно ни при каких значениях $f((x_1, y_2))$ и

$f((x_2, y_2))$. Следовательно, $P_2[P_3]$ не является дистанционным магическим графом. Пусть $m \geq 2, n \geq 4$. Обозначим через $x_1, x_2, \ldots, x_m$ вершины графа P_m и через $y_1, y_2, \ldots, y_n$ — вершины графа P_n. Предположим, что $P_m[P_n]$ имеет дистанционную магическую разметку f. Учитывая, что $w((x_1, y_1)) = w((x_1, y_3))$, получим $f((x_1, y_4)) = 0$. Это противоречит условию магичности. Таким образом, граф $P_m[P_n]$ не дистанционный магический. Теорема доказана.

Теорема 2. *Граф $P_m[C_n]$ допускает дистанционную магическую разметку:* 1) *для $m = 1$ только при $n = 1$ или $n = 4$;* 2) *для $m = 2$ только при $n = 4$;* 3) *для $m = 3$ только при $n = 1$. При $m > 3$ и $n = 1, n = 2, n = 3, n \geq 5$ граф $P_m[C_n]$ не является дистанционным магическим.*

Доказательство. Граф $P_1[C_n] = C_n$ является дистанционным магическим [1] только при $n = 4$. Граф $P_m[C_1] = P_m$ является дистанционным магическим [1] только при $m = 1$ или $m = 3$. При $m = 2, n = 2$ граф $P_2[C_2] = K_4$ не является дистанционным магическим [1]. Пусть $m = 2, n = 3$. Граф $P_2[C_3]$ — это 5-регулярный граф. Согласно [1] он не допускает дистанционную магическую разметку. Пусть $m = 2, n = 4$. Граф $P_2[C_4]$ будет r-регулярным порядка $2n = 8$, где $r = n + 2 = 6$. Предположим, что для $P_2[C_4]$ существует дистанционная магическая разметка f. Пусть $V(P_2) = \{x_1, x_2\}$ и $V(C_4) = \{y_1, y_2, y_3, y_4\}$. Для $P_2[C_4]$ имеем $V(P_2[C_4]) = \{(x_1, y_1), (x_1, y_2), (x_1, y_3), (x_1, y_4), (x_2, y_{1)}, (x_2, y_2), (x_2, y_3), (x_2, y_4)\}$.

Найдем значение магической постоянной $k = r(1 + 2n)/2 = 27$. Рассмотрим разметку вершин: $f(x_1, y_1) = 1, f(x_1, y_2) = 4, f(x_1, y_3) = 8, f(x_1, y_4) = 5, f(x_2, y_1) = 2, f(x_2, y_2) = 3, f(x_2, y_3) = 7, f(x_2, y_4) = 6$. Для f выполняются свойства магичности. Таким образом, граф $P_2[C_4]$ допускает дистанционную магическую разметку. Пусть $m = 2, n \geq 5$. Граф $P_2[C_n]$ содержит две вершины u и v такие, что $|N(u) \cap N(v)| = deg(u) - 1 = deg(v) - 1$. В этом случае u и v — это любые две не смежные вершины копии C_n в графе $P_2[C_n]$, расстояние между которыми равно двум. На основании [1] граф $P_2[C_n]$ не допускает дистанционной магической разметки. Пусть $m \geq 3, n = 2$. Граф $P_m[C_2] = P_m[P_2]$ не является дистанционным магическим (теорема 1). Пусть $m \geq 3, n \geq 5$. Обозначим через $x_1, x_2, \ldots, x_m$ вершины графа P_m и через $y_1, y_2, \ldots, y_n$ — вершины графа C_n. Предположим, что $P_m[C_n]$ имеет дистанционную магическую разметку f. Учитывая, что $w(x_1, y_1) = w(x_1, y_3)$, получим $f((x_1, y_n)) = f((x_1, y_4))$. Это противоречит условию магичности. Таким образом, $P_m[C_n]$ не является дистанционным магическим графом. Пусть $m \geq 3, n = 3$. При-

меним рассуждения аналогичные тем, которые использовали при $m \geq 3, n \geq 5$, например, для вершин (x_1, y_1) и (x_1, y_3). В результате получим, что $P_m[C_n]$ не является дистанционным магическим графом для $m \geq 3, n = 3$. Рассмотрим случай $m = 3, n = 4$. Обозначим $\Sigma_i = \sum_{j=1}^{4} f((x_i, y_j))$, где $i = 1, 2, \ldots, m$. Допустим, что для графа $P_3[C_4]$ существует дистанционная магическая разметка. Из условия магичности следует, что $\Sigma_1/2 + \Sigma_2 = \Sigma_2/2 + \Sigma_1 + \Sigma_3, \Sigma_1 = \Sigma_3$, тогда $\Sigma_2 = 3\Sigma_1$. Учитывая, что $\Sigma_1 + \Sigma_2 + \Sigma_3 = 78$, имеем $5\Sigma_1 = 78$. Пришли к противоречию, поэтому $P_3[C_4]$ не допускает дистанционной магической разметки. Теорема доказана.

Теорема 3. *Граф mC_4 допускает дистанционную магическую разметку для любого $m \geq 1$.*

Доказательство. Граф mC_4 — это 2-регулярный граф с $4m$ вершинами. Пусть x_{ij}, где $i = 1, 2, \ldots, m, j = 1, 2, 3, 4$ — вершины графа mC_4. При этом вершины $x_{i1}, x_{i2}, x_{i3}, x_{i4}$ принадлежат i-ой копии цикла C_4. Рассмотрим разметку вершин f, определяемую по формуле

$$f(x_{ij}) = \begin{cases} i, & 1 \leq i \leq m, j = 1, \\ 2m + 1 - i, & 1 \leq i \leq m, j = 2, \\ 4m + 1 - i, & 1 \leq i \leq m, j = 3, \\ 2m + i, & 1 \leq i \leq m, j = 4. \end{cases}$$

Отображение f является биекцией множества вершин графа mC_4 на множество $\{1, 2, \ldots, 4m\}$. Кроме этого для каждой вершины x_{ij} i-ой копии цикла $C_4, j = 1, 2, 3, 4$, получим $w(x_{i1}) = w(x_{i3}) = f(x_{i2}) + f(x_{i4}) = 4m + 1$, $w(x_{i2}) = w(x_{i4}) = f(x_{i1}) + f(x_{i3}) = 4m + 1$. Следовательно, по определению разметка f является дистанционной магической разметкой графа mC_4 с магической постоянной $k = 4m + 1$. Теорема доказана.

Список литературы

1. Miller M., Rodger C., Simanjuntak R. Distance magic labelings of graphs // Australian Journal of combinatorics. — 2003. — V. 28. — P. 305–315.

2. Sugeng K. A., Froncek D., Miller M., Ryan J., Walker J. On distance magic labeling of graphs // JCMCC. — 2009. — V. 71. — P. 39–48.

3. Shafiq M. K., Ali G., Simanjuntak R. Distance magic labelings of a union of graphs // AKCE J. Graphs. Combin. — 2009. — V. 6, № 1. — P. 191–200.

4. Froncek D., Kovár P., Kovárová P. Fair incomplete tournaments // Bull. Inst. Combin. Appl. — 2006. — V. 642. — P. 31–33.

О КРИТЕРИЯХ МИНИМАЛЬНОСТИ КОМПЛЕКСОВ ГРАНЕЙ В ЕДИНИЧНОМ КУБЕ

И. П. Чухров (Москва)

Комплексом граней называется неупорядоченный набор различных граней единичного куба B^n. Обозначим через N_M — множество вершин куба, которые содержатся в гранях комплекса M. Комплекс граней M называется *комплексом граней булевой функции* f, если множество наборов значений переменных, на которых функция обращается в единицу, совпадает с множеством N_M. Используемые, но не определяемые понятия можно найти в [1–3].

Комплексы граней называются *эквивалентными*, если они содержат одно подмножество вершин единичного куба, т.е. являются комплексами граней одной функции.

Комплексы граней называются *изоморфными*, если один комплекс может быть получен из другого комплекса перестановкой координат. Соответственно, *грани изоморфны*, если одна грань может быть получена из другой перестановкой координат. Комплексы граней называются π-*изоморфными*, если один комплекс может быть получен из другого комплекса заменой граней на изоморфные грани.

Функционал $\mathcal{L}$, определенный на множестве всех комплексов граней, является *мерой сложности*, если он удовлетворяет аксиомам неотрицательности, монотонности, выпуклости и инвариантности относительно изоморфизма [2, с. 298].

Комплекс граней называется $\mathcal{L}$-*минимальным*, если он имеет наименьшую меру сложности $\mathcal{L}$ среди эквивалентных комплексов граней.

Кратчайшим называется l-минимальный комплекс и *минимальным* называется L-минимальный комплекс, где l — число граней и L — сумма рангов граней в комплексе.

Для произвольного класса мер сложности $\mathcal{C}$ комплекс граней называется $\mathcal{C}$-*минимальным комплексом* (минимальным относительно класса мер сложности $\mathcal{C}$), если он является $\mathcal{L}$-минимальным для любой меры сложности из класса $\mathcal{C}$.

Мера сложности $\mathcal{L}$ удовлетворяет *усиленному свойству инвариантности* относительно изоморфизма, если π-изоморфные комплексы имеют одинаковую $\mathcal{L}$-сложность.

Обозначим через Λ — множество всех мер сложности на множестве комплексов граней и через Λ_π — класс мер сложности, которые удовлетворяют усиленному свойству инвариантности относительно

изоморфизма. Используемые при минимизации булевых функций меры сложности принадлежат Λ_π.

Комплекс граней называется *неприводимым*, если после удаления из него любой грани получается не эквивалентный комплекс граней. В неприводимом комплексе каждая грань содержит хотя бы одну вершину, которая не покрывается другими гранями из комплекса. Такая вершина называется *собственной вершиной грани* в неприводимом комплексе. Обозначим через $I_{M,\tilde{x}}$ — грань неприводимого комплекса M, которая содержит собственную вершину $\tilde{x}$. Любая грань, которая содержится в множестве N_M называется *допустимой* гранью для комплекса M. Будем говорить, что грань I *доминирует* грань I', если существует такая перестановка координат π, что $\pi(I') \subset I$.

Локальные алгоритмы, использующие информацию окрестности произвольного фиксированного порядка, не могут решить задачу минимизации булевых функций [1, с. 95]. Поэтому для обоснования минимальности комплекса требуются не локальные, а глобальные структурные свойства комплексов граней.

Подмножество вершин называется *протыкающим* для комплекса граней, если в каждой грани комплекса содержится хотя бы одна вершина этого подмножества.

Для множества вершин $Q \subseteq B^n$ подмножество вершин $X \subseteq Q$ называется *интервально независимым* для Q множеством вершин, если любая допустимая грань для множества Q содержит не более одной вершины из X. Для комплекса граней M множество вершин называется интервально независимым, если оно является интервально независимым для множества N_M.

Лемма 1. *Пусть $\mathcal{B}_M$ — подмножество собственных вершин для граней неприводимого комплекса M и определены условия:*

1. *Подмножество $\mathcal{B}_M$ является интервально независимым и протыкающим для комплекса граней.*

2. *Для каждой вершины $\tilde{x} \in \mathcal{B}_M$ ранг грани $I_{M,\tilde{x}}$ не больше, чем ранг любой допустимой грани комплекса содержащей вершину $\tilde{x}$.*

3. *Для каждой вершины $\tilde{x} \in \mathcal{B}_M$ грань $I_{M,\tilde{x}}$ изоморфна или доминирует любую допустимую грань комплекса содержащую вершину $\tilde{x}$.*

Тогда комплекс M является

— *кратчайшим, если выполнено условие* 1,

— *минимальным и кратчайшим, если выполнены условия* 1 *и* 2,

— *Λ_π-минимальным, если выполнены условия* 1 *и* 3.

Отметим, что в случае, когда *неприводимый комплекс является минимальным и не является кратчайшим*, может не выполняться

условие 1, т.е. нельзя выделить интервально независимое и протыкающее подмножество собственных вершин $\mathcal{B}_M$. Соответственно, в случае, когда *кратчайший комплекс не является минимальным* может выполняться условие 1 и не выполняться условие 2 для *максимальной* грани $I_{M,\tilde{x}}$ некоторой вершины $\tilde{x} \in \mathcal{B}_M$ [1, с. 92–93].

Кратчайшие и минимальные комплексы обладают свойством суммируемости для компонент связности [1, с. 117], но для произвольных мер сложности такое утверждение не верно.

Лемма 2. *Если неприводимые комплексы граней M_1 и M_2 удовлетворяют условиям* 1 *и* 3 *леммы* 1 *и множества вершин, содержащихся в комплексах, являются компонентами связности в единичном кубе, то комплекс $M_1 \cup M_2$ является Λ_π-минимальным.*

Следствие. *Любой минимальный комплекс для симметрической функции является Λ_π минимальным.*

Обозначим в единичном кубе B^n:

$\mathcal{M}^n_{\text{ker}}$ — множество ядровых комплексов граней;

$\mathcal{M}^n_{\cap\Lambda_\pi}$ — множество Λ_π-минимальных комплексов граней;

$\mathcal{M}^n_{\cap\Lambda}$ — множество комплексов граней минимальных для любой меры сложности;

$\mu_{\cap\Lambda}(n)$ — максимальное число Λ-минимальных комплексов функции n переменных.

Очевидно, что $\mathcal{M}^n_{\text{ker}} \subseteq \mathcal{M}^n_{\cap\Lambda} \subseteq \mathcal{M}^n_{\cap\Lambda_\pi}$. На самом деле имеет место строгое вложение этих множеств.

Теорема. *При $n \geq 4$*

$$\mathcal{M}^n_{\text{ker}} \subset \mathcal{M}^n_{\cap\Lambda} \subset \mathcal{M}^n_{\cap\Lambda_\pi}, \qquad \mu_{\cap\Lambda}(n) \geq C^{\left\lfloor \frac{n-2}{2} \right\rfloor}_{n-2}.$$

Список литературы

1. Дискретная математика и математические вопросы кибернетики. Т. 1. — М.: Наука, 1974.

2. Яблонский С. В. Введение в дискретную математику. — М.: Высшая школа, 2003.

3. Чухров И. П. О ядровых и кратчайших комплексах граней в единичном кубе // Дискретный анализ и исследование операций. — 2011. — Т. 18, № 2. — С. 75–94.

Секция «Математическая теория интеллектуальных систем»

О ВОССТАНОВЛЕНИИ ИЗОБРАЖЕНИЙ ПО КОДАМ В НЕКОТОРЫХ ВЫРОЖДЕННЫХ СЛУЧАЯХ

П. Г. Агниашвили (Москва)

Одной из ключевых характеристик изображения является его код. По своему смыслу код должен отражать определенную общность в восприятии изображений. В рассматриваемом дискретно-геометрическом подходе общим признаком является аффинная эквивалентность изображений. Данное направление получило развитие в работе [1], где, в частности, исследуется возможность восстановления изображений по их кодам в двумерном и трехмерном случаях.

В предлагаемой работе исследуется аналогичная проблема в общем случае произвольной конечной размерности. Отдельное внимание уделяется вырожденному случаю изображений, лежащих в двух параллельных гиперплоскостях.

Всюду далее рассматривается пространство $\mathbb{R}^n$, $n \geq 2$. Под точкой с индексом $p \in \mathbb{N}$ будем понимать упорядоченную пару $(\mathbf{x}, p)$, где $\mathbf{x} = (x_1, \ldots, x_n)$ — вектор из $\mathbb{R}^n$.

Изображением первого рода в $\mathbb{R}^n$ называется конечное множество индексированных точек, не лежащих в одной гиперплоскости и занумерованных индексами $1, \ldots, k$ в случае k точек, $k \in \mathbb{N}$. Для изображения первого рода A через $|A|$ будем обозначать число точек в изображении, а через $\mathbb{N}_{|A|} = \{1, \ldots, |A|\}$ — множество индексов у точек изображения. Два изображения первого рода A_1 и A_2, состоящие из одинакового числа точек ($|A_1| = |A_2|$), называются *a'-эквивалентными*, если существует аффинное преобразование, при котором каждая точка из A_1 с индексом $p \in \mathbb{N}_{|A_1|}$ отображается в точку из A_2 с тем же индексом $p \in \mathbb{N}_{|A_2|}$.

Изображением второго рода называется класс всех попарно a'-эквивалентных изображений первого рода.

Рассмотрим изображение A (первого или второго рода). Введем произвольную аффинную систему координат в $\mathbb{R}^n$ и пусть $(x_1^p, \ldots, x_n^p)$ – координаты точки с индексом $p \in \mathbb{N}_{|A|}$ в этой системе

координат. Для произвольных индексов $r_1, \ldots, r_{n+1}, s_1, \ldots, s_{n+1} \in \mathbb{N}_{|A|}$ определим индексированное число $\mu_{s_1 \ldots s_{n+1}}^{r_1 \ldots r_{n+1}}$ по формуле:

$$\mu_{s_1 \ldots s_{n+1}}^{r_1 \ldots r_{n+1}} = \begin{vmatrix} x_1^{r_1} & \cdots & x_n^{r_1} & 1 \\ \vdots & \ddots & \vdots & \vdots \\ x_1^{r_{n+1}} & \cdots & x_n^{r_{n+1}} & 1 \end{vmatrix} \Bigg/ \begin{vmatrix} x_1^{s_1} & \cdots & x_n^{s_1} & 1 \\ \vdots & \ddots & \vdots & \vdots \\ x_1^{s_{n+1}} & \cdots & x_n^{s_{n+1}} & 1 \end{vmatrix}.$$

В случае равенства знаменателя нулю полагаем, что значение $\mu_{s_1 \ldots s_{n+1}}^{r_1 \ldots r_{n+1}}$ не определено, и обозначаем такой случай знаком ∞. В случае ненулевых определителей индексированное число является отношением ориентированных объемов n-симплексов на соответствующих точках [2].

М-кодом изображения A называется множество всех индексированных чисел $\mu\text{-}T_A = \{\mu_{s_1 \ldots s_{n+1}}^{r_1 \ldots r_{n+1}} | r_i, s_j \in \mathbb{N}_{|A|}\}$.

Теорема 1. *Между множеством м-кодов и множеством изображений второго рода существует биекция, сопоставляющая каждому изображению его м-код.*

Кодом изображения A называется множество всех индексированных чисел $T_A = \{\rho_{s_1 \ldots s_{n+1}}^{r_1 \ldots r_{n+1}} | r_i, s_j \in \mathbb{N}_{|A|}\}$, где $\rho_{s_1 \ldots s_{n+1}}^{r_1 \ldots r_{n+1}} = |\mu_{s_1 \ldots s_{n+1}}^{r_1 \ldots r_{n+1}}|$. Данное определение согласуется и обобщает определение кода из [1].

Симплексным набором индексов для м-кода $\mu\text{-}T_A$ называется набор $S = (i_1, \ldots, i_{n+1})$, для которого $\mu_{i_1, \ldots, i_{n+1}}^{r_1, \ldots, r_{n+1}} \neq \infty$ при любых $r_i \in \mathbb{N}_{|A|}$. Другими словами, точки с индексами $i_1, \ldots, i_{n+1}$ не лежат в одной гиперплоскости, на что и указывает название набора.

Обозначим через μ_j^s элемент м-кода, у которого нижний набор является симплексным набором $(i_1, \ldots, i_{n+1})$, а верхний набор отличается от симплексного в j-ой позиции: $(i_1, \ldots, i_{j-1}, s, i_{j+1}, \ldots, i_{n+1})$. Рассмотрим два изображения A и $\hat{A}$ со следующими свойствами: $|A| = |\hat{A}|$, $S = (i_1, \ldots, i_{n+1})$ — общий симплексный набор, и выполняются равенства $|\mu_j^s| = |\hat{\mu}_j^s|$, $s \in \mathbb{N}_{|A|}, j \in \mathbb{N}_{n+1}$. Положим $M_+^s = \{i_j \in S | \mu_j^s = \hat{\mu}_j^s \neq 0\}$ и $M_-^s = \{i_j \in S | \mu_j^s = -\hat{\mu}_j^s \neq 0\}$.

Разделяющим разбиением набора S называется пара множеств (S_1, S_2), для которых выполняется: $S = S_1 \sqcup S_2$ и для любого индекса $s \in \mathbb{N}_{|A|}$ либо $M_+^s \subseteq S_1, M_-^s \subseteq S_2$, либо $M_+^s \subseteq S_2, M_-^s \subseteq S_1$.

Теорема 2. *Коды изображений A и $\hat{A}$ с перечисленными свойствами совпадают тогда и только тогда, когда существует разделяющее разбиение симплексного набора S.*

Аффинную оболочку конечного множества точек M в $\mathbb{R}^n$ называем гранью и обозначаем через $< M >$ [3]. Изображение A называется

допустимым, если для любых двух непересекающихся граней $< M_1 >$ и $< M_2 >$, содержащих все точки изображения A, выполняется соотношение: $\dim(M_1) + \dim(M_2) = \dim(A) - 1$.

Теорема 3. *Коду соответствует единственное изображение второго рода тогда и только тогда, когда изображение является допустимым.*

Теорема 3 является аналогом утверждений, доказанных в [1] для случаев $\mathbb{R}^2$ и $\mathbb{R}^3$, а также общего результата, полученного Руденко А. Д. для случая пространства произвольной конечной размерности. Согласно этим результатам, коду соответствует единственное изображение с точностью до a'-эквивалентности, если оно не лежит в двух параллельных гиперплоскостях. Теорема 3 применима и к такому вырожденному случаю. Следующее утверждение более детально разбирает данный вопрос.

Утверждение. *Пусть* $A = A_1 \sqcup A_2$, *и* $< A_1 > \cap < A_2 > = \varnothing$. *Изображение* A *допустимо* $\Leftrightarrow \dim(A_1) + \dim(A_2) = \dim(A) - 1$, *и* A_1, A_2 *допустимы.*

Используем полученный результат для классификации допустимых изображений, лежащих в двух параллельных гиперплоскостях, в случаях $\dim(A) = 2$ и $\dim(A) = 3$.

Случай $\dim(A) = 2$. В данном случае изображение лежит на двух параллельных прямых. Все точки расположены на прямой и в точке, не лежащей на этой прямой.

Случай $\dim(A) = 3$. В данном случае изображение лежит на двух параллельных плоскостях. Возможно два варианта:

1. Все точки расположены на плоскости и в точке, не лежащей на этой плоскости. При этом точки на плоскости не могут быть расположены на двух параллельных прямых.

2. Все точки расположены на двух скрещивающихся прямых.

Список литературы

1. Козлов В. Н. Элементы математической теории зрительного восприятия. — М.: Издательство Центра прикладных исследований при механико-математическом факультете МГУ, 2001.

2. Клейн Ф. Элементарная математика с точки зрения высшей, том 2, геометрия. — М.: Наука, 1987.

3. Кострикин А. И., Манин Ю. И. Линейная алгебра и геометрия. — М.: Просвещение, 1980.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЗАПРОСНЫХ ТЕХНОЛОГИЙ ДЛЯ СХЕМ БАЗ ДАННЫХ СУБД DIM

Д. В. Антонов, В. С. Рублев (Ярославль)

Для манипуляции данными СУБД DIM [1] необходимо использование одной из запросных технологий. Одной из них является язык запросов ODQL для СУБД DIM и порядок компиляции, состоящий в выполнении алгоритма, описанного в [1]. Но так как реализация системы идет при помощи мета-уровня, отображаемого реляционными БД, то возможен подход создания соответствующего реляционного запроса к мета-уровню. Для этого запрос ODQL должен быть транслирован в реляционный запрос.

Так как неясно, какая из технологий может оказаться эффективней по времени (технология реляционного запроса к мета-уровню требует дополнительных затрат времени на трансляцию в реляционный запрос, но полученный запрос может выполняться быстрее) необходимо проведение статистических экспериментов.

Для выявления полной картины нужно также сравнение с технологией, когда данные размещяются в реляционной БД и соответствующий запрос делается непосредственно к ней. Ясно, что написание самого реляционного запроса в этом случае намного сложнее, а время выполнения может быть максимально снижено. Потому необходимо сравнение всех трех технологий.

Возьмем в качестве примера схемы БД для этих запросов такое задание:

Корабли из множества *Ships*, число которых n_s, перевозят грузы из множества *Cargoes*, число которых n_c, в порты из множества *Ports*, число которых n_p. При этом корабль s везет груз c в порт p в количестве *k(s,p)*.

Необходимо написать следующий запрос:

Список наименований грузов, которые везут наиболее нагруженные корабли и при этом в наименьшее число портов среди таких кораблей.

Для начала составим запрос к схеме, созданной в реляционной СУБД, который будет оптимальным по трудоемкости, пример данного запроса можно найти в [1].

Затем составляется реляционный запрос к мета-уровню СУБД DIM:

Select Distinct *Parameters.Name*
From *Parameters*,
(
//(более 50 строк)

)

Where *sc.Value=c.Value* **AND** *sc.IdParameter=c.IdParameter*

AND *Parameters.Name=ShipName*

К схеме, созданной в СУБД DIM, запрос на языке SQL выглядит сложнее, чем аналогичный запрос к реляционной СУБД, так как данная схема имеет несколько иную организацию. Запрос на языке ODQL для нее выглядит следующим образом:

select *c.CargoName* **from** *Cargoes c*, *Ships_Cargoes sc*,

((**select objmaxsum** (sc.Quantity) **on** *s* **from** *Ships s* **links** *s* **contains**(sc) c) *s1*

intersection

(**select objmincount** (*p.obj*) **on** *s1* **from** *s1*, *Ports p* **links** *s1* **contains**(*sc*) *c*, *p* **parent** *sc*)

) *s2*

links *s2* **contains**(*sc*) *c*

Далее проводится тестирование времени выполнения запросов к схемам, содержащим различное количество записей в таблицах. Для проведения анализа необходимо составить таблицу, на основании которой делается вывод об эффективности запросных технологий и целесообразности их использования.

В таблице представлено соотношение времени (указано в секундах) выполнения части проведенных запросов с использованием указанных выше запросных технологий. Также, в ней имеются значения суммарного количества записей в 3 таблицах, которые заполнены случайными данными. Два заключительных номера обозначают особые случаи:

Восьмой — каждый корабль везет каждый груз в каждый порт (максимальный по трудоемкости).

Девятый — один корабль везет один груз в один порт (минимальный по трудоемкости).

	Суммарное количество записей	SQL	ODQL	SQL(DIM)
1	458752	2,265	3,397	2,718
2	917504	6,162	9,011	8,394
3	1736704	8,678	14,017	13,314
4	1818624	8,084	14,318	13,592
5	1835008	8,175	14,628	13,693
6	3637248	19,357	29,1	28,228
7	3997696	26,357	36,536	34,993
8	15000	43,1	50,1	51,6
9	15000	0,144	0,263	0,221

По таблице можно заметить, что время выполнения запроса на языке SQL все же идет быстрее. И, хотя ODQL запрос и выполняется в среднем на 35% дольше, чем SQL запрос, это не такая большая проблема, учитывая удобство языка ODQL, синтаксис которого понятнее и приятней, чем у запроса на SQL. Запрос на языке SQL, построенный к мета-уровню, оказался немного эффективнее, но здесь следует учитывать, что в таблице отображено время запроса, тогда как необходимо еще время на трансляцию ODQL в SQL.

Проанализировав время выполнения в особых случаях, можно сделать вывод, что разница во времени между максимальным и минимальным случаями с использованием технологии SQL составляет 42,956 с., ODQL — 49,837 с., тогда как SQL к мета-уровню — 51,379 с.

В данном случае заметно уменьшение разницы во времени запроса между ODQL и SQL с 35% до 16 %.

Таким образом, учитывая все эти измерения, можно сделать вывод о целесообразности использования запросной технологии ODQL.

Список литературы

1. Писаренко Д. С., Рублев В. С. Динамическая информационная модель. Концепция новой объектной технологии баз данных. — LAP LAMBERT Academic Publishing, Saarbrücken, Germany, 2011. — 112 — 112 с.

2. Рублев В. С., Смирнова Е. А. Объектная СУБД DIM и пути ее реализации // Материалы X Международной конференции "Интеллектуальные системы и компьютерные науки" — 2011. М.: Механико-математический факультет МГУ, 2011 — С. 92–95.

ЗАДАЧА ПОИСКА ТОЧКИ, ПОПАДАЮЩЕЙ В ПОЛУПЛОСКОСТЬ

И. А. Бабинов (Москва)

Рассмотрим следующую задачу, которую будем называть *задачей поиска точки, попадающей в полуплоскость*. Пусть $M = \{m_i | m_i = (x_i, y_i) \in \mathbb{R}^2, i = 1..n\}$ — множество точек общего положения. Нужно для заданных чисел A, B, C найти какую-нибудь точку $m_i = (x_i, y_i) \in M$, что $Ax_i + By_i + C > 0$, или сказать, что таких нет.

Сразу будем рассматривать геометрическую интерпретацию этой задачи: M — множество точек на плоскости, запрос — прямая $Ax + By + C$. Результат — точка, лежащая в соответствующей полуплоскости относительно этой прямой (эту полуплоскость задают знаки A, B, C).

Элементарной операцией будем называть арифметические операции, логические операции, а так же операции, которые в [1] считаются элементарными для реализации 2-3 дерева.

Временной сложностью алгоритма назовём количество элементарных операций, которые этот алгоритм производит для достижения результата.

Сложностью по памяти будем называть количество памяти, которое нужно для хранения вещественных чисел, а так же тех элементов, которые нужны для хранения бинарных деревьев, описанных в [1].

Теорема. *Существует алгоритм, решающий задачу поиска точки, попадающей в полуплоскость, с логарифмической по порядку роста временной сложностью и линейной от размеров базы данных сложностью по памяти.*

Для доказательства этой теоремы опишем алгоритм.

Для начала обозначим стороны выпуклой оболочки множества M за $E_i, i = 1..n$, а вершины за $V_i, i = 1..n$, причем вершины V_iV_{i+1} инцидентны стороне E_i. В базе для каждой стороны $E_i, i = 1..n$ будут храниться следующие данные.

1) V_i, V_{i+1} (если $i = n$, то вместо V_{i+1} будет V_1).

2) $\{V_k | \forall j : \rho(V_k, E_i) \geq \rho(V_j, E_i)\}$ (здесь $\rho(A, a)$ это расстояние от точки A до прямой a в метрике $\mathbb{R}^2$). Очевидно, что таких точек не более двух (следует из выпуклости).

3) Неориентированный угол (от 0 до π), который составляет с осью абсцисс прямая E_i, отсчитанный против часовой стрелки.

Все эти данные будут храниться в двоичном дереве поиска, где ключом будет являться угол из 3).

За α_q обозначим угол прямой-запроса (отсчитанный так же как в 3)), α_e — угол соответствующей стороны. Обработка запроса будет заключаться в следующих действиях:

1) Поиск ближайшей по углу стороны к прямой-запросу. То есть минимизация величины $\min(|\alpha_e - \alpha_q|, |\pi - (\alpha_e - \alpha_q)|)$ по всем сторонам выпуклой оболочки.

Организовать этот поиск не сложно. Первым делом нужно найти ближайшие к α_q справа и слева. Бинарное дерево поиска поддерживает возможность такого поиска. Аналогичную процедуру нужно

провернуть для $\pi - \alpha_q$. Останется выбрать ближайший из четырёх вариантов.

2) Проверка 3-х или 4-х точек, соответствующих найденной стороне: двух концов данной стороны и одной или двух точек, дальних от стороны.

3) Если какая-либо из этих точек попадает в полуплоскость, то выдать ее. В случае, если все эти точки не подходят, дать отрицательный ответ на запрос.

Алгоритм закончен.

Теперь приведем идею доказательства теоремы.

Докажем корректность приведённого алгоритма. Доказательство проведём по следующему плану: сначала заметим, что весь многоугольник (выпуклую оболочку) можно поместить между прямыми, параллельными прямой-запросу и проходящими через определённые вершины. А потом увидим, что достаточно проверить лишь те вершины, по которым проходят эти прямые.

Докажем первую часть. Пусть E_1 — сторона, которую алгоритм нашёл в 1 пункте. Тогда по одной из вершин можно провести прямую, параллельную запросу, для которой весь многоугольник лежит по одну сторону. Этот факт следует из выпуклости и минимальности угла между стороной и запросом. Проведём эту прямую и назовём l. Пусть (без ограничения общности) она прошла через V_1. Пусть V_i — дальняя от E_1 вершина. Тогда она будет дальней и для l (из всех вершин выпуклой оболочки). Это следует из минимальности угла и выпуклости многоугольника. Значит, проведя прямую l' параллельно l через V_i, мы добьёмся желаемого результата. Если же у E_1 две дальних точки, то одна из них будет являться дальней для l (если, конечно, l не совпадает с E_1, в этом случае обе точки будут дальними). Таким образом получим, что через одну из точек V_1, V_2 пройдёт l, и через одну из дальних для E_1 пройдёт l'. Таким образом проверки этих 3 или 4 точек будет достаточно.

Теперь, чтобы доказать теорему, оценим сложностные характеристики представленного алгоритма. Оценим временную сложность алгоритма.

1) Первый этап — поиск в бинарном дереве мощности n. Имеет временную сложность, как известно, $O(\log_2 n)$.

2) Второй этап — 3 (или 4) операции, сводящиеся к нескольким (не более константы) элементарным операциям.

Остальные этапы имеют сложность не более константы элементарных операций. Значит общая временная сложность алгоритма $O(\log_2 n)$.

Оценим сложность по памяти. Алгоритм хранит данные о каждой точке в бинарном дереве поиска. О каждой точке хранится не более константного количества данных (вещественных чисел), бинарное дерево требует дополнительно не более линейной сложности по памяти (описано в [1]). Значит общая сложность по памяти не более, чем линейна. Таким образом, теорема доказана.

Работа выполнена под руководством профессора, д.ф.-м.н. Э. Э. Гасанова.

Список литературы

1. Кнут Д. Искусство программирования. Том 1. 3-е издание. — М.: Мир, 2001.

РАЗРАБОТКА И ИССЛЕДОВАНИЕ СЕРВИСА РЕКОМЕНДАЦИЙ В МОБИЛЬНОЙ КОММЕРЦИИ НА ОСНОВЕ АЛГОРИТМА APRIORI

А. С. Бессалов, А. П. Рыжов (Москва)

В работе рассматривается построение профиля клиента телекоммуникационной компании на основе алгоритма Apriori поиска ассоциативных правил, входящего в состав алгоритмов интеллектуального анализа данных (Data Mining). Построенный профиль позволил выявить скрытые закономерности между различными параметрами, описывающими клиента (личная информация и транзакционные данные). Это позволило повысить эффективность бизнеса за счет более таргетированных предложений клиенту. Алгоритм протестирован на данных одной телекоммуникационной компании и широко применятся на практике, имея высокие показатели отклика клиентов на рекомендации

Ассоциативные правила позволяют находить закономерности между связанными событиями. Впервые эта задача была предложена для нахождения типичных шаблонов покупок, совершаемых в супермаркетах, поэтому иногда её ещё называют анализом рыночной корзины (market basket analysis) [1]. Примером такого правила служит утверждение, что покупатель, приобретающий товар A, приобретет товар B с вероятностью 75%. Приведем основные определения:

Пусть $I = \{i_1, i_2 \cdots, i_n\}$ — множество элементов, входящих в транзакцию. D — множество транзакций.

Ассоциативным правилом называется импликация $X \to Y$, где $X \subset I$, $Y \subset I$, и $X \cap Y = \varnothing$.

Правило $X \to Y$ имеет *поддержку* s *(support)*, если $s\%$ транзакций из D содержат $X \cup Y$,

$$supp(X \to Y) = supp(X \cup Y) \tag{1}$$

Правило $X \to Y$ справедливо с *достоверностью (confidence)* c, если с % транзакций из D, содержащих X, также содержат Y.

$$conf(X \to Y) = \frac{supp(X \cup Y)}{supp(X)} \tag{2}$$

Лифт — это отношение частоты появления условия в транзакциях, которые также содержат и следствие, к частоте появления следствия в целом:

$$lift(X \to Y) = \frac{conf(X \to Y)}{supp(Y)} \tag{3}$$

Одним из наиболее популярных алгоритмов поиска ассоциативных правил является алгоритм Apriori, выявляющий все правила по заданным параметрам поддержки и достоверности [1,2].

Постановка задачи построения профиля. Возьмём в качестве элементов транзакций личную информацию о клиенте, добавив предпочитаемые им услуги, и применим к этим данным алгоритм Apriori.

Плюсы такого подхода очевидны: можно выявить скрытые закономерности между признаками, описывающими клиента; можно выявить сегмент людей, которому можно предлагать ту или иную услугу;

Совокупность построенных правил будем называть *профилем клиента.*

Алгоритм построения профиля клиента. Процедура извлечения знаний из баз данных (Knowledge discovery in databases или KDD) состоит из следующих шагов:

1) Выборка данных;

2) Очистка;

3) Трансформация;

4) Интеллектуальный анализ данных (data mining);

5) Интерпретация результатов.

В аналитической платформе Deductor был разработан сценарий, строящий профиль пользователя дополнительными услугами сотовой связи (VAS услугами), построенный согласно процедуре KDD [3].

Профиль построен с использованием основной информации о клиенте телекоммуникационной компании. При этом, были устранены сильно коррелированные переменные: цветной дисплей телефона и touch screen (из наличия первого следует наличие второго), цена телефона и разрешение экрана телефона.

Алгоритм Apriori тестировался с различными входными параметрами. Для описываемого сценария были проанализированы 508 669 записи, 62 563 транзакции, 55 элементов транзакций. Наилучшие правила сгенерировались со следующими входными параметрами алгоритма Apriori (установлено экспериментальным путём): поддержка более 0,1%, достоверность более 5%, максимальная мощность часто встречающихся наборов равна 4. Получено 89 690 правил.

В качестве примера построенного в профиле правила приведём следующее: клиент из Москвы, оплативший телефонию, с высокой вероятностью сделает коммунальный платеж.

Применение профиля. Построенный профиль применяется на практике следующим образом: находим все правила, где в следствии стоит услуга, прогоняем через такие правила клиентов компании: для правила $A \to B$ находим клиента, у которого есть A, но нет B, и предлагаем ему B. В результате получим рекомендации с разными показателями поддержки, достоверности и лифта. Возникает вопрос: какая из характеристик рекомендаций является наиболее приоритетной? В данной работе полагаем, что таковой является лифт, однако, эту задачу можно решить экспериментальным путём, замерив зависимость каждой характеристики от отклика клиентов на рекомендации.

Применение такого подхода позволило увеличить продажи на десятки процентов, отклик — в 5–7 раз. Это позволяет сделать вывод о перспективности предложенного подхода в бизнесе дополнительных услуг сотовой связи.

Список литературы

1. Паклин Н. Б., Орешков В. И. Бизнес-аналитика: от данных к знаниям. — СПб., 2012.

2. Xindong Wu, Vipin Kumar. Top 10 algorithms in data mining. — Springer-Verlag London Limited, 2007.

3. BaseGroupLabs: `http://www.basegroup.ru`.

ОБ ОБОСНОВАНИИ АЛГОРИТМОВ СТАТИСТИЧЕСКОГО АНАЛИЗА В СИСТЕМАХ АКТИВНОГО АУДИТА

А. В. Галатенко, И. Н. Емельянов, А. Е. Лебедев (Москва)

Системы активного аудита [1] предназначены для выявления аномального поведения информационно-вычислительных комплексов, вызванного деятельностью злоумышленников, ошибками легальных пользователей, сбоями программных или аппаратных компонент и другими подобными им причинами. Большинство существующих систем активного аудита выявляют аномальное поведение с помощью заданного набора сигнатур, заданных, как правило, в форме регулярных выражений (в качестве примеров приведем систему [2]). Очевидным недостатком такого подхода является невозможность обнаружения новых атак, не занесенных в базу сигнатур. Другими словами, система обеспечения безопасности всегда оказывается на шаг позади злоумышленников. Кроме того, затруднено выявление маскирующихся пользователей. В качестве дополнения к сигнатурному анализатору можно предложить статистический анализатор [3, 4]. Основным недостатком статистических анализаторов является негарантированность работы — подавляющее большинство алгоритмов основано на эвристиках; отсутствуют доказательства правильности функционирования хотя бы в модельных случаях. Работы со строгим математическим исследованием, такие как [5, 6], являются редкими исключениями. Таким образом, возникает задача выявления как необходимых, так и достаточных условий правильности функционирования различных подсистем системы статистического анализа. В работе исследуются вопросы, связанные с описанием типичного поведения субъектов и объектов компьютерных систем.

Общая схема работы статистического анализатора

1. Строится описание типичного поведения, называемое долгосрочным профилем. Как правило, долгосрочный профиль представляет собой усреднение значений какой-либо характеристики поведения по “скользящему окну” — наблюдениям за фиксированный промежуток времени, или по всей истории, но с убывающими (как правило, экспоненциально) весами, чтобы более давние события имели меньшее влияние. Заметим, что в случае наличия тренда в типичном поведении такие оценки, вообще говоря, не являются состоятельными, и возникает задача установления условий на задание профиля, гарантирующих состоятельность. Для оценки погрешности хотелось бы получить оценки скорости сходимости.

2. Вычисляются параметры текущего поведения субъекта (краткосрочные профили), и производится сопоставление краткосрочных профилей с долгосрочными. В случае, если отличия являются существенными (например, значение функционала, задающего статистический критерий, превосходит некоторый порог), текущее поведение объявляется нетипичным.

Оценки сходимости вектора частот к вектору истинного распределения

Общая схема вычисления долгосрочных профилей может быть описана с помощью следующей модели. Пусть $\{x_t\}_{t=1}^{\infty}$ — последовательность независимых дискретных случайных величин, принимающих значения из множества $\{1,\dots,M\}$. Обозначим, для краткости, через $\mathbb{P}^l$ множество $\{(t_1,\dots,t_l) \in \mathbb{R}^l \mid t_j \geqslant 0, \sum\limits_{j=1}^{l} t_j = 1\}$. Предположим, что задано семейство M-мерных векторов $P(t) = (p_1(t),\dots,p_M(t)) \in \mathbb{P}^M$. Пусть для каждого t случайная величина x_t имеет распределение, задаваемое вектором $P(t)$, т.е. $\mathtt{P}\{x_t = m\} = p_m(t)$ для всех m, t. Обозначим, кроме того, через $q(t)$ разность $1 - p(t)$.

