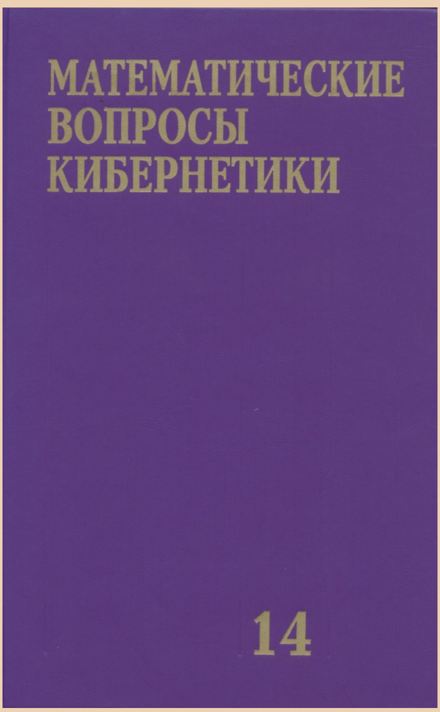

С. С. Марченков,
С. А. Матвеев

Булевы степени, определяемые классами линейных функций и конъюнкций

БУЛЕВЫ СТЕПЕНИ, ОПРЕДЕЛЯЕМЫЕ КЛАССАМИ ЛИНЕЙНЫХ ФУНКЦИЙ И КОНЪЮНКЦИЙ *)

С. С. МАРЧЕНКОВ, С. А. МАТВЕЕВ

(МОСКВА)

§ 1. Введение

Одним из интенсивно развивающихся направлений в теории алгоритмов является теория степеней неразрешимости. Каждая степень неразрешимости представляет собой класс множеств, эквивалентных относительно алгоритмической сводимости некоторого типа. Существует большое число типов алгоритмической сводимости: от сводимости по перечислимости до одно-однозначной сводимости (см. [6, 9]).

В 1974 г. Г. Рейна [5] предложил новый тип алгоритмической сводимости, основанный на простейших алгоритмах — конечных автоматах. Обнаружилось [1, 2, 5, 7, 8], что конечно-автоматная сводимость в значительной степени отличается от известных типов алгоритмической сводимости.

В развитие идеи из [5] в работе [4] было введено понятие булевой сводимости, которую можно трактовать как вариант конечно-автоматной сводимости, когда рассматриваются автоматы с несколькими входами и лишь одним состоянием. В [4] приведены самые общие свойства булевой сводимости и описаны частично упорядоченные множества $\mathscr{L}_Q$ булевых степеней, отвечающие некоторым простым классам Q булевых функций. Строение частично упорядоченных множеств $\mathscr{L}_Q$ в известной мере характеризует способность функций из классов Q «извлекать» информацию из бесконечных двоичных последовательностей.

В данной работе мы продолжаем изучение булевой сводимости. Рассматриваем два нетривиальных замкнутых класса булевых функций: класс L всех линейных функций и класс K_{01} всех конъюнкций, сохраняющих константы 0 и 1 (см. [3]). Этим классам отвечают L- и K_{01}-сводимости, а также частично упорядоченные множества $\mathscr{L}_L$ и $\mathscr{L}_{K_{01}}$ соответствующих степеней. Мы описываем структуру L- и K_{01}-степеней, исследуем степени, определяемые периодическими последовательностями, находим атомы и минимальные элементы множеств $\mathscr{L}_L$, $\mathscr{L}_{K_{01}}$, описываем начальные сегменты частично упорядоченного множества $\mathscr{L}_L$ и решаем вопрос о числе максимальных элементов в $\mathscr{L}_L$ и $\mathscr{L}_{K_{01}}$. В итоге получаем, что частично упорядоченные множества $\mathscr{L}_L$, $\mathscr{L}_{K_{01}}$ обладают существенно различными свойствами и, в частности, не изоморфны.

*) Работа выполнена при частичной финансовой поддержке Российского фонда фундаментальных исследований (проект 03–01–00783).

