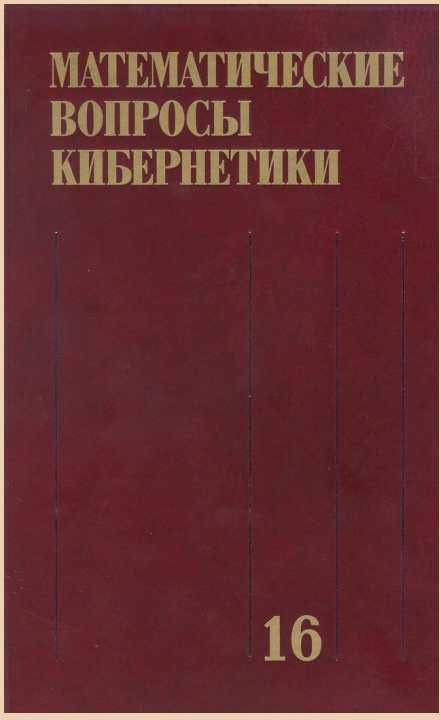
ИПМ им. М.В. Келдыша РАН • Электронная библиотека
Математические вопросы кибернетики • Выпуск 16



**Н. К. Косовский,
Т. М. Косовская**

Полиномиальность и NP-трудность задачи вычисления знака постоянного терма

Рекомендуемая форма библиографической ссылки: Косовский Н. К., Косовская Т. М. Полиномиальность и NP-трудность задачи вычисления знака постоянного терма // Математические вопросы кибернетики. Вып. 16. — М.: ФИЗМАТЛИТ, 2007. — С. 125–128. URL: http://library.keldysh.ru/mvk.asp?id=2007-125

ПОЛИНОМИАЛЬНОСТЬ И NP-ТРУДНОСТЬ ЗАДАЧИ ВЫЧИСЛЕНИЯ ЗНАКА ПОСТОЯННОГО ТЕРМА

Н. К. Косовский, Т. М. Косовская

(Санкт-Петербург)

Введение

Приводятся примеры двух различных простых и естественных логико-арифметических сигнатур, вычисление значения постоянных термов в первой из которых полиномиально, а вычисление знака постоянного терма во второй — NP-трудна.

В книге О. Б. Лупанова [3], в частности, доказан в эффект Шеннона для схем из функциональных элементов о том, что почти все булевы функции имеют почти экспоненциальную сложность при реализации их схемами из функциональных элементов. Если для некоторой задачи имеется полиномиальный алгоритм, то сложность реализации схемами из функциональных элементов каждой ее подзадачи ограниченной длины будет полиномиальна (см., например, последнюю теорему главы 2 из [4]). Поэтому дополнительный интерес представляет отделение задач полиномиальной сложности от задач, не являющихся таковыми. NP-трудные задачи (в случае, если P$\neq$NP) не являются полиномиальными [2].

Ниже рассматривается естественная задача вычисления значения знака постоянного терма в двух различных простых и естественных логико-арифметических сигнатурах.

Ниже доказано, что задача вычисления значения знака постоянного терма в сигнатуре $\langle \boldsymbol{N}_2; +, -, \cdot, /, \overline{\&}, \overline{\vee}\rangle$ полиномиальна. В то же время при добавлении в эту сигнатуру функции возведения в квадрат превращает эту же задачу (вычисления знака постоянного терма) в NP-трудную. (Здесь и далее символами $\overline{\&}$, $\overline{\vee}$ обозначаются операции поразрядной конъюнкции и поразрядной дизъюнкции чисел, записанных в двоичной системе счисления, $\boldsymbol{N}_2$ — носитель (множество двоичных записей натуральных чисел).)

Пример сигнатуры, в которой поставленная задача полиномиальна

Пусть M — множество констант.

О п р е д е л е н и е *постоянного терма в сигнатуре* $\langle M;\ f_1,\ \ldots,\ f_m\rangle$.

1. Константа из множества M является постоянным термом в указанной сигнатуре.

2. Если $t_1,\ \ldots,\ t_k$ — постоянные термы, f_i — имя k-местной функции из сигнатуры, то выражение $f_i(t_1,\ \ldots,\ t_k)$ является постоянным термом в указанной сигнатуре.

Т е о р е м а 1. *Пусть имеется конечный список функций* $f_1, \ldots, f_m$, *вычислимых на детерминированной машине Тьюринга за полиномиальное время, причем время вычисления каждой функции* f_j $(j=1,\ldots m)$ *не превосходит* $C\cdot s_j^l$ *(где* s_j *— сумма длин записей аргументов,* C, l *— некоторые константы). И пусть длина записи значения каждой функции не превосходит суммы длин записей ее аргументов.*

Тогда вычисление постоянного терма в сигнатуре $\langle \boldsymbol{N}_2; f_1, \ldots, f_m\rangle$ *осуществимо на детерминированной машине Тьюринга за полиномиальное время.*

Точнее, время вычисления этого терма не превосходит $CLn^l \leqslant Cn^{l+1}$, *где* L *— глубина терма,* n *— длина записи терма,* C *— константа.*

Д о к а з а т е л ь с т в о проведем методом возвратной математической индукции по глубине терма L.