Положим $\tilde{p}_m(t) = \sum\limits_{\tau=1}^{t} \omega_\tau(t) I_{\{x_\tau = m\}}$, где $\omega(t) = (\omega_1(t),\dots,\omega_t(t))$ — некоторый t-мерный весовой вектор $(\omega_\tau \geqslant 0, \tau = 1,\dots,t)$, заданный для каждого момента времени t. Тогда вектор $\tilde{P}(t) = (\tilde{p}_1(t),\dots,\tilde{p}_M(t))$ будем называть вектором частот; он будет использоваться в качестве предполагаемого распределения параметра. При этом общий случай (произвольный весовой вектор $\omega(t)$) соответствует схеме "суммирование с весами", а случай $\omega(t) = (\underbrace{0,\dots,0}_{t-n}, \underbrace{\frac{1}{n},\dots,\frac{1}{n}}_{n})$ соответствует схеме "скользящее окно".

Теорема. *Для того, чтобы для всех $\varepsilon > 0$ имело место равенство $\lim\limits_{t\to\infty} \mathtt{P}\{|\tilde{p}_m(t) - \mathtt{M}\tilde{p}_m(t)| \geqslant \varepsilon\} = 0$, необходимо и достаточно, чтобы $\lim\limits_{t\to\infty} \sum\limits_{\tau=1}^{t} \omega_\tau^2(t) p_m(\tau) q_m(\tau) = 0$. При этом имеет место оценка $\mathtt{P}\{|\tilde{p}_m(t) - \mathtt{M}\tilde{p}_m(t)| \geqslant \varepsilon\} \lesssim \frac{1}{\varepsilon^2} \sum\limits_{\tau=1}^{t} \omega_\tau^2(t) p_m(\tau) q_m(\tau)$.*

Пусть $\omega_\tau(t) = \omega_\tau \left(\sum\limits_{j=1}^{t} \omega_j \right)^{-1}$, где $\{\omega_n\}_{n=1}^{\infty}$ — некоторая фиксированная неубывающая последовательность неотрицательных чисел (требование неубывания соответствует тому, что чем раньше было наблюдение параметра, тем менее оно значимо). Тогда для вычисления вектора частот в момент времени $t+1$ достаточно хранить вектор частот $\tilde{P}(t)$, текущее время t и сумму $\Omega_t = \sum\limits_{n=1}^{t} \omega_n$, то есть $M+2$ числа. Действительно, пересчет вектора частот и хранимой информации происходит по формулам $\Omega_{t+1} = \Omega_t + \omega_{t+1}$, $\tilde{p}_m(t+1) = \frac{\Omega_t(\tilde{p}_m(t) + \omega_{t+1} I_{\{x_{t+1}=m\}})}{\Omega_{t+1}}$.

Следствие. *Пусть $\omega_n = n^a, a \geqslant 0$. Тогда имеет место сходимость $\tilde{p}_m(t)$ к своему математическому ожиданию.*

Список литературы

1. Галатенко А. В. Активный аудит // JetInfo. — № 8. — 1999. `http://www.jetinfo.ru/1999/8/1/article1.8.1999.html`

2. Материалы по системе активного аудита Snort // `www.snort.org`

3. Маркелов К. К. Статистические методы обнаружения аномалий // Критически важные объекты и кибертерроризм. Часть 1. — М.: МЦНМО, 2008.

4. Javitz H. S, Valdes A. The NIDES statistical component description and justification // Technical report. Computer Science Laboratory. — SRI International, 1994.

5. Галатенко А. В. Вероятностные модели гарантированно защищенных систем // Материалы конференции "Математика и безопасность информационных технологий". Москва, 2003. — С. — 234–236.

6. Грушо А. А., Тимонина Е. Е. Некоторые связи между дискретными статистическими задачами и свойствами вероятностных мер на топологических пространствах // Дискретная математика. — 2006. — Т. 18, № 4. — С. 128–136.

РАСШИФРОВКА ЛИНЕЙНЫХ ФУНКЦИЙ РАНЖИРОВАНИЯ

Э. Э. Гасанов (Москва)

Интенсивное развитие веб-технологий привело к появлению на рынке компаний, предлагающих услуги по продвижению сайтов. Задача таких компаний состоит в том, чтобы для заданного поискового запроса так изменить исходный веб-сайт, чтобы он оказался в первых строчках интернет-поисковиков по данному запросу. Предположим, что при фиксированном поисковом запросе интернет-поисковик каждому сайту сопоставляет некоторый вектор n-мерного евклидова пространства, называемый вектором сайта. Предположим нам известна эта функция сопоставления. Предположим также, что существует некая функция ранжирования в соответствии с которой интернет-поисковик упорядочивает вектора, соответствующие сайтам, и в таком порядке выводит ответ на данный запрос. Будем полагать, что функция ранжирования нам не известна, но мы хотели бы ее узнать, поскольку это поможет вывести наш сайт в верхние строчки списка поисковика. Стандартная процедура расшифровки функций [1,2], предполагающая возможность спросить у оракула значение функции на векторе значений аргументов, здесь не пройдет, поскольку если даже предположить, что мы сможем сформировать сайт с заданным вектором сайта, то поисковик не сообщит нам значение функции ранжирования на данном векторе. Зато если мы сформируем два сайта с разными векторами, то мы сможем узнать на каком из этих векторов значение функции ранжирования больше, только взглянув какой из сайтов выше в списке. Тем самым у нас возникает задача расшифровки с новым видом запросов к оракулу, который назовем запросом на сравнение.

Пусть Φ_n некоторый класс функций, действующих из $\mathbb{R}^n$ в $\mathbb{R}$. Отображение вида $\chi : \Phi_n \to \mathbb{Z}$ назовем *характеристикой функций из* Φ_n. Если $f \in \Phi_n$, то значение $\chi(f)$ назовем *характеристикой функции* f из Φ_n.

Под *запросом на сравнение* будем понимать пару наборов (α, β) значений переменных функции f, а под *ответом на запрос на сравнение* знак разности значений функции на этих наборах, т.е. число $\mathtt{sign}(f(\alpha) - f(\beta))$. Под *алгоритмом расшифровки* будем понимать условный эксперимент, который последовательно генерирует запросы на сравнение в зависимости от ответов на предыдущие запросы. Будем говорить, что *алгоритм расшифровывает характеристику* χ функции f *из* Φ_n, если значения ответов на запросы на сравнение, сгенерированные условным экспериментом, однозначно определяют

число $\chi(f)$ при условии, что $f \in \Phi_n$. Скажем, что *алгоритм расшифровывает характеристику функций из* Φ_n, если он расшифровывает характеристику каждой функции f из Φ_n.

Множество всех алгоритмов, расшифровывающих характеристику χ функций из класса Φ_n, обозначим через $\mathcal{A}(\Phi_n, \chi)$.

Сложностью $\varphi(A, \chi, f)$ *алгоритма* A *на характеристике* χ *функции* f будем называть число запросов на сравнение, требуемое алгоритму A для расшифровки характеристики χ функции f. Будем называть *сложностью алгоритма* A *для характеристики* χ *на классе* Φ_n величину $\varphi(A, \Phi_n, \chi) = \max\limits_{f \in \Phi_n} \varphi(A, \chi, f)$. Функцию $\varphi(\Phi_n, \chi) = \min\limits_{A \in \mathcal{A}(\Phi_n, \chi)} \varphi(A, \Phi_n, \chi)$ будем называть *сложностью расшифровки характеристики* χ *на классе* Φ_n.

Пусть L_n — класс линейных функций, т.е. функций вида $C_1x_1 + C_2x_2 + \ldots + C_nx_n + C_{n+1}$, где $C_i \in \mathbb{R}$, $i = 1, 2, \ldots, n+1$. Легко видеть, что свободный член не влияет на разность значений функции на разных наборах, поэтому будем считать, что $C_{n+1} = 0$.

Через a^i, $a \in \mathbb{R}$, $i \in \{1, 2, \ldots, n\}$, обозначим вектор из $\mathbb{R}^n$, у которого на i-м месте стоит число a, а в остальных позициях число 0. В частности, 0^1 — это нулевой вектор.

Везде далее будем считать, что $f(x_1, \ldots, x_n) = C_1x_1 + \ldots + C_nx_n$.

Рассмотрим характеристику $S_i(f) = \mathtt{sign}(C_i)$, $i \in \{1, 2, \ldots, n\}$, равную знаку i-го коэффициента.

Утверждение 1. *Для любого* $i \in \{1, 2, \ldots, n\}$ *имеет место равенство* $\varphi(L_n, S_i) = 1$.

В самом деле, характеристика $S_i(f)$ может быть расшифрована с помощью одного запроса на сравнение $(1^i, 0^1)$.

Для $s = (s_1, \ldots, s_n) \in \{-1, 0, 1\}^n$ обозначим

$$L_n^s = \{C_1x_1 + \ldots + C_nx_n : \mathtt{sign}(C_i) = s_i, i = 1, 2, \ldots, n\}.$$

Рассмотрим характеристику $M(f) = \mathtt{argmax}_{1 \le i \le n}|C_i|$, равную индексу максимального по абсолютному значению коэффициента.

Утверждение 2. *Для любого* $s \in \{-1, 0, 1\}^n$ *имеет место равенство* $\varphi(L_n^s, M) = n - 1$.

В самом деле, если $\mathtt{sign}(C_i) = a$, $\mathtt{sign}(C_j) = b$, то понять какое из чисел $|C_i|$, $|C_j|$ больше можно с помощью одного запроса на сравнение (a^i, b^j). А чтобы найти максимум надо сделать $n - 1$ сравнение.

Введем характеристику $R_i^\varepsilon(f) = \frac{|C_i|}{\varepsilon \cdot |C_{M(f)}|}$, $i \in \{1, 2, \ldots, n\}$, $\varepsilon \in (0, 1)$, которая позволяет вычислить $|C_i|$ с точностью до ε, если в

качестве единицы измерения взять модуль максимального коэффициента.

Для $s = (s_1, \ldots, s_n) \in \{-1, 0, 1\}^n$ и $m \in \{1, \ldots, n\}$, обозначим

$$L_n^{s,m} = \{f = C_1 x_1 + \ldots + C_n x_n : M(f) = m, \mathtt{sign}(C_i) = s_i, i = 1, \ldots, n\}.$$

Утверждение 3. *Для любых* $s \in \{-1, 0, 1\}^n$, $m, i \in \{1, \ldots, n\}$, $i \neq m$, $\varepsilon \in (0, 1)$ *имеет место равенство* $\varphi(L_n^{s,m}, R_i^\varepsilon) =]-\log_2 \varepsilon[$.

В самом деле, если $i \in \{1, \ldots, n\}$, то $0 \leq \frac{|C_i|}{|C_m|} \leq 1$. Разделим отрезок $[0, 1]$ на непересекающиеся отрезки длины ε. Понятно, что характеристика $R_i^\varepsilon(f)$ есть номер отрезка длины ε, в который попадает точка $\frac{|C_i|}{|C_m|}$. Если $\mathtt{sign}(C_i) = a$, $\mathtt{sign}(C_m) = b$, $c = b/2$, то задав запрос на сравнение (a^i, c^m), мы сравним точку $\frac{|C_i|}{|C_m|}$ с точкой $1/2$. Далее, действуя аналогично, мы бинарным поиском за $]-\log_2 \varepsilon[$ запросов на сравнение можем найти номер $R_i^\varepsilon(f)$.

Утверждения 1–3 дают нам следующий алгоритм распознавания основных характеристик линейных функций ранжирования. Сначала за n запросов на сравнение мы определяем знаки каждого коэффициента функции. Далее за $n - 1$ запрос на сравнение мы находим индекс максимального по модулю коэффициента. И наконец для любого сколь угодно малого ε мы за $(n-1)\cdot]-\log_2 \varepsilon[$ запросов на сравнение вычисляем с точностью до ε все коэффициенты функции при условии, что за единицу измерения взят модуль максимального коэффициента. Понятно, что знание такой информации вполне достаточно для успешного продвижения сайтов. С другой стороны этот результат говорит, что интернет-поисковикам не следует в качестве функций ранжирования брать линейные функции.

Список литературы

1. Коробков В. К. О монотонных функциях алгебры логики // Проблемы кибернетики. — 1965. — Вып. 13. — С. 5–28.

3. D. Angluin. Queries and concept learning // Machine Learning. — 1988. — V. 2. — P. 319–342.

РАСШИФРОВКА АРИФМЕТИЧЕСКИХ СУММ МАЛОГО ЧИСЛА МОНОТОННЫХ КОНЪЮНКЦИЙ

Э. Э. Гасанов (Москва), З. А. Ниязова (Ташкент)

Расшифровка функций — это условный эксперимент, который направлен на то, чтобы для неизвестной функции из известного класса, задавая вопросы о значение функции на выбранных наборах, за малое число вопросов полностью определить таблицу значений функции. Расшифровка булевых функций — это задача, которая исследовалась во многих статьях как отечественных, так и зарубежных авторов, среди которых можно выделить классический результат Ж. Анселя по расшифровке монотонных функций [1] и известную статью Д. Англуин [2]. В данной работе будет рассматриваться расшифровка псевдо-булевских функций, т. е. функций вида $f : \{0,1\}^n \to \mathbb{N}$.

Под *запросом* на значение функции будем понимать набор значений переменных функции, под *ответом* на запрос — значение функции на этом наборе. Под *алгоритмом расшифровки* будем понимать условный эксперимент, который последовательно генерирует запросы на значение функции в зависимости от ответов на предыдущие запросы. Будем говорить, что *алгоритм расшифровывает функцию f из F*, если значения функции на наборах, сгенерированных условным экспериментом, однозначно определяют таблицу значений функции f при условии, что $f \in F$. Скажем, что *алгоритм расшифровывает класс функций F*, если он расшифровывает каждую функцию f из F.

На наборах $\alpha = (\alpha_1, \ldots, \alpha_n)$ и $\beta = (\beta_1, \ldots, \beta_n)$ n-мерного булевого куба $E^n = \{0,1\}^n$ введем отношение частичного порядка "$\leq$", задаваемое соотношением: $\alpha \leq \beta \Leftrightarrow \alpha_i \leq \beta_i$ для любых $i \in \{1, 2, \ldots, n\}$. Будем писать $\alpha < \beta$, если $\alpha \leq \beta$ и $\alpha \neq \beta$. Скажем, что наборы α и β из E^n *несравнимы*, если $\alpha \not\leq \beta$ и $\beta \not\leq \alpha$. Подмножество булевого куба, состоящее из попарно несравнимых наборов будем называть *носителем*. Множество всех носителей n-мерного булевого куба обозначим через $\mathcal{B}_n$.

Псевдо-булевская функция f, определенная на n-мерном булевом кубе E^n и принимающая значение из расширенного натурального ряда $\mathbb{N} = \{0, 1, 2, \ldots\}$, называется *монотонной*, если для любых наборов α и β из E^n, таких что $\alpha \leq \beta$, справедливо $f(\alpha) \leq f(\beta)$.

Набор α назовем *нижней единицей* монотонной функции f, если $f(\alpha) = 1$ и $f(\beta) = 0$ для любого набора β такого, что $\beta < \alpha$.

Пусть $\alpha = (\alpha_1, \ldots, \alpha_n) \in E^n$. Булевскую функцию

$$K_\alpha(x_1, \ldots, x_n) = \bigwedge_{i:\, \alpha_i = 1} x_i$$

будем называть *монотонной конъюнкцией*, соответствующей набору α. По определению монотонная конъюнкция, соответствующая нулевому набору, — это функция тождественная единица.

Пусть $B \in \mathcal{B}_n$ — некоторый носитель. Определим псевдо-булевскую функцию f_B, значение которой на наборе x из E^n будет определяться числом наборов из B, не больших чем x, т.е. $f_B(x) = |B_x|$, где $B_x = \{\alpha \in B : \alpha \leq x\}$. Нетрудно заметить, что множество B является множеством нижних единиц монотонной функции f_B и $f_B = \sum_{\alpha \in B} K_\alpha$, где знак суммы означает обычную арифметическую сумму. Класс $\Phi_n = \{f_B : B \in \mathcal{B}_n\}$ будем называть классом *арифметических сумм монотонных конъюнкций*. В работе [3] рассматривается более общий случай линейных комбинаций монотонных конъюнкций, а именно функций вида $g_B = \sum_{\alpha \in B} k_\alpha K_\alpha$, где $B \in \mathcal{B}_n$, $k_\alpha \in \mathbb{N}$. Обозначим $\Delta_n = \{g_B : B \in \mathcal{B}_n\}$.

Множество всех алгоритмов, расшифровывающих класс Φ_n, обозначим через $\mathcal{A}(\Phi_n)$.

Сложностью $\varphi(A, f)$ алгоритма A на функции f будем называть число запросов на значение функции, требуемое алгоритму A для расшифровки функции f. Будем называть *сложностью алгоритма A на классе Φ_n* величину $\varphi(A, \Phi_n) = \max\limits_{f \in \Phi_n} \varphi(A, f)$. Функцию $\varphi(\Phi_n) = \min\limits_{A \in \mathcal{A}(\Phi_n)} \varphi(A, \Phi_n)$ будем называть *сложностью расшифровки класса Φ_n*.

Обозначим через $\Phi_{n,p}$ множество всех функций из класса Φ_n, которые задаются не более чем p нижними единицами, т.е.

$$\Phi_{n,p} = \{f_B \in \Phi_n : |B| \leq p\}.$$

Аналогично $\Delta_{n,p} = \{g_B \in \Delta_n : |B| \leq p\}$.

Пусть $A \in \mathcal{A}(\Phi_n)$. Обозначим $\varphi(A, \Phi_n, p) = \max\limits_{f \in \Phi_{n,p}} \varphi(A, f)$. Еще раз отметим, что алгоритм A расшифровывает класс Φ_n, т.е. он, вообще говоря, не знает никаких ограничений на количество нижних единиц у функции f.

Обозначим $\varphi(\Phi_n, p) = \min\limits_{A \in \mathcal{A}(\Phi_n)} \varphi(A, \Phi_n, p)$.

В работе [3] предложен алгоритм A_1 расшифровки класса Δ_n, для которого получена следующая оценка

$$\varphi(A_1, \Delta_n, p) \le np + p - p\log_2 .$$

В данной работе предлагается алгоритм A_2, учитывающий особенности функций из класса Φ_n.

Теорема 1. *Существует алгоритм A_2 расшифровки класса Φ_n, для которого выполнено равенство*

$$\varphi(A_2, \Phi_n, p) = \begin{cases} np - p - p\lfloor\log_2 p\rfloor + 2^{\lfloor\log_2 p\rfloor+1}, & \text{если } 0 < p < C_n^{[\frac{n}{2}]}, \\ 1, & \text{если } p = 0. \end{cases}$$

Легко видеть, что данная величина согласуется с неравенством из работы [3].

Для получения нижней оценки предложен алгоритм ответов на запросы алгоритмов расшифровки, который заставляет расшифровывающие алгоритмы задавать как можно больше вопросов. Этот алгоритм в совокупности с алгоритмом расшифровки A_2 позволяет получить точные значения сложности расшифровки для некоторых классов арифметических сумм монотонных конъюнкций.

Теорема 2. *Имеют место следующие равенства*

$$\varphi(\Phi_n, 1) = n + 1,\ \varphi(\Phi_n, 2) = 2n,\ \varphi(\Phi_n, 3) = 3n - 2.$$

Список литературы

1. Ансель Ж. О числе монотонных булевых функций n переменных // Кибернетический сборник. Новая серия. — М.: Мир, 1968. — Вып. 5. — С. 53–57.

2. Angluin D. Queries and concept learning // Machine Learning. — 1988. — V. 2. — P. 319–342.

3. Nakamura A., Abe N. Exact learning of linear combinations of monotone terms from function value queries // Theoretical Computer Science. — 1995. — V. 137, I. 1. — P. 159–176.

АЛГОРИТМИЧЕСКАЯ РАЗРЕШИМОСТЬ ПРОБЛЕМЫ АЛФАВИТНОГО ДЕКОДИРОВАНИЯ В РЕГУЛЯРНЫХ ЯЗЫКАХ

П. С. Дергач (Москва)

Целью этой работы является установление алгоритмической разрешимости проблемы однозначности алфавитного декодирования регулярных текстов.

Будем называть *абстрактным конечным автоматом* набор $V = (A, Q, B, \varphi, \psi)$, где A, Q, B — конечные множества, φ — функция, определенная на множестве $Q \times A$ и принимающая значения из Q, ψ — функция, определенная на множестве $Q \times A$ и принимающая значения из B. Множества A, Q, B называются соответственно *входным алфавитом*, *алфавитом состояний* и *выходным алфавитом* автомата V. Функция φ называется *функцией переходов*, а функция ψ — *функцией выходов* автомата V. *Входными словами* автомата V, $V = (A, Q, B, \varphi, \psi)$ называем произвольные конечные последовательности символов алфавита A. Для удобства рассматриваем при этом также "пустое" слово, не имеющее ни одного символа и обозначаемое Λ. *Выходными словами* алфавита V называем конечные последовательности символов алфавита B, *словами состояний* — конечные последовательности символов алфавита Q (в обоих случаях допускается и пустое слово Λ). Для каждого состояния автомата V можно рассмотреть набор $(A, Q, B, \varphi, \psi, q)$, определяющий автомат V с выделенным начальным состоянием q. Такие наборы $(A, Q, B, \varphi, \psi, q)$ называются *инициальными абстрактными конечными автоматами*; для них используется обозначение V_q.

Функции переходов и выходов автомата $V = (A, Q, B, \varphi, \psi)$ доопределим на множестве $Q \times A^*$ (сохраним за ними те же обозначения). Именно, полагаем по определению

$$\varphi(q, \Lambda) = q, \varphi(q, \alpha a) = \varphi(\varphi(q, \alpha), a),$$

где $q \in Q$, $\alpha \in A^*$, $a \in A$. Аналогично,

$$\psi(q, \Lambda) = \Lambda, \ \psi(q, \alpha a) = \psi(\varphi(q, \alpha), a).$$

Пусть $V_q = (A, Q, B, \varphi, \psi, q)$ — инициальный абстрактный конечный автомат, $B' \subseteq B$. Множество $M = \{\alpha \mid \alpha \in A^*, \ \psi(q, \alpha) \in B'\}$ называем *представимым в абстрактном конечном автомате* V_q с помощью подмножества B' выходных символов. Говорим также, что автомат V_q *представляет* M *посредством* B'. Пусть $M \subseteq A^* \setminus \{\Lambda\}$. Если существует конечный автомат V_q, представляющий событие

M посредством некоторого подмножества $B' \subseteq B$, то событие M называем *представимым*.

Пусть $A = \{a_1, \ldots, a_r\}$ — произвольный конечный непустой алфавит. Пусть P_1, P_2 — непустые множества слов в алфавите A. Здесь и далее для удобства пустое слово за элемент множества A^* не считается. Определим следующие операции над P_1 и P_2:

1. *Произведение* множеств P_1 и P_2 (обозначаем $P_1 \cdot P_2$) есть множество всех слов вида $\alpha_1\alpha_2$, где $\alpha_1 \in P_1,\ \alpha_2 \in P_2$.

2. *Итерация* множества P_1 (обозначаем $(P_1)^*$) есть множество всех слов вида $\alpha_1 \ldots \alpha_k$, где $\alpha_1 \in P_1,\ \ldots, \alpha_k \in P_1,\ k \geq 1$.

Множество P, $P \subseteq A^*$, называем *регулярным в алфавите* A, если его можно получить из множеств вида $\{a\},\ a \in A$, применением конечного числа операций $\cup, \cdot, ()^*$.

Введем понятие *регулярного выражения в алфавите* A. Регулярным выражением в алфавите A будем называть любое слово в алфавите $A \cup \{\vee, \cdot, (,), *\}$, полученное следующим образом:

1. Буквы алфавита A — регулярные выражения в алфавите A;

2. Пусть $\alpha,\ \beta$ — регулярные выражения в алфавите A. Тогда $(\alpha \vee \beta),\ (\alpha \cdot \beta),\ (\alpha)^*$ — регулярные выражения в алфавите A;

3. Регулярность произвольного выражения в алфавите A устанавливается в соответствиями с пп. 1, 2 за конечное число шагов.

Сопоставим индуктивно каждому регулярному выражению $\mathfrak{P}$ в алфавите A регулярное множество $|\mathfrak{P}|$ в алфавите A:

1. Множество $\{a\}$ — в случае $\mathfrak{P} = a,\ a \in A$;

2. Множество $|\mathfrak{P}_1| \cup |\mathfrak{P}_2|$ — в случае $\mathfrak{P} = (\mathfrak{P}_1 \vee \mathfrak{P}_2)$;

3. Множество $|\mathfrak{P}_1| \cdot |\mathfrak{P}_2|$ — в случае $\mathfrak{P} = (\mathfrak{P}_1 \cdot \mathfrak{P}_2)$;

4. Множество $(|\mathfrak{P}_1|)^*$ — в случае $\mathfrak{P} = (\mathfrak{P}_1)^*$.

Зафиксируем два конечных непустых алфавита A и B.

Пусть есть какое-то отображение $f : A \to B^*$:

$$f(a_1) = \beta_1$$
$$f(a_2) = \beta_2$$
$$\ldots$$
$$f(a_r) = \beta_r$$

Это соотношение называется *схемой кодирования*. Доопределим отображение f до отображения $\tilde{f} : A^* \to B^*$ следующим образом:

$$\tilde{f}(a_{i_1} a_{i_2} \ldots a_{i_n}) = \beta_{i_1}\beta_{i_2} \ldots \beta_{i_n}.$$

Это отображение $\tilde{f}$ будем называть *алфавитным кодированием.*

Пусть есть некоторое регулярное множество P в алфавите A и некоторое алфавитное кодирование f. Пусть $\beta \in \tilde{f}(P)$. Тогда $\alpha \in P$ называется *расшифровкой β при алфавитном кодировании $\tilde{f}$ на регулярном множестве P* или *расшифровкой β*, если $f(\alpha) = \beta$. Таких расшифровок может быть несколько. Если для любых различных $\alpha_1, \alpha_2 \in P$ выполняется $\tilde{f}(\alpha_1) \neq \tilde{f}(\alpha_2)$, то говорим, что *декодирование однозначно на P по $\tilde{f}$.*

Теорема 1. *Существует алгоритм, определяющий по произвольной паре $(\tilde{f}, \mathfrak{P})$, где $\tilde{f}$ — алфавитное кодирование из алфавита A в алфавит B, а $\mathfrak{P}$ — регулярное выражение в алфавите A, однозначно ли декодирование на $|\mathfrak{P}|$ по $\tilde{f}$.*

Список литературы

1. Яблонский С. В. Введение в дискретную математику. — М.: Наука, 1986.

2. Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Введение в теорию автоматов. — М.: Наука, 1985.

МИНИМИЗАЦИЯ СРЕДНЕГО ВРЕМЕНИ ДВИЖЕНИЯ В ТРАНСПОРТНОЙ СЕТИ

Г. В. Калачев (Москва)

Рассматривается следующая задача. Дана транспортная сеть, в которой есть N пунктов. Известно, сколько машин проезжает из i-го пункта в j-й за единицу времени. Для каждой дороги известна ее пропускная способность и время движения по ней при заданной загруженности. Рассматриваем случай, когда ситуация не зависит от времени. Требуется минимизировать среднее время движения машин в этой транспортной сети.

Представим эту сеть, как ориентированный граф (V, E) с N вершинами. Вершины графа будем обозначать их номерами от 1 до N. Ребро из i-й вершины в j-ю будем обозначать (ij).

Заданы следующие матрицы размера $N \times N$:

1. *Матрица назначений Φ*, элементы которой — будем обозначать φ^{ij} — неотрицательные вещественные числа, причем $\varphi^{ii} = 0; i = \overline{1, N}$. Эту матрицу также будем называть *входящим потоком.*

2. *Матрица пропускных способностей* C, элементы которой $c_{ij} \in \mathbb{R}_+ \cup \{\infty\}$. Если ребра (ij) нет в графе, то должно быть $c_{ij} = 0$.

3. Матрица P, элементы которой p_{ij} — функции из R_+ в R_+: $p_{ij}(\varphi)$ — время проезда по ребру (ij), если поток по нему равен φ.

Будем говорить, что $(\varphi_{kl}^{ij})_{i,j,k,l=1}^N$ — *распределение входящего потока* Φ, если при фиксированных i и j, φ_{kl}^{ij} — обычный поток с источником i, стоком j и величиной Φ_{ij}, т. е. выполнено:

$$\forall i,j,k : i \neq j \;\Rightarrow\; \sum_{l=1,l\neq k}^{N} (\varphi_{kl}^{ij} - \varphi_{lk}^{ij}) = \begin{cases} \varphi^{ij}, & \text{если } i = k, \\ -\varphi^{ij}, & \text{если } j = k, \\ 0, & \text{иначе.} \end{cases} \qquad (1)$$

Введем обозначения: $\varphi_{kl}^{j} := \sum_{i=1}^{N} \varphi_{kl}^{ij}$ — суммарный поток в j-ю вершину, идущий через ребро (kl); $\varphi_{kl} := \sum\limits_{j=1}^{N} \varphi_{kl}^{j}$ — суммарный поток по ребру (kl).

Тогда при фиксированном j, (φ_{kl}^{j}) — поток со многими источниками и одним стоком в вершине j. Интенсивность источников задается j-м столбцом матрицы Φ: суммируя (1) по i, для всех k и j получим

$$\sum_{l=1,l\neq k}^{N} (\varphi_{kl}^{j} - \varphi_{lk}^{j}) = \begin{cases} \varphi^{kj}, & \text{если } j \neq k, \\ -\sum\limits_{i=1,i\neq j}^{N} \varphi^{ij}, & \text{если } j = k. \end{cases}$$

Распределение (φ_{kl}^{ij}) потока Φ назовем *допустимым*, если оно удовлетворяет ограничениям:

1) $\varphi_{kl}^{ij} \geq 0$, т.е. каждый поток неотрицателен

2) $\varphi_{kl} \leq c_{kl}$, т.е. суммарный поток по ребру не превышает пропускную способность ребра.

Граф *пропускает входящий поток* Φ, если существует допустимое распределение (φ_{kl}^{j}) потока Φ.

Задача заключается в нахождении допустимого распределения потоков $\vec{\varphi}$, на котором достигает минимума функционал

$$P[\vec{\varphi}] := \sum_{k,l=1}^{N} \underbrace{p_{kl}(\varphi_{kl})\varphi_{kl}}_{q_{kl}(\varphi_{kl})}.$$

Он интерпретируется, как среднее время движения по транспортной сети, соответствующей нашему графу, где $p_{kl}(\varphi_{kl})$ — среднее время движения по дороге, соответствующей ребру kl, если поток по ней равен φ_{kl}.

Если функционал $P[\vec{\varphi}]$ линейный (т.е. p_{ij} — константы), то эта задача является задачей линейного программирования.

Утверждение 1. *Пусть функции $q_{ij}(x)$ выпуклы вниз при $x > 0$. Тогда задача минимизации функционала $P[\vec{\varphi}]$ на множестве допустимых потоков является задачей выпуклого программирования.*

Следствие. *Если выполнены условия утверждения 1, то решение задачи может быть найдено с заданной точностью за полиномиальное время при помощи метода эллипсоидов.*

Нужно отметить, что сложность метода эллипсоидов здесь очень большая, хотя и полиномиальная. Поэтому рассмотрим упрощенный вариант этой задачи. Откажемся от ограничений потоков пропускными способностями (положим $c_{ij} = \infty$). Пусть $q_{ij}(x)$ строго выпуклы вниз и непрерывно дифференцируемы. Тогда q'_{ij} строго возрастает и непрерывна, а значит существует обратная функция, которую обозначим ψ_{ij}. Если ребра (ij) в графе нет, то положим $\psi_{ij} \equiv 0$. При $y < q'_{ij}(0)$ доопределим $\psi_{ij}(y) = 0$.

Утверждение 2. *Пусть есть несколько источников и один сток в 0-й вершине. Обозначим: Φ_j — поток, выходящий из j-й вершины ($j > 0$); $g_{ij}(y) := \psi_{ij}(y) - \psi_{ji}(-y)$. Тогда минимум функционала $P[\varphi]$ будет достигаться на потоке вида $\hat{\varphi}_{ij} = \max(g_{ij}(\lambda_i - \lambda_j), 0)$, где λ_i — решение системы уравнений*

$$g_{i0}(\lambda_i) + \sum_{j=1}^{N} g_{ij}(\lambda_i - \lambda_j) = \Phi_i, i = \overline{1, N}. \tag{2}$$

Если g_{ij} возрастают, g_{i0} строго возрастают, то система (2) имеет не более одного решения.

Следствие. *Для решения этой задачи можно применять метод Ньютона, причем на каждой итерации придется решать СЛУ с матрицей, у которой количество ненулевых элементов в $i-$й строке на 1 больше степени i-й вершины графа.*

Область сходимости метода Ньютона сильно зависит от функций g_{ij}: чем они ближе к линейным, тем больше область сходимости. Случай линейной системы получается, если $p_{ij}(x) = ax$. Поскольку транспортной сети обычно соответствует разреженный граф, то можно применять алгоритмы для решения СЛУ с разреженными матрицами.

Есть интерпретация системы (2) в терминах электрических схем: представим, что есть электрическая схема с $N+1$ узлом, а ребра — некоторые нелинейные элементы, для которых зависимость тока от напряжения задается функциями g_{ij}. Тогда λ_j будет соответствовать потенциалу в j-й вершине, в 0-й вершине потенциал нулевой, можно считать, что она заземлена. На i-ю вершину подается ток, равный Φ_i. Решение системы означает поиск потенциалов в узлах схемы. Если система линейна, то ей соответствует схема из резисторов.

Работа выполнена под руководством профессора Э. Э. Гасанова.

Список литературы

1. Кормен Т., Лейзерсон Ч., Ривест Р. Алгоритмы. Построение и анализ. — М.: МЦМНО, 2001.

ОБ АВТОМАТНОЙ СЛОЖНОСТИ НЕКОТОРЫХ КЛАССОВ ПОСТА БУЛЕВЫХ ФУНКЦИЙ

М. А. Кибкало (Москва)

Определение сложности представления языков различными структурами — одна из традиционных задач теории автоматов. В случае представимости конечными автоматами под сложностью языка понимается число состояний в представляющем его приведенном автомате. В работе рассматривается сложность представления булевых функций конечными автоматами и устанавливаются точные значения и асимптотические оценки функции Шеннона для некоторых замкнутых классов булевых функций, входящих в решетку Поста.

В произвольном конечном алфавите A определим класс конечных языков, содержащих слова равной длины: $\mathcal{L}_n(A) = \{L \subseteq A^n\}$. Каждой $f \in P_2^n$ можно взаимно однозначно сопоставить конечный язык $L(f) \in \mathcal{L}_n(E)$, где $E = \{0,1\}$ по правилу: слово $\tilde{\alpha} = \alpha_1 \dots \alpha_n \in L(f) \Leftrightarrow f(\tilde{\alpha}) = f(\alpha_1, \dots, \alpha_n) = 1, \alpha_i \in E, i \in 1, \dots, n$.

Введем согласно [1] понятия инициального конечного автомата (ИКА) и представимости конечного языка в ИКА. Будем говорить, что ИКА $V_q = (E, Q, E, \varphi, \psi, q)$ представляет $f \in P_2^n$, если он представляет $L(f) \in \mathcal{L}_n(E)$.

Сложностью $S(V_q)$ ИКА V_q назовем число состояний в нем. Автоматной сложностью булевой функции $f \in P_2^n$ назовем наименьшую

сложность ИКА, представляющего язык $L(f) \in \mathcal{L}_n(E) : S(f,n) = \min_{V_q \sim L(f)} S(V_q)$. Пусть $\mathcal{K} \subseteq P_2$ — класс булевых функций, $\mathcal{K}(n) = \mathcal{K} \cap P_2^n$. Сложностью $\mathcal{K}(n)$ (функцией Шеннона класса $\mathcal{K}$) назовем $S(\mathcal{K},n) = \max_{f \in \mathcal{K}(n)} S(f,n)$. Поскольку множество $\mathcal{K}(n)$ определяет совокупность языков из класса $\mathcal{L}_n(E)$, назовем $S(\mathcal{K},n)$ функцией Шеннона соответствующего класса конечных языков.

Далее будем пользоваться нотацией классов Поста, введенной в [2]. Асимптотическое поведение функции Шеннона автоматной сложности классов Поста $C_i, i = 1-4$; D_1, D_3; $F_j^\mu(n), j = 1,4,5,8, \mu > 1, \mu \in \mathbb{N}$; $A_i, i = 1-4$; $F_r^\infty(n), r = 1-8$; $F_t^\mu(n), t = 2,3,6,7, \mu > 2, \mu \in \mathbb{N}$ описано в [4,5].

Положим $A(n) \asymp B(n)$, если $\exists c_1, c_2, 0 < c_1 \leqslant c_2$ такие, что

$$c_1 \cdot B(n) \lesssim A(n) \lesssim c_2 \cdot B(n)$$

Для получения оценок функции Шеннона для классов Поста D_2 и $F_t^2, t = 2,3,6,7$ воспользуемся результатами, изложенными в [4–7].

Теорема 1. *Пусть $\mathcal{K}$ — один из классов D_2, $F_t^2, t = 2,3,6,7$. Тогда:*

$$S(\mathcal{K},n) \asymp \frac{2^n}{n \cdot \sqrt{\log n}}.$$

При этом константы c_1, c_2 из определения отношения $\asymp$ равны

$$c_1 = \sqrt{2/\pi},\ c_2 = 2\sqrt{2/\pi}.$$

Приведем формулы, выражающие точные значения функции Шеннона для некоторых классов Поста. Для $p \in \mathbb{N}$ положим $\widetilde{n}(p) = 2^p + p$.

Теорема 2. Для любых $p \in \mathbb{N}, n \in [\widetilde{n}(p), \widetilde{n}(p+1))$ *и* $\mathcal{K} \in \{C_i, i = 1-4\}$ *существует такая* $f_n \in \mathcal{K}(n)$, *что*

$$S(\mathcal{K},n) = S(f_n,n) = 2^{n-p} - p - 2 + \sum_{i=0}^{p} 2^{2^i}.$$

Теорема 3. Для любых $p \in \mathbb{N}, n \in [\widetilde{n}(p), \widetilde{n}(p+1))$ *и* $\mathcal{K} \in \{D_1, D_3\}$ *существует такая* $f_{n,s} \in \mathcal{K}(n)$, *что*

$$S(\mathcal{K},n) = S(f_{n,s},n) = 2^{n-p} - p - 2 - u(p) + \sum_{i=0}^{p} 2^{2^i},$$

где $u(p) = \begin{cases} 2^{2^{p-1}-1}, & \textit{при } n = \widetilde{n}(p); \\ 0, & \textit{иначе.} \end{cases}$

Теорема 4. Для любых $p \in \mathbb{N}, p \geq 2$ *и* $\mathcal{K} \in \{F_j^\infty, j = 1, 4, 5, 8\}$ *существует такая* $f_{n,\infty} \in \mathcal{K}(n)$, *что при* $n \in [\widetilde{n}(p) + 1, \widetilde{n}(p+1) + 1)$

$$S(\mathcal{K}, n) = S(f_{n,\infty}, n) = \frac{3}{4} \cdot 2^{n-p} - p - v(j) + \sum_{i=0}^{p} 2^{2^i},$$

а при $n = \widetilde{n}(p) + 1$

$$S(\mathcal{K}, n) = S(f_{n,\infty}, n) = 2^{n-p} - p - 1 - v(j) + \sum_{i=0}^{p} 2^{2^i},$$

где $v(j) = \begin{cases} 1, & \textit{при } j = 1, 4; \\ 2, & \textit{при} j = 5, 8. \end{cases}$

Отметим, что сложность реализации булевых функций конечными автоматами не коррелирует со сложностью реализации булевых функций полиномами Жегалкина. Сложность полинома Жегалкина булевой функции f определяется как число его ненулевых коэффициентов и обозначается $S^{\oplus}(f)$. В данной работе показано, что сложность полиномов Жегалкина для булевых функций, представляемых сложными автоматами, может кардинально отличаться.

Теорема 5. *Существует последовательность* $n_p \to \infty$ *при* $p \to \infty$, *такая что для функций* $f'_{n_p}, f''_{n_p} \in P_2^{n_p}$ *выполнено:* $S(f'_{n_p}, n_p) = S(f''_{n_p}, n_p) \sim \frac{2^{n_p+1}}{n_p}$, *но* $S^{\oplus}(f'_{n_p}) \sim n_p$ *и* $S^{\oplus}(f''_{n_p}) \sim 2^{n_p}$. Автор выражает благодарность Кудрявцеву В. Б. и Бабину Д. Н. за ценные замечания и внимание к работе.

Список литературы

1. Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Введение в теорию автоматов. —М.: Наука, 1985.

2. Яблонский С. В., Гаврилов Г. П., Кудрявцев В. Б. Функции алгебры логики и классы Поста. —М.: Наука, 1966.

3. Угольников А. Б. О реализации функций из замкнутых классов схемами из функциональных элементов // Математические вопросы кибернетики. —М.: Наука, 1988. — Вып. 1. — С. 90–114.

4. Кузьмин А. Д. Реализация функций алгебры логики автоматами, нормальными алгорифмами и машинами Тьюринга // Проблемы кибернетики. — М.: Наука, 1955. — Вып. 13. — С. 75–96.

5. Кибкало М. А. Об автоматной сложности некоторых классов булевых функций // Интеллектуальные системы. — 2011. — Т. 14.

6. Коршунов А. Д. О числе монотонных функций // Проблемы кибернетики. — 1981. — Вып. 38. — С. 5–109.