§ 2. Основные понятия

Пусть $N = \{0, 1, 2, \ldots\}$. Рассматриваем бесконечные двоичные последовательности α, составленные из нулей и единиц, т. е. отображения $\alpha\colon\ N \to \{0, 1\}$. Если $i \in N$, то элемент $\alpha(i)$ последовательности α обозначаем α_i. Таким образом, $\alpha = \alpha_0\alpha_1\ldots$, где $\alpha_i \in \{0, 1\}$ при $i \in N$. Для любого $i \in N$ через $(\alpha)_i$ обозначаем подпоследовательность $\alpha_i\alpha_{i+1}\alpha_{i+2}\ldots$ последовательности α, а через $\mathbf{0}$ и $\mathbf{1}$ — последовательности $00\ldots$ и $11\ldots$

Пусть $f(x_1, \ldots, x_n)$ — булева функция, $\alpha = \alpha_0\alpha_1\ldots$, $\beta = \beta_0\beta_1\ldots$ — двоичные последовательности. Говорим, что функция f *сводит* последовательность α к последовательности β, если существуют такие числа $k, l \in N$, что для любого $i \in N$ выполняется соотношение

$$\alpha_{k+i} = f(\beta_{l+i}, \ldots, \beta_{l+i+n-1}). \tag{1}$$

В случае, когда $k = l = 0$, говорим, что функция f *стандартно сводит* последовательность α к последовательности β. Очевидно, что если функция f сводит последовательность α к последовательности β и выполняется соотношение (1), то функция f стандартно сводит последовательность $(\alpha)_k$ к последовательности $(\beta)_l$.

Пусть Q — множество булевых функций. Говорим, что последовательность α *Q-сводится* к последовательности β (обозначение $\alpha \leqslant_Q \beta$), если множество Q содержит функцию f, которая сводит α к β. Пишем $\alpha <_Q \beta$, если $\alpha \leqslant_Q \beta$ и неверно, что $\beta \leqslant_Q \alpha$. Последовательности α, β называем *Q-эквивалентными*, если $\alpha \leqslant_Q \beta$ и $\beta \leqslant_Q \alpha$. Совокупность всех последовательностей, Q-эквивалентных последовательности α, образует *Q-степень*, порожденную последовательностью α, которую мы обозначаем через $[\alpha]_Q$.

Пусть $\mathscr{L}_Q$ есть множество всех Q-степеней. Отношение $\leqslant_Q$ переносим с последовательностей на Q-степени: если a, b — Q-степени, то полагаем $a \leqslant_Q b$, когда $\alpha \leqslant_Q \beta$ для некоторых последовательностей $\alpha \in a$ и $\beta \in b$.

Для того чтобы Q-степень $[\alpha]_Q$ содержала последовательность α, а отношение $\leqslant_Q$ задавало на множестве $\mathscr{L}_Q$ частичный порядок, необходимо, чтобы отношение $\leqslant_Q$, рассматриваемое на множестве последовательностей, было рефлексивным и транзитивным. Свойство рефлексивности отношения $\leqslant_Q$ обеспечивается тем (см. [4]), что в множество Q включается хотя бы одна из селекторных функций e_j^n $(1 \leqslant j \leqslant n,\ n \geqslant 1)$, где функция e_j^n определяется тождеством

$$e_j^n(x_1, \ldots, x_j, \ldots, x_n) = x_j.$$

Свойство транзитивности отношения $\leqslant_Q$ обеспечивается замкнутостью множества Q относительно операции суперпозиции специального вида — r-суперпозиции (см. [4]). Мы говорим, что функция $h(x_1, \ldots, x_{m+n-1})$ получается из функций $f(x_1, \ldots, x_n)$ и $g(x_1, \ldots, x_m)$ с помощью операции *r-суперпозиции*, если

$$h(x_1, \ldots, x_{m+n-1}) = f(g(x_1, \ldots, x_m), g(x_2, \ldots, x_{m+1}), \ldots, g(x_n, \ldots, x_{m+n-1})).$$

Множество булевых функций, замкнутое относительно операции r-суперпозиции, называется *r-замкнутым*. Всякое множество, замкнутое относительно операции суперпозиции, замкнуто также относительно операции r-суперпозиции. Обратное, вообще говоря, неверно (см. [4]).