При $L=0$ (т. е. терм является константой) теорема очевидна.

Рассмотрим терм $t=f(t_1, \ldots, t_k)$ глубины L, где $t_1, \ldots, t_k$ — термы глубин $L_1, \ldots, L_k$ соответственно $(L_i<L)$. По индукционному предположению t_i вычисляется не более чем за $CL_in_i^l$ шагов где длина записи t_i равна n_i $(i=1,\ldots,k)$.

Пусть $|S|$ — длина записи слова S, $[t]$ — значение постоянного терма t.

По условию теоремы длина записи значения терма t не превосходит суммы длин записей термов $t_1, \ldots, t_k$. Используя это, дополнительной возвратной математической индукцией по L можно доказать, что

$$|\,[t]\,| \leqslant \sum_{i=1}^{k} |\,[t_i]\,| \leqslant \sum_{i=1}^{k} n_i < n.$$

По индукционному предположению время вычисления терма t_i не превосходит $CL_in_i^l$.

По условию теоремы время вычисления $f([t_1], \ldots, [t_k])$ не превосходит $C(\sum\limits_{i=1}^{k} |[t_i]|)^l \leqslant Cn^l$, а общее время вычисления терма t не превосходит

$$Cn^l + \sum_{i=1}^{k} CL_in_i^l \leqslant Cn^l + C(L-1)\sum_{i=1}^{k} n_i^l \leqslant$$

$$\leqslant Cn^l + C(L-1)(\sum_{i=1}^{k} n_i)^l = Cn^l + C(L-1)n^l = CLn^l.$$

Теорема доказана.

Л е м м а. *Функции сложения, вычитания, умножения, деления (второй аргумент отличен от нуля), поразрядные конъюнкция и дизъюнкция удовлетворяют условию теоремы.*

С л е д с т в и е. *Постоянные термы в сигнатуре* $\langle \boldsymbol{N}_2; +, -, \cdot, /, \overline{\&}, \overline{\vee}\rangle$ *полиномиально вычислимы.*

Пример сигнатуры, в которой поставленная задача NP-трудна

Пусть показатель ^{2} используется для обозначения функции возведения в квадрат.

Т е о р е м а 2. *Задача вычисления знака постоянного терма в сигнатуре* $\langle \boldsymbol{N}_2; +, -, \cdot, /, {}^2, \overline{\&}\rangle$ *является NP-трудной.*

Доказательство. Сведем задачу ВЫПОЛНИМОСТЬ (ВЫП) к рассматриваемой в формулировке теоремы задаче.

Пусть исходными данными для задачи ВЫП являются пропозициональные переменные $x_1, \ldots, x_r$, и простые дизъюнкции $c_1, \ldots, c_m$. Воспользуемся тем, что $2^r = \underbrace{2 \cdot \ldots \cdot 2}_{\text{r раз}}$. Каждой предметной переменной x_i $(i = 1, \ldots, r)$ ставим в соответствие число z_i, кодирующее i-й столбец в списке всех наборов значений переменных $x_1, \ldots, x_r$. Точнее,

$$z_r = \overline{1^{\langle r \rangle} 0^{\langle r \rangle}},$$

а при $i \in [1,\ r-1]$

$$z_i = \overline{1^{\langle p \rangle} 0^{\langle p \rangle}} + 2^{2p} \cdot \overline{1^{\langle p \rangle} 0^{\langle p \rangle}} + \ldots 2^{2pq} \cdot \overline{1^{\langle p \rangle} 0^{\langle p \rangle}} =$$
$$= (2^p - 1) \cdot 2^p \cdot (1 + 2^{2p} + \ldots + 2^{2pq}) = (2^p - 1) \cdot 2^p \cdot \frac{2^{2p(q+1)} - 1}{2^{2p} - 1},$$

где $p = 2^{i-1}$, $q = 2^{r-i} - 1$, $b^{\langle k \rangle}$ — слово, состоящее из букв b, повторенных k раз, $\overline{S}$ — двоичное число, соответствующее слову S, состоящему из двоичных цифр.

Отметим, что экспоненты, появившиеся в формуле, моделируются постоянными термами в заданной сигнатуре. А именно

$$2^p = 2^{2^{i-1}} = (\ldots(2\underbrace{)^2 \ldots)^2}_{\text{i-1 раз}},$$

$$2^{2p} = 2^{2 \cdot 2^{i-1}} = 2^{2^i} = (\ldots(2\underbrace{)^2 \ldots)^2}_{\text{i раз}},$$

$$2^{2p(q+1)} = 2^{2 \cdot 2^{i-1} \cdot 2^{r-i}} = 2^{2^r} = (\ldots(2\underbrace{)^2 \ldots)^2}_{\text{r раз}}.$$

Таким образом, каждой переменной x_i $(i = 1, \ldots, r)$ не более чем за полином шагов от длины записи исходных данных для ВЫП ставится в соответствие постоянный терм, содержащий функцию возведения в квадрат.