7. Сапоженко А. А. О числе антицепей в многослойных ранжированных множествах // Дискретная математика. — 1989. — Т. 1, вып. 2. — С. 110–128.

РЕДУКЦИЯ ОБЛАСТЕЙ ЗАВИСИМОСТИ ДЛЯ АБСТРАКТНЫХ ПРОЦЕССОВ В ПРОСТРАНСТВАХ ЗНАНИЙ

К. И. Костенко (Краснодар)

Абстрактное пространство знаний — это математический формализм, обеспечивающий возможность дедуктивного порождения многообразия известных и новых моделей интеллектуальных систем. Он основан на вычислимом множестве конфигураций M, элементы которого являются абстрактными образами отдельных знаний [1]. Полные структурные представления конфигураций (ПСП) имеют вид конечных нагруженных бинарных деревьев с конечными двоичными наборами, определяющими пути из корня, в качестве вершин. Вершины ПСП размечены целыми неотрицательными числами. Разметка висячих (внутренних) вершин ПСП конфигураций определяет элементарные конфигурации (семантические отношения между конфигурациями левого и правого поддеревьев таких вершин). Пусть I (I_α) — множество конечных двоичных наборов (наборов, начинающихся с $\alpha \in I$). Множество вершин ПСП конфигурации $z \in M$ обозначим как $D(z)$. Выражение $(z)_\alpha$ обозначает конфигурацию, ПСП которой задаётся поддеревом дерева $D(\mathrm{z})$ с корнем α в ПСП z.

Одним из компонентов формализма пространств знаний является пространство процессов. Фундаментальными инвариантами процессов являются время, унифицированные форматы начальных данных, реализации и результаты процессов, структуры процессов и схемы их взаимодействия. Специальным классом процессов являются эволюции конфигураций [2].

Реализации и функции процессов. Всякий процесс на M задаётся вычислимым семейством операторов перехода и остановки, сопоставляемых вершинам ПСП конфигураций. Это семейство называется базисом и представляется в виде $\oplus(T_\alpha, S_\alpha)$, где $\alpha \in I_0$. Здесь $T_\alpha : M \to N \cup \emptyset$ — оператор перехода, определяющий изменение разметки вершины α за один шаг процесса. Специальное значение $\emptyset$ используется в качестве разметки вершин, которые не входят в ПСП конфигураций. Операторы остановки $S_\alpha : M \to \{0, 1, \emptyset\}$ идентифицируют вершину α ПСП всякой конфигурации как заключительную ($S_\alpha(z) = 0$) и незаключительную ($S_\alpha(z) = 1$). Кроме того, $S_\alpha(z) = \emptyset$ т. и т. т., когда $\alpha \notin D(z)$.

Пусть задан процесс $E = \oplus(T_\alpha, S_\alpha)$. Обозначим как DT_α и DS_α подмножества множества I, составленные вершинами, применяемыми в ПСП произвольных конфигураций, от которых зависят операторы T_α и S_α. Назовём такие множества областями зависимости этих операторов. Процесс с базисом $\oplus(T_\alpha, S_\alpha)$ называется локальным, если области зависимости операторов T_α и S_α, $\alpha \in I_0$, — конечные.

Начальными данными всякого процесса являются вычислимые последовательности $\{(z^i, t^i) | i \in N\}$. Множество таких последовательностей обозначим как Ω. Для каждого $\omega \in \Omega$ процесс E с базисом $\oplus(T_\alpha, S_\alpha)$ порождает реализацию, определяемую следующими правилами.

1. ПСП конфигурации z^i в составе ω размещается в области I_1 в момент времени t^i. В остальные моменты времени содержимое I_1 не изменяется.

2. В начальный момент $t = 0$ разметки вершин из I_0 — пустые. В последующие моменты времени содержимое I_0 вычисляется с помощью операторов перехода T_α, $\alpha \in T_0$, по конфигурации, определяемой разметкой всех вершин из I.

Реализация процесса E на начальном данном ω, образует бесконечную последовательность $\{(z_i, i) | i \in N\}$, где z_i — это конфигурация, представленная в I в момент i. Результаты реализаций процесса E, для различных $\alpha \in I_0$, вычисляются с помощью операторов S_α. Результат реализации процесса E в $\alpha \in I_0$ образует вычислимая последовательность $\{(z_i)_\alpha, t_i) | S_\alpha(z_i) = 0\}$.

Каждый процесс E определяет множество вычислимых отображений $\pi(E) = \{ue_\alpha : \Omega \to \Omega | \alpha \in I\}$. Для таких отображений $ue_\alpha(\omega_1) = \omega_2$ означает, что результатом реализации процесса E на начальном данном ω_1 в вершине α является ω_2. Семейство всех отображений, реализуемых процессом E, обозначается как $\pi(E)$.

Области связности локальных процессов. Области I_α и I_β называются связными (сильно связными) для процесса E , если существует такое конечное множество $D \subseteq I$ $(D = \emptyset)$, что

$\forall\gamma \in I_\alpha \cup I_\beta (DT_\gamma \cup DS_\gamma \subseteq I_\alpha \cup I_\beta \cup D)$.

Пусть для локального процесса E заданы связные области I_α и I_β , где α не является началом β , а β не является началом α. Для таких процессов рассмотрим задачу. Если области I_α и I_β — сильно связные, то существует ли такой локальный процесс $E^* = \oplus({T^*}_\alpha, {S^*}_\alpha)$, в котором I_α и I_β являются сильно связными и выполняются условия:

1) $\pi(E) = \pi(E^*)$;

2a) существует такое конечное множество $D \subseteq I_\alpha \cup I_\beta$,что $\forall\gamma \in I_\alpha((DT_\gamma \cup DS_\gamma) \cap I_\beta \subseteq D)$ и $\forall\gamma \in I_\beta((DT_\gamma \cup DS_\gamma) \cap I_\alpha \subseteq D)$.

Определим аналогичную задачу для связных процессов, в которой условие 2a. заменено на условие

2b) существует конечное множество $D \subseteq I$, для которого истинны соотношения из 2a.

Решения данных задач представлены в теоремах.

Теорема 1. *Существует локальный процесс E, имеющий сильно связные области I_α и I_β, для которого не существует такого локального процесса, что выполняются условия* 1) *и* 2*a*).

Теорема 2. *Существует алгоритм, который для всякого локального процесса E, имеющего связные области I_α и I_β, определяет такой локальный процесс, для которого выполнены свойства* 1) *и* 2*b*).

То есть, для связных дизъюнктных областей всякого процесса возможна редукция областей зависимости операторов перехода и остановки из базиса этого процесса к конечному подмножеству I.

Список литературы

1. Костенко К. И. Абстрактное моделирование пространств знаний // Материалы Всероссийской конференции ЗОНТ2011. Новосибирск, 3–5 октября 2011. Т. 2. — С. 25–31.

2. Костенко К. И. Об алгоритмических свойствах пространств эволюций знаний // Экологический вестник научных центров Черноморского экономического сотрудничества. — 2007. — № 4. — С. 14–20.

ЦИКЛОВЫЕ ИНДЕКСЫ И ЗАДАЧА ВЫРАЗИМОСТИ АВТОМАТОВ ОТНОСИТЕЛЬНО СУПЕРПОЗИЦИИ БЕЗ ОБРАТНОЙ СВЯЗИ

А. А. Летуновский (Москва)

Вводится понятие циклового индекса автомата. Показана связь цикловых индексов автомата и множества выразимых через автомат констант. Также с помощью цикловых индексов автомата доказаны теоремы о выразимости групповых автоматов и произвольных автоматов Медведева.

Будем использовать основные понятия из [1]. Обозначим P_2 — множество всех булевых функций. P — множество всех автоматных функций. $R \subset P$ — произвольное конечное множество автоматных функций. $[R]$ — замыкание конечного подмножества относительно суперпозиции без обратной связи. Z — автоматная функция задержки. T — автоматная функция "триггер". Обозначим $< R >= [R \cup \{Z, P_2\}]$.

Назовем автоматную функцию, не зависящую от входа, константной автоматной функцией. Множество всех константных автоматных функций обозначим K. Без ограничения общности константную автоматную функцию можно отождествить со сверхсловом, которое является его выходом.

Пусть сверхслово β можно представить в виде $\beta = \gamma\alpha^\infty$. Выберем из всех таких представлений такое, что γ и α имеют наименьшую длину. Для выбранного представления назовем γ — наименьшим *предпериодом сверхслова* β,а α наименьшим *периодом сверхслова* β, а слова вида $\underbrace{\alpha\alpha...\alpha}_{n}$ будем называть периодом сверхслова β, здесь $n \in N$. Обозначим $|\alpha|$ длину слова α.

Для множества константных автоматных функций $K' \subseteq K$ обозначим через $\Theta(K')$ — множество длин минимальных периодов сверхслов $\{\beta_{K_i} : K_i \in K'\}$. Для случая одного слова $\beta = \gamma\alpha^\infty$ будем считать, что $\Theta(\beta) = |\alpha|$.

Нашей задачей будет описание множества $\Theta(< R > \cap K)$ для произвольного множества R.

Теорема 1. *Пусть R — конечное множество автоматных функций, тогда $\exists b, q$, зависящие от R, такие что*

$$\Theta(< R > \cap K) = \{t : \exists i \in N \quad t | bq^i\}.$$

Следствие 1. *Пусть R — конечное множество автоматных функций и β — константная автоматная функция, тогда существует алгоритм, позволяющий проверить свойство* $\beta \in < R >$.

Следствие 2. *Пусть R — конечное множество автоматных функций, тогда существует алгоритм, позволяющий проверить свойство* $\mid \Theta(< R > \cap K) \mid < \infty$.

Цикловые индексы автомата позволяют добиться прогресса в решении общей задачи выразимости [2, 3]. В частности верны следующие утверждения.

Теорема 2. *Пусть R — произвольная система автоматов, M — произвольный групповой автомат Медведева, тогда задача определения $M \in < R >$ является алгоритмически разрешимой.*

Теорема 3. *Пусть R — произвольная система автоматов, M — произвольный групповой автомат, тогда задача определения $M \in < R, Z_2 >$ является алгоритмически разрешимой.*

Теорема 4. *Пусть R — произвольная система автоматов, тогда задача $< R, T > \supseteq P_a^n$ является алгоритмически разрешимой.*

Список литературы

1. Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Введение в теорию автоматов. — М.: Наука, 1985.

2. Летуновский А. А. О выразимости константных автоматов суперпозициями // Интеллектуальные системы. — 2009. — Т. 13, вып. 1–4. — С. 397–406.

3. Летуновский А. А. О выразимости суперпозициями автоматов с разрешимыми группами // Интеллектуальные системы. — 2010. — Т. 14, вып. 1–4. — С. 379–392.

ОБ ОДНОМ АЛГОРИТМЕ РЕШЕНИЯ ЗАДАЧИ О ПРОТЫКАНИИ

Т. С. Лушникова (Москва)

В данной работе рассматривается алгоритм решения задачи о протыкании (далее — Алгоритм А1).

Задача о протыкании (другое название — о прокалывании) — это пара (X, V), где множество запросов $X = [0, 1]$, а библиотека V представляет из себя конечное множество, состоящее из отрезков с концами из $[0, 1]$, т.е. $V = \{[a_i, b_i], 0 \leq a_i < b_i \leq 1, i = 1..n\}$.

Результат запроса $x \in X$ — это такое множество отрезков из V, которым принадлежит точка x.

Содержательно эта задача состоит в том, чтобы для произвольного запроса $P \in X$, перечислить все те и только те отрезки из V, в которые попадает точка P. Будем предполагать, что ни у каких отрезков из множества V не совпадают начала или концы.

Структура базы данных. Пусть A — множество, состоящее из начал отрезков из V, а B — из концов соответствующих отрезков.

Создадим новое множество отрезков $C = A \cup B$. Обозначим элементы нового множества таким образом, чтобы $\forall c_i, c_j : \ i < j \Rightarrow c_i < c_j$. Возьмем $c_0 = 0, .., c_{k+1} = 1$ (если $c_1 \neq 0, c_k \neq 1$). Получим отрезки $[c_i, c_{i+1}], i = 0..k+1, k < 2n+2$ (где n — количество исходных отрезков).

Строим бинарное дерево поиска для множества отрезков C. На выходе имеем отрезок $C^i = [c_i, c_{i+1}]$. Теперь необходимо определить, каким отрезкам $[a_j, b_j], j = 1..n$ принадлежит отрезок C^i.

Заметим, что нужно еще проверить, не является ли точка P крайней для найденного отрезка. Тогда в ответ необходимо выписать еще и все отрезки, которым принадлежит соседний отрезок C^{i+1}.

Пусть количество отрезков $m = 2^r$, т.е. $|C| = 2^r + 1$.

Строим идеально сбалансированное бинарное дерево поиска. Количество листьев — m. Припишем каждому листу соответствующий отрезок $[c_i, c_{i+1}]$. Рассмотрим отрезок $[c_i, c_{i+1}]$ и соседний с ним $[c_{i+1}, c_{i+2}]$ (пусть они имеют общего родителя). Пусть этим отрезкам соответствуют листья дерева M_i,M_{i+1}. Их родитель M^0.

Обозначим через M_i, M_{i+1} все отрезки $[a_j, b_j]$, содержащие отрезок C^i, C^{i+1} соответственно. Предположим, что множество $(M_i \cap M_{i+1})$ уже где-то записано, и нам нужно еще где-то хранить только множество $(M_i \cup M_{i+1}) \setminus (M_i \cap M_{i+1})$. Заметим, что последнее множество состоит ровно из одного отрезка $[a_l, b_l]$(т.к. эти отрезки соседние). Припишем вершине M_i(или, соответственно, M_{i+1}) ссылку на отрезок $[a_l, b_l]$. Поднимемся в дереве на уровень выше. Рассмотрим соседние ветви. Их количество — $m/2$. Соседние ветви отличаются не более чем на два отрезка. Припишем ссылки на них в соответствующие вершины. И т.д.

Алгоритм поиска состоит из нескольких этапов:

1. На вход алгоритму подается точка P. Сравниваем P и значение, приписанное корню дерева (пусть c_k). Если $c_k < P$, тогда дальше рассматриваем правое поддерево c_k, иначе — левое. Пусть $c_k < P$ и значение правого "сына" c_k равно c_l. Теперь сравниваем

c_l и P, и, как и выше, если $c_l < P$, тогда дальше рассматриваем правое поддерево c_l, иначе — левое. Продолжаем сравнения до тех пор, пока не дойдем до листа дерева.

Одновременно со спуском вниз по дереву выписываем в ответ отрезки, лежащие в вершинах.

Таким образом мы находим отрезок $[c_i, c_{i+1}]$, такой, что $P \in [c_i, c_{i+1}]$ и все отрезки, которые нужно выписать в ответ.

2. Если в предыдущих шагах мы получили $P = c_{i+1}$, то идем вверх по дереву и "собираем" отрезки, содержащие отрезок $[c_{i+1}, c_{i+2}]$.

Теорема. *Алгоритм A1 решает задачу о прокалывании (X, V) для случая, когда ни у каких отрезков из множества V не совпадают начала или концы. Алгоритм A1 имеет следующие характеристики:*

$$\begin{aligned} T_{A1}(P) &\asymp \log_2 n + h(P), \\ Q_{A1} &\asymp n \log_2 n, \end{aligned}$$

где $h(P)$ — количество отрезков в ответе на запрос P.

Объем памяти. Посчитаем общее количество хранимой информации:

На нижнем уровне хранится не больше $m/2$ отрезков, на уровень выше — $(m/4) * 2$, на i-м уровне снизу — произведение (2^{i-1}) $m/(2^i)$, т. е. объем структуры — это сумма объема бинарного дерева $(4n)$ и объема внутренних ссылок, т.е. $(m/2 + 2 * m/4 + ... + h) = (\log_2 m)m/2 + 4n = 4n + n \log_2 n$.

Сложность алгоритма. Посчитаем сложность алгоритма отдельно для каждого этапа. 1. Сложность выполнения алгоритма на данном этапе равна сумме двух величин: сложности бинарного поиска $(\log_2 m)$, где $m = |C|$ и длины ответа.

2. Если мы получили $P = c_{i+1}$, то выполняем $\log_2 m$ операций. Иначе — 0.

Программная реализация. Данный алгоритм был реализован в виде программы. Опытным путем был вычислен объем памяти, необходимый для хранения ссылок на отрезки в следующих случаях:

- полностью вложенные отрезки: объем пропорционален $n \log_2 n$
- непересекающиеся отрезки: объем не превышает $2n$
- каждый отрезок пересекается не больше чем с 1 отрезком: объем не превышает $3n$

- максимальное количество отрезков, пересекающихся в одной точке — k, и k много меньше n: объем не превышает $c * n$, где c — константа и $c < 2 \log_2 k$

- максимальное количество отрезков, пересекающихся в одной точке — k, и k близко n: объем близок к $n \log_2 n$

Автор благодарит профессора Э. Э. Гасанова за постановку задачи и помощь в работе.

Список литературы

1. Гасанов Э. Э., Кудрявцев В. Б. Теория хранения и поиска информации. — М.: ФИЗМАТЛИТ, 2002.

О ВОССТАНОВЛЕНИИ ЧАСТИЧНО ЗАДАННЫХ МОНОТОННЫХ БУЛЕВЫХ ФУНКЦИЙ ПО КРИТЕРИЮ ПОЛНОГО СКОЛЬЗЯЩЕГО КОНТРОЛЯ

Г. А. Махина (Симферополь), К. В. Воронцов (Москва)

Задача восстановления монотонной булевой функции по подмножеству её нулей и единиц является одной из классических задач дискретной математики. Обычно среди множества всех возможных решений ищут функцию минимальной сложности [1]. Однако простота реализации является не единственным требованием, предъявляемым к монотонным булевым функциям в прикладных задачах. В задачах классификации обычно предполагается, что точки обучающей выборки порождаются некоторым вероятностным распределением и требуется построить функцию классификации с наименьшей вероятностью ошибок. Для формализации этого требования в комбинаторном подходе [2] рассматривается произвольная конечная генеральная совокупность и предполагается, что все её разбиения на обучающую и контрольную выборки равновероятны. Функционал полного скользящего контроля определяется как математическое ожидание частоты ошибок на контроле. Его верхние оценки получены в [2] для случая, когда алгоритм классификации выбирается из множества всех монотонных функций. Эффективные формулы получены в [3] для монотонного классификатора ближайшего соседа. В данной работе в конструкцию монотонного классификатора

ближайшего соседа вводится дополнительный параметр, позволяющий смещать границу между классами ниже или выше, и показывается, что наилучшая обобщающая способность достигается при проведении границы посередине, за исключением случаев сильной несбалансированности классов.

Рассмотрим задачу бинарной классификации объектов, описываемых n бинарными признаками. Пусть $U = \{x_1, \ldots, x_L\} \subset B^n$ — конечное множество объектов, $y_i = y(x_i) \in B$ — класс объекта x_i, $B = \{0, 1\}$. *Частота ошибок* классификатора $a\colon U \to B$ на выборке $X \subset U$ есть $\nu(a, X) = \frac{1}{|X|} \sum\limits_{x_i \in X} \big[a(x_i) \neq y_i\big]$. *Методом обучения* называется отображение $\mu\colon 2^U \to M^n$, которое произвольной обучающей выборке $X \subset U$ ставит в соответствие классификатор из M^n — множества всех монотонных булевых функций n аргументов.

Пусть все C_L^ℓ разбиений множества $U = X \sqcup \bar{X}$ на обучающую выборку X длины ℓ и контрольную $\bar{X}$ длины $k = L - \ell$, равновероятны. Определим функционал *полного скользящего контроля* [2] как математическое ожидание частоты ошибок на контроле:

$$Q(\mu, U) = \frac{1}{C_L^\ell} \sum_{X \subset U\colon\ |X| = \ell} \nu\big(\mu(X), \bar{X}\big).$$

Назовем *тенью* объекта x_i из X множество

$$S_X(x_i) = \begin{cases} \{x \in B^n\colon\ x \leq x_i\}, & \text{если } y_i = 0; \\ \{x \in B^n\colon\ x \geq x_i\}, & \text{если } y_i = 1. \end{cases}$$

Определим расстояние от объекта $u \in U$ до объекта $x_i \in X$ как расстояние Хэмминга $d(u, x)$ до ближайшего объекта x из его тени:

$$\rho(u, x_i) = \min_{x \in S_X(x_i)} d(u, x).$$

Определим множество ближайших соседей объекта u в выборке X:

$$N_X(u) = \operatorname{Arg} \min_{x_i \in X} \rho(u, x_i).$$

Если $|N_X(u)| > 1$, то *классификатор ближайшего соседа* будет относить объект u к тому классу, в который он «глубже погружен»:

$$a(u) = y(\arg \max_{x_i \in N_X(u)} d(u, x_i)).$$

Теорема. *Если выборка монотонна, то есть для всех* $x_i, x_j \in U$ *из* $x_i \leq x_j$ *следует* $y_i \leq y_j$, *то функция* $a(x)$ *монотонна.*

Определим функцию расстояния $\rho_\lambda(u, x_i)$ от объекта u до обучающего объекта x_i, зависящую от параметра $\lambda \in (-1, 1)$:

$$\rho_\lambda(u, x_i) = (1 + \lambda - 2y_i\lambda)\rho(u, x_i),$$

Параметр λ определяет положение границы между классами: чем меньше λ, тем ниже (ближе к нулям монотонной функции) проходит граница; при $\lambda = 0$ она проходит «посередине» между классами.

Для получения верхней оценки функционала Q введём пессимистичный метод обучения μ_p, который строит классификатор $\mu_p(X)$, ошибающийся на всех объектах, равноудаленных от обоих классов. Нижняя оценка Q_o получается для оптимистичного метода μ_o, при котором $\mu_o(X)$ правильно классифицирует все такие объекты.

Для каждого $x_i \in U$ определим три функции целочисленного аргумента $m \in \{0, \ldots, n\}$:

$$t_i(m) = \sum_{x_j \in X \setminus x_i} \big[\rho_\lambda(x_i, x_j) < (1 - \lambda + 2y_i\lambda)m\big];$$

$$s_i(m) = \sum_{x_j \in X \setminus x_i} \big[\rho_\lambda(x_i, x_j) = (1 - \lambda + 2y_i\lambda)m\big]\big[y_i \neq y_j\big];$$

$$p_i(m) = \sum_{x_j \in X \setminus x_i} \big[\rho_\lambda(x_i, x_j) = (1 - \lambda + 2y_i\lambda)m\big]\big[y_i = y_j\big]$$

Теорема. *Если выборка* U *монотонна, то* $Q_o \leq Q(\mu, U) \leq Q_p$,

$$Q_p = \sum_{i=1}^{L} \sum_{m=0}^{n} \frac{C^\ell_{L-t_i(m)-1} - C^\ell_{L-t_i(m)-s_i(m)-1}}{kC^\ell_L},$$

$$Q_o = \sum_{i=1}^{L} \sum_{m=0}^{n} \frac{C^\ell_{L-t_i(m)-p_i(m)-1} - C^\ell_{L-t_i(m)-s_i(m)-p_i(m)-1}}{kC^\ell_L}.$$

Численные эксперименты показывают, что границы Q_o, Q_p отличаются не сильно и достигают минимальных значений при $\lambda = 0$.

Работа выполнена при финансовой поддержке РФФИ (проект № 11-07-00480) и программы ОМН РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения».

Список литературы

1. Akers S. B. A truth table method for synthesis of combinational logic // IRE Trans. — 1961. — V. EC-10, №. 4. — P. 604–615.

2. Воронцов К. В. Комбинаторный подход к оценке качества обучаемых алгоритмов // Математические вопросы кибернетики. Выпуск 13. — М.: Физматлит, 2004. — С. 5–36.

3. Махина Г. А. Оценка обобщающей способности для монотонных алгоритмов классификации // 16-я международная конференция «Проблемы теоретической кибернетики». Нижний Новгород, 20–25 июня 2011. — С. 307–310.

ГИСТОГРАММНАЯ ФУНКЦИЯ АВТОМАТА И СВЯЗАННЫЕ С НЕЮ КЛАССЫ ЯЗЫКОВ

Д. В. Пархоменко (Москва)

Пусть задан конечный детерминированный автомат [1] $V = (A, Q, B, \varphi, \psi, q_0)$, $|A| = |B|$, и его автоматная функция $f_V \colon A^* \to B^*$.

Функцию $\kappa \colon B^* \to \mathbb{N} \cup \{0\}$, $\kappa(\beta) = |\{\alpha \in A^* \mid f_V(\alpha) = \beta\}|$ назовем гистограммной функцией автомата V [2].

Для любого натурального p : $L_p(V) = \{\beta \in B^* | \kappa_V(\beta) \geq p\}$. В частности, при $p = 1, L_1(V)$ суть множество слов, перечислимое автоматом V. Очевидно, для любого автомата V : $L_p(V) \subseteq L_{p-1}(V)$, для всех $p \geq 2$. Имеет место:

Теорема 1. *Для любого конечного инициального автомата V и для всякого $p \geq 1$, $L_p(V)$ — регулярный язык.*

Таким образом, каждый конечный инициальный автомат V задает, вообще говоря, бесконечную цепочку вложенных в друг друга регулярных языков:

$$L_1(V) \supseteq L_2(V) \supseteq L_3(V) \supseteq ...$$

Причем, как показывает следующее утверждение, все такие языки продолжаемы.

Утверждение. *Пусть дан автомат V. Если для некоторого натурального p, слово $\beta \in L_p(V)$, то найдется буква b выходного алфавита автомата V такая, что $\beta b \in L_p(V)$.*

Следствие. *Для любого натурального p и автомата $V, L_p(V)$ либо бесконечное множество, либо пустое.*

Для фиксированных алфавитов A, B рассмотрим $\mathcal{L}_p = \{L_p(V) | V$ — произвольный конечный инициальный автомат над $A, B\}$. Тогда верна следующая теорема.

Теорема 2. *Для любых натуральных $i \neq j$ выполнено: $\mathcal{L}_i \nsubseteq \mathcal{L}_j$.*

Замкнутость введенных классов языков относительно различных операций описывает следующая теорема.

Теорема 3. 1) *$\mathcal{L}_1$ замкнут относительно операций объединения, взятия автоматного образа и итерации. Но не замкнут относительно пересечения и конкатенации.* 2) *$\mathcal{L}_p$, при $p > 1$, не замкнут относительно операций пересечения, объединения, но замкнут относительно операции взятия автоматного образа.*

Согласно вышеприведенному, для любого p, каждый язык из $\mathcal{L}_p$ — суть регулярный. Однако не всякий регулярный язык является языком типа $\mathcal{L}_p$. Для формулировки критерия регулярности языка типа $\mathcal{L}_p$ рассмотрим конечный инициальный автомат $V = (A, Q, B, \varphi, \psi, q_0)$, $|A| = |B|$ у которого некоторые состояния помечены, как финальные $Q = Q_F \bigsqcup Q \diagdown Q_F$.

Верна следующая теорема.

Теорема 4. *Пусть $p > 1$ — натуральное, а автомат $V = (A, Q, B, \varphi, \psi, q_0)$ представляет некоторый язык L с помощью множества финальных состояний Q_F. Существует алгоритм проверки принадлежности $L \in \mathcal{L}_p$ сложности не превосходящей*

$$O(p(p-1) \cdot |Q|).$$

Работа выполнена на кафедре МаТИС механико-математического факультета МГУ им. М. В. Ломоносова по руководством д.ф.м.н. профессора Д. Н. Бабина.

Список литературы

1. Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Элементы теории автоматов. — М.: Изд-во МГУ, 1985.

2. Пархоменко Д. В. Метод распознавания множества слов автоматом // Интеллектуальные системы. —2011. — Т.15, вып. 1–4.

3. Бабин Д. Н. О замкнутых классах автоматных функций // Материалы 9-й конференции Интеллектуальные системы и компьютерные науки. — 2005. — Т.1, ч. 1. — С. 48–53.

О СЛОЖНОСТИ ПОИСКА ПОДСЛОВА В СЛОВЕ С ПОМОЩЬЮ ДРЕВОВИДНЫХ ГРАФОВ

Е. М. Перпер (Москва)

Пусть $W_n^k = \cup_{s=1}^n \{1,2,\ldots,k\}^s$ — множество слов длины не более n над алфавитом $\{1,2,\ldots,k\}$. Для каждого слова $w \in W_n^k$ его длину будем обозначать как $l(w)$. Через $w[a..b]$, где $1 \leq a \leq l(w), 1 \leq b \leq l(w)$, будем обозначать подслово слова w, начинающееся с его a-й буквы и заканчивающееся его b-й буквой, если $a \leq b$, и пустое слово иначе. Через $w[a], 1 \leq a \leq l(w)$, будем обозначать a-ю букву слова w. Будем говорить, что слова $w \in W_n^k$ и $v \in W_n^k$ *равны* или *совпадают* (и писать $w = v$) , если $l(v) = l(w)$ и $v[1] = w[1], v[2] = w[2], \ldots, v[l(v)] = w[l(w)]$. Будем считать, что любые два пустых слова совпадают. Скажем, что слово w *лексикографически следует* за словом v, а слово v *лексикографически предшествует* слову w, если выполняется одно из следующих двух условий: 1) $\exists i \in N, i \leq \min(l(v), l(w)) : v[i] < w[i]$ и $\forall j \in N, j < i : v[j] = w[j]$; 2) $l(v) < l(w)$ и $\forall j \in N, j \leq l(v) : v[j] = w[j]$. Будем записывать это следующим образом: $w > v$ (либо $v < w$). Рассмотрим $X = W_n^k$ — множество запросов; $Y = \{1,2,\ldots,k\}^n$ — множество записей. Введём бинарное отношение ρ, которое позволит устанавливать, когда запись $y \in Y$ удовлетворяет запросу $x \in X$ (*отношение поиска*): $x\rho y \Leftrightarrow \exists i \in N : x = y[i..l(x) + i - 1], x \in X, y \in Y$. Будем рассматривать задачу информационного поиска (ЗИП) $I =< X, V, \rho >$, где $V = \{v_1, v_2, \ldots, v_p\}$, $V \subseteq Y$. Назовём эту задачу *задачей поиска подслова*. Множество V в дальнейшем будем называть *библиотекой*. Содержательно будем считать, что задача $I =< X, V, \rho >$ состоит в перечислении для произвольно взятого запроса $x \in X$ всех тех и только тех записей из V , которые находятся в отношении ρ с запросом x, то есть удовлетворяют запросу x. Задачу I будем рассматривать в рамках информационно-графовой модели данных [1,2]. *Информационный граф* (ИГ) — это ориентированный граф, моделирующий обработку запроса, который изначально находится в корне графа, при помощи вычисления функций двух типов: предикатов и переключателей. *Предикат* сопоставляется ребру и принимает два значения: 1 (и тогда считается, что запрос проходит по этому ребру) и 0 (в этом случае запрос по ребру не проходит). *Переключатель* сопоставляется вершине; если из этой вершины исходит t рёбер, то они нумеруются числами от 1 до t, и значением, которое принимает переключатель, является номер единственного

ребра, по которому пройдёт запрос. Некоторым вершинам графа приписано какое-либо слово из библиотеки. Если для любого запроса множество слов, приписанных вершинам, в которые проходит запрос, совпадает со множеством слов библиотеки, удовлетворяющих запросу, то будем говорить, что информационный граф решает ЗИП I. Две основные характеристики информационного графа — объём и сложность. *Объём* $Q(u)$ графа u — это количество рёбер в графе u. *Сложность* $T(u,x)$ графа u на запросе x есть время обработки графом данного запроса. В качестве предикатов и переключателей мы будем рассматривать достаточно простые функции — сравнение двух небольших целых чисел либо нахождение буквы по её позиции в слове, и время вычисления таких функций будем считать равным 1. Число $T(u) = \max\limits_{x \in X} T(u,x)$ будем называть сложностью информационного графа u. В данной работе рассматриваются древовидные ИГ. Информационный граф будем называть *древовидным*, если, за исключением корня, в каждую его вершину, которой не приписано слово из библиотеки, входит ровно одно ребро (при этом из неё может выходить сколько угодно рёбер). Обозначим множество древовидных информационных графов, решающих задачу $I =< X, V, \rho >$, где $X = W_n^k, V \subseteq \{1,2,\ldots,k\}^n, |V| = p$, через $D(V)$. Пусть $Q(p,n) = \max_{V \subseteq \{1,2,\ldots,k\}^n, |V|=p} \min_{d \in D(V)} Q(d)$.

Теорема 1. *Пусть* $h = (n+1)/2$ *— простое число и* $p \leq (k^h - k)/h$. *Тогда найдётся такая библиотека* $V \subseteq \{1,2,\ldots,k\}^n, |V| = p$, *что если граф* $d \in D(V)$, *то* $Q(d) \gtrsim pn^2/8$ *при* $p \to \infty$.

Доказательство. Пусть V' — множество слов длины h таких, что каждое из них предшествует любой циклической перестановке своих символов (кроме тождественной). Всего таких слов $(k^h - k)/h$, т.е. не менее, чем p. Упорядочим слова из V' в порядке лексикографического следования. Каждому слову $v'_i \in V', 1 \leq i \leq p$, сопоставим слово $v_i \in V$ такое, что $v_i[j] = v_i[h+j] = v'_i[j], 1 \leq j \leq h-1, v_i[h] = v'_i[h]$. Заметим, что все подслова длины h всех слов из библиотеки V разные. Тогда все подслова большей длины тоже разные. Итого, в библиотеке V не менее $(h + (h-1) + \ldots + 1) * p = ph(h+1)/2 = p(n+1)(n+3)/8$ разных подслов длины не менее h. Рассмотрим теперь какой-либо древовидный информационный граф d, решающий задачу $I =< X, V, \rho >$. Пусть w — подслово слова $v \in V$, причём $l(w) \geq h$. Любую букву слова w всегда можно заменить на другую так, чтобы полученное слово не было подсловом v, так как у любой пары подслов v не совпадают по меньшей мере 2 буквы. Значит, $\forall i \leq l(w)$ вдоль пути, по которому проходит запрос w, должна най-

тись функция $f_{w,i}$ такая, что $f_{w,i}(x) \neq f_{w,i}(w)$, если $x[i] \neq w[i]$, где x — запрос, $l(x) \geq i$. Значит, пути, по которым проходят запросы w и x, не совпадают. Пусть w_1 и w_2 — 2 различных подслова слов из V, $l(w_1) \geq h, l(w_2) \geq h$. Если $l(w_1) = l(w_2)$, то $\exists i : w_1[i] \neq w_2[i]$. Пусть теперь $l(w_1) \neq l(w_2)$. Не ограничивая общности, будем считать, что $l(w_1) > l(w_2)$; тогда функция $f_{w_1,l(w_1)}$ неприменима к w_2. Таким образом, пути, по которым проходят запросы w_1 и w_2, никогда не совпадают. Так как информационный граф d древовидный, то для каждого подслова $w, l(w) \geq h$ слова из библиотеки найдётся ребро, по которому проходит только запрос, совпадающий с этим подсловом. Значит, всего рёбер в графе не меньше, чем $p(n+1)(n+3)/8$, что и требовалось доказать.

Теорема 2. *Для любой библиотеки $V \subseteq \{1, 2, \ldots, k\}^n, |V| = p$ найдётся граф $d \in D(V)$ такой что $Q(d) \lesssim pn^2k/2$ и $T(d) \leq 2n + r$ при $p \to \infty$, где $r = r(V)$ — наибольшее по всем возможным запросам количество слов из библиотеки $V \subseteq Y$, удовлетворяющих запросу.*

Эта теорема напрямую вытекает из результатов, полученных в работе [3].

Следствие. *Пусть $h = (n+1)/2$ — простое число и $p \leq (k^h - k)/h$. Тогда $Q(p, n) = O(pn^2)$ при $p \to \infty$.*

Автор выражает благодарность профессору Эльяру Эльдаровичу Гасанову за научное руководство.

Список литературы

1. Гасанов Э. Э., Кудрявцев В. Б. Теория хранения и поиска информации. — М.: Физматлит, 2002.

2. Кудрявцев В. Б., Гасанов Э. Э., Подколзин А. С. Введение в теорию интеллектуальных систем. — М.: Издательский отдел факультета ВМиК МГУ, 2006. — С. 94–117.

3. Перпер Е. М. О функциональной сложности поиска подстроки // Интеллектуальные системы. — 2011. — Т. 15, вып. 1–4. — С. 553–570.

СЛАБОЗАМКНУТЫЕ КЛАССЫ БУЛЕВЫХ ФУНКЦИЙ

О. А. Петрова (Москва)

В работе рассматриваются булевы функции и пары (f, t), гдеf — булева функция, t — временная задержка (большая или равная 0).

Над множествами

$$C_1' = (f, t), f \in C_1, t = 0, 1, 2, \ldots$$

и

$$C_1'' = (f, t), f \in C_1, t = 1, 2, \ldots,$$

где C_1 — это множество булевых функций, вводятся понятия формулы и синхронной суперпозиции, а также синхронного замыкания и синхронной полноты.

Утверждение. *Синхронно-замкнутых классов в C_1' континуум.*

Для каждого класса функций из C_1' определена первая проекция как множество булевых функций, встречающихся в данном классе с некоторой задержкой.

Множество булевых функций называется слабозамкнутым, если оно является первой проекцией синхронно-замкнутого класса в C_1'.

Множество булевых функций называется положительно-слабозамкнутым, если оно является первой проекцией синхронно-замкнутого класса в C_1''.

Очевидно, что положительно-слабозамкнутое множество является слабозамкнутым.

Положительно-слабозамкнутыми классами являются все классы Поста, но не только они.

Будем относить пару множеств булевых функций (M_1, M_2), таких, что $M_2 \subseteq M_1$, к первому типу, если не существует положительно-слабозамкнутого класса L, такого, что $M_2 \subset L \subset M_1$.

Будем относить пару множеств булевых функций (M_1, M_2), таких, что $M_2 \subseteq M_1$, ко второму типу, если не существует положительно-слабозамкнутого класса L, такого, что $M_2 \subset L \subset M_1$, но существует слабозамкнутый класс L' (не являющийся положительно-слабозамкнутым), такой, что $M_2 \subset L' \subset M_1$.

Будем относить пару множеств булевых функций (M_1, M_2), таких, что $M_2 \subseteq M_1$, к третьему типу, если существует положительно-слабозамкнутый класс L, такого, что $M_2 \subset L \subset M_1$.

В работе изучены слабозамкнутые и положительно-слабозамкнутые классы с точки зрения отношения по включению. Все пары классов Поста разбиты на множества пар классов первого, второго и третьего типа.

В классе линейных функций исследованы все сдабозамкнутые и положительно-слабозамкнутые классы, построена диаграмма этих классов по включению.

Основные результаты работы:

Теорема 1. *В множестве линейных функций пары классов* (L_5, L_4), (L_5, O_4), (L_4, O_1), (O_i, O_j), *где* O_j *является предполным в* O_i, *относятся к первому типу; пары классов* (L_1, L_2), (L_1, L_3), (L_1, L_5), (L_2, L_4), (L_3, L_4), (L_2, O_5), (L_3, O_6), (L_1, O_9) *относятся ко второму типу. В множестве линейных функций всего* 28 *слабозамкнутых классов,* 14 *из которых являются замкнутыми классами Поста, и всего* 17 *положительно-слабозамкнутых классов,* 14 *из которых являются замкнутыми классами Поста.*

Теорема 2. *Пары классов* (D_3, D_1), (D_2, O_1), (D_1, D_2), (D_1, L_4), (D_3, L_5) *относятся к первому типу.*

Теорема 3. *Пары классов* (A_1, A_2), (A_1, A_3), (A_2, A_4), (A_3, A_4) *относятся к первому типу; пары классов* (A_1, S_6), (A_1, P_6), (A_3, S_5), (A_2, P_5) *относятся ко второму типу.*

Теорема 4. *Пары классов* (C_1, C_2), (C_1, C_3), (C_2, C_4), (C_3, C_4) *относятся ко второму типу.*

Теорема 5. *Пары классов* (P_6, P_5), (P_6, P_3), (P_5, P_1), (P_3, P_1), (P_6, O_8), (P_5, O_5), (P_3, O_6), (P_1, O_1), (S_6, S_5), (S_6, S_3), (S_5, S_1), (S_3, S_1), (S_6, O_8), (S_5, O_6), (S_3, O_5), (S_1, O_1) *относятся к первому типу.*

Теорема 6. *Пары классов* (F_μ^5, F_μ^6), (F_μ^7, F_μ^6), $(F_\mu^5, F_{\mu+1}^5)$, $(F_\mu^6, F_{\mu+1}^6)$, $(F_\mu^7, F_{\mu+1}^7)$, (F_∞^6, P_1), (F_∞^7, P_3), (F_μ^1, F_μ^2), (F_μ^3, F_μ^2), $(F_\mu^1, F_{\mu+1}^6)$, $(F_\mu^2, F_{\mu+1}^2)$, $(F_\mu^3, F_{\mu+1}^3)$, (F_∞^2, S_1), (F_∞^3, S_3) *относятся к первому типу; пары классов* (F_μ^8, F_μ^7), (F_μ^8, F_μ^5), $(F_\mu^8, F_{\mu+1}^8)$, (F_μ^4, F_μ^3), (F_μ^4, F_μ^1), $(F_\mu^4, F_{\mu+1}^4)$ *относятся ко второму типу.*

Теорема 7. *Пары классов* (C_4, D_1), (C_4, A_4), (C_4, F_2^5), (A_4, F_2^6), (F_2^6, D_2) *относятся к первому типу; пары классов* (C_2, A_2), (C_3, A_3), (C_1, L_1), (C_2, L_2), (C_3, L_3), (C_3, F_2^8), (A_3, F_2^7) *относятся ко второму типу; пары классов* (C_1, A_1), (C_1, D_3) *относятся к третьему типу.*

Список литературы

1. Кудрявцев В. Б., Блохина Г. Н., Кнап Ж., Кудрявцев В. В. Алгебра логики. — Москва — Любляна, 2006.

ОБ АСИМПТОТИЧЕСКИХ ОЦЕНКАХ ДЛЯ БИГРАММНЫХ ЯЗЫКОВ

А. А. Петюшко (Москва)

Пусть A ($|A| < \infty$) — конечный алфавит.