§ 3. Класс линейных функций

Обозначим через L класс всех линейных булевых функций. Класс L состоит из всех функций $f(x_1, \ldots, x_n)$, представимых в виде

$$f(x_1, \ldots, x_n) = x_{i_1} \oplus \ldots \oplus x_{i_m} \oplus c, \tag{2}$$

где $1 \leqslant i_1 < i_2 < \ldots < i_m \leqslant n$, $m \geqslant 0$ и $c \in \{0, 1\}$.

Линейную функцию, определенную равенством (2), назовем *нетривиальной*, если $m \geqslant 2$.

Поскольку константные функции 0 и 1 принадлежат классу L, то частично упорядоченное множество $\mathscr{L}_L$ имеет наименьший элемент, который содержит последовательности **0** и **1** (см. [4]).

Доказательство следующей комбинаторной леммы очевидно.

Лемма. *Пусть A — конечный алфавит, α — бесконечная последовательность символов алфавита A, g: $A^n \to A$ и для некоторого $k \in N$ и всех $j \geqslant k$ справедливо равенство*

$$\alpha_{n+j} = g(\alpha_j, \ldots, \alpha_{n+j-1}). \tag{3}$$

Тогда последовательность α является периодической.

Теорема 1. *Последовательность α сводится к себе нетривиальной линейной функцией в том и только том случае, когда α — периодическая последовательность.*

Доказательство. Пусть α — периодическая последовательность с длиной периода d. Тогда α сводится к себе линейной функцией $x_1 \oplus x_{d+1} \oplus \oplus x_{2d+1}$.

Обратно, пусть последовательность α сводится к себе нетривиальной линейной функцией (2). Тогда по определению сводимости найдутся такие числа k, l из N, что для любого $j \geqslant 0$ верно

$$\alpha_{k+j} = \alpha_{l+j+i_1-1} \oplus \ldots \oplus \alpha_{l+j+i_m-1} \oplus c.$$

Поскольку $m \geqslant 2$, множество $\{l + i_1 - 1, \ldots, l + i_m - 1\} \triangle \{k\}$ непусто (здесь $\triangle$ обозначает симметрическую разность множеств). Выберем в нем максимальный элемент h и преобразуем равенство так, чтобы левая часть содержала лишь элемент α_{h+j}. Мы получим рекуррентное соотношение, аналогичное соотношению (3). Для завершения доказательства теоремы остается применить к последовательности α сформулированную выше лемму.

Инверсией последовательности $\alpha_0\alpha_1\ldots$ назовем последовательность $\bar{\alpha}_0\bar{\alpha}_1\ldots$

Следствие 1. *Пусть α — непериодическая последовательность. Тогда L-степень последовательности α состоит в точности из всех последовательностей вида $\beta_0 \ldots \beta_k(\alpha)_l$, где $k, l \in N$ и $\beta_0, \ldots, \beta_k \in \{0, 1\}$, и их инверсий.*

Следствие 2. *Пусть непериодическая последовательность α сводится к последовательности β нетривиальной линейной функцией. Тогда L-степени последовательностей α и β различны.*

Следствие 3. *Для произвольной непериодической последовательности α существуют такие непериодические последовательности β и γ, что $\beta <_L \alpha <_L \gamma$.*

Доказательство. Для всех $i \geqslant 0$ определим элементы последовательности β соотношением $\beta_i = \alpha_i \oplus \alpha_{i+1}$, а элементы последовательности γ — соотношением $\gamma_i = \alpha_0 \oplus \ldots \oplus \alpha_i$. Тогда нетривиальная линейная функция $x_1 \oplus x_2$ будет осуществлять как сводимость β к α, так и сводимость α

к γ, и в силу следствия 2 последовательности β и γ не будут принадлежать L-степени последовательности α.