Операцией r-поразрядного отрицания $\overline{\neg}$ константы из $\boldsymbol{N}_2$, длина записи которой не превосходит r, будем называть замену всех символов 1 в записи на символ 0, а всех символов 0 (включая ведущие нули, отсутствующие в записи длины r) на символ 1. В арифметической записи $\overline{\neg} a = 2^r - a$, если $|a| \leqslant r$.

Поразрядная дизъюнкция может быть выражена через r-поразрядное отрицание и поразрядную конъюнкцию по обычным формулам, при этом длина записи терма при исключении поразрядной дизъюнкции вырастет линейно.

Истинность всех дизъюнкций $c_1, \ldots, c_m$ хоть на одном наборе значений переменных равносильна тому, что значение постоянного терма, полученного из пропозициональной формулы $c_1 \& \ldots \& c_m$ заменой $\&$ на $\overline{\&}$, $\vee$ на $\overline{\vee}$, $\neg$ на $\overline{\neg}$ и переменных $x_1, \ldots, x_r$ на построенные постоянные термы, больше нуля. Таким образом, задача ВЫП полиномиально сводится к проверке, положительности постоянного терма в сигнатуре $\langle \boldsymbol{N}_2; +, -, \cdot, /, {}^2, \overline{\&} \rangle$. Теорема доказана.

Замечание. Открытым остается вопрос, будет ли NP-трудной задача вычисления знака постоянного терма в сигнатуре $\langle \boldsymbol{N}_2; +, -, \cdot, /, {}^2 \rangle$ (т. е. из сигнатуры в теореме 2 убрана поразрядная логическая операция).

Вычисление значения постоянного терма схемами

Постоянный терм можно задавать схемой вычисления, определенной в [1], при этом сигнатура, в которой построен терм, в [1] называется базисом схемы вычисления. Ниже приведены определения из [1].

Базисом называется конечный набор B функций $Q^k \to Q$, $k \in \{1, 2\}$.

Схемой в базисе B называется последовательность присваиваний $S = s_0, s_1, ..., s_l$. Для любого $i \geqslant 1$ присваивание имеет вид либо $s_i := f_i(s_j, s_k)$, либо $s_i := f_i(s_j)$, где $f_i \in B$, $j, k < i$.

Число $l(S)$ называется *размером* схемы S.

Значение $v(S)$ схемы S определяется индуктивно. Значение $v(S)$ схемы S длины 0 по определению равно 1. Если $s_l := f(s_j, s_k)$, то $v(s_l) = f(v(s_j), v(s_k))$, а если $s_l := f(s_j)$, то $v(s_l) = f(v(s_j))$.

Теорема 3. *Задача определения знака значения схемы вычисления в базисе* $\langle +, -, \cdot, /, {}^2, \overline{\&} \rangle$ *является NP-трудной.*

Замечание. В процессе вычисления по схеме возможно сверхполиномиальное увеличение длины промежуточных результатов, что частично объясняет справедливость теоремы 3.

Доказательство. Отметим, что по всякому постоянному терму t в заданной сигнатуре за полиномиальное время можно построить вычисляющую его схему в том же базисе, длина записи которой не превосходит полинома от длины записи терма t.

Схемами в базисе, содержащем умножение, можно реализовать функцию возведения в квадрат. Так если s_l вычисляет значение терма t, то вычисление терма t^2 будет производить схема, у которой добавлено присваивание $s_{l+1} := s_l \cdot s_l$. То есть при исключении из базиса функции возведения в квадрат размер схемы не изменится, а длина ее записи не превосходит полинома от длины записи исходной схемы.

Таким образом, за полином шагов по всякому постоянному терму t в сигнатуре $\langle \boldsymbol{N}_2; +, -, \cdot, /, {}^2, \overline{\&} \rangle$ можно построить в базисе $\langle +, -, \cdot, /, \overline{\&} \rangle$ схему, вычисляющую его значение, длина записи которой не превосходит полинома от $|t|$.

Если задача проверки знака значения построенной схемы полиномиальна от длины ее записи, то и значение исходного постоянного терма может быть вычислено за полином шагов от длины его записи. Это противоречит теореме 2. Теорема доказана.

Замечание. Открытым остается вопрос о возможности исключения из базиса поразрядной логической операции.

СПИСОК ЛИТЕРАТУРЫ

1. Вялый М. Н., Тарасов С. П. О сложности операций с числами, представленными арифметическими схемами // Дискретные модели в теории управляющих систем: VII Международная конференция, Покровское, 4–6 марта 2006 г.: Труды. — М.: МАКС Пресс, 2006. — С. 82–87.
2. Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи. — М.: Мир, 1982.
3. Лупанов О. Б. Асимптотические оценки сложности управляющих систем. — М.: Изд-во МГУ, 1984.
4. Нигматуллин Р. Г. Сложность булевых функций. — М.: Наука, 1991.

Поступило в редакцию 15 VIII 2006