Определение 1. *Биграммой* в алфавите A называется двухбуквенное слово $ab \in A^*, a, b \in A$ ($ab \neq ba$ при $a \neq b$).

Определение 2. Назовем *кратностью β в слове α* и обозначим через $\theta_\beta(\alpha)$, где $\beta \in A^*, \alpha \in A^*$, причем β — непустое слово, отображение $A^* \to N \cup \{0\}$, которое определяется как количество различных разложений слова α в виде $\alpha = \alpha'\beta\alpha''$ (α' и α'' могут быть пустыми). При длине слова α, меньшем чем длина слова β, значение $\theta_\beta(\alpha)$ положим равным 0.

С учетом введенных определений, по каждому слову $\alpha \in A^*$ можно построить квадратную матрицу биграмм $(\Theta(\alpha))_{i,j=1}^{|A|}$ размера $|A| \times |A|$ такую, что на месте (i, j) матрицы будет стоять значение $\theta_{a_i a_j}(\alpha)$ (при условии, что все буквы алфавита $A = \{a_1, a_2, ..., a_{|A|}\}$ пронумерованы и нумерация зафиксирована).

Обозначим через Ξ множество квадратных матриц размера $|A| \times |A|$, каждый элемент которых является неотрицательным целым числом. Т.о., $\forall \alpha \in A^*$ имеем $\Theta(\alpha) \in \Xi$. Также, здесь и далее через $\Theta(\alpha)$ будем обозначать матрицу биграмм, построенную по конкретному слову α, а через Θ - просто некоторую матрицу из Ξ, при этом будем считать, что на месте (i, j) матрицы Θ будет стоять значение $\theta_{a_i a_j}$.

Определение 3. Назовем *биграммным языком* $L(\Theta)$, порожденным матрицей $\Theta \in \Xi$, множество всех слов, имеющих одну и ту же матрицу биграмм Θ, т.е. $L(\Theta) = \{\beta \in A^* | \Theta(\beta) = \Theta\}$.

Построим по матрице $\Theta(\alpha)$ (или по произвольной матрице $\Theta \in \Xi$) ориентированный граф $G_{\Theta(\alpha)}$ на плоскости. Вершинами у этого графа будут все буквы из алфавита A, при этом ребра будут соответствовать биграммам с учетом их кратностей, т.е. кратность $\theta_{ab}(\alpha)$ будет порождать $\theta_{ab}(\alpha)$ ориентированных ребер $a \to b$. Аналогично, кратность $\theta_{cc}(\alpha)$ будет порождать $\theta_{cc}(\alpha)$ петель $c \to c$.

Определение 4. *Матрицей Кирхгофа* $ML(\Theta)$, построенной по матрице биграмм $\Theta \in \Xi$, называется квадратная матрица размером $|A| \times |A|$, т. ч. на месте (i, j) стоит элемент

$$l_{ij} = \begin{cases} -\theta_{a_i a_j}, & i \neq j; \\ \sum_{a_j \neq a_i} \theta_{a_i a_j}, & i = j. \end{cases}$$

Лемма. *Если матрица биграмм* $\Theta \in \Xi$ *такова, что соответствующий ориентированный граф* G_Θ *является эйлеровым* [1], *то все главные миноры* $D^{(i,i)}$, *полученные вычеркиванием из* $ML(\Theta)$ i*-й строки и* i*-го столбца, равны между собой при различных* i (*и равны* D).

На основе работы [2] можно доказать, что верна следующая

Теорема 1. *Пусть задана матрица биграмм* Θ, *которой соответствует эйлеров или почти эйлеров граф* G_Θ, *причем для* $\forall i \exists j \neq i$, *т.ч.* $\theta_{a_i a_j} > 0$ *или* $\theta_{a_j a_i} > 0$. *Тогда:*

1. *Если* $\exists i'$, *т.ч.* $\sum_{a_i \in A} \theta_{a_i a_{i'}} > \sum_{a_i \in A} \theta_{a_{i'} a_i}$, *то*

$$N_\Theta = \frac{\prod_{a_i \in A} (\sum_{a_j \in A} \theta_{a_i a_j} - 1 + \delta_{i' i})!}{\prod_{a_i, a_j \in A} \theta_{a_i a_j}!} D^{(i'i')};$$

где $\delta_{i' i}$ — *символ Кронекера.*

2. *Если* $\forall i, j \ \sum_{a_i \in A} \theta_{a_i a_j} = \sum_{a_i \in A} \theta_{a_j a_i}$, *то*

$$N_\Theta = \left(\sum_{a_i, a_j \in A} \theta_{a_i a_j} \right) \frac{\prod_{a_i \in A} (\sum_{a_j \in A} \theta_{a_i a_j} - 1)!}{\prod_{a_i, a_j \in A} \theta_{a_i a_j}!} D.$$

Определение 5. Назовем *частотным языком* на биграммах с кратностями, заданным матрицей биграмм $\Theta \in \Xi$, следующий язык при $k \in N$:

$$F_\Theta = \bigcup_{k=1}^{\infty} L(k\Theta)$$

Определение 6. Назовем две ненулевые матрицы Θ_1 и Θ_2 из Ξ *кратными*, если существует действительный коэффициент $c \in R, c \neq 0$, такой что верно $\Theta_1 = c\Theta_2$. В противном случае ненулевые матрицы назовем некратными.

Теорема 2. *Пусть матрица биграмм* Θ *задает эйлеров граф* G_Θ. *Тогда:*

1. *Если существует такое разложение* Θ *в сумму двух ненулевых некратных матриц* $\Theta = \Theta_1 + \Theta_2$ *такое, что обе матрицы* Θ_1 *и* Θ_2 *задают эйлеровы графы* G_{Θ_1} *и* G_{Θ_2}, *то язык* F_Θ *нерегулярен.*

2. *В противном случае язык* F_Θ *регулярен.*

Определение 7. Матрица биграмм Θ называется *положительной*, если все элементы этой матрицы — натуральные целые числа.

Теорема 3. *Пусть задана положительная матрица биграмм* Θ *с эйлеровым графом* G_Θ. *Тогда при* $k \to \infty$ *мощность языка* $L(k\Theta)$

$$|L(k\Theta)| \cong c_2 * \frac{c_1^k}{k^{n(n-1)/2}},$$

где $c_1 = c_1(\Theta) > 1, c_2 = c_2(\Theta)$ — *некоторые константы, зависящие только от изначальной матрицы биграмм* Θ, *а* $n = |A|$ — *мощность алфавита.*

Обозначим через Ξ_k множество матриц размера $|A| \times |A|$, каждый элемент которых представляет собой неотрицательное целое число, не превосходящее $k > 0$. Также будем считать, что $|A| = n > 1$.

Через N_f^k обозначим количество матриц биграмм $\Theta \in \Xi_k$, задающих конечные (непустые) языки F_Θ; N_i^k — количество матриц биграмм $\Theta \in \Xi_k$, задающих счетные языки F_Θ; N_{reg}^k — количество матриц биграмм $\Theta \in \Xi_k$, задающих счетные регулярные языки F_Θ; N_{nreg}^k — количество матриц биграмм $\Theta \in \Xi_k$, задающих счетные нерегулярные языки F_Θ; N^k — общее количество матриц биграмм $\Theta \in \Xi_k$.

Теорема 4. *С учетом введенных выше обозначений верны следующие соотношения:*

1) $\exists k_0$, *т.ч.* $\forall k > k_0$ $\frac{1}{n(n-1)} < \frac{N_i^k}{N_f^k} < 1$;

2) $\lim_{k\to\infty} \frac{N_i^k}{N^k} = 0$;

3) $\lim_{k\to\infty} \frac{N_{reg}^k}{N_{nreg}^k} = 0$.

Следствие. *Если обозначить за* N_q^k *количество матриц биграмм* $\Theta \in \Xi_k$, *задающих непустые языки* F_Θ, *то* $\lim_{k\to\infty} \frac{N_q^k}{N^k} = 0$.

Список литературы

1. Оре О. Теория графов. — М.: Наука, 1980.

2. Hutchinson J. P., Wilf H. S. On Eulerian circuits and words with prescribed adjacency patterns // Journal of Combinatorial Theory. — 1975. — Ser. A, V. 18. — P. 80–87.

РЕШЕНИЕ ДИНАМИЧЕСКОЙ ЗАДАЧИ ПОИСКА ИДЕНТИЧНЫХ ОБЪЕКТОВ

А. А. Плетнев (Москва)

Функционирование базы данных — это обработка потока запросов типа поиск, вставка и удаление. При этом в результате запросов типа вставка и удаление база данных изменяется, а на запросы типа поиск выдается ответ. Если поток запросов на поиск существенно преобладает над запросами на изменение базы данных, то такие базы данных называются статическими. Для исследования таких баз данных предназначены информационные графы (ИГ) [1]. Если же поток запросов на изменение базы данных сравним с потоком запросов на поиск, то такие базы данных называются динамическими, и моделированию таких баз данных посвящена данная работа.

Предлагаемая модель динамических баз данных построена на взаимодействии конечного детерминированного автомата и информационного графа. Задача автомата перестраивать информационный граф при изменении базы данных, тем самым обрабатывая динамические запросы пользователя. Эту структуру будем называть динамическим информационным графом.

В определении понятия ИГ используются 4 множества: множество запросов X; множество записей Y; множество F одноместных предикатов, заданных на множестве X; множество G одноместных переключателей, заданных на множестве X. Понятие ИГ над базовым множеством $\mathcal{F} = \langle F, G \rangle$, где $F = \{f_j, j \in I\}$, $G = \{g_i, i \in J\}$, I, J — множества индексов, берется из [1]. Определим три множества функций изменения индексов: $R^1 = \{r_c^1 : I^{n_c^1} \times J^{n_c^2} \times Y^{n_c^3} \to I,\ c \in C_1\}$, $R^2 = \{r_c^2 : I^{n_c^1} \times J^{n_c^2} \times Y^{n_c^3} \to J,\ c \in C_2\}$, $R^3 = \{r_c^3 : Y^{n_c} \to Y,\ c \in C_3\}$. Введем три множества переменных: $Z = \{z_i\}_{i=1}^{\infty}$, где z_i принимают значения из I, $V = \{v_j\}_{j=1}^{\infty}$, где v_j принимают значения из J, $W = \{w_k\}_{k=1}^{\infty}$, где w_k принимают значения из Y.

Рассмотрим произвольный ИГ U. Заменим каждый индекс предиката на некоторую переменную из Z, каждый индекс переключателя на переменную из V, а каждую запись на переменную из W. После этого сопоставления получим нагруженный граф, который назовем простым шаблоном. Если каждый индекс предиката мы заменим на некоторую формулу над множеством переменных Z и множеством функций R^1, каждый индекс переключателя на формулу над множеством переменных V и множеством функций R^2, а каждую запись на формулу над множеством переменных W и множеством функций R^3, то полученный нагруженный граф назовем шаблоном.

Будем говорить, что ИГ U и простой шаблон $\mathcal{T}$ согласованы, если они совпадают как графы, и если в ИГ U встречаются одинаковые индексы предикатов (переключателей и записей), то в соответствующих местах шаблона $\mathcal{T}$ находятся одинаковые переменные из $Z(V$ и $W)$. Возникшее соответствие между переменными и индексами назовем интерпретацией данного согласования.

Локальным преобразованием назовем пару $p = (\mathcal{T}_1, \mathcal{T}_2)$, где $\mathcal{T}_1$ — простой шаблон, $\mathcal{T}_2$ — шаблон, в формулах которого встречаются только переменные, входящие в простой шаблон $\mathcal{T}_1$, и возможно еще одна переменная из множества W.

Если ИГ U и простой шаблон $\mathcal{T}_1$ согласованы, то применением локального преобразования $p = (\mathcal{T}_1, \mathcal{T}_2)$ к ИГ U назовем ИГ U', получающийся из шаблона $\mathcal{T}_2$ подстановкой вместо каждой формулы значения данной формулы в интерпретации согласования ИГ U и простого шаблона $\mathcal{T}_1$.

Диаметром ИГ назовем максимальную длину простой цепи графа. Далее будем рассматривать класс $\mathcal{G}(N, D)$, $N, D \in \mathbb{N}$, информационных графов диаметра не более D, таких, что степень инцидентности любой вершины графа не превосходит N.

Назовем кодом вершины ИГ пару (k_1, k_2), где $k_1 = 0$, если вершина предикатная; $k_1 = 1$, если она переключательная; $k_2 = 0$, если вершина корень; $k_2 = 1$, если вершина листовая; $k_2 = 2$ в остальных случаях. Кодом ребра назовем число, которое равняется 0, если оно предикатное и 1, если переключательное. Кодом ИГ на запросе x назовем информацию о коде каждой вершины и ребра ИГ, а также информацию о значениях всех предикатов и переключателей на запросе x (так же возможно, что код содержит дополнительную информация о пометках на ребрах и вершинах графа). Через $\mathcal{K}(N, D)$ обозначим множество кодов ИГ из $\mathcal{G}(N, D)$. Понятно, что $|\mathcal{K}(N, D)| < \infty$.

Пусть $N, D \in \mathbb{N}$, $\mathcal{P}$ — некоторое конечное множество локальных преобразований, шаблоны которых порождены ИГ из $\mathcal{G}(N, D)$, U — ИГ над базовым множеством $\mathcal{F} = \langle F, G\rangle$ из класса $\mathcal{G}(N, \infty)$, $\mathcal{A}$ — конечный автомат, входной алфавит, которого есть $\mathcal{K}(N, D)$, а выходной алфавит описывает реакции автомата, такие как перемещение автомата по графу, выбор локального преобразования из $\mathcal{P}$, сигнал на завершение работы и, возможно, расстановку или изменение пометок на рассматриваемой окрестности графа. Пару $(\mathcal{A}, U)$ назовем динамическим информационным графом (ДИГ) типа (N, D) над $\mathcal{F}$ и $\mathcal{P}$.

Определим *функционирование* ДИГ $(\mathcal{A}, U)$ на запросе. Если за-

прос есть запрос на поиск, то функционирование ДИГ совпадает с функционированием ИГ U и не задействует автомат $\mathcal{A}$. Если запрос является запросом на вставку или удаление, то функционирование ДИГ происходит следующим образом. В начальный момент текущей вершиной объявляется корень ИГ и считается, что лишних пометок на графе нет. На вход автомата подается код окрестности текущей вершины. Если выход автомата предписывает передвижение по графу, то текущая вершина изменяется. Если выход автомата предписывает некоторое локальное преобразование, то в случае если окрестность текущей вершины согласована с левой частью преобразования, то рассматриваемая окрестность заменяется на результат применения данного локального преобразования. Если окрестность текущей вершины не согласована с левой частью преобразования, то функционирование завершается с ошибкой. Если выход автомата предписывает изменение пометок рассматриваемой окрестности, то эти изменения выполняются. Если выход автомата сигнализирует о завершении работы, то обработка запроса завершается успешно.

Пусть $B \subset Y$, $|B| < \infty$. Скажем, что ДИГ решает задачу поиска идентичных объектов (ЗПИО) $I = \langle X, B, = \rangle$, если ответ на произвольный запрос $x \in X$ типа поиска равен $\{x\}$, если $x \in B$, и пуст в противном случае; и если функционирование на произвольном запросе типа вставки (удаления) записи $y \in Y$ завершается успешно, результирующий граф не содержит лишних пометок и решает ЗПИО $\langle X, B \cup \{y\}, = \rangle$ ($\langle X, B \setminus \{y\}, = \rangle$).

Теорема. *Существует ДИГ типа* $(4, 4)$ *который решает задачу поиска идентичных объектов.*

Автор благодарит профессора Э. Э. Гасанова за постановку задачи и помощь в работе.

Список литературы

1. Гасанов Э. Э., Кудрявцев В. Б. Теория хранения и поиска информации. — М.: ФИЗМАТЛИТ, 2002.

ОБ ЭВОЛЮЦИИ СХЕМ БАЗ ДАННЫХ СУБД DIM

В. С. Рублев (Ярославль)

В основе введения новой объектной СУБД DIM [1, 2] лежит динамика информации, т. е. данных объектов, их свойств, типов и методов обработки данных. Поскольку в данной технологии темпоральный характер баз данных отражает *отношение истории* объектов,

свойств, классов, то для каждой из перечисленных сущностей, историю изменения которых следует хранить во времени, вводятся два дополнительных параметра: *момент рождения* и *момент смерти*.

Динамика схем баз данных DIM, включающая динамику классов и их связей, отражена во многих работах (см. например, [3–5]) как эволюция схем баз данных. Однако от эволюции динамику схем баз данных отличает дополнение ее отношением истории классов, связей, объектов, которая определяет динамику этих сущностей. Так как динамика схем существенным образом зависит от технологии баз данных, для DIM должен быть разработан свой подход. При этом помимо проверки целостности данных (объектов и их связей) выдвигается требование максимального использования преобразуемых данных, что трудно сделать вручную при большом изменении схемы.

Для построения алгоритма эволюции схемы базы данных вводится *орграф эволюции схемы* следующим образом:

1. В качестве вершин орграфа выбираются классы старой схемы, не вошедшие в новую схему (в дальнейшем будем их называть *старыми вершинами*), и классы новой схемы, отсутствующие или измененные по отношению к старой схеме (в дальнейшем будем их называть *новыми вершинами*), а также общие вершины старой и новой схем, для которых изменились связи с другими классами (в дальнейшем будем их называть *общими вершинами*).

2. Из *старой* вершины, соответствующей классу старой схемы, проводится дуга в отличную от нее *новую* вершину, соответствующую классу новой схемы, если некоторые параметры первого класса переносятся во второй. Такая дуга помечается именами переносимых параметров и в дальнейшем называется *дугой переноса*.

3. Вершины старой схемы соединяются связями классов старой схемы. То же делается для вершин новой схемы, но выделяются новые и изменившиеся по отношению к старой схеме связи, которые определяются как *дуги связи* для новых и общих вершин орграфа.

Из орграфа эволюции схемы выделяются компоненты связности, в каждую из которых включается компонента связности подграфа новых и общих вершин, связанная *дугами связи* и дополненная только теми старыми вершинами, которые связаны с ее новыми вершинами *дугами переноса*.

Предлагается следующий волновой алгоритм для каждой компоненты связности орграфа эволюции:

1. В качестве *начальной* выбирается любая *новая* вершина компоненты связности, которая не соответствует классу связи новой схемы и которая не имеет дуг связи с родительскими и включающи-

ми вершинами-классами для этой вершины-класса. Такая вершина должна существовать в силу ограничения определенности (см. [1]).

2.1. Для выбранной вершины и каждой *дуги переноса*, ведущей в нее из старых вершин, осуществляется перенос данных в соответствии с именами переносимых параметров дуги.

2.2. Вводится *отношение истории* между классами начала дуг переноса и выбранным классом (для первых классов определяется текущая дата в качестве значения параметра *Дата смерти*, а для класса выбранной вершины это значение определяется для параметра *Дата рождения*).

2.3. Если при переносе данных от старого класса к новому должен произойти перенос связи включения к классу общей вершины и тип включения не изменяется, то вводится история такой связи.

2.4. Для соответствующих объектов этих классов, связанных переносимым значением, вводится отношение истории объектов, при котором старый объект получает текущую дату в качестве значения *параметра* Дата смерти, а новый объект получает эту дату в качестве значения параметра *Дата рождения*.

2.5. Если в п. 2.3 связь включения получила историю, то в таблицу соответствующего отношения включения старых объектов для каждой записи старой связи определяется для поля *Дата смерти* значение текущей даты, а в таблицу соответствующую отношению новых объектов заносятся записи для нового отношения объектов со значением поля *Дата рождения*, равного текущей дате.

2.6. Выбранная вершина помечается.

3. Если есть еще выбранные непомеченные вершины, то для каждой из них выполняется предыдущий шаг алгоритма; иначе выполняется следующий шаг.

4. Если есть еще невыбранные вершины компоненты, то выбираются те вершины, которые связаны с помеченными *дугами связи*, не отвечающим связям включения с изменением типа включения и для каждой из них выполняется шаг 2 алгоритма.

5.1. Если среди помеченных вершин есть еще невыбранные вершины компоненты, которые являются классами связи включения и связаны с помеченными *дугами связи*, отвечающим связям включения с изменением типа включения, то они выбираются; иначе алгоритм заканчивает свою работу.

5.2. Если связь включения изменяет тип, то вводится история такой связи.

5.3. Для нового класса связи отношения включения, если он есть, пополняются значениями переноса параметры переноса, если есть дуги переноса, ведущие к этому классу.

5.4. Выбранная вершина связи включения помечается и снова выполняется предыдущий шаг 5.

Список литературы

1. Писаренко Д. С., Рублев В. С. Объектная СУБД Динамическая информационная модель DIM и ее основные концепции // Моделирование и анализ информационных систем, т.16, 1 — Ярославль: ЯрГУ, 2009. — С. 62–91.

2. Рублев В. С., Писаренко Д. С. Динамическая информационная модель. Концепция новой объектной технологии баз данных. — Lap Lambert Academic Publishing, Saarbrücken, Germany, 2011.

3. Кукс С. В. Аксиоматизация эволюции схемы xml-баз данных // Программирование. — 2003. — Т. 29, № 3. — С. 140–146.

4. Leonardi E., Bhowmick S. S. Detecting changes on unordered xml documents using relational databases: a schema-conscious approach // CIKM. — 2005. — P. 509–516.

5. Симановский А. А. Поддержка эволюции схем данных XML-реляционных баз данных. // Программирование. — 2008. — Т. 34, № 1. — С. 16–26.

ОБ АЛОРИТМАХ ПРОВЕРКИ ПРАВИЛЬНОСТИ СЕМЕЙСТВ ФУНКЦИЙ

Д. О. Рыков (Москва)

Данная статья посвящена изучению правильных семейств булевых функций, применяемых для задания латинских квадратов [2–4]. Один из способов проверки семейства функций на правильность опирается на критерий правильности, сформулированный в работе [1]. Задача проверки правильности может значительно упроститься при введении ограничений на семейство функций. В данной работе на основе предложенного в статье [1] критерия правильности будет построен модифицированный критерий, в котором также будет учтена информация о структуре графа существенной зависимости, что приведет к уменьшению требуемого на проверку времени в некоторых случаях. После этого будет описан алгоритм проверки правильности, использующий эту идею. Также будет построен алгоритм проверки правильности для семейств монотонных функций и оценена его сложность.

Семейство булевых функций $f = (f_1, \ldots, f_n)$ от переменных $x_1, \ldots, x_n$ называется правильным, если для любых двух различных

наборов значений переменных $x' = (x'_1, \ldots, x'_n)$ и $x'' = (x''_1, \ldots, x''_n)$ существует $\alpha \in \overline{1,n}$ такое, что $x'_\alpha \neq x''_\alpha$, $f_\alpha(x') = f_\alpha(x'')$.

Графом существенной зависимости семейства функций $f = (f_1, \ldots, f_n)$ от переменных $x_1, \ldots, x_n$ называется ориентированный граф $G_f = (V, E)$, где $V = \{1, 2, \ldots, n\}$, а $E = \{(i, j) : f_j$ существенно зависит от $x_i\}$.

Теорема 1 [1]. *Семейство булевых функций $f = (f_i)$, $i \in [1, n]$ правильно тогда и только тогда, когда для любого подмножества I, $I \subseteq [1, n]$, произведение функций $\prod\limits_{i \in I} f_i$ не зависит существенно от множества переменных $x_I = (x_i)$, $i \in I$.*

Теорема 2. *Семейство булевых функций $f = (f_i)$, $i \in [1, n]$ правильно тогда и только тогда, когда для любого подмножества I, $I \subseteq [1, n]$, такого, что вершинный подграф $< I >$ - сильный, произведение функций $\prod\limits_{i \in I} f_i$ не зависит существенно от множества переменных $x_I = (x_i)$, $i \in I$.*

Модифицированный алгоритм проверки правильности. Пусть нам известно семейство $f = (f_1, \ldots, f_n)$ из n функций и его граф. Предположим, что он содержит k сильных компонент $S_1, \ldots, S_k$, состоящих из $l_1, \ldots, l_k$ вершин соответственно и занумерованных в таком порядке, что в конденсации G^* графа существенной зависимости G дуги могут идти только от сильных компонент с меньшим номером к сильным компонентам с большим номером. Тогда r-ый шаг алгоритма будет выглядить так.

Шаг r. Проверяем на правильность семейство $f_{S_r} = (f_{s_r})$, $s_r \in S_r$. Функции сильной компоненты S_r могут зависет только от переменных сильных компонент $S_1, \ldots, S_r$. Поэтому для семейства функций сильной компоненты S_r проверка правильности сводится к перебору по парам наборов длины $l_1 + l_2 + \cdots + l_r$, в которых первые $l_1 + \cdots + l_{r-1}$ значений совпадают. В случае, если семейство f_{S_r} оказалось правильным, переходим к шагу $r + 1$. Если же оно не оказалось правильным, то и семейство $f = (f_1, \ldots, f_n)$ не является правильным.

На r-м шаге необходимо сделать $O(l_r 2^{l_1 + l_2 + \cdots + l_{r-1} + 2l_r})$ действий.

Значит, сложность алгоритма равна $f(n) = O(\sum\limits_{t=1}^{k} l_t 2^{\sum\limits_{p=1}^{t}(l_p + l_t)})$, где $l_1 + \cdots + l_k = n$.

Утверждение. *Семейство монотонных функций правильно тогда и только тогда, когда оно содержит константу, причем при удалении этой константы из семейства получается два правиль-*

ных семейства функций.

Алгоритм проверки правильности семейства монотонных функций. Проверим семейство $f = (f_1, \ldots, f_n)$ монотонных функций на правильность.

Шаг 1. Случай 1. $n = 1$.

1) $f_1 = 0$ или $f_1 = 1$. Завершим работу с ответом: "f — правильное семейство".

2) $f_1 \neq 0$ и $f_1 \neq 1$. Завершим работу с ответом: "семейство f не является правильным".

Случай 2. $n \neq 1$. Перейти к шагу 2.

Шаг 2. Ищем среди функций семейства f константу путем проверки каждой функции семейства на равенство константам 0 и 1. Рассмотрим случаи:

Случай 1. Если константной функции не найдется, то завершим работу с ответом: "семейство f не является правильным".

Случай 2. $f_k = 0$ или $f_k = 1$. Тогда

Шаг 3. Для $i \in [1, k-1]$ вычислить функции $g_i(x_1, \ldots, x_{n-1}) := f_i(x_1, \ldots, x_{k-1}, 0, x_k, \ldots, x_{n-1})$. Для $i \in [k, n-1]$ вычислить функции $g_i(x_1, \ldots, x_{n-1}) := f_{i+1}(x_1, \ldots, x_{k-1}, 0, x_k, \ldots, x_{n-1})$. Перейти к шагу 4.

Шаг 4. Рекурсивно проверить семейство $g = (g_1, \ldots, g_{n-1})$ на правильность.

1) Семейство g правильно. Перейти к шагу 5.

2) Семейство g не является правильным. Завершим работу с ответом: "семейство f не является правильным".

Шаг 5. Для $i \in [1, k-1]$ вычислить функции $g_i(x_1, \ldots, x_{n-1}) := f_i(x_1, \ldots, x_{k-1}, 1, x_k, \ldots, x_{n-1})$. Для $i \in [k, n-1]$ вычислить функции $g_i(x_1, \ldots, x_{n-1}) := f_{i+1}(x_1, \ldots, x_{k-1}, 1, x_k, \ldots, x_{n-1})$. Перейти к шагу 6.

Шаг 6. Рекурсивно проверить семейство $g = (g_1, \ldots, g_{n-1})$ на правильность.

1) Семейство g правильно. Завершим работу с ответом: "f — правильное семейство".

2) Семейство g не является правильным. Завершим работу с ответом: "семейство f не является правильным".

Сложность алгоритма равна $f(n) = O(n^2 2^n)$.

Список литературы

1. Носов В. А. Критерий регулярности булевского неавтономного автомата с разделенным входом // Интеллектуальные системы. — 1998. — Т. 3, вып. 3–4. — С. 269–280.

2. Носов В. А. О построении классов латинских квадратов в булевой базе данных // Интеллектуальные системы. — 1999. — Т. 4, вып. 3–4. — С. 307–320.

3. Носов В. А. Построение параметрического семейства латинских квадратов в векторной базе данных // Интеллектуальные системы. — 2004. — Т. 8, вып. 1–4. — С. 517–528.

4. Носов В. А., Панкратьев А. Е. О функциональном задании латинских квадратов // Интеллектуальные системы. — 2008. — Т. 12, вып. 1–4. — С. 317–332.

ОБ ОДНОМ ТОЧНОМ ОПИСАНИИ МНОЖЕСТВА ДОПУСТИМЫХ ИСХОДОВ ИГРЫ С ОТНОШЕНИЯМИ ПРЕДПОЧТЕНИЯ НА ОСНОВЕ ПОЛНОТЫ СЕМЕЙСТВА ГОМОМОРФИЗМОВ

Т. Ф. Савина (Москва)

Основными задачами математической теории игр являются построение и изучение математических моделей принятия оптимальных решений в условиях конфликта интересов игроков. Интересы игроков задаются с помощью целевых функций, однако на практике построение таких функций вызывает значительные трудности. Объектом изучения данной статьи являются игры с отношениями предпочтения, в которых целевая структура задается с помощью рефлексивных бинарных отношений.

Игра n ($n \geq 2$) игроков с отношениями предпочтения определяется как система объектов

$$G = \langle X_1, \ldots, X_n, A, \rho_1, \ldots, \rho_n, F \rangle, \tag{1}$$

где X_i — множество стратегий игрока i ($i = 1, \ldots, n$), A — множество исходов, F — отображение множества ситуаций $X_1 \times \ldots \times X_n$ в множество исходов A, ρ_i — отношение предпочтения игрока i ($i = 1, \ldots, n$), заданное на A.

Для игр с отношениями предпочтения вида (1) как для алгебраических систем [1] естественным образом введено понятие гомоморфизма [2]. Отметим, что для игр с упорядоченными исходами (отношение предпочтения есть отношение порядка) понятие гомоморфизма было введено В. В. Розеном [3]. Вопрос о сохранении оптимальных решений при переходе от одной игры с отношениями

предпочтения к другой с помощью гомоморфизма был рассмотрен в работе [4] на базе условий ковариантности и контравариантности гомоморфизмов.

Под оптимальными решениями в игре с отношениями предпочтения понимаются равновесие, равновесие по Нэшу, допустимые и вполне допустимые исходы [5]. В работе [6] указано точное описание множества ситуаций равновесия и множества ситуаций равновесия по Нэшу игры на основе полноты семейства гомоморфизмов. В настоящей статье дано точное описание множества допустимых исходов игры. Введем определение допустимого исхода.

Исход $a \in A$ называется *допустимым в игре* G, если для каждого игрока $i \in N$ выполнено

$$\neg\,(\exists x_i \in X_i)\,\bigl(\forall x_{N\setminus i} \in X_{N\setminus i}\bigr)\,F\,\bigl(x_i, x_{N\setminus i}\bigr) \overset{\rho_i}{>} a.$$

Пусть K и K — два класса игр с отношениями предпочтения множества игроков $N = \{1, \ldots, n\}$. Зафиксируем в этих классах некоторые принципы оптимальности; будем обозначать через $Opt\,G$ множество оптимальных решений игры $G = \langle (X_i)_{i\in N}\,,\, A,\, (\rho_i)_{i\in N}\,,\, F\rangle \in$ K, через $Opt\,\Gamma$ — множество оптимальных решений игры $\Gamma = \langle (Y_i)_{i\in N}\,,\, B,\, (\sigma_i)_{i\in N}\,,\, \Phi\rangle \in K$.

Набор отображений $\boldsymbol{f} = (\varphi_1, \ldots, \varphi_n,\, \psi)$, где $\varphi_i\colon X_i \to Y_i$ $(i \in N)$ и $\psi\colon A \to B$ называется *гомоморфизмом* игры G в игру Γ, если для любого индекса $i \in N$, любых элементов $a_1,\ a_2 \in A$ и любой ситуации $x = (x_1, \ldots, x_n) \in X$ выполняются следующие два условия:

$$Hom1\colon \qquad \psi(F(x_1, \ldots, x_n)) = \Phi(\varphi_1(x_1), \ldots, \varphi_n(x_n)),$$

$$Hom2\colon \qquad a_1 \overset{\rho_i}{\lesssim} a_2 \;\Rightarrow\; \psi(a_1) \overset{\sigma_i}{\lesssim} \psi(a_2).$$

Гомоморфизм $\boldsymbol{f}$ игры G в игру Γ называется *строгим,* если для каждого $i \in N$ дополнительно выполняется условие

$$Str\colon \qquad a_1 \overset{\rho_i}{<} a_2 \;\Rightarrow\; \psi(a_1) \overset{\sigma_i}{<} \psi(a_2).$$

Зафиксируем некоторый класс H гомоморфизмов из игр класса K в игры класса K. Гомоморфизмы класса H называются *ковариантными относительно классов* (K, K), если для любых двух игр $G \in$ K и $\Gamma \in K$ и любого гомоморфизма $\boldsymbol{f} \in H$ $\quad$ $\boldsymbol{f}$-образ оптимального решения игры G есть оптимальное решение в игре Γ, и *контравариантными относительно классов* (K, K), если для любых двух

игр $G \in$ K и $\Gamma \in K$ и любого гомоморфизма $\boldsymbol{f} \in H$ $\boldsymbol{f}$-прообраз оптимального решения игры Γ есть оптимальное решение в игре G.

Семейство гомоморфизмов $(\boldsymbol{f}_j)_{j\in J}$ называется *ковариантно полным*, если для каждого оптимального решения $p \in Opt\, G$ существует такой индекс $j \in J$, что $\boldsymbol{f}_j(p) \in Opt\, \Gamma_j$.

Лемма. *Семейство гомоморфизмов $(\boldsymbol{f}_j)_{j\in J}$ является ковариантно полным семейством контравариантных гомоморфизмов тогда и только тогда, когда выполнено равенство:*

$$Opt\, G = \bigcup_{j\in J} \boldsymbol{f}_j^{-1}(Opt\, \Gamma_j).$$

Пусть K — класс игр с упорядоченными исходами игроков N, в которых множества стратегий игроков конечны, K — класс игр того же множества игроков с функциями выигрыша. В качестве оптимальных решений игры $G \in$ K возьмем множество ее допустимых исходов, а в качестве оптимальных решений игры $\Gamma \in K$ — множество ее индивидуально рациональных исходов. Тогда справедлива следующая теорема.

Теорема. 1. *Относительно указанных классов игр и их оптимальных решений все строгие сюръективные гомоморфизмы являются контравариантными.*

2. *Для каждой игры $G \in$ K семейство всех ее строгих сюръективных гомоморфизмов в игры $\Gamma \in K$ является ковариантно полным.*

Список литературы

1. Богомолов А. М., Салий В. Н. Алгебраические основы теории дискретных систем. — М.: Наука. Физматлит, 1997.

2. Савина Т. Ф. Гомоморфизмы игр с отношениями предпочтения // Материалы X Международного семинара «Дискретная математика и ее приложения» (Москва, МГУ, 1–6 февраля 2010 г.). — М.: Изд-во механико-математического факультета МГУ, 2010. С. 426–428.

3. Розен В. В. Гомоморфизмы игр с упорядоченными исходами // Математические модели поведения. Методы и модели принятия решений. Межвуз. науч. сб. — Изд-во СГУ, 1981. — С. 90–104.

4. Савина Т. Ф. Ковариантные и контравариантные гомоморфизмы игр с отношениями предпочтения // Изв. Сарат. ун-та. Нов. сер. Сер. Математика. Механика. Информатика. — 2009. — Т. 9, вып. 3. — С. 66–70.

5. Савина Т. Ф. Оптимальные решения в играх с отношениями предпочтения // Изв. Сарат. ун-та. Нов. сер. Сер. Математика. Механика. Информатика. — 2011. — Т. 11, вып. 2. — С. 32–36.

6. Савина Т. Ф. О полных семействах гомоморфизмов игр с отношениями предпочтения // Сб. науч. тр. Механика. Математика. — Саратов: Изд-во Сарат. ун-та, 2011. — С. 92–95.

ПОДХОД К УПРАВЛЕНИЮ ПРОГРАММОЙ ИНСТРУКЦИЯМИ НА РУССКОМ ЯЗЫКЕ

Е. А. Семенов (Москва)

Рассмотрим простой подход к задаче управления действиями программы инструкциями на естественном (русском) языке путем голосования. Задача состоит в том чтобы перевести текст на русском языке в последовательность команд, которые программа способна выполнить. Будем считать программу конечным набором независимых команд (реакций на действия пользователя). Тогда задача сводится к разбиению входящего текста на *инструкции*, каждая из которых заставляет программу выполнить какую-либо одну команду, и выбору команды для каждой инструкции.

Пусть конкретная программа может выполнять N независимых команд. Выделим для этой программы конечный словарь D "важных" слов. Будем разделять три вида таких слов: глаголы (V), побочные слова (A) и слова параметрические (P).

$$D = V \cup A \cup P.$$

Такое разделение обусловлено следующим правилом разбиения текста на инструкции: во-первых, будем учитывать только "важные" слова (т. е. слова не из словаря будем игнорировать). Во-вторых, каждую инструкцию будем считать начинающейся с глагола (или деепричастия, которые тоже входят в подмножество словаря "глаголы"). На самом деле, фразы повелительного наклонения почти всегда начинаются с глагола ("пойди туда-то", "сделай то-то"), поэтому такое правило вполне оправдано. Другие слова - не глаголы - делятся на побочные, которые помогают выбрать ту или иную команду, и параметрические, которые просто задают параметры, с которыми выбранная команда будет выполнена.

Далее, всем глаголам и побочным словам из словаря сопоставим каким-то образом (сначала случайно) векторы длины N коэффициентов голосования этих слов за всевозможные команды программы. Голосование будет осуществляться линейным образом: когда входящий текст уже разбит на инструкции, для каждой инструкции складываются все векторы попавших в нее побочных слов и глагола, создавая таким образом результирующий вектор голосования. Номер его наибольшего элемента будет номером команды, на которую указывает данная инструкция, а параметрические слова, участвующие в ней, задают для этой команды набор параметров. В случае если нет однозначного наибольшего элемента у результирующего вектора, система должна "переспросить" пользователя, какую команду тот имел в виду (т. е. происходит обучение с учителем).

Таким образом, остается лишь обучить систему, т.е. расставить верные коэффициенты в векторы голосования. Для этого предлагается выразить все пары (*инструкция, команда*) в виде систем неравенств и использовать для их решения методы линейного программирования.

Рассмотрим инструкцию, состоящую из слов, соответствующих векторам a^1, a^2, ..., a^m. Пусть эта инструкция должна указывать на l-ю команду. Тогда имеет место следующая система неравенств:

$a_1^1 + a_1^2 + ... + a_1^m < a_l^1 + a_l^2 + ... + a_l^m$,
$a_2^1 + a_2^2 + ... + a_2^m < a_l^1 + a_l^2 + ... + a_l^m$,
...
$a_N^1 + a_N^2 + ... + a_N^m < a_l^1 + a_l^2 + ... + a_l^m$.

Таким образом, каждая пара (инструкция, команда) добавляет в общую систему $N - 1$ неравенство относительно $(|V| + |A|) \times N$ переменных коэффициентов голосования.

Пусть на какой-то инструкции система выбирает команду неверно, при этом есть уже k инструкций, обрабатываемых верно. Тогда рассмотрим общую систему из $(k+1) \times (N-1)$ неравенств, в которой последний "блок" определен с помощью обращения к пользователю (он указывает верную команду). Будем считать что пользователь никогда не ошибается, т.е. система всегда совместна.

Тогда применим к этой системе *симплекс-метод* линейного программирования [1], минимизируя сумму коэффициентов всех векторов и находя решение, удовлетворяющее общей системе неравенств.

Вообще говоря, в случае пополняемого словаря обучение не обязано сходиться, ведь с появлением каждого нового слова систему необходимо переучивать. Рассмотрим случай когда словарь D конечен, $|D| = d$, $|V| = v$, $|A| = a$. Принимая во внимание то, что

в каждой инструкции участвует ровно один глагол, всевозможные варианты инструкций ограничиваются числом

$$C = v \times 2^a.$$

Значит, в худшем случае обучение завершится за такое количество итераций переобучения.

В качестве оптимизации подхода предлагается считать инструкции монотонными, т. е. если все слова одной инструкции, связанной с командой j, содержатся внутри другой инструкции, то объемлющая инструкция также обязана голосовать за команду под номером j. В таком случае, проведя аналогию между множеством инструкций и булевым кубом (i-е слово из словаря либо входит в инструкцию, либо не входит - таким образом, 1 либо 0 на i-й позиции), согласно лемме 7.1 из [2], количество монотонных инструкций ограничивается числом

$$C_m = v \times \mathbf{C}_a^{a/2},$$

т. е. в случае использования монотонных инструкций, в худшем случае потребуется такое количество переобучений.

Работа выполнена под руководством профессора Э. Э. Гасанова.

Список литературы

1. Хемди А. Т. Введение в исследование операций. — М.: Издательский дом «Вильямс», 2005.

2. Чашкин А. В. Лекции по дискретной математике. — М.: Издательство механико-математического факультета МГУ, 2007.

КОНСТРУИРОВАНИЕ ДВИЖУЩИХСЯ ИЗОБРАЖЕНИЙ КЛЕТОЧНЫМИ АВТОМАТАМИ

Е. Е. Титова (Москва)

В работе исследуется задача построения движущихся объектов в полосе. Рассматривается последовательность из m одинаковых элементарных автоматов $\mathcal{A}$ с двумя входами, называемая *экраном*. Входы автомата называются левым и правым и ими соответственно являются состояния левого и правого соседа. Правый вход последнего m-го автомата доопределяется как тождественный ноль, а левый вход первого автомата называется свободным и подключен у выходу управляющего автомата $\mathcal{A}_e$. Тройку $G = \langle \mathcal{A}_e, \mathcal{A}, m \rangle$, будем называть *генератором*.