Непериодичность последовательности γ следует из доказанных в [4] свойств булевой сводимости. Предположим теперь, что последовательность β периодическая с длиной периода p. Легко видеть, что для всех $i \geqslant 0$ справедливо представление $\alpha_{i+1} = \alpha_0 \oplus \beta_0 \oplus \ldots \oplus \beta_i$. В то же время, из периодичности последовательности β вытекает, что для некоторого $k \in N$ и всех $j \geqslant k$ значение суммы $\beta_j \oplus \ldots \oplus \beta_{j+p-1}$ не зависит от выбора j. Следовательно, для всех $j \geqslant k$ выполняется равенство $\beta_j \oplus \ldots \oplus \beta_{j+2p-1} = 0$. Таким образом, последовательность α является периодической с длиной периода $2p$. Полученное противоречие завершает доказательство.

Следствие 4. *В частично упорядоченном множестве $\mathcal{L}_L$ нет максимальных L-степеней, определяемых непериодическими последовательностями.*

Элемент a называется атомом в $\mathcal{L}_L$, если он не является наименьшим в $\mathcal{L}_L$ и из $b <_L a$ следует, что b — наименьший элемент в множестве $\mathcal{L}_L$.

Следствие 5. *В частично упорядоченном множестве $\mathcal{L}_L$ нет атомов, определяемых непериодическими последовательностями.*

Утверждение 1. *Пусть β — периодическая последовательность с периодом $b_1 = \beta_j \ldots \beta_{j+d-1}$ и*

$$b_2 = \beta_{j+1} \ldots \beta_{j+d-1}\beta_j, \ldots, b_d = \beta_{j+d-1}\beta_j \ldots \beta_{j+d-2}.$$

Тогда последовательность α сводится к последовательности β неконстантной линейной функцией в том и только том случае, когда α — периодическая последовательность, период или инверсия периода которой получается покомпонентным сложением по модулю 2 некоторых из слов $b_1, \ldots, b_d$.

Доказательство. Пусть последовательность α сводится к последовательности β неконстантной линейной функцией (2). Тогда существуют такие числа k, $l \in N$, что для любого $i \in N$ выполняется равенство

$$\alpha_{k+i} = \beta_{l+i+i_1-1} \oplus \ldots \oplus \beta_{l+i+i_m-1} \oplus c. \tag{4}$$

Можно считать, что рассматриваются достаточно большие значения i, для которых слово $\beta_{l+i+i_1-1} \ldots \beta_{l+i+i_m-1}$ не пересекается с предпериодом последовательности β. В этом случае при изменении параметра i от некоторого i_0 до i_0+d-1 величина β_{l+i+i_p-1} $(1 \leqslant p \leqslant m)$ принимает последовательно значения всех символов некоторого слова β_s $(1 \leqslant s \leqslant d)$. Иными словами, выполняется равенство

$$\beta_{l+i_0+i_p-1}\beta_{l+i_0+i_p} \ldots \beta_{l+i_0+i_p+d-2} = \beta_{j+s-1} \ldots \beta_{j+d-1}\beta_j \ldots \beta_{j+s-2}.$$

Отсюда согласно равенству (4) заключаем, что α — периодическая последовательность, период (в случае $c=0$) или инверсия периода (в случае $c=1$) которой получается покомпонентным сложением по модулю 2 некоторых из слов $b_1, \ldots, b_d$.

Обратно, пусть α — периодическая последовательность, период (инверсия периода) которой получается покомпонентным сложением слов $b_{i_1}, \ldots, b_{i_m}$. Нетрудно видеть, что в этом случае последовательность α сводится к последовательности β неконстантной линейной функцией $x_{i_1} \oplus \ldots \oplus x_{i_m}$ (соответственно $x_{i_1} \oplus \ldots \oplus x_{i_m} \oplus 1$). Утверждение доказано.

Следствие 1. *Всякая периодическая последовательность с длиной периода d L-сводится к периодической последовательности α, где $\alpha_{di} = 1$ при $i \in N$ и $\alpha_j = 0$ в остальных случаях.*

Заметим, что если α и β — периодические последовательности с минимальными длинами периодов d_1, d_2 и $\alpha \leqslant_L \beta$, то d_1 делит d_2, поскольку, в силу утверждения 1, для сводимости α к β необходимо, чтобы число d_2 являлось длиной периода последовательности α.

Следствие 2. *Пусть α, β — такие периодические последовательности с длинами периодов d_1 и d_2, что $\alpha_{d_1 i} = \beta_{d_2 i} = 1$ при $i \in N$ и $\alpha_j = 0, \beta_k = 0$ в остальных случаях. Тогда $\alpha \leqslant_L \beta$ в том и только том случае, когда d_1 делит d_2.*

Доказательство. Необходимость доказана выше. Для доказательства достаточности остается заметить, что если d_1 делит d_2, то число d_2 является длиной периода последовательности α, и последовательность α L-сводится к последовательности β по следствию 1 из утверждения 1.

Следствие 3. *В частично упорядоченном множестве $\mathscr{L}_L$ нет максимальных элементов, определяемых периодическими последовательностями.*

Следствие 4. *В частично упорядоченном множестве $\mathscr{L}_L$ имеется счетное число атомов, определяемых периодическими последовательностями.*

Доказательство. Рассмотрим L-степени, определенные для простых чисел p периодическими последовательностями α^p, где $\alpha^p_{pi} = 1$ при $i \geqslant 0$ и $\alpha^p_j = 0$ в остальных случаях. Начальный сегмент множества $\mathscr{L}_L$, определяемый L-степенью $[\alpha^p]_L$, состоит помимо наименьшего элемента из всех степеней, порождаемых периодическими последовательностями с минимальной длиной периода p. Отсюда следует, что все такие начальные сегменты конечны, а следовательно, каждый из них содержит хотя бы один атом. При этом любые два такие начальные сегменты будут пересекаться только по наименьшему элементу, поскольку последовательности с различными простыми минимальными длинами периодов не могут сводиться друг к другу.

Утверждение 2. *Любая последовательность стандартно сводится неконстантной линейной функцией от n переменных не более чем к 2^{n-1} различным последовательностям.*

Доказательство. Пусть линейная функция (2) стандартно сводит последовательность α к последовательности β. Ограничимся рассмотрением случая $m \geqslant 2$. Согласно определению стандартной сводимости, для всех $j \geqslant 0$ справедливо равенство

$$\alpha_j = \beta_{j+i_1-1} \oplus \ldots \oplus \beta_{j+i_m-1} \oplus c$$

или, в эквивалентной записи,

$$\beta_{j+i_m-1} = \alpha_j \oplus \beta_{j+i_1-1} \oplus \ldots \oplus \beta_{j+i_{m-1}-1} \oplus c. \tag{5}$$

Полученное равенство позволяет определить все элементы последовательности β через элементы последовательности α и элементы $\beta_0, \ldots, \beta_{i_m-2}$, которые можно выбрать $2^{i_m-1} \leqslant 2^{n-1}$ способами.

Следствие. *Если L-степень a не является наименьшей в $\mathscr{L}_L$, то множество всех L-степеней, расположенных в $\mathscr{L}_L$ выше степени a, счетно.*

Доказательство. Согласно [4], степень a содержит лишь счетное число различных последовательностей. Рассмотрим произвольную последовательность $\alpha \in a$. Поскольку степень a не является наименьшей в $\mathscr{L}_L$, последовательность α не может сводиться ни к какой последовательности β константной функцией. В то же время, из утверждения 2 следует, что каждая неконстантная линейная функция сводит α лишь к конечному числу различных последовательностей. Отсюда следует, что множество всех L-степеней, расположенных выше степени a, не более чем счетно. Далее применяем следствие 4 из теоремы 1 и следствие 3 из утверждения 1.