Среди состояний элементарного автомата выделим непустое подмножество L и элементы этого множества будем называть *метками.*

Изображением на экране в момент времени t будем называть множество номеров элементарных автоматов, состояния которых в момент времени t являются метками, и обозначать через I_t.

Пусть $A = \{i_1, i_2, \ldots, i_k\}$, где $i_1, i_2, \ldots, i_k \in \mathbb{Z}$, то для $b \in \mathbb{Z}$ будем обозначать $A + b = \{i_1 + b, i_2 + b, \ldots, i_k + b\}$. Обозначим $N_m = \{1, 2, \ldots, m\}$.

Пусть в момент времени t_0 на экране находится изображение I_{t_0}. Будем говорить, что изображение на экране движется со скоростью $v = 1/s, s \in \mathbb{N}$ на промежутке времени $t \in [t_0, t_0 + sl), l \in \mathbb{N}$, если выполняются следующие условия:

1. $I_{(t_0-1)} = (I_{t_0} - 1) \bigcap N_m$;

2. Если $t \in [t_0+sj, t_0+s(j+1)), 0 \leq j < l$ то $I_t = (I_{t_0+sj-1}+1) \bigcap N_m$ или $I_t = \{1\} \bigcup ((I_{t_0+sj-1} + 1) \bigcap N_m)$;

3. $I_{t_0+sl+1} = (I_{t_0+sl} + 1) \bigcap N_m$ или $I_{t_0+sl+1} = \{1\} \bigcup ((I_{t_0+sl} + 1) \bigcap N_m)$.

Утверждение 1. *Существует элементарный автомат $\mathcal{A}$ с 2 состояниями, управляющий автомат $\mathcal{A}_e$, т.ч. для любого $m \in \mathbb{N}$ генератор $\langle \mathcal{A}_e, \mathcal{A}, m \rangle$ может генерировать на экране изображение, в любой промежуток времени движущееся со скоростью $v = 1$.*

Утверждение 2. *Существует элементарный автомат $\mathcal{A}$ с 4 состояниями, управляющий автомат $\mathcal{A}_e$, т.ч. для любого $m \in \mathbb{N}$ генератор $\langle \mathcal{A}_e, \mathcal{A}, m \rangle$ может генерировать на экране изображение, состоящее из одной точки, которая может двигаться с любой наперед заданной скоростью $v = 1/s, s \in \mathbb{N}, s \geq 2$ на любом наперед заданном промежутке времени.*

В этом алгоритме множество меток содержит два состояния, кроме этого есть состояние 0 и сигнал, движущийся со скоростью 1. Первая из меток остается неизменной до тех пор, пока автомат слева от нее не станет движущимся сигналом. Как только это произойдет, метка меняется на вторую, которая передает следующему за ней автомату сигнал стать меткой первого типа, а сама исчезает в следующий момент времени. Движущий сигнал можно подавать с любой частотой, тем самым двигая точку с любой скоростью $v = 1/s, s \in \mathbb{N}, s \geq 2$.

Утверждение 3. *Существует элементарный автомат $\mathcal{A}$ с 12 состояниями, управляющий автомат $\mathcal{A}_e$, т.ч. для любого $m \in \mathbb{N}$ генератор $\langle \mathcal{A}_e, \mathcal{A}, m \rangle$ может генерировать на экране изображение, состоящее из одного отрезка, который может двигаться с любой наперед заданной скоростью $v = 1/s, s \in \mathbb{N}, s \geq 2$ на любом наперед*

заданном промежутке времени.

Здесь считаем, что отрезок состоит из трех типов точек — левый край, внутренние точки и правый край. Если отрезок имеет длину 1, считаем, что он состоит из одной граничной точки, если длину 2, то из двух граничных точек без внутренних. Каждый из краев отрезка будем двигать согласно предыдущему алгоритму. Множество состояний элементарного автомата получается из декартова произведения двух множеств состояний автомата из предыдущего алгоритма исключением состояний, которые никогда не появятся на экране, и добавлением состояния для внутренних точек отрезка.

Утверждение 4. *Существует элементарный автомат $\mathcal{A}$ с 9 состояниями, управляющий автомат $\mathcal{A}_e$, т.ч. для любого $m \in \mathbb{N}$ генератор $\langle \mathcal{A}_e, \mathcal{A}, m\rangle$ может генерировать на экране изображение, состоящее из k точек, $k \in \mathbb{N}$ с координатами $1 \le i_1 < i_2 < \ldots < i_k \le m$, удовлетворяющими условиям $i_j - i_{j-1} \ge j+1$ для любого $2 \le j \le k$. При этом изображение может двигаться в любой заранее заданный промежуток времени с наперед заданной скоростью $v = 1/s$, где $s \ge i_k - i_1 + k + 1 \ge k^2/2 + 3k/2, s \in \mathbb{N}$.*

Идея этого алгоритма похожа на идею алгоритма из утв. 2. Сложность в том, что сигнал должен распознать, какой из точек он предназначен. Можно для каждой точки запустить отдельный тип сигнала, но тогда количество состояний элементарного автомата будет зависеть от числа точек в изображении. Этого хочется избежать. Поэтому каждый сигнал содержит некоторый след — цепочку автоматов в специальном состоянии. При прохождении через метку длина следа уменьшается на 1. Когда сигнал без следа достигает метки, это означает, что он предназначен этой метке и она продвигается на 1. Если подавать такие сигналы слишком часто, то они начнут друг на друга накладываться, что приведет к увеличению числа состояний. Отсюда следует нижняя оценка скорости движения изображения, реализуемой данным алгоритмом.

Утверждение 5. *Существует элементарный автомат $\mathcal{A}$ с 50 состояниями, управляющий автомат $\mathcal{A}_e$, т.ч. для любого $m \in \mathbb{N}$ генератор $\langle \mathcal{A}_e, \mathcal{A}, m\rangle$ может генерировать на экране изображение, состоящее из k отрезков, $k \in \mathbb{N}$ с координатами левых концов, $1 \le l_1 < l_2 < \ldots < l_k \le m$,и с координатами правых концов, $1 \le r_1 < r_2 < \ldots < r_k \le m$ удовлетворяющими условиям $l_j - l_{j-1} \ge j+1$ и $r_j - r_{j-1} \ge j+1$ для любого $2 \le j \le k$. При этом изображение может двигаться в любой заранее заданный промежуток времени с наперед заданной скоростью $v = 1/s$, где $s \in \mathbb{N}, s \ge i_k - i_1 + k + 1 \ge k^2/2 + 3k/2$.*

Данный алгоритм получается из предыдущего по аналогии с ал-

горитмом из утв. 3. Можно действовать иначе: каждый отрезок двигать по алгоритму из утв. 3, т. е. для каждого отрезка запускать отдельную пару сигналов, но тогда снова количество состояний элементарного автомата будет зависеть от числа отрезков в изображении.

Автор выражает искреннюю благодарность научному руководителю, профессору Э. Э. Гасанову за постановку задачи и научное руководство.

Список литературы

1. Кудрявцев В. Б., Подколзин А. С., Болотов А. А. Основы теории однородных структур. — М.: Наука, 1990.

2. Титова Е. Е. Конструирование изображений клеточными автоматами // Интеллектуальные системы. — 2008. — Т. 12, вып. 1–4. — С. 105–121.

3. Титова Е. Е. Линейное по времени конструирование изображений клеточными автоматами // Интеллектуальные системы. — 2011. — Т. 15, вып. 1–4.

О ПОЛНОТЕ В КЛАССЕ ЛИНЕЙНО-АВТОМАТНЫХ ФУНКЦИЙ С ОПЕРАЦИЯМИ СУПЕРПОЗИЦИИ

А. А. Часовских (Москва)

Все необходимые определения можно найти в работах [1], [2]. Ранее была решена задача о полноте в классе (L, K) линейно-автоматных функций L с операциями композиции K [2]. В классе (L, K) были найдены все предполные классы, число которых оказалось счетным. В настоящей работе рассматривается задача о полноте для класса (L, S) линейно-автоматных функций с операциями суперпозиции S. Построено счетное множество S-предполных классов, являющееся приведенной S-критериальной системой.

Бесконечной последовательности нулей и единиц α, $\alpha = \alpha(0)$, $\alpha(1)$, ..., $\alpha(t)$, ..., $\alpha(t) \in E_2$, $t = 0, 1, ...$ сопоставим формальный ряд переменной ξ:

$$\alpha(\xi) = \sum_{t=0}^{\infty} \alpha(t)\xi^t.$$

Положим

$$R_2 = \{ \quad \alpha(\xi) \quad | \quad \alpha \in E_2^\infty \quad \},$$

$$PR_2 = \{ \quad \alpha(\xi) \quad | \quad \alpha \in E_2^\infty,$$

α— периодическая (с предпериодом) последовательность $\quad \}$.

На множестве R_2 естественным образом введем операции сложения и умножения. Пусть $\alpha_i = \sum_{t=0}^{\infty} \alpha_i(t)\xi^t$, $i = 1, 2$. Положим:

$$\alpha_1(\xi) + \alpha_2(\xi) = \sum_{t=0}^{\infty} (\alpha_1(t) + \alpha_2(t))\, \xi^t,$$

$$\alpha_1(\xi) \cdot \alpha_2(\xi) = \sum_{t=0}^{\infty} \left(\sum_{j=0}^{t} \alpha_1(j) \cdot \alpha_2(t-j) \right) \xi^t.$$

Множество PR_2 совпадает с кольцом отношений многочленов, каждый элемент которого, будучи представленным в несократимом виде, имеет знаменатель со свободным членом 1,

$$PR_2 = \{ \quad u(\xi)/v(\xi) \quad | \quad u, v \in E_2[\xi], \quad v(0) = 1 \quad \}.$$

Пусть $n \in N$, $\mu_i \in PR_2$, $i = 0, 1, \ldots, n$. Отображение $f(x_1, \ldots, x_n)$ из R_2^n в R_2, задаваемое для любых α_i, $\alpha_i \in R_2$, $i = 1, 2, \ldots, n$, равенством

$$f(\alpha_1, \alpha_2, \ldots, \alpha_n) = \sum_{i=1}^{n} \mu_i \alpha_i + \mu_0,$$

называется *линейно-автоматной функцией*. Для линейно-автоматной функции $f(x_1, x_2, \ldots, x_n)$, задаваемой приведенным равенством, положим

$$U(f) = \{ \quad \mu_i \quad | \quad i = 1, 2, \ldots, n \quad \},$$

а переменная x_i этой функции называется *непосредственной*, если μ_i, будучи представленной в несократимом виде, имеет числитель со свободным членом 1.

Через L обозначим множество всех линейно-автоматных функций. Для множества M', $M' \subseteq L$, положим:

$$U(M') = \cup_{f \in M'} U(f).$$

На множестве L будем рассматривать операции суперпозиции (переименование переменных, отождествление переменных, подстановка). Замыкание множества M', $M' \subseteq L$, по операциям суперпозиции будем обозначать $S(M')$. Множество M', $M' \subseteq L$, называется

S-замкнутым, если $S(M') = M'$. Множество M', $M' \subseteq L$, называется *S-полным*, если $S(M') = L$. Множество M', $M' \subset L$, называется *S-предполным*, если M' не является S-полным, но для любой f, $f \in L \setminus M'$, множество $M' \cup \{f\}$ является S-полным. Множество S-замкнутых классов Ω называется *S-критериальной системой* в точности тогда, когда для любого множества M', $M' \subseteq L$, равенство $S(M') = L$ равносильно невключению множества M' ни в один из классов θ, $\theta \in \Omega$. S-критериальная система Ω называется *приведенной*, если из нее нельзя удалить ни одного класса так, чтобы оставшееся множество составляло критериальную систему.

Далее, рассматривая дроби u/v из PR_2, считаем, что $(u, v) = 1$. Положим:

$$1 + \xi PR_2 = \{ \quad 1 + \xi \cdot u/v \quad | \quad u/v \in PR_2 \quad \}.$$

$$M_1 = \{ \quad a + \xi^2 \cdot u/v \quad | \quad a \in E_2, \quad u/v \in PR_2 \quad \},$$

$$M_0 = \{ \quad u/v \quad | \quad u/v \in PR_2, \quad \deg u \leq \deg v \quad \}.$$

Пусть p_1,p_2,... — последовательность различных неприводимых многочленов, содержащая все неприводимые многочлены, причем $p_1 = \xi$. Положим:

$$M_i = \{ \quad u/v \quad | \quad u/v \in PR_2, \quad (v, p_i) = 1 \quad \},$$

$i = 2, 3, \ldots$.

Рассмотрим следующие подмножества в L.

$$T_a = \{ \quad f \quad | \quad \text{для любых} \quad \alpha_i(\xi), \quad \alpha_i(\xi) \in R_2, \quad \alpha_i(0) = a, \\ i = 1, 2, \ldots, n, \quad \text{выполнено} \quad f(\alpha_1(\xi), \alpha_2(\xi), \ldots, \alpha_n(\xi))(0) = a \quad \},$$

$a = 0, 1$,

$$V_1 = \{ \quad f \quad | \\ f \quad \text{имеет не более одной непосредственной переменной} \quad \},$$

$$V_{\text{н}} = \{ \quad f \quad | \\ f \quad \text{имеет нечетное число непосредственных переменных} \quad \},$$

$$M(p_i) = \{ \quad f \quad | \quad U(f) \subset M_i \quad \},$$

$i = 1, 2, \ldots,$

$$M = \{ \quad f \quad | \quad U(f) \subset M_0 \quad \},$$

Через Ω_s обозначим следующее множество:

$$\{ \quad T_0, T_1, V_1, V_{\text{н}}, M, M(p_i) \quad | \quad i = 1, 2, 3, \ldots \quad \}.$$

Имеет место

Теорема. *Множество Ω_s является приведенной S-критериальной системой в L, состоящей из S-предполных классов.*

Автор выражает благодарность В. Б. Кудрявцеву и С. В. Алешину за постоянную поддержку в работе.

Список литературы

1. Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Элементы теории автоматов. — М.: МГУ, 1978.

2. Часовских А. А. О полноте в классе линейных автоматов // Математические вопросы кибернетики. — М.: Наука, 1991. — Вып. 3. — С. 140–166.

Секция «Дискретная геометрия»

РАЗЛОЖЕНИЕ СЛУЧАЙНОГО ТЕНЗОРА ЗАДАННОГО ТЕНЗОРНОГО РАНГА НАД ПОЛЕМ $GF(2)$

А. Я. Белянков (Москва)

Ставится вопрос об алгоритме, получающем на входе d-индексную таблицу значений $T_{i_1\dots i_d} \in \mathrm{GF}(2)$,

$$T_{i_1\dots i_d} = \sum_{\rho=1}^{r} t_{i_1}^{1,\rho} \dots t_{i_d}^{d,\rho}, \qquad 1 \le i_1 \le n_1, \dots, 1 \le i_d \le n_d, \qquad (1)$$

а на выходе восстанавливающем правую часть (1), причем известно, что все $t_{i_\delta}^{\delta,\rho}$ были сгенерированы как независимые случайные значения из $\mathrm{GF}(2)$ (0 и 1 равновероятны). Поставленный вопрос примыкает к рассмотрениям, изложенным в [1].

Прямой перебор величин $t_{i_\delta}^{\delta,\rho}$ характеризуется объемом $2^{(n_1+\dots+n_d)r}$. Линейно упорядочивая слагаемые в правой части (1) можно сократить объем перебора приблизительно в $r!$ раз. Однако и после этого прямой перебор может оказаться неприемлемо трудоемким.

Покажем возможность учета случайного вида слагаемых в правой части (1). Пусть X_δ есть множество последовательностей $(\xi_1, \dots, \xi_{n_\delta})$ элементов $\mathrm{GF}(2)$, а $T(x) = T(x_1, \dots, x_d)$ есть определенная на множестве $X = X_1 \times \dots \times X_d$ d-линейная функция

$$T(x) = \sum_{i_1=1}^{n_1} \dots \sum_{i_d=1}^{n_d} T_{i_1\dots i_d} x_1^{i_1} \dots x_d^{i_d} =$$

$$= \sum_{\rho=1}^{r} \prod_{\delta=1}^{d} \left\langle t^{\delta,\rho}, x_\delta \right\rangle = \sum_{\rho=1}^{r} \prod_{\delta=1}^{d} \sum_{i_\delta=1}^{n_\delta} t_{i_\delta}^{\delta,\rho} x_\delta^{i_\delta}.$$

Считая, что $0 \le r_1 \le r$, положим $r_2 = r - r_1$, $T = T^1 + T^2$, где

$$T^1(x) = \sum_{\rho=1}^{r_1} \prod_{\delta=1}^{d} \left\langle t^{\delta,\rho}, x_\delta \right\rangle, \qquad T^2(x) = \sum_{\rho=r_1+1}^{r} \prod_{\delta=1}^{d} \left\langle t^{\delta,\rho}, x_\delta \right\rangle.$$

Независимость величин $t^{\delta,\rho}_{i_\delta}$ влечет независимость случайных событий $T^i(x) = \tau^i$, $i = 1, 2$. Так как $0 = 0 + 0 = 1 + 1$, $1 = 1 + 0 = 0 + 1$, то

$$\begin{aligned} \mathrm{P}(T = 0) &= \mathrm{P}(T^1 = 0)\mathrm{P}(T^2 = 0) + \mathrm{P}(T^1 = 1)\mathrm{P}(T^2 = 1), \\ \mathrm{P}(T = 1) &= \mathrm{P}(T^1 = 1)\mathrm{P}(T^2 = 0) + \mathrm{P}(T^1 = 0)\mathrm{P}(T^2 = 1), \end{aligned}$$

так что

$$\mathrm{P}(T = 0) - \mathrm{P}(T = 1) = (\mathrm{P}(T^1 = 0) - \mathrm{P}(T^1 = 1))(\mathrm{P}(T^2 = 0) - \mathrm{P}(T^2 = 1))$$

(здесь $T = T(x)$, $T^1 = T^1(x)$, $T^2 = T^2(x)$). Введя обозначение $t_r(x) = \mathrm{P}(T(x) = 0) - \mathrm{P}(T(x) = 1)$, подчеркивающее зависимость от r и от x, перепишем последнюю формулу в виде $t_r(x) = t_{r_1}(x)t_{r_2}(x)$.

Теорема. 1. *Зависимость $t_r(x)$ от r экспоненциальна*:

$$\mathrm{P}(T(x) = 0) - \mathrm{P}(T(x) = 1) = t_1(x)^r.$$

2. *Для $t_1(x)$ справедлива явная формула*

$$t_1(x) = \begin{cases} 1 - 2^{1-d}, & \text{если все } x_1, \ldots, x_d \text{ ненулевые}, \\ 1, & \text{в противном случае}. \end{cases}$$

Следствие. *Если все $x_1, \ldots, x_d$ ненулевые, то*

$$\mathrm{P}(T(x) = 0) - \mathrm{P}(T(x) = 1) = (1 - 2^{1-d})^r. \tag{2}$$

Наметим в общих чертах применение этих результатов для восстановления разложения вида (1) по известной таблице $T_{i_1 \ldots i_d}$, случайно сгенерированной указанным выше образом. Знание таблицы позволяет вычислять значения $T(x)$ и оценивать статистические характеристики $T(x)$. Важнейшая характеристика — левая часть формулы (2), для экспериментальной оценки которой следует накопить статистику событий $T(x) = \tau$, $\tau \in \{0, 1\}$. Если осуществлять это накопление, варьируя все ненулевые $x_1, \ldots, x_d$, то полученная оценка должна быть близка к правой части (2).

Эта же характеристика укажет на совпадение пробного набора $(t^1, \ldots, t^d)$ ($t^\delta \neq 0$ для всех δ) с одним из $(t^{1,\rho} \ldots, t^{d,\rho})$, $1 \leq \rho \leq r$. Для определенности положим $\rho = r_1 = 1$ и осуществим накопление событий $T(x) = \tau$, ограничив варьирование теми ненулевыми $x_1, \ldots, x_d$,

для которых $\langle t^1, x_1\rangle \dots \langle t^d, x_d\rangle = 0$, т. е. (при указанном совпадении) в точности $T^1(x) = 0$, $\mathrm{P}(T^1 = 0) - \mathrm{P}(T^1 = 1) = 1$. Тогда

$$\mathrm{P}(T = 0) - \mathrm{P}(T = 1) = 1 \cdot (\mathrm{P}(T^2 = 0) - \mathrm{P}(T^2 = 1)) = (1 - 2^{1-d})^{r-1}$$

(мы применили следствие к $T^2(x)$ и учли, что $r_2 = r-1$). Совпадение сопровождается статистически значимым повышением оценки левой части (2): $(1 - 2^{1-d})^{r-1} > (1 - 2^{1-d})^r$. Аналогичное ограничение варьирования теми $x_1, \dots, x_d$, для которых $\langle t^1, x_1\rangle \dots \langle t^d, x_d\rangle = 1$, при совпадении дает равенства $T^1(x) = 1$, $\mathrm{P}(T^1 = 0) - \mathrm{P}(T^1 = 1) = -1$ и

$$\mathrm{P}(T = 0) - \mathrm{P}(T = 1) = -(1 - 2^{1-d})^{r-1}.$$

Развитие и детализация этих рассмотрений позволяет выделять сравнительно перспективные t^δ, компоновать из них перспективные пары и т. д., заканчивая наборами $(t^1, \dots, t^d)$ и получая приемлемый объем перебора.

Выполнены эксперименты по разложению случайно сгенерированной трилинейной формы, близкой по характеристикам к трилинейной форме $\mathrm{tr}(ABC)$ от 3×3-матриц A, B, C над $\mathrm{GF}(2)$. Алгоритм уверенно находит искомое разложение за минуты на обычном ноутбуке.

Однако попытка использовать разработанный алгоритм для тензорного разложения самой формы $\mathrm{tr}(ABC)$ (на решение подобных задач и нацелено настоящее исследование) пока не привела к успеху. Трудности происходят, повидимому, из весьма большой симметричности формы $\mathrm{tr}(ABC)$. Даже при рассмотрении над простейшим полем $\mathrm{GF}(2)$ число различных тензорных разложений минимальной длины оказывается очень большим.

Список литературы

1. Белянков А. Я. Вычисление векторного произведения трехмерных векторов с использованием 5 умножений // Материалы X Международного семинара "Дискретная математика и ее приложения" (1–6 февраля 2010 г.). — М.: Изд-во механико-математического факультета МГУ, 2010. — С. 470–472.

О СУЩЕСТВОВАНИИ ВОССТАНАВЛИВАЮЩЕГО НАПРЯЖЕНИЯ

М. Д. Ковалёв (Москва)

В настоящей заметке рассматриваются конструкции из рычагов и шарниров в плоскости, допускающие внутренние напряжения. Получен отрицательный ответ на ранее поставленный вопрос о существовании восстанавливающего напряжения [1]. А именно, приведён пример конструкции для которой можно восстановить положения всех свободных шарниров, зная её пространство внутренних напряжений и положения закреплённых шарниров, однако, этого нельзя сделать зная не всё пространство внутренних напряжений а лишь какое-либо одно внутреннее напряжение

Шарнирником p называем погружение графа $G(V,E)$, $|E| = r$, удовлетворяющего определённым условиям [2], в плоскость. При этом вершинам графа отвечают точки (шарниры), а рёбрам — отрезки прямых (рычаги). Вершины графа $G(V,E)$, а значит, и шарниры, могут быть двух сортов: свободные (пусть их число m , и закреплённые (пусть их число n). Это погружение можно мыслить как плоскую конструкцию, составленную из рычагов, соединённых шарнирами, причём, некоторые из шарниров жёстко закреплены в плоскости.

Пусть p_i — радиус-вектор i-го шарнира. Условие равновесия сил, приложенных к i-му свободному шарниру со стороны смежных шарниров, имеет вид

$$\sum_j \omega_{ij}(p_j - p_i) = 0,$$

где суммирование проводится по всем шарнирам p_j, смежным с p_i, а скаляр $\omega_{ij}{=}\omega_{ji}$ — называется внутренним напряжением рычага p_ip_j. Если в R^2 задан шарнирник p, то его внутренние напряжения $\omega{=}\{\omega_{ij}\}$ определяются как нетривиальные решения однородной системы линейных уравнений

$$\sum_j \omega_{ij}(p_j - p_i) = 0, \qquad 1 \le i \le m. \tag{1}$$

Таким образом, множество внутренних напряжений ω заданного шарнирника p вместе с нулевым напряжением представляет собой линейное подпространство $W(p)$ пространства W^r, всех мыслимых напряжений рычагов шарнирника с графом $G(V,E)$.

Зафиксируем положения $p^0_{m+1}, ..., p^0_{m+n}$ закрепленных шарниров в R^2. Пусть $W(p^0)$ — есть множество решений $\omega = \{\omega_{ij}\}$ системы уравнений (1) при заданных $p_1 = p^0_1, ..., p_m = p^0_m$.

Зафиксировав ω и считая неизвестными радиус-векторы $p_1, p_2, ..., p_m$ свободных шарниров, перепишем систему (1) так

$$(\sum_{j,(v_i,v_j)\in E} \omega_{ij})p_i - \sum_{j,(v_i,v_j)\in E_1} \omega_{ij}p_j = \sum_{j,(v_i,v_j)\in E_2} \omega_{ij}p^0_j, \qquad 1 \le i \le m.$$

Матрица $\Omega = \Omega(\omega)$ этой системы является симметрической. Пусть $p(\omega) = (p_1(\omega), ..., p_m(\omega))$ — множество всех решений этой системы линейных уравнений при фиксированном $\{\omega_{ij}\} = \omega \in W(p^0)$. Мы говорим, что шарнирник p^0 восстановим по своему пространству внутренних напряжений $W(p^0) \subset W^r$, если

$$\bigcap_{\omega\in W(p^0)} p(\omega) = p^0.$$

Условие

$$\det \Omega(\omega) \neq 0, \tag{2}$$

где ω — какой-либо ненулевой вектор из $W(p^0)$, является достаточным для восстановимости шарнирника p^0 по пространству его напряжений.

Если имеет место неравенство (2), то говорят, что шарнирник p^0 *восстановим* по напряжению ω, а напряжение ω называется *восстанавливающим*. В работе [1] был поставлен вопрос: является ли условие (2) необходимым для восстановимости шарнирника p^0 в случае многомерного пространства $W(p^0)$? Для шарнирников на прямой ответ положителен [3]. Исследуя этот вопрос разумно ограничиться [2, 3] лишь рассмотрением шарнирников с рычагами ненулевой длины, и допускающих ненулевое на всех рычагах напряжение. Отметим также, что шарнирники, для которых существует внутреннее напряжение со всеми $\omega_{ij} > 0$ называются паутинными, и они восстановимы по каждому такому напряжению [4].

Мы приведём пример, дающий отрицательный ответ на поставленный вопрос. Шарнирник примера можно мыслить симметричным относительно осей декартовой прямоугольной системы координат в плоскости. Закреплённые его шарниры лежат в точках

$(1,0), (0,1), (-1,0), (0,-1)$. Свободные же шарниры лежат в вершинах трёх концентричных квадратов K_a, K_b, K_c. Верхние вершины квадратов K_a, K_b, K_c имеют координаты $(0, 1+a), (0, 1+a+b)$ и $(0, 1+a+c)$ соответственно. Шарниры внешних квадратов K_b и K_c соединены рычагами с вершинами внутреннего квадрата K_a. Ясно, что если один из рычагов какого-либо из этих квадратов имеет ненулевое напряжение, то и все рычаги этого квадрата имеют то же самое напряжение. Эти напряжения однозначно определяют напряжения рычагов, направленных к центру симметрии. Для одного квадрата они тоже все одинаковы. Пусть w_b и w_c — напряжения рычагов, соединяющих шарниры квадратов K_b и K_c с K_a, а w — напряжения рычагов, исходящих из закреплённых шарниров в вершины квадрата K_a. Здесь пространство внутренних напряжений трёхмерно, в качестве координат в нём можно взять величины w, w_b, w_c.

Оказывается, если взять $a = 1, b = 2, c = 2$ (в этом случае квадраты K_b и K_c совпадают), то для любого внутреннего напряжения ω этого шарнирника $\det \Omega(\omega) = 0$, поэтому шарнирник не обладает восстанавливающим напряжением. С другой стороны, ядро матрицы $\Omega(\omega)$ порождается, как нетрудно проверить, векторами

$$[0,\ 0,\ 0,\ 0,\ w_c,\ -w_c,\ w_c,\ -w_c,\ -w_b,\ w_b,\ -w_b,\ w_b,]\,.$$

Откуда ясно, что пересечение решений системы (1), отвечающих всем возможным внутренним напряжениям шарнирника, состоит лишь из одной точки. Таким образом, наш шарнирник восстановим по пространству внутренних напряжений.

Список литературы

1. Ковалев М. Д. О восстановимости шарнирников по внутренним напряжениям // Известия РАН. Серия математическая. — 1997. — Т. 61. — С. 37–66.

2. Ковалев М. Д. Геометрическая теория шарнирных устройств // Известия РАН. Серия математическая. — 1994. — Т. 58, № 1. — С. 45–70.

3. Ковалев М. Д. О шарнирниках, восстановимых по единственному напряжению // Записки научных семинаров ПОМИ. — 2003. — Т. 299. — С. 169–192.

4. Connelly R. Rigidity and Energy // Invent. Math. — 1982. — V. 66, № 1. — P. 11–33.

СВОЙСТВА КЛАССОВ АФФИННОЙ ЭКВИВАЛЕНТНОСТИ ГЕОМЕТРИЧЕСКИХ ОБРАЗОВ АВТОНОМНЫХ АВТОМАТОВ

Д. О. Матов (Саратов)

Пусть $A = (S, X, Y, \delta, \lambda)$ — синхронный КДА типа Мили. Пусть $|X| = n$, $|Y| = m$. С инициальным автоматом (A, s) связано автоматное отображение $\Lambda_A^s : X^* \to Y^*$. Геометрическое пространство Γ для автомата (A, s) определяется по следующему алгоритму [1]:

1) Осуществим взаимно однозначное отображение $f : X \to \{1, 2, \ldots, n\}$.

2) Определим ось абсцисс $\tilde{X}$ пространства Γ как отрезок $[0, n+1]$.

3) Каждому слову $p = x_{i_1} \ldots x_{i_k}$ сопоставим точку $\tilde{x} \in Q$ на оси абсцисс:

$$\tilde{x} = \frac{f(x_{i_1})}{(n+1)^0} + \frac{f(x_{i_2})}{(n+1)^1} + \ldots + \frac{f(x_{i_k})}{(n+1)^{k-1}}.$$

Аналогично определяется взаимно однозначное соответствие g элементов множества Y и чисел от 1 до m, ось ординат $\tilde{Y}$ пространства Γ и отображение слов из Y^* во множество рациональных чисел. Каждой паре $(p, q) \in \Lambda_A^s$ в пространстве Γ сопоставляется точка с координатами $(\tilde{x}, \tilde{y})$, где

$$\tilde{x} = \sum_{j=1}^{k} \frac{f(x_{i_j})}{(n+1)^{j-1}}, p = x_{i_1} \ldots x_{i_k},$$

$$\tilde{y} = \sum_{j=1}^{k} \frac{g(y_{i_j})}{(m+1)^{j-1}}, q = y_{i_1} \ldots y_{i_k}.$$

Множество таких пар $(\tilde{x}, \tilde{y})$ понимается под *геометрическим образом* Ω_A^s автомата (A, s).

Два геометрических образа называются *аффинно-эквивалентными*, если множество точек одного образа может быть преобразовано в множество точек другого образа некоторым поточечным аффинным преобразованием.

Класс инициальных автономных автоматов, у которых $|S| = N$ и $|Y| = M$ будем обозначать $K(N, M)$. Также будем рассматривать класс $K(*, M) = \bigcup K(N, M), N = 1, 2, \ldots, \infty$, т. е. все автономные автоматы с заданной мощностью выходного алфавита.

Обозначим через $\Omega(*, M)$ множество геометрических образов автоматов из $K(*, M)$. Будем рассматривать те аффинные преобразования образов, путем применения которых можно некоторый образ $\Omega_i \in \Omega(*, M)$ преобразовать в другой образ $\Omega_j \in \Omega(*, M)$. В данной статье рассматривается подкласс преобразований следующего вида:

$$\tilde{x}' = \tilde{x}, \tilde{y}' = a\tilde{y} + b$$

(здесь $\tilde{x}, \tilde{y}$ — координаты исходной точки, $\tilde{x}', \tilde{y}'$ — преобразованной точки).

Будем говорить, что образы Ω_i, Ω_j *совместимы* выбранным видом аффинного преобразования, если при его применении ко всем точка из Ω_i получается Ω_j.

Бинарное отношение $\rho \subset \Omega^2$, образованное парами совместимых образов, является отношением эквивалентности на множестве $\Omega(*, M)$ и задает разбиение этого множества на классы эквивалентности.

В работах [3] и [4] изучались свойства описанных преобразований геометрических образов. В данной статье рассматриваются классы эквивалентности геометрических образов автономных автоматов.

Следующая лемма переносит соотношение между координатами точек образов на соотношение между выходными реакциями.

Лемма 1. *Пусть A, B — пара сравнимых автоматов, геометрические образы $\Omega(A)$ и $\Omega(B)$ которых совместимы. Пусть реакции этих автоматов на произвольное слово $p \in X^*$ имеют вид $q_A = y_{i_1} y_{i_2} \ldots y_{i_k}$ и $q_B = y_{j_1} y_{j_2} \ldots y_{j_k}$. Тогда, если пара (a, b) задает коэффициенты преобразования для совмещения $\Omega(A)$ и $\Omega(B)$, то номера символов выходного алфавита, составляющих q_A и q_B, связаны соотношением:*

$$g(y_{i_1}) = a \cdot g(y_{j_1}) + b,$$

$$g(y_{i_t}) = a \cdot g(y_{j_t}), \quad 2 \leq t \leq k,$$

где $g(y)$ означает номер символа y в выходном алфавите.

Поведение инициального автономного автомата A можно задать в виде его реакции на входное слово бесконечной длины. Обозначим эту реакцию через $w(A)$. Очевидна следующая лемма:

Лемма 2. *Последовательность $w(A)$ является периодической, начиная с некоторой позиции, поэтому может быть представлена в виде $w(A) = p(t)$, где $p, t \in Y^*$ — это предпериод и период, соответственно.*

Рассматриваемое преобразование сохраняет длины периодов:

Теорема 1. *Если $\Omega(A)$ и $\Omega(B)$ совместимы, то длины периодов $w(A)$ и $w(B)$ равны.*

По заданному автомату $A \in K(*, M)$, используя представление его поведения из леммы 2 и опираясь на лемму 1, можно определить все геометрические образы, которые находятся с $\Omega(A)$ в одном классе эквивалентности. При этом сложность этого алгоритма полиномиально зависит от количества состояний автомата и мощности выходного алфавита. Кроме того, справедливы следующие теоремы.

Теорема 2. *Мощность каждого класса эквивалентности образов кратна M.*

Теорема 3. *Мощность каждого класса эквивалентности не превосходит M^2, причем для любого такого M, что $lM \geq 1$, существует класс, состоящий из M^2 образов.*

Список литературы

1. Тяпаев Л. Б. Решение некоторых задач для конечных автоматов на основе анализа их поведения // Изв. Сарат. ун-та. Сер. Математика. Механика. Информатика. — 2006. — Т. 6, вып. 2. — С. 121–133.

2. Тяпаев Л. Б., Матов Д. О. Базисы геометрических образов для динамических систем, определяемых некоторыми классами автоматов // Компьютерные науки и информационные технологии. Материалы Междунар. науч. конф. — Саратов, 2009. — С. 201–204.

3. Матов Д. О. Классы аффинной эквивалентности геометрических образов автономных автоматов // Компьютерные науки и информационные технологии. Материалы науч. конф. — Саратов, 2010. — С. 103–108.

4. Матов Д. О. Аффинные преобразования геометрических образов конечных автоматов // Проблемы теоретической кибернетики. Материалы Междунар. науч. конф. — Нижний Новгород, 2011. — С. 303–306.

СУБОТНОШЕНИЕ ШТЕЙНЕРА СТЕПЕНИ 4 ЕВКИДОВОЙ ПЛОСКОСТИ

Е. И. Степанова (Москва)

Широко известна *проблема Штейнера*: для данного набора точек M в метрическом пространстве найти набор кривых минимальной суммарной длины, соединяющих все эти точки. Решением этой проблемы является граф-дерево, множество вершин которого включает данный набор точек и, возможно, какие-то другие точки метрического пространства. Оно называется *минимальным деревом Штейнера*, и его длина обозначается $smt(M)$. Проблема Штейнера в случае евклидовой плоскости NP-полна, поэтому имеет смысл рассматривать ее связь с другими задачами и оценивать связанные с ней величины.

Если мы запретим использовать в дереве-решении дополнительные точки, отличные от тех, которые требуется соединить, то получим *минимальное остовное дерево*.

Связь между описанными выше величинами можно оценить с помощью отношения длины минимального дерева Штейнера к длине минимального остовного дерева. Оно называется *отношением Штейнера* для данного набора точек. Если рассмотреть инфимум отношения Штейнера по всем наборам точек в данном метрическом пространстве, то получим отношение Штейнера этого метрического пространства. Известно, что для евклидовой плоскости оно не больше $\sqrt{3}/2$ [1, 3]. В 1968 году Гильберт и Поллак выдвинули гипотезу, что для евклидовой плоскости оно в точности равно $\sqrt{3}/2$, однако это утверждение до сих пор не доказано.

Задача о минимальном заполнении конечного метрического пространства впервые была поставлена Ивановым и Тужилиным в [2]. Задача состоит в поиске взвешенного графа наименьшего веса, затягивающего данное конечное метрическое пространство M так, что для любых двух точек метрического пространства вес любого пути, соединяющего их в графе, не меньше расстояния между ними в метрическом пространстве. Вес минимального заполнения будем обозначать через $mf(M)$.

Минимальное дерево Штейнера и минимальное заполнение связаны величиной, которая называется *суботношением Штейнера*. Оно равно отношению веса минимального заполнения к длине минимального дерева Штейнера.

Точная нижняя грань суботношения Штейнера по всем наборам точек в данном метрическом пространстве $\mathbb{X}$, число точек в которых не превосходит n, называется *n-точечным суботношением Штей-*

нера, или *суботношением Штейнера степени* n данного метрического пространства. Оно обозначается $ssr_n(\mathbb{X})$. Инфимум суботношения Штейнера по всем наборам точек называется *суботношением Штейнера* и обозначается $ssr(\mathbb{X})$.

В случаях минимального дерева Штейнера и минимального заполнения множество точек метрического пространства, которое требуется соединить, называется *граничным множеством*. Остальные точки этих деревьев называются *внутреннними*.

Отметим теперь некоторые факты, касающиеся введенных выше понятий в случае евклидовой плоскости $\mathbb{R}^2$ [1, 2, 3, 4].

Утверждение 1. *Для конечного набора точек на евклидовой плоскости всегда существуют минимальное дерево Штейнера и минимальное заполнение.*

Утверждение 2. *Все ребра минимального дерева Штейнера в* $\mathbb{R}^2$ *являются отрезками. В каждой вершине ребра-отрезки сходятся под углом не менее* $2\pi/3$.

Каждая вершина минимального дерева Штейнера имеет степень не больше трех, при этом все внутренние вершины имеют степень 3.

Тип дерева минимального заполнения определен неоднозначно. Однако верно следующее утверждение.

Утверждение 3. *Минимальное заполнение можно считать бинарным деревом, у которого все граничные вершины имеют степень* 1, *а все внутренние вершины имеют степень* 3.

Рассмотрим теперь подмножество метрического пространства, число точек в котором не превосходит n, обозначим его M_n. Пусть p_i, где $i = 1, 2, \ldots, n$, — элементы M_n, ρ_{ij} — расстояние между точками p_i и p_j.

Утверждение 4. *Вес минимального заполнения трех точек в любом метрическом пространстве можно вычислить по следующей формуле*:

$$mf(M_3) = \frac{\rho_{12} + \rho_{23} + \rho_{31}}{2}.$$

Утверждение 5. *Вес минимального заполнения четырех точек в любом метрическом пространстве можно вычислить по следующей формуле:*

$$mf(M_4) = \frac{1}{2}\big(\min\{\rho_{12} + \rho_{34}, \rho_{13} + \rho_{24}, \rho_{14} + \rho_{23}\} +$$

$$\max\{\rho_{12} + \rho_{34}, \rho_{13} + \rho_{24}, \rho_{14} + \rho_{23}\}\big).$$

Ивановым и Тужилиным в [2] было показано, что для любых трех точек на евклидовой плоскости суботношение Штейнера не меньше, чем $\sqrt{3}/2$, причем это число достигается, и только на правильных треугольниках. Основным результатом автора является следующая теорема.

Теорема. *Суботношение Штейнера для четырех точек на евклидовой плоскости равно* $\sqrt{3}/2$*, причем отношение веса минимального заполнения к длине минимального дерева Штейнера равно этому числу только для равнобоких трапеций, у которых основания видны из точки пересечения диагоналей под углом* $\pi/3$*.*

Автор благодарит А. О. Иванова, А. А. Тужилина за постоянное внимание к работе, а также всех участников семинара «Минимальные сети», проходящего на механико-математическом факультете МГУ, за проявленный интерес, многочисленные полезные обсуждения и дискуссии.

Работа была выполнена при частичной поддержке РФФИ (проект №10-01-00748-а), гранта президента РФ поддержки ведущих научных школ (проект НШ-3224.2010.1), Программы Развитие научного потенциала высшей школы (проект РНП 2.1.1.3704) и ФЦП Научные и научно-педагогические кадры инновационной России на 2009-2013 годы (номера Госконтрактов: 14.740.11.0794 и 02.740.11.5213).

Список литературы

1. Иванов А. О., Тужилин А. А. Теория экстремальных сетей. — Мо., Ижевск: Институт компьютерных исследований, 2003.

2. Иванов А. О., Тужилин А. А. Одномерная проблема Громова о минимальном заполнении // Матем. Сборник. — В печати.