Утверждение 3. *Пусть последовательность α сводится к последовательности β линейной функцией, отличной от константы. Тогда существует алгоритм, позволяющий вычислять элементы последовательности β через элементы последовательности α. Кроме того, если последовательность α периодическая, то и последовательность β периодическая.*

Доказательство. Пусть линейная функция (2) сводит последовательность α к последовательности β. Тогда по определению сводимости существуют такие числа k, l из N, что для любого $j \geqslant 0$ выполнено равенство

$$\alpha_{k+j} = \beta_{l+j+i_1-1} \oplus \ldots \oplus \beta_{l+j+i_m-1} \oplus c.$$

Как и в доказательстве утверждения 2, ограничимся рассмотрением случая $m \geqslant 2$ и перепишем равенство в виде

$$\beta_{l+j+i_m-1} = \alpha_{k+j} \oplus \beta_{l+j+i_1-1} \oplus \ldots \oplus \beta_{l+j+i_{m-1}-1} \oplus c.$$

Из этого равенства видно, что при любом $s \geqslant l + i_m - 1$ элемент β_s последовательности β однозначно определяется элементами $\beta_0, \ldots, \beta_{s-1}$ и $\alpha_{s+k-l-i_m+1}$.

Докажем теперь вторую часть утверждения. Предположим дополнительно, что последовательность α — периодическая с длиной периода p. В целях упрощения обозначений будем, не ограничивая общности рассуждений, считать сводимость стандартной, а последовательность α чисто периодической. В этом случае для элементов последовательности β, начиная с β_{i_m-1}, будет справедливо представление (5).

Рассмотрим последовательность γ пар $\gamma_i = (\alpha_i, \beta_i)$. Из формулы (5) следует, что для всех $i \geqslant i_m - 1$ элемент β_i выражается через элементы $\gamma_{i-i_m+1}, \ldots, \gamma_{i-1}$. В то же время из периодичности последовательности α следует, что для всех $i \geqslant p$ верно $\alpha_i = \alpha_{i-p}$. Таким образом, для всех $i \geqslant r = \max(i_m - 1, p)$ элемент γ_i выражается через элементы $\gamma_{i-r}, \ldots, \gamma_{i-1}$. Применяя теперь к последовательности γ лемму, получим, что последовательность γ, а значит, и последовательность β периодична.

Утверждение 4. *Пусть непериодическая последовательность α сводится к последовательности β неконстантными линейными функциями*

$$x_{i_1} \oplus \ldots \oplus x_{i_k} \oplus c_1 \tag{6}$$

и

$$x_{j_1} \oplus \ldots \oplus x_{j_l} \oplus c_2, \tag{7}$$

где $1 \leqslant i_1 < \ldots < i_k, 1 \leqslant j_1 < \ldots < j_l$. Тогда $k = l$, $c_1 = c_2$ и если $k = l \geqslant 2$, то наборы

$$(i_2 - i_1, i_3 - i_2, \ldots, i_k - i_{k-1}), (j_2 - j_1, j_3 - j_2, \ldots, j_l - j_{l-1}) \tag{8}$$

совпадают.

Доказательство. По определению сводимости найдутся такие числа p, q из N, что для всех $j \geqslant 0$

$$\alpha_{p+j} = \beta_{q+j+i_1-1} \oplus \ldots \oplus \beta_{q+j+i_k-1} \oplus c_1,$$

и такие числа r, s из N, что для всех $j \geqslant 0$

$$\alpha_{r+j} = \beta_{s+j+j_1-1} \oplus \ldots \oplus \beta_{s+j+j_l-1} \oplus c_2.$$

Таким образом, для всех $j \geqslant 0$ будет выполнено равенство

$$\beta_{q+r+j+i_1-1} \oplus \ldots \oplus \beta_{q+r+j+i_k-1} \oplus c_1 = \beta_{s+p+j+j_1-1} \oplus \ldots \oplus \beta_{s+p+j+j_l-1} \oplus c_2. \quad (9)$$

Рассмотрим множество

$$M = \{q+r+i_1-1, \ldots, q+r+i_k-1\} \triangle \triangle \{s+p+j_1-1, \ldots, s+p+j_l-1\}.$$

Если M непусто, то выберем в нем наибольший элемент h и преобразуем равенство (9) так, чтобы левая часть содержала лишь элемент β_{h+j}. Мы получим для последовательности β рекуррентное соотношение, аналогичное соотношению (3). Из леммы будет следовать периодичность последовательности β, что влечет за собой периодичность последовательности α. Противоречие показывает, что множество M пусто.

Из равенства $M = \varnothing$ вытекает, что $k = l$ и

$$q+r+i_1-1 = s+p+j_1-1, \ldots, q+r+i_k-1 = s+p+j_l-1. \quad (10)$$

При $k \geqslant 2$ получим, в частности, что наборы (8) совпадают. Наконец, при выполнении соотношений (10) из равенства (9) следует, что $c_1 = c_2$. Утверждение доказано.

Введем на множестве всех неконстантных линейных функций отношение эквивалентности: функции (6) и (7) будем считать эквивалентными, если либо $k = l = 1$, либо $k = l \geqslant 2$ и наборы (8) совпадают. Множество всех классов эквивалентности неконстантных линейных функций обозначим через L^*.

Для произвольной L-степени a, определенной непериодической последовательностью, положим

$$U_a = \{b \in \mathscr{L}_L \colon b \leqslant_L a, \ b \neq [\mathbf{0}]_L\}.$$

Из утверждения 3 следует, что множество U_a состоит только из L-степеней, определяемых непериодическими последовательностями.

Рассмотрим теперь произвольный класс эквивалентности $M \in L^*$ и пусть функция $f \in M$ сводит непериодическую последовательность β к последовательности α, где $\alpha \in a$. Обозначим через b L-степень последовательности β. Следствие 1 из теоремы 1 и определение эквивалентности функций показывают, что степень b не зависит от выбора функции f в множестве M и последовательности α в степени a. Таким образом, корректно определено отображение φ_a: $L^* \to U_a$, при котором произвольный класс эквивалентности $M \in L^*$ переходит в ту L-степень из U_a, которая содержит последовательности, сводящиеся к последовательностям из a функциями из M.

Следствие 1 из теоремы 1 вместе с утверждением 4 показывают инъективность отображения φ_a. Сюръективность этого отображения следует из определения множества U_a. Таким образом, построенное отображение является биекцией L^* на U_a.

Пусть теперь L-степени b, c принадлежат U_a, причем $b \leqslant_L c$. Выберем произвольные последовательности $\alpha \in a$, $\beta \in b$, $\gamma \in c$. Поскольку $b \in U_a$, то β сводится к α некоторой функцией $f \in \varphi_a^{-1}(b)$. Аналогично, γ сводится к α некоторой функцией $g \in \varphi_a^{-1}(c)$. Кроме того, из $b \in U_c$ следует, что β

сводится к γ некоторой функцией $h \in \varphi_c^{-1}(b)$. В силу транзитивности L-сводимости функция f получается из функций h и g применением операции r-суперпозиции. Легко видеть, что верно и обратное: если $b, c \in U_a$, $\alpha \in a$, $\beta \in b$, $\gamma \in c$, β сводится к α неконстантной линейной функцией f, γ сводится к α неконстантной линейной функцией g и существует неконстантная линейная функция h, для которой f получается из функций h и g применением операции r-суперпозиции, то $b \leqslant_L c$.