3. Cieslik D. The Steiner ratio of metric spaces. A Report. — Preprintreihe Mathematik, 2010.

4. Ivanov A. O., Tuzhilin A. A. One-dimensional Gromov minimal filling // `arXiv:1101.0106v2 [math.MG] (http://arxiv.org)`

О СИММЕТРИЧНЫХ МНОГОГРАННИКАХ С НЕСИММЕТРИЧНЫМИ ГРАНЯМИ

В. И. Субботин (Новочеркасск)

В работе рассматриваются некоторые свойства симметричных замкнутых выпуклых многогранников в трёхмерном евклидовом пространстве.

Замкнутый выпуклый многогранник в трёхмерном евклидовом пространстве называется симметричным, если он имеет хотя бы одну нетривиальную ось симметрии. Будем говорить, что ось симметрии замкнутого выпуклого многогранника в трёхмерном евклидовом пространстве *проходит через грань* многогранника, если она перпендикулярна этой грани и пересекает относительную внутренность этой грани. *Звездой грани* A многогранника называется совокупность граней, имеющих с гранью A хотя бы одну общую вершину. *Центром* симметричного многогранника называется точка пересечения его осей симметрии.

Ранее [1] были перечислены все многогранники, *сильно симметричные относительно вращения граней*, а также метрически двойственные им сильно симметричные относительно вращения многогранных углов. В частности, среди перечисленных в [1] многогранников имеются восемь многогранников, не являющихся даже комбинаторно эквивалентными правильным или архимедовым (полуправильным) многогранникам. Напомним, что замкнутый выпуклый многогранник называется сильно симметричным относительно вращения граней, если каждая грань многогранника, рассматриваемая как фигура, отделённая от многогранника, имеет ось симметрии L, проходящую через неё, и ось L является осью симметрии всего многогранника. При этом порядок оси L многогранника может быть меньше порядка оси L грани.

Грань, через которую проходит ось симметрии многогранника будем называть симметричной; в противном случае — несимметричной. Несимметричную грань F многогранника будем называть *изолированной*, если все грани, входящие в звезду F, симметричны. Если в многограннике каждая несимметричная грань изолирована, то будем говорить, что замкнутый выпуклый многогранник в трёхмерном евклидовом пространстве является *многогранником с изолированными несимметричными гранями* (многогранники 1-го класса). *Поясом* несимметричных граней будем называть последовательность несимметричных граней, каждая из которых имеет с предыдущей и с последующей гранью только по одному общему ребру; последняя грань пояса также имеет только одно общее ребро

с первой гранью. Будем рассматривать многогранники, каждая несимметричная грань которых входит в один и только в один пояс, и для каждого пояса P существует симметричная грань G такая, что каждая грань пояса P имеет только одно общее ребро с G, и каждое ребро грани G является ребром некоторой грани пояса P (многогранники 2-го класса — *с изолированными несимметричными поясами*). Из этого определения следует, что звезда каждой несимметричной грани, помимо симметричных граней, содержит только две несимметричных грани: предыдущую и последующую грань пояса.

На основе метода доказательства перечисления многогранников, сильно симметричных относительно вращения граней, в ранее анонсировано перечисление всех многогранников с изолированными несимметричными гранями. Ниже даны наброски доказательств теорем о перечислении многогранников с изолированными несимметричными гранями и о перечислении многогранников с изолированными несимметричными поясами. Как следствие указано точное максимальное число граней многогранника в каждом из этих двух классов.

Теорема 1. *Каждый многогранник с изолированными несимметричными гранями может быть получен путём усечения вершин или рёбер из некоторого многогранника, сильно симметричного относительно вращения граней.*

Доказательство. Пусть M — многогранник с изолированными несимметричными гранями. Рассмотрим многогранник P, сильно симметричный относительно вращения, у которого количество осей симметрии и их направления совпадают с направлением осей симметрии многогранника M. Многогранник P является пересечением полупространств, ограниченных плоскостями, перпендикулярными осям симметрии многогранника M. Многогранник P можно попытаться получить из многогранника M следующим образом. Параллельный сдвиг плоскостей эквивалентных несимметричных граней от центра многогранника M на одно и то же расстояние сохраняет симметричность симметричных граней многогранника M. Осуществляя таким образом параллельные сдвиги плоскостей несимметричных граней, мы добьёмся того, что полупространства, определяемые плоскостями граней многогранника M, образуют многогранник S с симметричными гранями. Многогранник S является сильно симметричным и, вообще говоря, отличным от многогранника P, потому что порядки осей симметрии многогранников P и S при этом не обязательно совпадают. Для завершения доказательства теоремы достаточно взять многогранник S и системой плоскостей, соответствующей несимметричным граням многогранника M, про-

звести отсечение вершин или рёбер многогранника S. Теорема 1 доказана.

Теорема 2. *Каждый многогранник с изолированными несимметричными поясами может быть получен: либо путём надстраивания усечённых осесимметричных пирамид на гранях некоторого многогранника, сильно симметричного относительно вращения граней; либо путём отсечения вершин и рёбер некоторых граней многогранника, сильно симметричного относительно вращения.*

Доказательство. Доказательство аналогично доказательству предыдущей теоремы. Рассмотрим многогранник M, с изолированными несимметричными поясами. Пусть G — грань многогранника M, окружённая поясом несимметричных граней. Сдвигая параллельно в направлении центра многогранника M плоскость грани G, а также плоскости всех граней, ей эквивалентных, на одно и то же расстояние, получим многогранник S, сильно симметричный относительно вращения. Теперь достаточно взять сильно симметричный многогранник S и построить на грани с осью симметрии грани G пирамиду. Затем плоскостью, перпендикулярной указанной оси, отсечь вершину пирамиды оставляя многогранник выпуклым. Осуществляя это построение для каждой эквивалентной грани, получим многогранник M с изолированными несимметричными поясами. Если указанный параллельный сдвиг плоскости грани G не приводит к многограннику, сильно симметричному относительно вращения, то плоскости граней пояса, окружающего грань G, либо саму грань G, параллельно сдвигаем в направлении от центра многогранника M на одно и то же расстояние для эквивалентных граней. Доказательство завершается так же, как и в случае многогранника с изолированными несимметричными гранями. Теорема 2 доказана.

Заметим, что из доказанных теорем очевидно следует, что число комбинаторных типов как многогранников с изолированными несимметричными гранями так и с изолированными несимметричными поясами, ограничено, если не учитывать бесконечные серии усечённых призм, антипризм, пирамид, усечённых пирамид и бипирамид. Например, максимальное число граней многогранника с изолированными несимметричными поясами равно 302; максимальное число граней многогранника с изолированными несимметричными гранями равно 182.

Список литературы

1. Субботин В. И. Перечисление многогранников, сильно симметричных относительно вращения // Труды участников международной школы-семинара по геометрии и анализу памяти Н. В. Ефимова (Абрау-Дюрсо, 5–11 сент. 2002 г.) — Ростов-на-Дону, 2002. — С. 77–78.

НЕПАРАМЕТРИЧЕСКИЕ ОЦЕНКИ ЭНТРОПИИ И РАССТОЯНИЯ МЕЖДУ СТРОКАМИ

Е. А. Тимофеев (Ярославль)

В настоящей статье рассматривается задача выбора метрики для повышения эффективности непараметрической оценки энтропии, основанном на методе ближайшей точки.

Пусть $\Omega = A^{\mathbf{N}}$ — пространство правосторонних последовательностей (A — конечный алфавит, $\mathbf{N} = \{1, 2, \dots\}$). Пусть даны $n+1$ независимых случайных величин $\xi_{\mathbf{0}}, \dots, \xi_{\mathbf{n}}$, принимающих значения в Ω и одинаково распределенных по мере μ. Будем считать, что μ – эргодическая стационарная (инвариантная относительно сдвига) вероятностная мера.

Требуется оценить энтропию меры μ. Напомним, что *энтропия* (энтропия на символ) определяется как

$$h = -\lim_{n\to\infty} \frac{1}{n} \mathbf{E} \ln \mu(C_n(\xi)), \tag{1}$$

где $C_n(\mathbf{x}) = \{\mathbf{y} \in \Omega : y_1 = x_1, \dots, y_n = x_n)\}$.

В [1] предложены и исследованы статистики для нахождения размерностей мер в метрических пространствах. Для пространства последовательностей Ω с метрикой ρ эти статистики определяются следующим образом:

$$\eta_n^{(k)}(\rho) = k \left(r_n^{(k)}(\rho) - r_n^{(k+1)}(\rho) \right), \tag{2}$$

$$r_n^{(k)}(\rho) = -\frac{1}{(n+1)} \sum_{j=0}^{n} \ln \left(\min_{i:i\neq j}{}^{(k)} \rho(\xi_{\mathbf{i}}, \xi_{\mathbf{j}}) \right), \tag{3}$$

где $\min^{(k)}\{X_1, \dots, X_N\} = X_k$, если $X_1 \le X_2 \le \dots \le X_N$.

Отметим, что для упрощения формулировок, случайные величины $\xi_{\mathbf{0}}, \dots, \xi_{\mathbf{n}}$ считаются бесконечными последовательностями. Нетрудно показать, что достаточно использовать только $m = O(\ln n)$ первых символов этих последовательностей, если мера удовлетворяет следующему условию

$$\exists \alpha > 0 \quad : \quad \mu(C_n(\mathbf{x})) = O(e^{-n\alpha}), \text{ для } \mu - \text{почти всех } \mathbf{x} \in \Omega. \tag{4}$$

Подчеркнем, что для упрощения теоретического исследования оценок такого вида более удобно рассматривать только оценки величины $1/h$ — обратной к энтропии.

Большинство непараметрических оценок обратной энтропии основано либо на алгоритме сжатия Лемпеля-Зива, либо на методе ближайших соседей (см. обзор в [1]), и эти оценки имеют вид, например, $r_n^{(k)}(\rho)/\ln n$. Для таких оценок доказывается сходимость почти всюду, но такие оценки очень трудно применять в прикладных задачах, поскольку $\log_2 n \leq 30-40$, а скорость сходимости таких оценок $O(1/\log n)$.

Для оценки обратной энтропии (2) сходимость доказывается при трудно проверяемых условиях [1], но скорость сходимости получается степенной — $O(n^{-c})$, где c — некоторая константа. В [2] была проведена вычислительная проверка оценки (2) для нескольких одномерных динамических систем с известной энтропией. Проверка показала, что эта оценка имеет точность 0.01 для $n = 10^4$. В экспериментах применялась метрика ρ_0, основанная на первом несовпадении символов строк (метрика (5) с $\lambda(t) = 0$).

Однако теоретические исследования показали, что эта проблема имеет очень сложную природу. В работе [3] для марковской меры и метрики ρ_0 показано, что смещение является периодической функцией с периодом пропорциональным $\log n$ для тех мер, у которых логарифмы вероятностей перехода соизмеримы. Для остальных марковских мер оценка является асимптотически несмещенной. Таким образом, смещение является разрывной функцией от параметров марковской меры.

Хорошее согласование результатов эксперимента в [2] с теоретическими значениями энтропии объясняется тем, что для небольших значений энтропии ($h < 3$) это смещение настолько мало, что его нельзя заметить в вычислительном эксперименте. Так, например, для $A = \{0, 1\}$ амплитуда смещения меньше, чем 10^{-6}.

В настоящей работе для уменьшения смещения предлагается следующий подход. Расширим класс используемых в оценке метрик и добавим некоторую оптимизацию по метрикам этого класса.

Для точек $\mathbf{x} = (x_1, x_2, \dots)$ и $\mathbf{y} = (y_1, y_2, \dots)$ из Ω определим метрику

$$\rho(a\mathbf{x}, b\mathbf{y}) = \begin{cases} e^{-1}\rho(\mathbf{x}, \mathbf{y}), & a = b; \\ e^{-\lambda(-\log \rho(\mathbf{x}, \mathbf{y}))}, & a \neq b; \end{cases} \tag{5}$$

где $\lambda(t)$ — неубывающая функция, такая, что $\lambda(0) = 0$ и $\lambda(t) \leq 1$, $0 \leq t < \infty$.

Эта метрика билипшицево эквивалентна метрике ρ_0 (метрика (5) с $\lambda(t) = 0$). Поэтому статистика (2) является оценкой обратной энтропии.

Утверждение. *Для $k = O(n^c)$, где $c < 1$,*

$$\lim_{n\to\infty} \frac{\mathbf{E} r_n^{(k)}(\rho)}{\ln n} = \frac{1}{h}.$$

Обозначим через $r_n^{(k,m)}$ статистику (3), в которой на m-м шаге нахождения метрики (5) считаем все расстояния равными 1 (т. е. используются только первые m символов заданных строк).

Теорема 1. *Для статистики $r_n^{(k,m)}$ и для любой метрики (5) справедливо*

$$\mathbf{D} r_n^{(k,m)} \le \frac{k^2 m^4}{4(n+1)}.$$

Теорема 2. *Пусть $\lambda(t) = \log_\beta(\beta + (1-\beta)\beta^t)$ и μ — симметричная мера Бернулли, тогда для $\beta = 1/|A|$*

$$\mathbf{E}\eta_n^{(k)}(\rho) = 1/\ln|A| + O(n^{-1}).$$

Работа выполнена при поддержке гранта Правительства РФ по постановлению № 220, договор 11.G34.31.0053.

Список литературы

1. Тимофеев Е. А. Статистически оцениваемые инварианты мер //Алгебра и анализ. — 2005. — Т. 17, № 3. — С. 204–236.

2. Kaltchenko A., Timofeeva N. Entropy estimators with almost sure convergence and an $O(n^{-1})$ Variance // Advances in Mathematics of Communications. — 2008. — V. 2, №1. — P. 1–13.

3. Тимофеев Е. А. Смещение непараметрической оценки энтропии для марковской меры // Записки научных семинаров ПОМИ. — 2010. — Т. 377. — С. 134–158.

Секция «Теория кодирования и математические вопросы теории защиты информации»

О СОВЕРШЕННЫХ 2-РАСКРАСКАХ ГРАФОВ ДЖОНСОНА $J(v,3)$

А. Л. Гаврилюк (Екатеринбург), С. В. Горяинов (Челябинск)

Графом Джонсона $J(v,k)$ называется граф, вершинами которого являются все k-элементные подмножества некоторого v-элементного множества; два подмножества смежны, если они имеют точно $k-1$ общих элементов. Графы $J(v,k)$ и $J(v,v-k)$ изоморфны, поэтому далее считаем, что $k \leq v/2$. Граф Джонсона является дистанционно-регулярным, см. [1], имеет диаметр k и $k+1$ различных собственных значений: $\theta_i = (k-i)(v-k-i)-i,\ i=0,\ldots,k$.

Совершенной раскраской графа Γ в t цветов (далее, для краткости t-раскраской) называется разбиение множества вершин Γ на t классов (цветов) $C_1,\ldots,C_t$ такое, что для любых $i,j \in \{1,\ldots,t\}$ любая вершина из класса C_i смежна с одним и тем же числом вершин, а именно, c_{ij}, из класса C_j. Матрица $C = (c_{ij})_{i,j=1,\ldots,t}$ называется *матрицей параметров* t-раскраски. Мы не различаем раскраски, полученные переименованием цветов.

Известно, см. [2], что собственные значения матрицы параметров совершенной раскраски являются собственными значениями графа. В частности, если C — матрица параметров совершенной 2-раскраски графа Джонсона $J(v,k)$, то она имеет два собственных значения: $\theta_0 = k(v-k)$ — валентность графа $J(v,k)$ и θ_i, $i>0$.

Изучение совершенных 2-раскрасок графов Джонсона связано с гипотезой Дельсарта о несуществовании совершенных кодов в этих графах и более общей задачей изучения полностью регулярных кодов, см. [2–4]. Из работ [3] и [4] следует описание 2-раскрасок $J(v,k)$, матрицы параметров которых имеют собственные значения θ_1 или θ_k (поэтому для графов $J(v,3)$ 2-раскраски с собственным значением θ_2 были единственным неизученным случаем). В серии работ [2, 5, 6] были описаны совершенные 2-раскраски графов Джонсона

$J(v,k)$ (при $k>2$ и $v\le 8$) и $J(v,2)$. В частности, в работе [2] был поставлен вопрос о существовании 2-раскраски графа $J(9,3)$ с матрицей параметров $\begin{pmatrix} 10 & 8 \\ 8 & 10 \end{pmatrix}$, отрицательный ответ на который дает следующая теорема [7]:

Теорема 1. *При нечетных v граф $J(v,3)$ не допускает совершенных 2-раскрасок, матрица параметров которых имеет собственное значение θ_2.*

В работе [2] для четного v описана группа автоморфизмов графа $J(v,3)$, имеющая точно три орбиты на множестве вершин графа, и показано, что объединение любых двух орбит из этих трех ведет к совершенной 2-раскраске графа (вершины объединяемых орбит красятся в один цвет, а оставшиеся — в другой). В настоящей работе доказано, что $J(v,3)$ при $v>10$ не допускает 2-раскрасок с собственным значением θ_2, отличных от описанных выше.

Теорема 2. *При четных $v>10$ множество совершенных 2-раскрасок графа $J(v,3)$, матрица параметров которых имеет собственное значение θ_2, исчерпывается следующими матрицами*

$$\begin{pmatrix} 3(2m-5) & 6 \\ 4(m-2) & 2m-1 \end{pmatrix}, \begin{pmatrix} 3(m-3) & 3m \\ m-2 & 5m-7 \end{pmatrix},$$
$$\begin{pmatrix} 3(m-1) & 3(m-2) \\ m+4 & 5m-13 \end{pmatrix},$$

и любая такая раскраска изоморфна одной из описанных в [2].

Список литературы

1. Brouwer A. E., Neumaier A., Cohen A. M. Distance-regular graphs. — Berlin, New-York, Heidelberg: Springer-Verlag, 1989.

2. Августинович С. В., Могильных И. Ю. Совершенные раскраски графов Джонсона $J(8,3)$ и $J(8,4)$ в два цвета // Дискрет. анализ и исслед. операций. — 2010. — Т. 17, № 2. — P. 3–19.

3. Meyerowitz A. D. Cycle-balanced partitions in distance-regular graphs // J. Combin. Inform. System Sci. — 1992. — V. 17. — P. 39–42.

4. Martin W. J. Completely regular designs of strength one // J. Algebr. Comb. — 1994. — V. 3. — P. 170–185.

5. Могильных И. Ю. О несуществовании некоторых совершенных 2-раскрасок графов Джонсона // Дискрет. анализ и исслед. операций. — 2009. — Т. 16, № 5. — P. 52–68.

6. Mogilnykh I. Yu., Avgustinovich S. V. Perfect 2-colorings of Johnson graphs $J(6,3)$ and $J(7,3)$ // Lect. Notes Comp. Sci. — 2008. — V. 5228. — P. 11–19.

7. Gavrilyuk A. L., Goryainov S. V. On perfect 2-colorings of Johnson graphs $J(v, 3)$ // (направлена в Journal of Combinatorial Designs).

О СОВЕРШЕННОСТИ МОДУЛЯРНЫХ СХЕМ РАЗДЕЛЕНИЯ СЕКРЕТА

Т. В. Галибус, Г. В. Матвеев (Минск)

Модулярное разделение секрета, предложенное М. Миньоттом, с самого начала обладало одним существенным недостатком. Схема Миньотта не совершенна, т. е. запрещенные группы участников обладают некоторой информацией о секрете, отличной от имеющейся априорной. Появившееся вскоре ее усовершенствование [2], предложенное С. Асмусом и Д. Блюмом, несколько улучшало положение. М. Куискуатер, Б. Пренель и Д. Вандевалле [7] показали, что схема Асмуса—Блюма с последовательными простыми модулями близка в асимптотическом смысле к совершенной и даже идеальной для пороговых структур доступа.

Мы предлагаем иной более радикальный способ улучшить качество модулярной схемы. Он является развитием нашей работы [1]. Оказывается, что модулярное разделение секрета можно изучать и в кольце многочленов от нескольких переменных и, что в этом кольце возможно построение совершенных схем для произвольных структур доступа и идеальных схем для пороговых структур.

В самом деле, в кольце многочленов от нескольких переменных над полем Галуа $F_q[x_1, x_2, .., x_n] = F_q[x]$ есть все необходимое для модулярного разделения секрета. В качестве секрета выбирается полином $s(x) \in F_q[x]$, а в качестве модуля участника — нульмерный идеал. В этом случае корректно определен вычет $s(x)(\bmod I)$, при условии, что задано мономиальное упорядочение, а для восстановления секрета имеется CRT-алгоритм [4]. Разумеется, все эти вычисления основаны на теории базисов Гребнера. При этом мы ограничиваемся лишь случаем обратного lex-упорядочения мономов.

Для построения совершенной схемы, реализующей произвольную структуру доступа нужна теорема 4 из нашей работы [1] и специально сконструированные для этой цели идеалы $I_1, I_2, ..., I_k$, обладающие свойством, названным нами *равноостаточностью*.

Нульмерные идеалы $I_1, I_2, .., I_l$ называются *равноостаточными*, если $RT(I_{i_1} I_{i_2} ... I_{i_k}) = RT(I_{j_1} I_{j_2} ... I_{j_k})$, где $1 \leq i_1 < i_2 < ... < i_k \leq l, 1 \leq j_1 < j_2 < ... < j_k \leq l, k = 1, 2, ..., n$, где $RT(I)$ — множество приведенных мономов.

Все рассматриваемые нами идеалы триангулируемы и автоматически нульмерны, а значит, приведенный базис Гребнера каждого такого идеала $\{t_1, t_2, ..., t_n\}$ имеет вид:

$$t_i = 1 \cdot x_i^{d_i} + a_{d_{i-1}} x_i^{d_i - 1} + ... + a_1 x_i + a_0, a_{d_{i-1}}, ..., a_1, a_0 \in F_q[x_1, x_2, ..., x_{i-1}].$$

Положим $D(I) = (d_1, d_2, ..., d_n)$.

Для равноостаточности существенным является еще и свойство эквипроективности аффинного многообразия. Мы не приводим здесь формальное определение. Его можно найти в работе [3].

Два нульмерных идеала I_1 и I_2 называются *сильно разделенными*, если их нули удовлетворяют условию: $(\alpha_1, \alpha_2, ..., \alpha_n) \in V(I_1), (\beta_1, \beta_2, ..., \beta_n) \in V(I_2) \Rightarrow \alpha_i \neq \beta_j, 1 \leq i, j \leq n$.

Теорема 1. *Пусть триангулируемые идеалы $I_1, I_2, ..., I_k$ попарно сильно разделены, выполнено условие $D(I_1) = D(I_2) = ... = D(I_k)$, а многообразия $V(I_1), V(I_2), ..., V(I_k)$ — эквипроективны. Тогда идеалы $I_1, I_2, ..., I_k$ равноостаточны.*

Нам удалось показать, что к числу равноостаточных идеалов относятся и идеалы симметрических отношений, введенные Обри и Валибузом [3].

Пусть f — сепарабельный полином степени n в кольце $\mathbb{F}_q[x]$. Пусть $\Omega = (\alpha_1, \alpha_2, ..., \alpha_n)$, где $\alpha_1, \alpha_2, ..., \alpha_n$ — корни полинома f в алгебраическом замыкании $\overline{F_q}$. Обозначим через S_n симметрическую группу, и определим ее действие на Ω следующим образом:

$$\forall \sigma \in S_n \quad \sigma.\Omega = (\alpha_{\sigma(1)}, \alpha_{\sigma(2)}, ..., \alpha_{\sigma(n)}).$$

Идеалом симметрических отношений многочлена f называется идеал, аннулирующий любую подстановку $\sigma.\Omega$ корней f:

$$I = \{p(X) | p(\alpha_{\sigma(1)}, \alpha_{\sigma(2)}, ..., \alpha_{\sigma(n)}) = 0, \forall \sigma \in S_n.$$

Теорема 2. *Идеалы $I_1, I_2, ..., I_k$ симметрических отношений, соответствующие попарно взаимно простым сепарабельным многочленам $g_1, g_2, ..., g_k, \deg g_i = n, i = 1, 2, ..., k$ являются равноостаточными.*

Отметим, что множества приведенных мономов произведений равноостаточных идеалов симметрических отношений равно как и

максимальных равноостаточных идеалов представляют собой дискретные n-мерные прямоугольники:

$$\{0,1,...,kd_1-1\}\times\{0,1,...,d_2-1\}\times...\times\{0,1,...,d_n-1\}.$$

Теорема 3. *Используя равноостаточные идеалы симметрических отношений можно построить совершенную модулярную схему разделения секрета для произвольной структуры доступа и идеальную схему для пороговой структуры доступа в кольце полиномов от нескольких переменных над полем Галуа.*

Случай кольца полиномов от одной переменной был рассмотрен нами ранее [5, 6].

Список литературы

1. Галибус Т. В., Матвеев Г. В. Комбинаторика нульмерных идеалов и модулярное разделение секрета // Материалы IX Международного семинара "Дискретная математика и ее приложения", посвященного 75-летию со дня рождения академика О. Б. Лупанова (18–23 июня 2007 г.). — М.: Изд-во механико-математического факультета МГУ, 2007. — С. 424–426.

2. Asmuth C. A., Bloom J. A modular approach to key safeguarding // IEEE Transactions on Information Theory. — 1983. — V. 29. — P. 156–169.

3. Aubry P., Valibouze A. Using Galois ideals for computing relative resolvents // J. Symbolic Computation. — 2000. — V. 30. — P. 635–651.

4. Becker T., Weispfenning V. Gröbner Bases, A Computational Approach to Commutative Algebra. — Berlin, Heidelberg, New-York: Springer-Verlag, 1993.

5. Galibus T., Matveev G. Generalized Mignotte sequences in polynomial rings // Electronic Notes on Theoretical Computer Science. — 2007. — V. 186. — P. 39–45.

6. Galibus T., Matveev G., Shenets N. Some structural and security properties of the modular secret sharing // SYNASC'08. — California: IEEE Comp. Soc. CPC, 2009. — P. 197–200.

7. Quisquater M., Prenel B., Wandevalle J. On the security of the threshold scheme based on the Chinese remainder theorem // Lecture Notes in Computer Science. — 2002. — V. 2274. — P. 199–210.

ОБ ЭНТРОПИИ МНОЖЕСТВА ДЕРЕВЬЕВ ВЫВОДА В РАЗЛОЖИМОЙ СТОХАСТИЧЕСКОЙ КС-ГРАММАТИКЕ, ИМЕЮЩЕЙ ВИД «ЦЕПОЧКИ»

Л. П. Жильцова, И. М. Мартынов (Нижний Новгород)

Рассматривается множество деревьев вывода высоты t для слов языка, порождаемого разложимой стохастической контекстно-свободной грамматикой, причем классы нетерминальных символов грамматики линейно упорядочены отношением следования. В работе исследуется зависимость энтропии рассматриваемого множества деревьев от t при $t \to \infty$.

Стохастической КС-грамматикой называется система $G = \langle V_T, V_N, R, s\rangle$, где V_T и V_N — конечные алфавиты терминальных и нетерминальных символов (терминалов и нетерминалов) соответственно, $s \in V_N$ — аксиома, $R = \cup_{i=1}^{k} R_i$, где k — мощность алфавита V_N и R_i — множество правил с одинаковой левой частью A_i. Каждое правило r_{ij} из R_i имеет вид

$$r_{ij} : A_i \overset{p_{ij}}{\to} \beta_{ij},\ j = 1, ..., n_i,$$

где $A_i \in V_N$, $\beta_{ij} \in (V_T \cup V_N)^*$ и p_{ij} — вероятность применения правила r_{ij}, причем $0 < p_{ij} \leq 1$ и $\sum_{j=1}^{n_i} p_{ij} = 1$.

Каждому слову α КС-языка соответствует последовательность правил грамматики (вывод), с помощью которой α выводится из аксиомы s. Выводу слова соответствует дерево вывода [1], вероятность которого определяется как произведение вероятностей правил, образующих вывод.

По стохастической КС-грамматике строится матрица A первых моментов. Для нее элемент a_j^i определяется как $\sum_{l=1}^{n_i} p_{il} s_{il}^j$, где величина s_{il}^j равна числу нетерминальных символов A_j в правой части правила r_{il}. Перронов корень матрицы A обозначим через r.

Будем применять обозначение $A_i \to A_j$, если в грамматике существует правило вида $A_i \overset{p_{ij}}{\to} \alpha_1 A_j \alpha_2$, где $\alpha_1, \alpha_2 \in (V_T \cup V_N)^*$. Рефлексивное транзитивное замыкание отношения $\to$ обозначим $\to_*$.

Классом нетерминалов назовем максимальное по включению подмножество $K \subseteq V_N$ такое, что $A_i \to_* A_j$ для любых $A_i, A_j \in K$. Для различных классов нетерминалов K_1 и K_2 будем говорить, что класс K_2 непосредственно следует за классом K_1 (и обозначать $K_1 \prec K_2$), если существуют $A_1 \in K_1$ и $A_2 \in K_2$, такие, что $A_1 \to A_2$. Рефлексивное транзитивное замыкание отношения $\prec$ обозначим через $\prec_*$.

Пусть $\mathcal{K} = \{K_1, K_2, \ldots, K_m\}$ — множество классов нетерминалов грамматики, $m \geq 2$. Перенумеруем классы таким образом, что $K_i \prec_* K_j$ при $i \neq j$ тогда и только тогда, когда $i < j$.

Будем говорить, что грамматика имеет вид «цепочки», если классы нетерминалов образуют линейный порядок по отношению $\prec$:

$$K_1 \prec K_2 \prec \ldots \prec K_i \prec \ldots \prec K_m.$$

Матрица первых моментов A такой грамматики имеет вид

$$A = \begin{pmatrix} A_{11} & A_{12} & 0 & \cdots & 0 & 0 \\ 0 & A_{22} & A_{23} & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & A_{m-1,m-1} & A_{m-1,m} \\ 0 & 0 & 0 & \cdots & 0 & A_{m,m} \end{pmatrix}.$$

Один класс нетерминалов представлен в матрице множеством подряд идущих строк и соответствующим множеством столбцов с теми же номерами. Для класса K_i квадратная подматрица, образованная соответствующими строками и столбцами, обозначается через A_{ii}. Подматрица A_{ij} является нулевой, если $K_i \not\prec K_j$.

Для каждого класса K_i матрица A_{ii} неразложима. Без ограничения общности можно считать, что она строго положительна и непериодична. Обозначим через r_i перронов корень матрицы A_{ii}. Для неразложимой матрицы перронов корень является вещественным и простым [2]. Очевидно, $r = \max_i\{r_i\}$. Рассматриваются согласованные грамматики, для которых вероятности p_{ij} правил индуцируют распределение вероятностей на множестве всех деревьев вывода слов КС-языка. Необходимым и достаточным условием согласованности является неравенство $r \leq 1$.

Обозначим через J множество классов, для которых $r_i = r$.

Пусть D^t — множество всех деревьев вывода высоты t для слов, порождаемых стохастической КС-грамматикой.

Для $d \in D^t$ через $p_t(d)$ обозначим условную вероятность дерева d, т.е. $p_t(d) = \frac{p(d)}{P(D^t)}$.

Под энтропией множества деревьев D^t будем понимать величину

$$H(D^t) = -\sum_{d \in D^t} p_t(d) \log p_t(d).$$

Теорема 1. *Пусть G — стохастическая КС-грамматика, име-*

ющая вид «цепочки». Тогда при $r < 1$

$$H(D^t) \sim t \cdot \left(\log r - \sum_{i=1}^{k} \sum_{j=1}^{n_i} w_{ij} \log p_{ij} \right),$$

где w_{ij} *— константы, определяемые грамматикой;*

$w_{ij} > 0$ *для любого нетерминала* $A_i \in K_{h_i}$, *где* $K_{h_i} \in J$,

$w_{ij} \geq 0$ *в остальных случаях.*

Теорема 2. *Пусть* G *— стохастическая КС-грамматика, имеющая вид «цепочки». Тогда при* $r = 1$

$$H(D^t) \sim t^2 \cdot \sum_{A_i \in K_{h_i}, K_l \prec_* K_{h_i}} d_i \sum_{j=1}^{n_i} p_{ij} \log p_{ij},$$

где K_l *— последний класс из* J *в цепочке классов.*

Таким образом, для грамматики, имеющей вид «цепочки», сохраняется такой же вид зависимости энтропии от t, как и в случае неразложимой грамматики [3, 4].

Список литературы

1. Ахо А., Ульман Дж. Теория синтаксического анализа, перевода и компиляции. Том 1. — М.: Мир, 1978.

2. Гантмахер Ф. Р. Теория матриц. — М.: Наука, 1967.

3. Жильцова Л. П. О нижней оценке стоимости кодирования и асимптотически оптимальном кодировании стохастических контекстно-свободных языков // Дискретный анализ и исследование операций. Серия 1. — 2001.— Т. 8, № 3. — С. 26–45.

4. Жильцова Л. П. Закономерности в деревьях вывода слов стохастического контекстно-свободного языка и нижняя оценка стоимости кодирования. Критический случай // Дискретный анализ и исследование операций. — Серия 1. — 2003.— Т. 10, № 3. — С. 23–53.

ПОСТРОЕНИЕ ТРАНЗИТИВНЫХ МДР-КОДОВ НА ОСНОВЕ ДИЭДРАЛЬНОЙ ГРУППЫ

Д. С. Кротов, В. Н. Потапов (Новосибирск)

Пусть $Q_q = \{0, \dots, q-1\}$. Множество Q_q^n с определённым на нём расстоянием Хэмминга называется *q-значным n-мерным кубом* (*гиперкубом*). *Изотопией* гиперкуба называется преобразование $\overline{x} \mapsto \overline{\tau x}$, где $\overline{x} = (x_1, \dots, x_n) \in Q_q^n$, $\overline{\tau x} = (\tau_1 x_1, \dots, \tau_n x_n)$, $\tau_i \in S_q$ — перестановки на множестве Q_q, $i \in \{1, \dots, n\}$. *Парастрофией* гиперкуба называется преобразование $\overline{x} \mapsto \overline{x}_\varepsilon$, где $\overline{x}_\varepsilon = (x_{\varepsilon 1}, \dots, x_{\varepsilon n})$, $\varepsilon \in S_n$ — перестановка координат. Введём обозначения $A_\varepsilon = \{\overline{x}_\varepsilon \mid \overline{x} \in A\}$, $\overline{\tau} A = \{\overline{\tau x} \mid \overline{x} \in A\}$. Определим группу автотопий $\mathrm{Ist}(A) = \{\overline{\tau} \mid \overline{\tau} A = A\}$ и группу парастрофий $\mathrm{Prs}(A) = \{\varepsilon \mid A_\varepsilon = A\}$, переводящих множество $A \subseteq Q_q^n$ в себя. Известно, что группа изометрий гиперкуба Q_q^n представима в виде полупрямого произведения $\mathrm{Ist}(Q_q^n) \leftthreetimes \mathrm{Prs}(Q_q^n)$. Подгруппу группы изометрий гиперкуба, переводящую множество $A \subseteq Q_q^n$ в себя обозначим $\mathrm{Aut}(A)$.

Множество $A \subseteq Q_q^n$ называется *транзитивным*, если для любых двух вершин $\overline{x}, \overline{y}$ из A найдутся парастрофия $\varepsilon \in \mathrm{Prs}(Q_q^n)$ и изотопия $\overline{\tau} \in \mathrm{Ist}(Q_q^n)$ такие, что $\overline{\tau y} = \overline{x}_\varepsilon$ и $\overline{\tau} A = A_\varepsilon$, т. е. группа изометрий $\mathrm{Aut}(A)$ действует транзитивно на A. Множество $A \subseteq Q_q^n$ называется *изотопно транзитивным*, если группа $\mathrm{Ist}(A)$ действует транзитивно на A. Ясно, что одну из вершин в определении транзитивности (изотопной транзитивности) можно зафиксировать. Заметим, что при $q = 2$ понятие изотопной транзитивности совпадает с понятием аффинности множества.

Множество $M \subset Q_q^n$ называется МДР-*кодом* (с расстоянием 2) длины n, если $|M| = q^{n-1}$ и расстояние между двумя различными вершинами кода не менее 2. Функция $f : Q_q^n \to Q_q$ называется *n-арной квазигруппой порядка q*, если $f(\overline{x}) \neq f(\overline{y})$ для любых двух соседних вершин $\overline{x}, \overline{y} \in Q_q^n$ ($d(\overline{x}, \overline{y}) = 1$). Нетрудно видеть, что любой МДР-код $M \subset Q_q^{n+1}$ можно представить как график некоторой n-арной квазигруппы. Кроме того, для любых двух квазигрупп f и g множество $\{(\overline{x}, \overline{y}) \mid f(\overline{x}) = g(\overline{y})\}$ является МДР-кодом. Будем называть n-арную квазигруппу транзитивной (изотопно транзитивной), если её график (МДР-код) является транзитивным (изотопно транзитивным); n-арные квазигруппы называются *эквивалентными*, ес-

ли их графики изометричны. Ясно, что две эквивалентные n-арные квазигруппы являются транзитивными одновременно.

Нетрудно видеть, что любая группа является изотопно транзитивной 2-квазигруппой. Если $f(x,0) = f(0,x) = x$ для любого $x \in Q_q$, то 2-квазигруппа f называется *лупой*. Изотопно транзитивные лупы называются *G-лупами*. В [1] показано, что при простом q любая G-лупа является группой (циклической), в [3] аналогичный результат был получен для $q = 3p$, где $p > 3$ — простое. С другой стороны в [2] показано, что для любого непростого порядка q, за исключением случая, когда в разложении числа q на простые отсутствует 2 и кратные сомножители, имеются G-лупы порядка q неэквивалентные группам.

Рассмотрим следующие лупы порядка $2p$:

1) группа $Z_p \times Z_2$ с операцией $x_\zeta + y_\xi = (x + y \mod p)_{(\zeta\oplus\xi)}$;

2) группа D_p с операцией
$x_\zeta \circ y_\xi = ((-1)^\xi x + y \mod p)_{(\zeta\oplus\xi)}$;

3) лупа C_p с операцией $x_\zeta * y_\xi = ((-1)^\xi x + y + \zeta\xi \mod p)_{(\zeta\oplus\xi)}$.

Группа D_p называется *диэдральной*.

Обращением n-арной квазигруппы $f(x_1,\dots,x_n)$ по i-ой переменной называется n-арная квазигруппа $f^{(i)}$, определённая формулой $y = f(x_1,\dots,x_n) \Leftrightarrow x_i = f^{(i)}(x_1,\dots,x_{i-1},y,x_{i+1},\dots,x_n)$.

Утверждение 1. *a) Обращение любой группы ей изотопно. b) Обращение лупы C_p по любой из двух переменных ей изотопно.*

Пусть $G < \mathrm{Ist}(Q_q^n)$, определим $P_i(G) = \{\sigma_i \mid (\sigma_1,\dots,\sigma_n) \in G\}$.

Будем называть 2-квазигруппу f *регулярно* изотопно транзитивной, если найдётся такая транзитивно действующая подгруппа $G_f < \mathrm{Ist}(\{\overline{x} \mid x_3 = f(x_1,x_2)\})$, для которой группы перестановок $P_i(G_f)$ регулярны при $i \in \{1,2,3\}$.

Утверждение 2. *Лупа C_p является регулярной G-лупой.*

Утверждение 3. *Пусть n-арная квазигруппа f и m-арная квазигруппа h изотопно транзитивны и $P_{n+1}G_f = P_{n+1}G_h$ — регулярная подгруппа, где G_f — транзитивно действующая подгруппа группы $\mathrm{Ist}(\{\overline{x} \mid x_{n+1} = f(x_1,\dots,x_n)\})$. Тогда МДР-код $\{(\overline{x},\overline{y}) \mid f(\overline{x}) = h(\overline{y})\}$ является изотопно транзитивным.*

Если $\circ$ — групповая операция на Q_q, то n-арная квазигруппа $f(x_1,\dots,x_n) = x_1 \circ \dots \circ x_n$ называется итерированной группой. Определим рекуррентно понятие *итерирования квазигруппы* для произвольной 2-квазигруппы f. Пусть m-арная и k-арная квазигруппы $f^{(i)}(f_1(\overline{x_1}), f_2(\overline{x_2}))$ и $f^{(i)}(f_3(\overline{z_1}), f_4(\overline{z_2}))$ получены итерированием 2-

квазигруппы f, тогда $(m+k-1)$-арная квазигруппа g является итерированием f, если и только если она представима как график МДР-кода $\{(\overline{x_1},\overline{x_2},\overline{z_1},\overline{z_2}) \mid f^{(i)}(f_1(\overline{x_1}),f_2(\overline{x_2})) = f^{(i)}(f_3(\overline{z_1}),f_4(\overline{z_2}))\}$. Нетрудно видеть, что каждой n-арной квазигруппе, полученной итерированием 2-квазигруппы f, соответствует некоторое двоичное дерево разложения в суперпозицию.

Из утверждения 3 нетрудно доказать

Утверждение 4. *a) Итерированная группа является изотопно транзитивной мультиарной квазигруппой. b) Если G-лупа f регулярна, то мультиарная квазигруппа, полученная итерированием f является изотопно транзитивной.*

Следующая лемма является обобщением утверждения из [4].

Лемма. *Пусть a) m_i-арные квазигруппы h_i, $i \in \{1,\dots,n\}$, суть итерированные группы, b) n-арная квазигруппа f изотопно транзитивна с транзитивно действующей подгруппой автотопий G_f, c) для любого $i \in \{1,\dots,n\}$ и $\overline{\sigma} \in G_f$ существует изотопия $\overline{\tau}_i \in S_{n_i}$ такая, что $h_i(\overline{\tau}_i z_i) = \sigma_i h(\overline{z_i})$, где $\overline{z_i}$ — наборы из n_i переменных. Тогда m-арная квазигруппа $f(h_1(\overline{z_1}),\dots,h_n(\overline{z_n}))$, где $m = m_1 + \dots + m_n$, является изотопно транзитивной.*

Из леммы и утверждения 4 следует

Теорема. *Пусть f — n-арная квазигруппа, полученная итерированием группы $Z_p \times Z_2$ или лупы C_p, m_i-арные квазигруппы h_i, $i \in \{1,\dots,n\}$ получены итерированием группы D_p. Тогда МДР-код $M = \{(x,\overline{z_1},\dots,\overline{z_n}) \mid x = f(h_1(\overline{z_1}),\dots,h_n(\overline{z_n}))\}$ является изотопно транзитивным.*

Следствие. *При $q = 2p$ число попарно не эквивалентных изотопно транзитивных n-арных квазигрупп порядка q растёт экспоненциально при $n \to \infty$.*

Работа выполнена при финансовой поддержке РФФИ, проект 10-01-00616.

Список литературы

1. Wilson R. L. Jr. Isotopy-isomorphy loops of prime order // J. Algebra. — 1974. — V. 31. — P. 117–119.

2. Goodaire E. G., Robinson D. A. A class of loops which are isomorphic to all loop isotopes // Canadian J. Math. — 1982. — V. 34. — P. 662–672.

3. Kunen K. G-loops and permutation groups // J. Algebra. — 1999. — V. 220, № 2. — P. 694–708.

4. Потапов В. Н. О нижней оценке числа транзитивных совершенных кодов // Дискрет. анализ и исслед. операций. Сер. 1. — 2006. — Т. 13, № 4. — С. 49–59.

МАТРИЧНЫЕ КАНАЛЫ СВЯЗИ

В. К. Леонтьев, Г. Л. Мовсисян, А. А. Осипян (Москва)

Пусть $B = \{0,1\}$, B^n — множество двоичных слов длины n и $A_{n,m}$ — множество всех матриц с элементами из поля B.

Подмножество $A = \{A_0, A_1, A_N\} \subseteq A_{n,m}$ определяет матричный канала A, если любое слово $x \in B^n$ при передаче по A переходит в одно из слов B^m вида $z = xC,\ C \in A$. В дальнейшем $A_0 = E$.

Код $V = \{v_1, v_2, v_q\}$ исправляет ошибки матричного канала $A = \{A_0, A_1, A_N\}$, если выполняется условие $v_i A_t \neq v_j A_k$ для $i, j = \overline{0,q}\ \ t, k = \overline{0,N},\ \ i \neq j$.

Рассмотрим один из важных случаев матричного канала $A = \{A_0, A_1, A_N\}$, в котором A является подгруппой группы невырожденных матриц. В этом случае можно считать, что на множестве B^n действует группа A обычным способом, т. е. $z = xC,\ C \in A$. Окрестность $A^1(x)$ точки x — это транзитивное множество $A^1(x) = \{z; z = xC, C \in A\}$ и $A^1(x) = A^k(x)$ для $k = 1, 2 \ldots$ Так как транзитивные множества $A^1(x)$ производят разбиение B^n, то если взять по произвольному представителю из каждого транзитивного множества, то получим код V, исправляюший ошибки матричного канала A. Этот код является максимальным по мощности и число точек в нем определяется леммой Бернсайда [1].

Максимальный код, исправляющий ошибки матричного канала A, обозначим через $V(A)$.

Теорема 1. *Имеет место формула*

$$|V(A)| = \frac{1}{|A|} \sum_{c \in A} N(C),$$

где $N(C)$ — число собственных векторов матрицы C, соответствующих собственному значению $\lambda = 1$.

Рассмотрим канал связи, по которому переданный двоичный вектор длины n, может преобразоваться в вектор той же длины с транспонированными соседними компонентами, т. е. $x_i x_{i+1} \to x_{i+1} x_i$, где $i = \overline{0, n-1}$. Окрестностью длины один булевого вектора x назовем множество различных векторов получаемых из x путем не более одной транспозиции и обозначим через $S_1(x)$.

Подмножество $V = \{v_1, \ldots, v_p\}$ множества B^n назовем кодом исправляющим ошибки рассматриваемого канала, если $S_1(v_i) \cap$

$S_1(v_j) = \emptyset, \quad i, j = \overline{1, m}, \quad i \neq j$. Задача состоит в определении максимальной мощности V_{max} кода, исправляющего ошибки представленного канала.

Код $U = \{u_1, u_2, u_q\}$ исправляет ошибки аддитивного канала [2] $A = (y_1, y_2, y_m)$, если выполняется условие $u_i \oplus y_t \neq u_j \oplus y_k$ для $i, j = \overline{0, q}, \quad t, k = \overline{1, N} \quad i \neq j$.

Теорема 2 [3]. *Если $n = 2^r - 1$ и $A \backslash (000)$ — произвольный базис пространства B^n, то существует совершенный код, исправляющий ошибки аддитивного канала A с мощностью $\frac{2^n}{n+1}$.*

Следствие. *Код, исправляющий ошибки аддитивного канала $A = \{(0, 00), (1, 1, 00), (0, 1, 10, 0), (0, 00, 1, 1)\}$, также является и кодом исправляющим ошибки канала с транспозициями.*

Теорема 3. *Для последовательности $n = 2^k$, где k — достаточно большое натуральное число, имеем следующую оценку мощности кода исправляющего ошибки транспозиций:*

$$\frac{2^n}{n} \lesssim V_{max} \lesssim \frac{2^{n+1}}{n}.$$

Список литературы

1. Де Брейн. Теория перечисления Пойя // Прикладная комбинаторная теория. — М.: Мир, 1968. — С. 61–106.

2. Деза М. Е. Сравнение произвольных аддитивных шумов по эффективности их обнаружения или исправления // Проблемы передачи информации. — М. 1965. — Т. 1, № 3. — С. 29–39.

3. Леонтьев В. К., Мовсисян Г. Л., Маргарян Ж. Г. Коррекция кодов в аддитивном канале // Вестник РАУ. Физико-математические и естественные науки. — 2010. — № 2. — С. 12–25.

ПОЛУЧЕНИЕ НИЖНИХ ОЦЕНОК НА НЕЛИНЕЙНОСТЬ БУЛЕВОЙ ФУНКЦИИ ЧЕРЕЗ РАЗМЕРНОСТЬ НЕКОТОРЫХ ПОДПРОСТРАНСТВ

М. С. Лобанов (Москва)

Алгебраической иммунностью булевой функции называют величину $AI(f) = \min\limits_{g \neq 0, \ gf \equiv 0 \text{ или } g(f+1) \equiv 0} deg(g)$.

Известно [3, 4], что для любой f над F_2^n выполнено $AI(f) \leq \lceil \frac{n}{2} \rceil$.

Нелинейностью r-го порядка $nl_r(f)$ булевой функции f над F_2^n называется $\min\limits_{\deg(l)\le r} d(f,l)$, где $d(f,l)$ – это расстояние Хэмминга.

Ранее в [1, 2] были доказаны точные оценки на нелинейность первого и второго порядков через значение алгебраической иммунности, а в [5] оценка (неточная) для нелинейности r-го порядка.

$$nl_1(f) \ge 2\sum_{i=0}^{AI(f)-2}\binom{n-1}{i}, nl_2(f) \ge \sum_{i=0}^{k-1}\binom{n}{i} - \sum_{i=0}^{k-1} 2^i \binom{n-2i-1}{k-1-i},$$

$$nl_r(f) \ge \sum_{i=0}^{AI(f)-r-1}\binom{n}{i} + \sum_{i=AI(f)-2r}^{AI(f)-r-1}\binom{n-r}{i}.$$

При значении $AI(f)$, близком к $\lceil\frac{n}{2}\rceil$, оценки получаются довольно сильными, но для функций с низкой $AI(f)$ эти оценки дают не очень хорошие результаты. В статье [6] $nl_r(f)$ оценивается не через $AI(f)$, а через величины $\min\limits_{g\ne 0,\ gf\equiv 0} deg(g)$ и $\min\limits_{g\ne 0,\ g(f+1)\equiv 0} deg(g)$, что позволяет для некоторых функций с низкой $AI(f)$ получить лучшие нижние оценки на $nl_r(f)$.

Нам удалось доказать теорему, которая обобщает как результат автора [2] о получении нижних оценок на $nl_r(f)$ через значение $AI(f)$, так и результат [6], и которая позволяет для многих функций получить более сильные оценки на $nl_r(f)$.

Пусть $h(x_1,\dots,x_n)$ — булева функция от n переменных. Положим $An_k(h) = \{g(x_1,\dots,x_n) |\, gh = 0,\ deg(g) \le k\}$.

Утверждение 1. *Пусть f и f_0 — функции от n переменных, $1 \le k_1, k_2 \le n$, $\dim(An_{k_1}(f)) \ge \dim(An_{k_1}(f_0))$ и $\dim(An_{k_2}(f+1)) \ge \dim(An_{k_2}(f_0+1))$. Тогда $d(f,f_0) \ge \dim(An_{k_1}(f)) - \dim(An_{k_1}(f_0)) + \dim(An_{k_2}(f+1)) - \dim(An_{k_2}(f_0+1))$.*

Пусть h — булева функция от n переменных. Определим $B_{k_1,k_2}(h) = \{g(x_1,\dots,x_n) |\, \deg(g) \le k_1, \deg(gh) \le k_2\}$.

Из [2] следует оценка $\dim(B_{k,k}(h)) \ge \sum_{i=0}^{k-r}\binom{n}{i} + \sum_{i=k-2r+1}^{k-r}\binom{n-r}{i}$.

Утверждение 2. *Пусть $k_1 \ge k_2$, тогда верно равенство:*

$$\dim(An_{k_1}(f)) + \dim(An_{k_2}(f+1)) = \dim(B_{k_1,k_2}(f)).$$

Как простое следствие утверждений 1 и 2 получаем:

Следствие 1. *Пусть f и f_0 — функции от n переменных, $1 \le k_2 \le k_1 \le n$, $\dim(An_{k_1}(f)) \ge \dim(An_{k_1}(f_0))$ и $\dim(An_{k_2}(f+1)) \ge \dim(An_{k_2}(f_0+1))$. Тогда $d(f,f_0) \ge \dim(B_{k_1,k_2}(f)) - \dim(B_{k_1,k_2}(f_0))$.*

Отдельно рассмотрев случай приближения константами, из следствия 1 получаем следующую оценку на нелинейность r-го порядка.

Теорема. *Пусть для $f(x_1,\dots,x_n)$ выполнено*

$$\min_{1\le deg(g)\le r} \dim(An_{k_1}(g)) \ge \dim(An_{k_1}(f)),$$

$$\min_{1\le deg(g)\le r} \dim(An_{k_1}(g)) \ge \dim(An_{k_1}(f+1)).$$

Тогда при $k_1 \ge k_2$

$$nl_r(f) \ge \min\Big(\min_{deg(g)\le r} \dim(B_{k_1,k_2}(g)) - \dim(B_{k_1,k_2}(f)), wt(f), wt(f+1)\Big),$$

а при $k_1 < k_2$

$$nl_r(f) \ge$$

$$\ge \min\Big(\min_{deg(g)\le r} \dim(B_{k_2,k_1}(g)) - \dim(B_{k_2,k_1}(f+1)), wt(f), wt(f+1)\Big).$$

Докажем утверждение, которое может быть полезным для проверки условий теоремы 1.

Утверждение 3. *Верно неравенство* $\min\limits_{1\le deg(g)\le r} \dim(An_k(g)) \ge \sum_{i=0}^{k-r} \binom{n-r}{i}$.

Теорема 1 обобщает соответствующие результаты из работ [2, 4, 6]. Для многих конкретных функций эта теорема дает более сильные оценки на $nl_r(f)$.

Определим для $n = 4k+1$ функцию $f_n(x_1,\dots,x_n)$:

$$f_n(x_1,\dots,x_n) = \begin{cases} 0, & \text{если} \quad wt(x_1,\dots,x_n) \le 2k, \\ 1, & \text{если} \quad wt(x_1,\dots,x_n) > 2k, \end{cases}$$

Определим $f = f_n \cdot (x_1 \vee x_2 \vee \dots \vee x_k) \vee x_1 x_2 \dots x_k$. Несложно доказать, что $AI(f) = k$. Из [2, 5] и из [6] следует одна и таже оценка:

$$nl_r(f) \ge \min_{deg(g)\le r} \dim(B_{k-1,k-1}(g)) \ge \sum_{i=0}^{k-r-1} \binom{n}{i} + \sum_{i=k-2r}^{k-r-1} \binom{n-r}{i}.$$

В то же время из теоремы 1 и утверждения 3 можно получить заметно более сильную оценку

$$nl_r(f) \geq \sum_{i=0}^{2k-r} \binom{n}{i} + \sum_{i=2k-2r+1}^{2k-r} \binom{n-r}{i} - 2\sum_{i=0}^{k} \binom{n-k}{i}.$$

Работа выполнена при поддержке РФФИ (проект 11-01-00508).

Список литературы

1. Лобанов М. С. Точное соотношение между нелинейностью и алгебраической иммунностью // Дискретная математика. — 2006. — Т. 18, вып. 3. — С. 152–159.

2. Лобанов М. С. Точные соотношения между нелинейностью и алгебраической иммунностью // Дискретный анализ и исследование операций. — 2008. — Т. 15, вып. 5. — С. 47–60.

3. Courtois N. and Meier W. Algebraic attacks on stream ciphers with linear feedback // Advances in cryptology. EUROCRYPT 2003. — Berlin, Heidelberg: Springer-Verl., 2003. — P. 345–359. (Lecture Notes in Computer Science. — V. 2656).

4. Meier W., Pasalic E., Carlet C. Algebraic attacks and decomposition of Boolean functions // Advances in cryptology. EUROCRYPT 2004. — Berlin, Heidelberg: Springer-Verl., 2004. — P. 474–491. (Lecture Notes in Computer Science. V. 3027).

5. Mesnager S. Improving the lower bound on the higher order nonlinearity of Boolean functions with prescribed algebraic immunity // Cryptology ePrint archive(http://eprint.iacr.org/), Report 2007/117.

6. Rizomiliotis P. Improving the high order nonlinearity lower bound for Boolean functions with given algebraic immunity // Discrete applied mathematics. — 2010. — V. 158, i. 18. — P. 2049–2055.

БЫСТРАЯ НУМЕРАЦИЯ ЭЛЕМЕНТОВ ГРАССМАНИАНА

Ю. С. Медведева (Новосибирск)

Грассманиан $G_q(n,k)$ — множество всех k-мерных подпространств векторного пространства F_q^n над конечным полем размера q. Задача кодирования элементов грассманиана рассматривалась во

многих работах, например [1, 2] и имеет приложение в сетевом кодировании [3]. Нумерационным кодированием элементов грассманиана $G_q(n,k)$ является сопоставление каждому элементу грассманиана его номеру, т. е. числу из промежутка $[0,\ldots,|G_q(n,k)|-1]$. В работе [4] представлен алгоритм нумерационного кодирования элементов грассманиана, сложность которого $O(nk(n-k)\log n\log\log n)$. Мы предлагаем улучшенный алгоритм нумерационного кодирования элементов грассманиана, сложность которого не превосходит $O(n^2\log^2 n\log\log n)$. Улучшенный алгоритм основан на методе быстрой нумерации комбинаторных объектов из работы Б. Я. Рябко [5].

Любое подпространство $X\in G_q(n,k)$ может быть представлено в виде матрицы $k\times n$, строки которой составляют базис X. Такую матрицу $k\times n$ назовем *матрицей ступенчатого вида по строкам*, если соблюдены следующие условия: старший коэффициент каждой строки находится правее старшего коэффициента предыдущей, все старшие коэффициенты имеют значение 1, каждый старший коэффициент является единственным ненулевым элементом в своём столбце. Каждое подпространство X можно представить в виде единственной матрицы ступенчатого вида по строкам. Вектором идентификации $v(X)$ подпространства $X\in G_q(n,k)$ называется вектор длины n, состоящий из нулей и единиц, имеющий вес k, позиции единиц в котором совпадают с номерами столбцов в которых находятся старшие коэффициенты матрицы ступенчатого вида по строкам [4]. *Расширенным представлением* $EXT(X)$ подпространства $X\in G_q(n,k)$ назовем матрицу $(k+1)\times n$, верхней строкой которой является вектор идентификации $v(X)=(v(X)_n,\ldots,v(X)_1)$, а нижней частью — матрица ступенчатого вида по строкам, представляющая X:

$$EXT(X)=\begin{pmatrix} v(X)_n & \ldots & v(X)_2 & v(X)_1 \\ X_n & \ldots & X_2 & X_1 \end{pmatrix}.$$

Обозначим номер элемента гауссманиана X среди всех элементов $G_q(n,k)$, упорядоченных соответственно лексикографическому порядку их расширенных представлений, как $I_{EXT}(X)$.

Обозначим $N\left(\begin{smallmatrix} v_j & \ldots & v_2 & v_1 \\ X_j & \ldots & X_2 & X_1 \end{smallmatrix}\right)$ количество элементов $G_q(n,k)$ таких, что последние столбцы их расширенных представлений имеют вид $\left(\begin{smallmatrix} v_j & \ldots & v_2 & v_1 \\ X_j & \ldots & X_2 & X_1 \end{smallmatrix}\right)$. Введем величины $P\left(\begin{smallmatrix} v_1 \\ X_1 \end{smallmatrix}\right)=N\left(\begin{smallmatrix} v_1 \\ X_1 \end{smallmatrix}\right)/\begin{bmatrix} n \\ k \end{bmatrix}_q$, $P\left(\begin{smallmatrix} v_j \\ X_j \end{smallmatrix}\middle|\begin{smallmatrix} v_{j-1} & \ldots & v_2 & v_1 \\ X_{j-1} & \ldots & X_2 & X_1 \end{smallmatrix}\right)=N\left(\begin{smallmatrix} v_j & \ldots & v_2 & v_1 \\ X_j & \ldots & X_2 & X_1 \end{smallmatrix}\right)/N\left(\begin{smallmatrix} v_{j-1} & \ldots & v_2 & v_1 \\ X_{j-1} & \ldots & X_2 & X_1 \end{smallmatrix}\right)$, $q\left(\begin{smallmatrix} v_1 \\ X_1 \end{smallmatrix}\right)=$

$$\sum_{\substack{u\\ W<X_1}} P\left(\begin{smallmatrix} u\\ W\end{smallmatrix}\right),\ q\left(\begin{smallmatrix} v_j\\ X_j\end{smallmatrix}\middle|\begin{smallmatrix} v_{j-1}&\dots&v_2&v_1\\ X_{j-1}&\dots&X_2&X_1\end{smallmatrix}\right)= \sum_{\substack{u\\ W<X_j}} P\left(\begin{smallmatrix} u\\ W\end{smallmatrix}\middle|\begin{smallmatrix} v_{j-1}&\dots&v_2&v_1\\ X_{j-1}&\dots&X_2&X_1\end{smallmatrix}\right)$$

для $j = 1, 2, \dots, n$, где $\begin{bmatrix} n\\ k\end{bmatrix}_q$ — q-ичный гауссовский коэффициент, равный мощности $G_q(n,k)$ и определяемый следующим образом: $\begin{bmatrix} n\\ k\end{bmatrix}_q = \prod_{i=0}^{q-1} \frac{q^{n-i}-1}{q^{k-i}-1}$.

Эти величины можно вычислить по формулам:

$$P\left(\begin{smallmatrix} v_j\\ X_j\end{smallmatrix}\middle|\begin{smallmatrix} v_{j-1}&\dots&v_2&v_1\\ X_{j-1}&\dots&X_2&X_1\end{smallmatrix}\right)=$$

$$= \begin{bmatrix} n-j\\ k-w_j\end{bmatrix}_q \Big/ \begin{bmatrix} n-j+1\\ k-w_{j-1}\end{bmatrix}_q = \begin{cases} \frac{q^{n-j-k+w_j+1}-1}{q^{n-j+1}-1}, & \text{если } v_j = 0,\\ \frac{q^{k-w_j+1}-1}{q^{n-j+1}-1}, & \text{если } v_j = 1,\end{cases}$$

$$q\left(\begin{smallmatrix} v_j\\ X_j\end{smallmatrix}\middle|\begin{smallmatrix} v_{j-1}&\dots&v_2&v_1\\ X_{j-1}&\dots&X_2&X_1\end{smallmatrix}\right)= \begin{cases} q^{k-w_{j-1}} \cdot \frac{q^{n-j-k+w_{j-1}+1}-1}{q^{n-j+1}-1}, & \text{если } v_j = 1,\\ \frac{\{X_j\}}{q^{w_{j-1}}} \cdot \frac{q^{n-j-k+w_{j-1}+1}-1}{q^{n-j+1}-1}, & \text{если } v_j = 0,\end{cases}$$

где $\{X_j\}$ — значение, получаемое при чтении вектора X_j как числа в q-ичной системе исчисления; w_j — сумма первых j компонент вектора $v(X)$. Справедливо равенство $I_{EXT}(X) = \begin{bmatrix} n\\ k\end{bmatrix}_q \left(q\left(\begin{smallmatrix} v_1\\ X_1\end{smallmatrix}\right)+q\left(\begin{smallmatrix} v_2\\ X_2\end{smallmatrix}\middle|\begin{smallmatrix} v_1\\ X_1\end{smallmatrix}\right)P\left(\begin{smallmatrix} v_1\\ X_1\end{smallmatrix}\right)+q\left(\begin{smallmatrix} v_3\\ X_3\end{smallmatrix}\middle|\begin{smallmatrix} v_2&v_1\\ X_2&X_1\end{smallmatrix}\right)P\left(\begin{smallmatrix} v_2\\ X_2\end{smallmatrix}\middle|\begin{smallmatrix} v_1\\ X_1\end{smallmatrix}\right)P\left(\begin{smallmatrix} v_1\\ X_1\end{smallmatrix}\right)+\dots\right)$. Идея нашего метода заключается в расстановке скобок в правой части таким образом, что при ее вычислении большинство операций производится над короткими числами. Такой расстановкой скобок является:

$$I_{EXT}(X) = \begin{bmatrix} n\\ k\end{bmatrix}_q \left(\left(q\left(\begin{smallmatrix} v_1\\ X_1\end{smallmatrix}\right)+q\left(\begin{smallmatrix} v_2\\ X_2\end{smallmatrix}\middle|\begin{smallmatrix} v_1\\ X_1\end{smallmatrix}\right)P\left(\begin{smallmatrix} v_1\\ X_1\end{smallmatrix}\right)\right)+\left(\left(q\left(\begin{smallmatrix} v_3\\ X_3\end{smallmatrix}\middle|\begin{smallmatrix} v_2&v_1\\ X_2&X_1\end{smallmatrix}\right)+\right.\right.\right.$$

$$\left.\left.\left.+q\left(\begin{smallmatrix} v_4\\ X_4\end{smallmatrix}\middle|\begin{smallmatrix} v_3&\dots&v_1\\ X_3&\dots&X_1\end{smallmatrix}\right)P\left(\begin{smallmatrix} v_3\\ X_3\end{smallmatrix}\middle|\begin{smallmatrix} v_2&v_1\\ X_2&X_1\end{smallmatrix}\right)\right)P\left(\begin{smallmatrix} v_2\\ X_2\end{smallmatrix}\middle|\begin{smallmatrix} v_1\\ X_1\end{smallmatrix}\right)P\left(\begin{smallmatrix} v_1\\ X_1\end{smallmatrix}\right)\right)+\dots\right).$$

Опишем алгоритм вычисления номера $I_{EXT}(X)$. Вычисляются значения $P\left(\begin{smallmatrix} v_j\\ X_j\end{smallmatrix}\middle|\begin{smallmatrix} v_{j-1}&\dots&v_2&v_1\\ X_{j-1}&\dots&X_2&X_1\end{smallmatrix}\right)$ и $q\left(\begin{smallmatrix} v_j\\ X_j\end{smallmatrix}\middle|\begin{smallmatrix} v_{j-1}&\dots&v_2&v_1\\ X_{j-1}&\dots&X_2&X_1\end{smallmatrix}\right)$ $(j = 1, \dots, n)$ по формулам (1), (2). Введем величины ρ_j^i, λ_j^i, $(i = 0, \dots, \log n;$

$j = 1, \ldots, n/2^i$). Их значения последовательно вычисляются по формулам $\rho_j^0 = P\left(\begin{smallmatrix} v_j \\ X_j \end{smallmatrix} \middle| \begin{smallmatrix} v_{j-1} & \ldots & v_2 & v_1 \\ X_{j-1} & \ldots & X_2 & X_1 \end{smallmatrix}\right)$, $\lambda_j^0 = q\left(\begin{smallmatrix} v_j \\ X_j \end{smallmatrix} \middle| \begin{smallmatrix} v_{j-1} & \ldots & v_2 & v_1 \\ X_{j-1} & \ldots & X_2 & X_1 \end{smallmatrix}\right)$ для $j = 1, \ldots, n$; $\rho_j^i = \rho_{2j-1}^{i-1}\rho_{2j}^{i-1}$, $\lambda_j^i = \lambda_{2j-1}^{i-1} + \rho_{2j-1}^{i-1}\lambda_{2j}^{i-1}$, для $i = 2, \ldots, \log n$, $j = 1, \ldots, n/2^i$.

Получаем искомый номер по формуле

$$I_{EXT}(X) = \lambda_1^{\log n} \cdot \begin{bmatrix} n \\ k \end{bmatrix}_q .$$

Сложность вычисления номера элемента грассманиана $X \in G_q(n,k)$ с помощью предложенного алгоритма равна $O(\log n M(n^2))$, где $M(a)$ время умножения двух чисел длины a. При использовании алгоритма быстрого умножения из [6], для которого $M(a) = a \log a \log\log a$, сложность вычисления номера равна $O(n^2 \log^2 n \log\log n)$.

Список литературы

1. Gadouleau M., Yan Z. Constant-rank codes and their connection to constant-dimension codes // IEEE Trans. Inform. Theory. — 2010. — V. IT-56. — P. 3207–3216.

2. Skachek V. Recursive code construction for random networks // IEEE Trans. Inform. Theory. — 2010. — V. IT-56. — P. 1378–1382.

3. Koetter R., Kshcischang F. R. Coding for errors and erasures in random network coding // IEEE Trans. Inform. Theory. — 2008. — V. 54, № 8. — P. 3579–3591.

4. Silberstein N., Etzion T. Enumerative coding for Grassmannian space // `http://arxiv.org/abs/0911.3256.`

5. Рябко Б. Я. Быстрая нумерация комбинаторных объектов // Дискрет. матем. — 1998. — Т. 10, вып. 2. — С. 101–119.

6. Schönhage A., Strassen V. Schnelle Multiplikation großer Zahlen // Computing. — 1971. — № 7. — P. 281–292.

ОБ ИСПОЛЬЗОВАНИИ ГИПЕРЭЛЛИПТИЧЕСКИХ КРИВЫХ НАД КОНЕЧНЫМИ ВЕКТОРНЫМИ ПОЛЯМИ

А. В. Неласая, Г. Л. Козина (Запорожье)

Большинство современных стандартов цифровой подписи основано на операциях в группе точек эллиптических кривых, опреде-

ленных над конечными полями. Стойкость таких криптопреобразований основана на большой вычислительной сложности задачи дискретного логарифмирования на эллиптической кривой при длине модуля основного поля не менее 160 бит. Следовательно, при программной реализации таких криптосистем необходимо подключение библиотек длинной арифметики. Естественным обобщением эллиптических кривых являются кривые более высокого рода — гиперэллиптические кривые. Поначалу считалось, что криптографические преобразования на гиперэллиптических кривых настолько сложны, что их скорость не может достичь приемлемого уровня. Однако анализ последних работ в этой области показывает, что применение современных аппаратных платформ и новых методов вычислений позволяет значительно улучшить скоростные показатели таких преобразований.

Особенностями использования гиперэллиптических кривых является уменьшение размера основного поля пропорционально роду кривой без потери стойкости (с сохранением порядка группы) с одновременным усложнением формулы групповой операции. Это видно из формулы Хассе—Вейля для оценки порядка якобиана гиперэллиптической кривой (групповой структуры, определенной на гиперэллиптической кривой с использованием порядка дивизоров):

$$\left\lceil (\sqrt{q}-1)^{2g} \right\rceil \leq \#J/F_q \leq \left\lfloor (\sqrt{q}+1)^{2g} \right\rfloor,$$

где q — порядок основного поля $GF(q)$, над которым определена кривая.

Традиционно, сложность формулы групповой операции на кривых выражается в виде суммы количества умножений, инверсий и возведений в квадрат в основном поле. Но при сравнении сложности для кривых разного рода такой подход не пригоден, поскольку, как упоминалось выше, размер основного поля уменьшается пропорционально роду кривой. Соответственно, одна и та же арифметическая операция в основных полях разной размерности будет иметь разную сложность. Интересная метрика для этого случая была предложена в [1]. В ней сложность выражается в терминах количества процессорных инструкций, таких как «сдвиг» и «исключающее или».

Основное преимущество при использовании гиперэллиптических кривых с точки зрения снижения сложности криптографических преобразований заключается в возможности отказа от использования библиотек длинных чисел при реализации арифметики основного поля для определенных параметров криптосистемы, что значительно повышает их быстродействие, вопреки теоретическим оценкам. Это происходит за счет того, что на обслуживание внутренних

механизмов работы библиотеки длинных чисел уходит дополнительное количество вычислительной мощности (процессорное время и объем оперативной памяти), которое никогда не учитывают теоретические оценки.

Развитие вычислительной техники предоставляет новые возможности для повышения скорости реализации криптографических алгоритмов. В частности, переход от 32-разрядных к 64-разрядным процессорам позволил реализовать арифметику основного поля для гиперэллиптических кривых третьего рода с порядком группы длиной 192 бита, что обеспечивает достаточную криптографическую стойкость, полностью отказавшись от использования библиотеки длинной арифметики [2]. Это позволило на порядок увеличить скоростные показатели данных преобразований. Имея в распоряжении 128-разрядный процессор, можно было бы подобным образом реализовать криптосистему на гиперэллиптической кривой второго рода. В качестве прогноза в этом случае можно ожидать более высоких показателей скорости, чем для эллиптических кривых.

В работе для решения этой проблемы предлагается другой подход, основанный на использовании в качестве основного поля конечного векторного поля [3].

Конечное векторное поле $GVF(p^n)$ одно из расширений $GF(p^n)$ конечного поля Галуа $GF(p)$. Элементами конечного векторного поля являются векторы, представленные набором $(a, b, \ldots, f)$ коэффициентов при соответствующих базисных векторах $e, i, ..., z$:

$$\nu = a \cdot e + b \cdot i + \cdots + f \cdot z.$$

Количество базисных векторов, составляющих элемент конечного векторного поля, равно n. Коэффициенты при базисных векторах являются элементами поля $GF(p)$. Операция сложения двух векторов определяется сложением координат при соответствующем базисном векторе по модулю p. Операция умножения вектора на число определяется умножением каждого из коэффициентов на это число по модулю p. Операция умножения двух векторов определяется по принципу перемножения многочленов, причем результат произведения двух базисных векторов определяется по таблице, составленной таким образом, чтобы обеспечить ассоциативность операции.

Важным отличием операций в $GVF(p^n)$ от операций в $GF(p^n)$ является отсутствие необходимости приведения результата умножения по модулю неприводимого многочлена. Это делает ее идеально распараллеливаемой. Следовательно, целесообразным является определение гиперэллиптической кривой второго рода над векторным полем длины 4. Тогда арифметика основного поля будет включать

лишь 32-битные целочисленные операции, для выполнения которых удобно использовать архитектуру XMM-расширения процессора и внутренних параллельных команд группы SSE2.

Такое сочетание использования 64-битной аппаратной платформы, математического аппарата гиперэллиптических кривых и параллельного программирования создает условия для дальнейшего роста производительности криптосистем на гиперэллиптических кривых.

Принципиальным моментом и направлением будущих исследований является теоретическое обоснование возможности построения алгебраической структуры якобиана гиперэллиптической кривой над конечным векторным полем и развитие соответствующей теории при положительном решении этого вопроса.

Список литературы

1. Wollinger T. Software and hardware implementation of hyperelliptic curve. Dissertation for the degree of doctor-ingenious. — Bochum, 2004.

2. Долгов В. И., Неласая А. В. Программная реализация криптографических операций на гиперэллиптических кривых // Системы обработки информации. — 2010. — Вип. 3 (84). — С. 17–19.

3. Молдовян Н. А. Группы векторов для алгоритмов электронной цифровой подписи // Вестник СПб ун-та. Серия 10. Прикладная математика, информатика, процессы управления. — 2009. — № 1. — С. 96–102.

О РАССТОЯНИЯХ ОТ КЛАССА МАКСИМАЛЬНО-НЕЛИНЕЙНЫХ ФУНКЦИЙ ДО НЕКОТОРОГО КЛАССА БУЛЕВЫХ ФУНКЦИЙ

Р. Р. Омаров (Москва)

Надежность криптографических систем зависит от свойств булевых функций использованных при их построении. Например «близость» этих функций к «плохим» классам булевых функций с хорошо изученными свойствами облегчает поиск слабостей в таких системах. Одним из таких классов является класс линейных функций.

В данной работе в качестве «плохого» класса рассматриваются функции, у которых в полиноме Жегалкина присутствует не более k нелинейных слагаемых. Приведем необходимые определения.

Пусть n — произвольное натуральное число. Через V_n будем обозначать векторное пространство наборов длины n с компонентами из $\{0,1\}$ с операцией $\oplus$ покоординатного сложения векторов по модулю 2. Пусть f, g — произвольные булевы функции от n переменных.

Через $wt(f)$ будем обозначать *вес* булевой функции f — количество наборов, на которых она равна 1.

Расстоянием от булевой функции f до булевой функции g называется величина $dist(f,g) = wt(f \oplus g)$. Под *расстоянием между двумя множествами булевых функций* M *и* N будем понимать $dist(M,N) = \min\limits_{\substack{g\in M\\ h\in N}} dist(g,h)$.

Булева функция f от n переменных называется *аффинной*, если существуют $a = (a_1,\ldots,a_n) \in V_n$ и $c \in \{0,1\}$ такие, что $f(x) = a_1x_1 \oplus \ldots \oplus a_nx_n \oplus c$. Множество всех аффинных булевых функций от n переменных будем обозначать A_n.

Величина $N_f = dist(f, A_n)$ называется *нелинейностью* функции $f(x)$.

Лемма [1]. *Для любой булевой функции $f(x)$ от n переменных справедливо неравенство $N_f \le 2^{n-1} - 2^{n/2-1}$. Для четных n эта оценка достижима.*

Булевы функции $f(x)$, для которых N_f равно максимально возможному значению среди всех функций от n переменных, называют *максимально-нелинейными* функциями.

Через AE_n^k будем обозначать класс всех почти аффинных функций от n переменных, а именно, функций вида $X_{I_1} \oplus \ldots \oplus X_{I_k} \oplus l(x)$, где $X_{I_t} = \prod\limits_{j\in I_t} x_j$, I_t – произвольные подмножества (возможно, пустые $X_\varnothing = 0$) множества $\{1,\ldots,n\}$, $t = \overline{1,k}$ и $l(x) \in A_n$.

Теорема. *Пусть B_{2n} — множество всех максимально-нелинейных функций от $2n$ переменных, тогда*

$$dist(B_{2n}, AE_{2n}^k) \ge 2^{2n-1} - 3^k \cdot 2^{n-1}.$$

Доказательство. Пусть $f(x) \in B_{2n}$, а $g(x) = X_{I_1} \oplus \ldots \oplus X_{I_k} \oplus l(x)$ произвольная функция из класса AE_{2n}^k. Обозначим через $f'(x) = f(x) \oplus l(x)$, $g'(x) = X_{I_1} \oplus \ldots \oplus X_{I_k}$, $I_S = \bigcup\limits_{j\in S} I_j$. Тогда

$$wt(f(x) \oplus g(x)) = wt(f'(x)) + \sum_{\substack{x\in V_{2n}\\ g'(x)=1}} (-1)^{f'(x)}.$$

Индукцией по k покажем, что

$$\sum_{\substack{x\in V_{2n}\\ g'(x)=1}} (-1)^{f'(x)} = \sum_{i=0}^{k-1}(-2)^i \sum_{\substack{S\subseteq\{1,\dots,k\}\\ |S|=i+1}} \sum_{X_{I_S}=1} (-1)^{f'(x)}. \qquad (1)$$

Легко убедиться, что формула (1) справедлива при $k=2$. Предположим, что она верна при $k=t-1$. Докажем ее при $k=t$.

$$\sum_{\substack{x\in V_{2n}\\ g'(x)=1}} (-1)^{f'(x)} = \sum_{\substack{x\in V_{2n}\\ X_{I_1}\oplus\dots\oplus X_{I_{t-1}}=1}} (-1)^{f'(x)} + \sum_{\substack{x\in V_{2n}\\ X_{I_t}=1}} (-1)^{f'(x)} -$$

$$-2\cdot \sum_{\substack{x\in V_{2n}\\ X_{I_1}\cdot X_{I_t}\oplus\dots\oplus X_{I_{t-1}}\cdot X_{I_t}=1}} (-1)^{f'(x)} = \sum_{i=0}^{t-2}(-2)^i \sum_{\substack{S\subseteq\{1,\dots,t-1\}\\ |S|=i+1}} \sum_{X_{I_S}=1} (-1)^{f'(x)} +$$

$$+ \sum_{\substack{x\in V_{2n}\\ X_{I_t}=1}} (-1)^{f'(x)} - 2\cdot \sum_{i=0}^{t-2}(-2)^i \sum_{\substack{S\subseteq\{1,\dots,t-1\}\\ |S|=i+1}} \sum_{\substack{X_{I_S}=1\\ X_{I_t}=1}} (-1)^{f'(x)} =$$

$$= \sum_{i=0}^{t-2}(-2)^i \sum_{\substack{S\subseteq\{1,\dots,t-1\}\\ |S|=i+1}} \sum_{X_{I_S}=1} (-1)^{f'(x)} + \sum_{\substack{x\in V_{2n}\\ X_{I_t}=1}} (-1)^{f'(x)} +$$

$$+ \sum_{i=1}^{t-1}(-2)^i \sum_{\substack{S\subseteq\{1,\dots,t\}\\ |S|=i+1\\ t\in S}} \sum_{X_{I_S}=1} (-1)^{f'(x)} = \sum_{i=0}^{t-1}(-2)^i \sum_{\substack{S\subseteq\{1,\dots,t\}\\ |S|=i+1}} \sum_{X_{I_S}=1} (-1)^{f'(x)}.$$

Заметим, что $\{x : x\in V_{2n}, X_A=1\} = \{x\oplus\xi^A : x\in L_A\} = \xi^A + L_A$, где $A\subseteq\{1,\dots,n\}$, $L_A=\{x : x_i=0, i\in A\}$, а $\xi^A\in V_{2n} : \xi_i^A = 1, i\in A, \xi_i^A=0, i\notin A$. Тогда для некоторой максимально-нелинейной функции $\tilde{f}(y)$ [1, с. 240] верно

$$\sum_{\substack{x\in V_{2n}\\ X_A=1}} (-1)^{f'(x)} = \sum_{x\in\xi^A+L_A} (-1)^{f'(x)} = 2^{dim L_A - n} \sum_{y\in L_A^\perp} (-1)^{\tilde{f}(y)\oplus\langle\xi^A,y\rangle} =$$

$$= 2^{n-|A|} \sum_{y\in L_A^\perp} (-1)^{\tilde{f}(y)\oplus\langle\xi^A,y\rangle}.$$

Запишем (1) с учетом этого

$$\sum_{\substack{x\in V_{2n}\\ g'(x)=1}}(-1)^{f'(x)}=\sum_{i=0}^{k-1}(-2)^i\sum_{\substack{S\subseteq\{1,\dots,k\}\\ |S|=i+1}}2^{n-|I_S|}\sum_{y\in L_{I_S}^{\perp}}(-1)^{\bar{f}(y)\oplus\langle\xi^{I_S},y\rangle}.$$

Функция $f(x)\in B_{2n}$, следовательно $wt(f'(x))\geq 2^{2n-1}-2^{n-1}$. Учитывая это и то, что $dimL_{I_S}^{\perp}=|I_S|$, получим

$$wt(f(x)\oplus g(x))\geq 2^{2n-1}-2^{n-1}-\sum_{i=0}^{k-1}2^i\sum_{\substack{S\subseteq\{1,\dots,k\}\\ |S|=i+1}}2^{n-|I_S|}\cdot 2^{|I_S|}=$$

$$=2^{2n-1}-2^{n-1}\cdot\sum_{i=0}^{k}2^iC_k^i=2^{2n-1}-3^k\cdot 2^{n-1}.$$

В силу произвольности выбора функций $f(x)$ и $g(x)$ получим

$$dist(B_{2n},AE_{2n}^k)\geq 2^{2n-1}-3^k\cdot 2^{n-1}.$$

Список литературы

1. Логачёв О. А., Сальников А. А., Ященко В. В. Булевы функции в теории кодирования и криптологии. — М.: МЦНМО, 2004.

О ПЕРИОДЕ ПОСЛЕДОВАТЕЛЬНОСТИ СОСТОЯНИЙ ШИФРСИСТЕМЫ RC4

М. А. Пудовкина (Москва)

Шифрсистема RC4 разработана Р. Ривестом в 1987 г., зависит от параметра m (для практических приложений выбирается $m=256$). Рассмотрим автономный автомат A, моделирующий шифрсистему RC4 с функцией переходов состояний f. Пусть S_m — множество всех подстановок на множестве $\{0,\dots,m-1\}$, $\mathbb{Z}_m$ — кольцо вычетов по модулю m, $\mathbb{N}$ — множество натуральных чисел, $f:\mathbb{Z}_m^2\times S_m\to\mathbb{Z}_m^2\times S_m$ — функция переходов состояний шифрсистемы RC4, $(i_t,j_t,s_t)\in$

$\mathbb{Z}_m^2 \times S_m$ — состояние в момент времени $t = 0, 1, ...$, $(0, 0, s_0)$ — начальное состояние, где подстановка s_0 генерируется из ключа шифрования.

Функция переходов состояний f в момент времени t задаётся как

1) $i_t = i_{t-1} + 1 (\mathrm{mod}\, m)$;

2) $j_t = j_{t-1} + s_{t-1}(i_t) (\mathrm{mod}\, m)$;

3) $s_t(i_t) = s_{t-1}(j_{t-1})$ $s_t(j_t) = s_{t-1}(i_{t-1})$ $s_t(c) = s_{t-1}(c)$ при $c \notin \{i_t, j_t\}$.

Пусть $W(i_0, j_0, s_0) = (i_0, j_0, s_0), (i_1, j_1, s_1), ..., (i_t, j_t, s_t), —$ последовательность состояний функции переходов f, порождённая начальным состоянием (i_0, j_0, s_0), а $W_{i_0,j_0}(s_0) = s_0, s_1, ..., s_t, ...$ — соответствующая последовательность подстановок.

На конференции Рускрипто 2012 А. В. Бабашом, Д. С. Кудияровым [1] анонсировано, что при $m = 2^n$, $n \in \mathbb{N}$, для любой подстановки $s_0 \in S_m$ период последовательности $W_{0,0}(s_0)$ кратен 2^{n-1}. Кроме того, если $s_0(1) \neq 1 + 2^{n-1}$, то период последовательности $W_{0,0}(s_0)$ кратен m.

Покажем, что справедливо более общее свойство.

Утверждение. *Пусть* $(w, v, s_0) \in \mathbb{Z}_m^2 \times S_m$. *Тогда период* q *последовательности подстановок* $W_{w,v}(s_0)$ *совпадает с периодом* p *последовательности состояний* $W(w, v, s_0)$ *и* $p \equiv 0 (\mathrm{mod}\, m)$.

Доказательство. Без ограничения общности проведём доказательства для случая $w = 0$, поскольку на циклах состояний алгоритма RC4 всегда существуют такие состояния. Ясно, что $p \geq q$. Предположим, что $p > q$. Это означает существование в последовательности $W(0, v, s_0)$ состояний $(0, v, s_0)$ и (i_q, j_q, s_0) для некоторого $j_q \in \mathbb{Z}_m$ и $i_q = q (\mathrm{mod}\, m)$.

Тогда $(1, j_1, s_1), (i_{q+1}, j_{q+1}, s_1) \in W(0, v, s_0)$, где

$$j_1 = s_0(1) + v (\mathrm{mod}\, m), i_{q+1} = q + 1 (\mathrm{mod}\, m),$$

$$j_{q+1} = j_q + s_0(i_{q+1}) (\mathrm{mod}\, m),$$

причём $\{i_1, j_1\} = \{i_{q+1}, j_{q+1}\}$.

Если $i_{q+1} = 1$, то $j_{q+1} = j_1$ и $(i_1, j_1, s_1) = (i_{q+1}, j_{q+1}, s_1)$, т.е. $p = q$. В противном случае, $i_{q+1} = j_1$ и $j_{q+1} = i_1 = 1$.

Аналогичным образом, $\{i_c, j_c\} = \{i_{q+c}, j_{q+c}\}$ для любого $c \in \mathbb{Z}_p$. Если $(i_c, j_c) = (i_{q+c}, j_{q+c})$, то $(i_c, j_c, s_c) = (i_{q+c}, j_{q+c}, s_c)$, т. е. $p = q$.

Таким образом, для всех $c \in \mathbb{Z}_p$ имеем

$$i_c = j_{q+c} = c(\mathrm{mod}\, m), \tag{1}$$

$$j_c = i_{q+c} = q + c(\mathrm{mod}\, m). \tag{2}$$

В силу равенств (1), (2) и $j_t = j_{t-1} + s_{t-1}(i_t)(\mathrm{mod}\, m)$ имеем $s_{t-1}(i_t) = 1$ для всех $t \in \mathbb{Z}_p$. Из равенства (2) при $c = 0$ получаем $j_0 = v = q(\mathrm{mod}\, m)$. Таким образом,

$$j_1 = v + 1(\mathrm{mod}\, m), , j_t = v + t(\mathrm{mod}\, m) \tag{3}$$

для всех $t \in \mathbb{Z}_p$. Из описания функции переходов состояний алгоритма RC4 следует, что равенства (3) справедливы тогда и только тогда, когда $j_1 = i_2(\mathrm{mod}\, m)$, $j_t = i_{t+1}(\mathrm{mod}\, m)$ для всех $t \in \mathbb{Z}_p$. Это, в свою очередь, возможно тогда и только тогда, когда $v = 1$. Если же $v \neq 1$, то равенства (3) одновременно не выполняются, а это означает, что $p = q$.

Если $v = 1$, то из работы [2] следует, что на цикле длины $m(m-1)$ лежат $m(m-1)$ различных подстановок. Таким образом, снова $p = q$.

Очевидно, что $p \equiv 0(\mathrm{mod}\, m)$. Утверждение доказано.

Список литературы

1. Бабаш А. В., Кудияров Д. С. О периодичности функционирования генератора псевдослучайных чисел RC4 // `http://www.ruscrypto.ru/sources/conference/rc2012/`

2. Pudovkina M. Short cycles of the alleged RC4 keystream generator // Proceedings of 3nd International Workshop on Computer Science and Information Technologies (CSIT'2001). — UFA, 2001.

О РЕКУРСИВНО ДИФФЕРЕНЦИРУЕМЫХ БИНАРНЫХ КВАЗИГРУППАХ

П. Н. Сырбу (Кишинев, Молдова)

Рекурсивно дифференцируемые квазигруппы возникли в теории рекурсивных МДР-кодов [1–4].

Пусть (Q, A) — n-арный группоид и k — целое неотрицательное число. n-Арная операция $A^{(k)}$, определенная равенствами

$$A^{(k)}(x_1^n) = A(x_{k+1}^n, A^{(0)}(x_1^n), \ldots, A^{(k-1)}(x_1^n)), \text{ если } k < n,$$

$$A^{(k)}(x_1^n) = A(A^{(n-k)}(x_1^n), \ldots, A^{(k-1)}(x_1^n)), \text{ если } k \geq n,$$

называется рекурсивной производной порядка k. По определению ставим $A^{(0)}(x_1^n) = A(x_1^n)$, для любых $x_1, \ldots, x_n \in Q$.

Если рекурсивные производные $A^{(0)}, A^{(1)}, \ldots, A^{(s)}$ являются квазигрупповыми операциями, то (Q, A) называется рекурсивно s-дифференцируемой квазигруппой. В частности, если (Q, A) — бинарная квазигруппа, то, обозначая $A = "\cdot"$ и $A^{(s)} = "\overset{s}{\triangle}"$,$\forall s \in N$, получаем:

$$x\overset{0}{\triangle}y = x \cdot y,\ x\overset{1}{\triangle}y = y \cdot xy,$$
$$x\overset{k}{\triangle}y = (x\overset{k-2}{\triangle}y) \cdot (x\overset{k-1}{\triangle}y),\ \forall k \geq 2.$$

В [5] доказано, что если $(Q, \cdot)$ — абелева группа, то $x\overset{n}{\triangle}y = x^{b_n} \cdot y^{b_{n+1}}$, $\forall x, y \in Q$, где $(b_n)_{n \in N^*}$ — ряд Фибоначчи. В случае произвольных бинарных квазигрупп в [5] доказан критерий: бинарная квазигруппа $(Q, \cdot)$ рекурсивно 1-дифференцируема тогда и только тогда, когда операции $(*)$ и $(/)$ ортогональны, где $x * y = y \cdot x$, $\forall x, y \in Q$, а $(/)$ является левым делением в $(Q, \cdot)$.

Ниже будет показано, что если бинарная квазигруппа $(Q, \cdot)$ рекурсивно 1-дифференцируема, то $(Q, \overset{1}{\triangle})$ сохраняет ряд ее свойств.

Предложение 1. *Пусть $(Q, \cdot)$ — бинарная рекурсивно 1-дифференцируемая квазигруппа и пусть $(Q, \overset{1}{\triangle})$ ее рекурсивная производная первого порядка. Тогда:*

i. Любая конгруэнция θ квазигруппы $(Q, \cdot)$ является конгруэнцией в $(Q, \overset{1}{\triangle})$.

ii. Нормальная конгруэнция θ квазигруппы $(Q, \cdot)$ является нормальной конгруэнцией в $(Q, \overset{1}{\triangle})$ тогда и только тогда, когда все левые трансляции в $(Q, \overset{1}{\triangle})$ допустимы относительно θ.

Доказательство. i. Пусть θ является конгруэнцией в $Q(\cdot)$. Тогда $x\theta y \Rightarrow cx\theta cy$ и $xc\theta yc$, для любого $c \in Q$, следовательно $x \cdot cx\theta x \cdot cy$, $x \cdot cy\theta y \cdot cy$ и $c \cdot xc\theta c \cdot yc$,$\forall c \in Q$, откуда получаем $x \cdot cx\theta y \cdot cy$ и $c \cdot xc\theta c \cdot yc$, $\forall c \in Q$ или, переходя к операции $(\overset{1}{\triangle})$: $c\overset{1}{\triangle}x\theta c\overset{1}{\triangle}y$ и $x\overset{1}{\triangle}c\theta y\overset{1}{\triangle}c$, $\forall c \in Q$, то есть θ является конгруэнцией в $(Q, \overset{1}{\triangle})$.

ii. Следует из i. и из определения допустимой (относительно бинарного отношения) подстановки.

Предложение 2. *Если* $(Q,\cdot)$ — *бинарная рекурсивно* 1-*дифференцируемая квазигруппа, то подквазигруппа* H *квазигруппы* $(Q,\overset{1}{\triangle})$ *является подквазигруппой и в* $(Q,\cdot)$ *тогда и только тогда, когда* H *замкнута относительно* $(\cdot)$.

Доказательство. Пусть H подквазигруппа в $(Q,\overset{1}{\triangle})$ и пусть она замкнута относительно $(\cdot)$. Тогда уравнение $x\cdot a=b$, где $a,b\in H$, имеет единственное решение в H, так как $x\overset{1}{\triangle}a=a\cdot xa=a\cdot b$. Рассмотрим теперь второе уравнение: $a\cdot x=b$, где $a,b\in H$. Подставляя вместо x произведение $x'\cdot a$, имеем $x'\overset{1}{\triangle}a=b$, следовательно $x=x'\cdot a\in H$ тогда и только тогда, когда H замкнуто относительно $(\cdot)$.

Обозначим (левую, правую) мультипликативную группу квазигруппы $(Q,\cdot)$ следующим образом: $(<L_a\mid a\in Q>=LM(Q,\cdot),<R_b\mid b\in Q>=RM(Q,\cdot))<L_a,R_b\mid a,b\in Q>=M(Q,\cdot)$.

Биективное отображение $\varphi:Q\to Q$ называется полуавтоморфизмом квазигруппы $(Q,\cdot)$, если $\varphi(x\cdot yx)=\varphi(x)\cdot\varphi(y)\varphi(x)$, $\forall x,y\in Q$.

Обозначим через $SAut(Q,\cdot)$ группу всех полуавтоморфизмов квазигруппы $(Q,\cdot)$

Предложение 3. *Пусть* $(Q,\cdot)$ — *бинарная рекурсивно* 1-*дифференцируемая квазигруппа и пусть* $(Q,\overset{1}{\triangle})$ — *ее первая рекурсивная производная. Верны следующие утверждения:*

i. $RM(Q,\overset{1}{\triangle})\subseteq M(Q,\cdot)$; ii. $Aut(Q,\cdot)\subseteq Aut(Q,\overset{1}{\triangle})$;

iii. $Aut(Q,\overset{1}{\triangle})=SAut(Q,\cdot)$; iv. $SAut(Q,\cdot)\subseteq SAut(Q,\overset{1}{\triangle})$;

v. $Aut(Q,\cdot)$ *может быть вложена в каждую из групп:*

$AutLM(Q,\overset{1}{\triangle})$, $AutRM(Q,\overset{1}{\triangle})$, $Aut(Q,\overset{1}{\triangle})$.

Доказательство. i. Из равенства $x\overset{1}{\triangle}a=a\cdot xa$ следует $R_a=L_a^{(\cdot)}R_a^{(\cdot)}$, где $L_a^{(\cdot)}$ является левой трансляцией в квазигруппе $Q(\cdot)$, а R_a ($R_a^{(\cdot)}$) является правой трансляцией в квазигруппе $Q(\overset{1}{\triangle})$ (соотв. $Q(\cdot)$).

ii. Если $\varphi\in Aut(Q,\cdot)$, то $\varphi(x\overset{1}{\triangle}y)=\varphi(y\cdot xy)=\varphi(y)\cdot\varphi(x)\varphi(y)=\varphi(x)\overset{1}{\triangle}\varphi(y)$, $\forall x,y\in Q$, т.е. $\varphi\in Aut(Q,\overset{1}{\triangle})$.

iii. $\varphi \in Aut(Q, \overset{1}{\triangle}) \Leftrightarrow \varphi(x \overset{1}{\triangle} y) = \varphi(x) \overset{1}{\triangle} \varphi(y) \Leftrightarrow \varphi(y \cdot xy) = \varphi(y) \cdot \varphi(x)\varphi(y) \Leftrightarrow \varphi \in SAut(Q, \cdot)$.

iv. Следует из ii. и iii.

v. Следует из ii. и того, что $Aut(Q, \overset{1}{\triangle})$ вложима в группу автоморфизмов каждой из указанных групп умножений [6].

Работа выполнена при частичной поддержке ВСНТР АН Молдовы (CSSDT ASM), грант 12.839.08.07F.

Список литературы

1. Гонсалес С., Коусело Е., Марков В. Т., Нечаев А. А. Рекурсивные МДР-коды и рекурсивно дифференцируемые квазигруппы // Дискрет. матем. — 1998. — Т. 10, вып. 2. — С. 3–29.

2. Гонсалес С., Коусело Е., Марков В. Т., Нечаев А. А. Групповые коды и их неассоциативные обобщения // Дискрет. матем. — 2004. — Т. 16, вып. 1. — С. 146–156.

3. Гонсалес С., Коусело Е., Марков В. Т., Нечаев А. А. Параметры рекурсивных МДР-кодов // Дискрет. матем. — 2000. — Т. 12, вып. 4. — С. 3–24.

4. Абашин А. С. Линейные рекурсивные МДР-коды размерностей 2 и 3 // Дискрет. матем. — 2000. — Т. 12, вып. 2. — С. 140–153.

5. Izbash V., Syrbu P. Recursively differentiable quasigroups and complete recursive codes // Commentat. Math. Univ. Carol. — 2004. — V. 45, № 2. — P. 257–263.

6. Щукин К. К. Действие группы на квзигруппе. Учебное пособие по спецкурсу. — Кишинев: КГУ, 1985.

О БУЛЕВЫХ ФУНКЦИЯХ ИЗ ПЕРЕСЕЧЕНИЯ НЕСКОЛЬКИХ СПЕЦИАЛЬНЫХ КЛАССОВ

Ю. В. Таранников (Москва)

Булева функция от n переменных — это отображение из $\mathbf{F}_2^n$ в $\mathbf{F}_2$. Весом $|u|$ набора $u \in \mathbf{F}_2^n$ называется число его ненулевых компонент, а вес $\mathrm{wt}(f)$ функции f — число наборов $u \in \mathbf{F}_2^n$, таких что $f(u) \neq 0$. Функция f называется *уравновешенной,* если $\mathrm{wt}(f) = 2^{n-1}$. *Преобразованием Уолша* булевой функции f называется целочисленная функция над $\mathbf{F}_2^n$, определяемая как $W_f(u) = \sum\limits_{x \in F_2^n} (-1)^{f(x)+<u,x>}$. Для каждого $u \in \mathbf{F}_2^n$ значение $W_f(u)$ называется *коэффициентом*

Уолша. Коэффициенты Уолша называются *спектральными коэффициентами.*

Булева функция называется *платовидной,* если для некоторого натурального c все ее коэффициенты Уолша принадлежат множеству $\{0, \pm 2^c\}$. Если при этом все коэффициенты Уолша не равны 0, то функция называется *бент-функцией.* Нелинейностью $\mathrm{nl}(f)$ функции f называется расстояние от f до класса аффинных функций, выражающееся через коэффициенты Уолша, как хорошо известно, формулой $\mathrm{nl}(f) = 2^{n-1} - \frac{1}{2} \max\limits_{u \in \mathbf{F}_2^n} |W_f(u)|$.

Булева функция f, заданная на $\mathbf{F}_2^n$, называется *корреляционно-иммунной порядка* m, $1 \le m \le n$, $\mathrm{wt}(f') = \mathrm{wt}(f)/2^m$ для любой ее подфункции f' от $n - m$ переменных. Уравновешенная корреляционно-иммунная функция порядка m называется *m-устойчивой.* Спектральная характеризация корреляционно-иммунных функций гласит, что функция f на $\mathbf{F}_2^n$ является корреляционно-иммунной порядка m тогда и только тогда, когда для любого $u \in \mathbf{F}_2^n$, $1 \le |u| \le m$, выполнено $W_f(u) = 0$. Верен также факт, что если f — m-устойчивая, $m \le n - 2$, то все ее коэффициенты Уолша делятся на 2^{m+2}.

Булева функция f на $\mathbf{F}_2^n$ называется *совершенной* (c_0, c_1)-*раскраской* (или (c_0, c_1)-*регулярной*), если 1) для любого набора $x \in \mathbf{F}_2^n$, такого что $f(x) = 0$, мы имеем $|\{y \in F_2^n \,|\, d(x, y) = 1, f(y) = 1\}| = c_0$; 2) для любого набора $x \in \mathbf{F}_2^n$, такого что $f(x) = 1$, мы имеем $|\{y \in F_2^n \,|\, d(x, y) = 1, f(y) = 0\}| = c_1$. Булеву функцию, являющуюся совершенной (c, c)-раскраской, будем называть *совершенной c-раскраской.* Известно, что всякая совершенная (c_0, c_1)-раскраска является корреляционно-иммунной функцией порядка $\frac{c_0 + c_1}{2} - 1$, более того, если для некоторого $u \in \mathbf{F}_2^n$ выполнено $W_f(u) \ne 0$, то $|u| \in \{0, \frac{c_0 + c_1}{2}\}$.

Хорошо известен ряд соотношений между характеристиками булевых функций, причем точное равенство в некоторых соотношениях может достигаться только при принадлежности функции определенным классам. Так, например, для нелинейности m-устойчивой функции от n переменных при $m \le n - 2$ верно $\mathrm{nl}(f) \le 2^{n-1} - 2^{m+1}$, причем если достигается равенство, то $m \ge \frac{n-3}{2}$ и f — платовидная.

Аналогичный факт имеет место и для корреляционно-иммунных функций высокого порядка, под которыми будем понимать корреляционно-иммунные функции от n переменных порядка $m = n - k$, где k — константа. Переменную x_i будем называть линейной для функ-

ции f, если x_i в полиноме Жегалкина функции f присутствует только в единственном слагаемом — собственно x_i. При добавлении к m-устойчивой функции f новой линейной переменной разница между числом ее переменных и порядком устойчивости не изменяется, поэтому линейные переменные m-устойчивой функции не представляют интереса для ее изучения. Ранее я доказал [1], что для любого натурального k существует минимальное $p(k)$, такое что число переменных n у любой $(n-k)$-устойчивой функции, не имеющей линейных переменных, не превосходит $p(k)$. Величина $p(k)$ важна также тем, что число корреляционно-иммунных функций порядка $n-k$ от n переменных при $k = \mathrm{const}$, $n \to \infty$, равно $\Theta(n^{p(k)})$. Для числа $p(k)$ мною [1] были получены неравенства $3 \cdot 2^{k-2} - 2 \le p(k) \le (k-1)2^{k-2}$. Для $k = 4$ точное значение $p(k) = 10$ установил Д. П. Кириенко [2] при помощи компьютерного поиска, он же получил точную формулу для числа корреляционно-иммунных функций порядка $n-4$ [3], "человеческое" доказательство факта $p(4) = 10$ дано А. И. Зверевым [4], впрочем, это доказательство во многом моделирует компьютерный перебор.

В связи с тем, что уже больше 10 лет не было продвижений в оценке $p(k)$ при $k > 4$, стало интересным исследование хотя бы вопроса возможности достижимости верхней оценки в неравенстве $p(k) \le (k-1)2^{k-2}$. Пусть существует функция f, для которой в этом неравенстве достигается точное равенство. Образуем для этой функции f матрицу M, выписав по ее строкам каждый набор $u \in \mathbf{F}_2^n$ в точности $\frac{W_f^2(u)}{4^{n-k+2}}$ раз. По спектральным свойствам корреляционно-иммунных функций [1], [2] матрица M содержит 4^{k-2} строк, в каждой из которых не более $k-1$ нулей, и $n = (k-1)2^{k-2}$ столбцов, в каждом из которых не менее 2^{k-2} нулей. Отсюда каждая строка M содержит ровно $k-1$ нулей, и f является совершенной раскраской, а также каждый столбец M содержит ровно 2^{k-2} нулей. Последний факт означает, например, что равны между собой все автокорреляционные коэффициенты на наборах веса 1 (тоже интересное и важное криптографическое свойство). Таким образом, матрица M представляет собой достаточно жесткую комбинаторную структуру, для которой имеют место еще и дополнительные свойства [1, 2], в частности, в любых ее h столбцах, $1 \le h \le k-2$, любая комбинация символов встречается четное число раз, не меньшее 2^{k-h-1} (если вообще встречается). Кроме того, в [4] доказано утверждение, которое на языке гиперграфов можно сформулировать так: если по-

строить гиперграф, вершины которого соответствуют столбцам M, гиперребра — строкам M, так что каждое гиперребро соединяет те и только те вершины, для которых в соответствующих им столбцах стоит 0 на пересечении с рассматриваемой строкой, то гиперграф должен быть связен, не считая изолированных вершин (которые соответствуют линейным переменным и которых, как мы договорились, у функции f нет).

С помощью указанных соображений и дополнительных комбинаторных рассуждений доказана теорема.

Теорема. *При $k \geq 4$ выполнено $p(k) < (k-1)2^{k-2}$.*

Работа выполнена при поддержке гранта РФФИ 10–01–00475.

Список литературы

1. Тарасников Ю. В. О корреляционно-иммунных и устойчивых булевых функциях // Математические вопросы кибернетики. Вып. 11. — М.: Физматлит, 2002. — С. 91–148.

2. Тарасников Ю. В., Кириенко Д. П. Спектральный анализ корреляционно-иммунных функций высокого порядка // Материалы XI Межгосударственной школы-семинара "Синтез и сложность управляющих систем" (Нижний Новгород, 2000). Ч. 2. — М.: МГУ, 2001 — С. 177–189.

3. Кириенко Д. П. О числе корреляционно-иммунных и устойчивых функций порядка $n-4$ // Материалы VIII Международного семинара "Дискретная математика и ее приложения" (2–6 февраля 2004 г.). — М.: Изд-во мех-мат ф-та МГУ, 2004. — С. 421–424.

4. Zverev A. On the structure of the spectrum support of Boolean functions // Boolean functions in cryptology and information security. Proceedings of the NATO Advanced Study Institute on Boolean functions in cryptology and information security (Zvenigorod, 2007). — NATO Science for Peace and Security. Series D: Information and Communication Security. — IOS Press, 2008. — V. 18. — P. 331–340.

О НЕКОТОРЫХ УПАКОВКАХ В БУЛЕВОМ КУБЕ

Р. И. Татаринов (Москва)

В данной работе рассматриваются упаковки конечномерных линейных пространств над $\mathbb{Z}_2$ равными с точностью до параллельного

переноса фигурами. Эта задача естественным образом возникает в теории кодов, исправляющих ошибки.

Введём необходимые обозначения.

Пусть $\mathbb{E}^n$ — булев куб размерности $n \geq 0$, то есть n-мерное линейное пространство над $\mathbb{Z}_2$. На нём можно рассматривать норму Хэмминга $|\cdot|$ и *скалярное произведение* $(x_1, \ldots, x_n) \cdot (y_1, \ldots, y_n) = \sum_{i=1}^{n} x_i \cdot y_i$. Нулевой элемент пространства $\mathbb{E}^n$ обозначим как 0^n; 0^0 — единственный элемент пространства $\mathbb{E}^0$.

Будем считать, что для булевых кубов обычным над $\mathbb{Z}_2$ образом определены *линейные* и *аффинные отображения* и *преобразования* (биекции), а также *сдвиги* (параллельные переносы). В частности, нетривиальные сдвиги относятся к аффинным отображениям, но не к линейным.

Фигурой будем называть любое непустое подмножество булева куба $\mathbb{E}^n$, *0-фигурой* — фигуру, содержащую 0^n, а *несущим пространством* соответствующей 0-фигуры — сам $\mathbb{E}^n$.

Аффинной оболочкой $\langle \mathcal{F} \rangle$ фигуры $\mathcal{F}$ будем называть минимальное содержащее её аффинное подпространство, а *размерностью* фигуры — размерность этого подпространства.

Задача. Расположить в $\mathbb{E}^n$ множество непересекающихся сдвигов исходной фигуры $\mathcal{F}$. Решением или *упаковкой* будем называть множество векторов, осуществляющих эти сдвиги. Если рассматривать лишь линейные решения, получим задачу *линейной упаковки*.

Решение *оптимально*, если оно имеет максимальную мощность среди решений данной задачи для данной фигуры. Назовём *плотной* упаковкой такую, где каждая точка несущего пространства оказывается покрыта. Плотная упаковка всегда оптимальна.

Нетрудно проверить, что после аффинного преобразования фигура и её упаковка переходят также в фигуру и упаковку для последней. К тому же случай фигуры неполной размерности (то есть меньшей, чем размерность несущего пространства), легко свести к случаю полной размерности (см., например, [1]).

Поэтому перед тем, как что-либо предпринимать, мы имеем право привести фигуру в условии к виду «рогатого шара»:

Простым шаром размерности $n \geq 0$ назовём множество

$$\{v \in \mathbb{E}^n \mid |v| \leq 1\}.$$

Рогатый шар — 0-фигура, состоящая из простого шара и ещё каких-либо векторов (*рогов*).

Благодаря известной (см., например, [1]) связи между упаковками и совершенными кодами с расстоянием 3, можно доказать следующую теорему.

Будем называть фигуру $\mathcal{F} \subseteq \mathbb{E}^n$ *регулярной* тогда и только тогда, когда выполнен набор условий:

1) $|\mathcal{F}|$ имеет вид $2^m, m \in \mathbb{Z}_{\geq 0}$;

2) Нет такого $\mathcal{S} \subset \mathcal{F}$, что $|\mathcal{S}| = |\mathcal{F}| - 2 > 0$ и $\sum_{v \in \mathcal{S}} v = 0^n$.

Теорема 1. *Если для фигуры существует плотная упаковка, эта фигура регулярна.*

Регулярность — афинно-инвариантное свойство фигуры, а второе условие из определения регулярности можно записать иначе:

(2′) $|\mathcal{F}| = 2$, либо нет таких $u, v \in \mathcal{F}$, что $u \neq v$ и $\sum_{w \in \mathcal{F}} w = u + v$.

Оказывается, что при фиксированном числе рогов и достаточно большой размерности условие регулярности будет достаточным.

Класс всех рогатых шаров, имеющих ровно k рогов, будем обозначать $\mathbb{B}_k$.

Теорема 2. *Для любого $k \in \mathbb{Z}_{\geq 0}$ множество $\mathbb{B}_k$ содержит лишь конечное число регулярных фигур, не имеющих плотной линейной упаковки. В частности, мощности всех таких фигур меньше $2^{2^{k+1}+2k-2}$.*

Для поиска оптимальных, но не плотных линейных упаковок пригодится следующая пара близких по смыслу понятий, характеризующих близость фигуры к регулярности.

Будем говорить, что фигура $\mathcal{F} \subseteq \mathbb{E}^n$ имеет *формально-регулярное дополнение до размерности $m \in \mathbb{Z}_{\geq 0}$*, если $|\mathcal{F}| \leq 2^m$, и не существует такого $\mathcal{S} \subseteq \mathcal{F}$, что $|\mathcal{S}| = 2^m - 2 > 0$ и $\sum_{v \in \mathcal{S}} v = 0^n$.

Будем говорить, что фигура $\mathcal{F} \subseteq \mathbb{E}^n$ имеет *регулярное дополнение до размерности $m \in \mathbb{Z}_{\geq 0}$*, если $\mathcal{F} \subseteq \mathcal{R} \subseteq \mathbb{E}^n$ для некоторой регулярной $\mathcal{R}$ мощности 2^m.

Заметим, что фигура, имеющая регулярное дополнение до размерности m, имеет также формально-регулярное дополнение до этой размерности, причём оба эти свойства аффинно-инвариантны.

Линейная задача оптимальной упаковки очень естественно сводится к линейной задаче плотной упаковки, что приносит следующий результат (верный как для регулярных, так и для формально-регулярных дополнений):

Теорема 3. *Пусть d — размерность оптимальной линейной упаковки фигуры $\mathcal{F} \subseteq \mathbb{E}^n$. Если $\mathcal{F}$ не имеет (формально-) регулярного дополнения до размерности $\lceil \log_2 |\mathcal{F}| \rceil$, то $d \leq n - \lceil \log_2 |\mathcal{F}| \rceil - 1$, иначе $d \leq n - \lceil \log_2 |\mathcal{F}| \rceil$. Для любого $k \in \mathbb{Z}_{\geq 0}$ для всех элементов $\mathbb{B}_k$,*

кроме конечного их числа, указанные неравенства превращаются в точные равенства.

Заметим, что в теоремах 2 и 3 речь идёт в некотором смысле об одном и том же множестве исключений. Как мы увидим дальше, для низких размерностей это множество пусто.

Теорема 4. *В теоремах* 2 *и* 3 *множество исключений не только конечно, но и пусто при* $k = 0, 1, 2$.

Следствие. *Пусть фигура* $\mathcal{F} \subseteq \mathbb{E}^n$ *является шаром с одним рогом*: h. *Плотная упаковка фигуры* $\mathcal{F}$ *существует тогда и только тогда, когда выполнен набор условий*:

1) n *имеет вид* $2^m - 2, m \in \mathbb{Z}_{\geq 0}$;

2) $|h| \neq n-1, |h| \neq n-2$.

Следствие. *Пусть фигура* $\mathcal{F} \subseteq \mathbb{E}^n$ *является шаром с двумя рогами*: u, v. *Плотная упаковка фигуры* $\mathcal{F}$ *существует тогда и только тогда, когда выполнен набор условий*:

1) n *имеет вид* $2^m - 3, m \in \mathbb{Z}_{\geq 0}$;

2) $|u| < n-1, |v| < n-1$;

3) $|u+v| \neq n-1, |u+v| \neq n-2$.

Список литературы

1. Cohen G., Litsyn S., Vardy A., Gilles Zémor Tilings of binary spaces // SIAM Journal on Discrete Mathematics. — 1996. — V. 9, i. 3. — P. 393–412.

О ДИЗАЙНАХ СПЕЦИАЛЬНОГО ВИДА НА ПОДМНОЖЕСТВАХ БУЛЕВА КУБА

Т. А. Урбанович (Москва)

Системой Штейнера $S(t, k, v)$ называется пара (V, B), где V — произвольное v-элементное множество (называемое носителем), $B \subset 2^V$ — набор k-элементных подмножеств множества V (называемых блоками), и выполнено условие, что для любого t-элементного подмножества множества V существует единственное множество из B, содержащее его.

$S(t,k,v)$ системы Штейнера (V_1,B_1) и (V_2,B_2) называются *изоморфными*, если существует биекция между V_1 и V_2, переводящая B_1 в B_2.

Зафиксируем значения параметров t, k и v следующим образом: $t=2$, $k=4$ и $v=4^h$, где h — произвольное натуральное число. В качестве множества V будем рассматривать произвольное подмножество n-мерного булева куба F_2^n.

Будем говорить, что $S(2,4,4^h)$ система Штейнера (V,B) *обладает свойством* $(*)$, если выполнено условие: $\forall b\in B:\ \sum_{x\in b}x=0$.

Рассмотрим следующую задачу: требуется описать вид 4^h-элементных множеств V (являющихся подмножествами булевых кубов), для которых существует $B\subset 2^V$ такое, что (V,B) — система Штейнера $S(2,4,4^h)$ со свойством $(*)$.

Теорема 1. *Пусть (V,B) — система Штейнера $S(2,4,4^h)$ со свойством $(*)$, тогда для любого V', получающегося из V невырожденным аффиным преобразованием, существует $B'\subset 2^{V'}$ такое, что (V',B') — система Штейнера $S(2,4,4^h)$ со свойством $(*)$.*

Теорема 2. *Пусть $|V|=4^h$ и аффинный ранг V равен $2h$, тогда существует $B\subset 2^V$ такое, что (V,B) — система Штейнера $S(2,4,4^h)$ со свойством $(*)$.*

Теорема 3. *Пусть $|V|=16$ и существует $B\subset 2^V$ такое, что (V,B) — система Штейнера $S(2,4,4^h)$ со свойством $(*)$, тогда множество V аффинно эквивалентно одному из трех множеств:*

$$\langle e_1,e_2,e_3,e_4\rangle,$$

$$\left\{\begin{array}{ccccc} & e_1 & e_2 & e_1+e_2\\ & e_3 & e_4 & e_3+e_4\\ 0 & e_5 & e_1+e_3 & e_1+e_3+e_5\\ & e_2+e_5 & e_1+e_2+e_4 & e_1+e_4+e_5\\ & e_2+e_3+e_5 & e_2+e_3+e_4 & e_4+e_5 \end{array}\right\},$$

$$\left\{\begin{array}{ccccc} & e_1 & e_2 & e_1+e_2\\ & e_3 & e_4 & e_3+e_4\\ 0 & e_5 & e_6 & e_5+e_6\\ & e_1+e_3+e_5 & e_2+e_4+e_5+e_6 & e_1+e_2+e_3+e_4+e_6\\ & e_1+e_4+e_6 & e_2+e_3+e_4+e_5 & e_1+e_2+e_3+e_5+e_6 \end{array}\right\},$$

где e_i — произвольные линейно независимые вектора в булевом кубе.

Таким образом, теорема 3 представляет собой аффинную классификацию систем Штейнера $S(2,4,16)$, обладающих свойством $(*)$.

Приведем две рекуррентные конструкции, позволяющие увеличивать мощность носителя, с сохранением свойств существования или не существования систем Штейнера с данным носителем и свойством $(*)$.

Теорема 4. *Пусть (V,B) — система Штейнера $S(2,4,4^h)$ со свойством $(*)$, тогда для V', имеющего вид*

$$V' = \begin{pmatrix} & 0 & 1 & 0 \\ V & \vdots & \vdots & \vdots \\ & 0 & 1 & 0 \\ & 0 & 1 & 1 \\ V & \vdots & \vdots & \vdots \\ & 0 & 1 & 1 \\ & 1 & 0 & 0 \\ V & \vdots & \vdots & \vdots \\ & 1 & 0 & 0 \\ & 1 & 0 & 1 \\ V & \vdots & \vdots & \vdots \\ & 1 & 0 & 1 \end{pmatrix},$$

существует $B' \subset 2^{V'}$ такое, что (V',B') — система Штейнера $S(2,4,4^h)$ со свойством $(*)$.

Теорема 5. *Пусть для V не существует множества B такого, что (V,B) — система Штейнера $S(2,4,4^h)$ со свойством $(*)$, и V*

не содержит набора из всех единиц. Тогда для V', имеющего вид

$$V' = \begin{pmatrix} & e & 0 & 1 \\ V & \vdots & \vdots & \vdots \\ & e & 0 & 1 \\ & e & 1 & 0 \\ V & \vdots & \vdots & \vdots \\ & e & 1 & 0 \\ e & & 0 & 1 \\ \vdots & V & \vdots & \vdots \\ e & & 0 & 1 \\ e & & 1 & 0 \\ \vdots & V & \vdots & \vdots \\ e & & 1 & 0 \end{pmatrix},$$

где e — вектор, состоящий из всех единиц, не существует $B' \subset 2^{V'}$ такого, что (V', B') — система Штейнера $S(2, 4, 4^h)$ со свойством $(*)$.

Теорема 6. *Если в условиях теорем 4 и 5 множество V является носителем спектра платовидной функции, то множество V' так же им является.*

Список литературы

1. Colbourn C., Dinitz J. Handbook of combinatorial designs. Second Edition. — Chapman and Hall/CRC, 2006.

СУЩЕСТВЕННАЯ ЗАВИСИМОСТЬ БЕНТ-ФУНКЦИЙ КАСАМИ ОТ ПРОИЗВЕДЕНИЙ ПЕРЕМЕННЫХ

А. А. Фролова (Новосибирск)

Рассмотрим конечное поле $GF(2^n)$ как векторное пространство размерности n над $GF(2)$. На поле определяется функция *след* следующим образом

$$tr(\beta) = \beta + \beta^2 + \beta^{2^2} + \ldots + \beta^{2^{n-1}},\ \beta \in GF(2^n).$$

Любая булева функция от n переменных представляется как функция из $GF(2^n)$ в $GF(2)$ с помощью следа:

$$f(\beta) = tr(\sum_{j=0}^{2^n-1} a_j \beta^j), \text{ где } a_j \in GF(2^n).$$

Функция, заданная выражением $f(\beta) = tr(\lambda\beta^k)$, называется *мономиальной*. *Бент-функцией* называется максимально нелинейная булева функция от четного числа переменных (см. подробнее [1]).

Булева функция от n переменных (n четное) вида $f(\beta) = tr(\lambda\beta^k)$ называется *булевой функцией Касами*, если $k = 2^{2d} - 2^d + 1$, где НОД$(n, d) = 1$, $0 < d < n$. Булева функция Касами является бент-функцией, если λ не принадлежит множеству $\{\gamma^3 : \gamma \in GF(2^n)\}$ [2].

Производная по направлению $a \in GF(2^n)$ булевой функции f определяется как $D_a f(\beta) = f(\beta) + f(\beta + a)$. Обозначим через $deg(f)$ степень полинома Жегалкина функции f.

Теорема 1. *Пусть f — булева функция Касами от n переменных (n четное, $n \geq 8$), степень функции $deg(f) = t$. Тогда справедливы следующие утверждения*:

(i) при $4 \leq t \leq n/2$, производная $D_{a_1} \dots D_{a_{t-3}} f(\beta)$ тождественно не равна нулю для произвольных линейно независимых векторов $a_1, \dots, a_{t-3} \in GF(2^n)$.

(ii) при $4 \leq t \leq (n+3)/3$, производная $D_{a_1} \dots D_{a_{t-2}} f(\beta)$ тождественно не равна нулю для произвольных линейно независимых векторов $a_1, \dots, a_{t-2} \in GF(2^n)$.

Введем следующее понятие.

Булеву функцию назовем *k-существенно зависимой*, если для любого произведения из k различных переменных в полиноме Жегалкина функции найдется моном, содержащий это произведение. Наибольшее число k, для которого функция является k-существенно зависимой, назовем *порядком* существенной зависимости функции.

Теорема 2. *Пусть f — булева функция Касами от n переменных (n четное, $n \geq 8$), степень функции $deg(f) = t$. Тогда справедливы следующие утверждения*:

(i) при $4 \leq t \leq n/2$, функция f является $(t-3)$-существенно зависимой.

(ii) при $4 \leq t \leq (n+3)/3$, функция f является $(t-2)$-существенно зависимой.

По результатам непосредственного исследования бент-функций Касами от малого числа переменных и теоремы 2 можно предположить, что порядок данных функций равен $t-2$ при степени функции

равной t ($t \geq 4$). В дальнейшем интересно исследовать, как может измениться порядок существенной зависимости функции под действием на нее аффинного преобразования.

Работа выполнена при поддержке гранта РФФИ (проект 11-01-00997).

Список литературы

1. Токарева Н. Н. Нелинейные булевы функции: бент-функции и их обобщения. — Издательство LAP LAMBERT Academic Publishing (Saarbrucken, Germany), 2011. — ISBN: 978-3-8433-0904-2.

2. Langevin P., Leander G. Monomial bent function and Stickelberger's theorem // Finite Fields and Their Applications. — 2008. — V. 14. — P. 727–742.

СПИСОК ПЛЕНАРНЫХ ДОКЛАДОВ, ПРОЧИТАННЫХ НА СЕМИНАРЕ

А. Б. Угольников (Москва) *О результатах О. Б. Лупанова и его последователей в некоторых задачах теории сложности*

М. П. Минеев, В. Н. Чубариков (Москва) *О новых применениях арифметики в криптографии*

М. М. Глухов (Москва) *О мерах близости булевых функций к линейным функциям*

В. Б. Алексеев (Москва) *О развитии теории дискретных функций на кафедре математической кибернетики*

А. А. Евдокимов (Новосибирск) *Динамические системы дискретных моделей регуляторных контуров генных сетей: анализ и сложность функционирования, восстановление структуры*

С. А. Ложкин (Москва) *Представления булевых функций и асимптотические оценки различной степени точности для сложности их реализации в некоторых классах схем*

Н. П. Долбилин (Москва) *Параллелоэдры: результаты и проблемы*

Н. П. Редькин (Москва) *О сложности индивидуальных булевых функций*

М. А. Федоткин (Нижний Новгород) *Системы управления конфликтными потоками неоднородных требований и принцип Ляпунова — Яблонского*

И. В. Кучеренко (Москва) *Решение проблемы описания границ рекурсивных классов обратимых клеточных автоматов*

В. Н. Шевченко (Нижний Новгород) *Триангуляции выпуклых конусов и реализация их f-векторов*

В. А. Буевич (Москва) *Алгоритмическая неразрешимость задачи Слупецкого для автоматов*

В. Б. Кудрявцев (Москва) *Интеллектуальные системы. Теория и приложения*

В. А. Захаров (Москва) *Модели и алгоритмы в задаче проверки эквивалентности программ*

Н. Ю. Золотых, А. Ю. Чирков (Нижний Новгород) *Сложность расшифровки пороговых функций многозначной логики*

С О Д Е Р Ж А Н И Е

Пленарные доклады

Секция «Синтез, сложность и надежность управляющих систем»

Секция «Функциональные системы»

Секция «Комбинаторный анализ»

Секция «Теория графов»

Секция «Математическая теория интеллектуальных систем»

Секция «Дискретная геометрия»

Секция «Теория кодирования и математические вопросы теории защиты информации»