Таким образом, для любых двух степеней $b, c \in U_a$ утверждение $b \leqslant_L c$ эквивалентно существованию для любой функции $f \in \varphi_a^{-1}(b)$ и любой функции $g \in \varphi_a^{-1}(c)$ такой неконстантной линейной функции h, что функция f получается из функций h и g применением операции r-суперпозиции. Поскольку множество L^* не зависит от степени a, получаем, что для любых двух L-степеней a и a', определенных непериодическими последовательностями, частично упорядоченные множества $\langle U_a; \leqslant_L\rangle$ и $\langle U_{a'}; \leqslant_L\rangle$ изоморфны.

Из проведенных выше рассуждений следует, что справедливо

Утверждение 5. *Все начальные сегменты частично упорядоченного множества $\mathscr{L}_L$, определенные L-степенями, которые порождаются непериодическими последовательностями, изоморфны.*

Пусть $\langle X; \leqslant\rangle$ — частично упорядоченное множество. Если $a, b \in X$ и $a \leqslant b$, то интервалом $[a, b]$ множества $\langle X; \leqslant\rangle$ называется множество

$$\{c \in X\colon\ a \leqslant c \leqslant b\}.$$

Если любой интервал частичного порядка конечен, то такой частичный порядок будем называть локально конечным.

Утверждение 6. *Частично упорядоченное множество $\langle \mathscr{L}_L \setminus \{[\mathbf{0}]_L\}; \leqslant_L\rangle$ является локально конечным.*

Доказательство. Сужение частичного порядка $\leqslant_L$ на множество всех периодических L-степеней локально конечно в силу утверждения 1. Докажем теперь, что сужение частичного порядка $\leqslant_L$ на множество всех непериодических L-степеней также является локально конечным. Из утверждений 1 и 3 следует, что доказательство утверждения будет тем самым завершено.

Пусть a, b — L-степени, порожденные непериодическими последовательностями, и $a \leqslant_L b$. Интервал $[a, b]$ рассматриваемого частично упорядоченного множества совпадает с множеством $A = \{c \in U_b\colon a \leqslant_L c\}$.

Как показано выше, множество A представляет собой образ при отображении φ_b множества всех классов эквивалентности $M \in L^*$ таких, что произвольная функция f из $\varphi_b^{-1}(a)$ получается с помощью операции r-суперпозиции из подходящей функции $g \in M$ и некоторой неконстантной линейной функции h. Легко показать, однако, что множество всех таких классов M конечно. Действительно, пусть неконстантная линейная функция

$$x_{s_1} \oplus \ldots \oplus x_{s_m} \oplus c_3,$$

где $1 \leqslant s_1 < \ldots < s_m$, получается из неконстантных функций (6) и (7) с помощью операции r-суперпозиции. Тогда выполнено равенство

$$s_m = i_k + j_l - 1.$$

Из равенства следует, что $i_k \leqslant s_m$ и $j_l \leqslant s_m$, поэтому при фиксированном наборе $(s_1, \ldots, s_m, c_3)$ функции (6) и (7) можно выбрать лишь конечным числом способов. Таким образом, для фиксированной функции f' из $\varphi_b^{-1}(a)$ найдется лишь конечное число различных упорядоченных пар неконстантных функций (g', h'), таких что функция f' получается из функций g'

и h' с помощью операции r-суперпозиции. Обозначим эти пары через $(g_1, h_1), \ldots, (g_n, h_n)$. Легко видеть, что каждый класс эквивалентности M, удовлетворяющий сформулированному выше условию, совпадает при некотором i $(1 \leqslant i \leqslant n)$ с классом эквивалентности, порожденным функцией g_i. Утверждение доказано.

Итак, частично упорядоченное множество $\mathscr{L}_L$ имеет наименьший элемент, но не имеет максимальных элементов. Количество атомов в $\mathscr{L}_L$ счетно, каждый из атомов определяется периодической последовательностью. Все начальные сегменты множества $\mathscr{L}_L$, определяемые непериодическими последовательностями, бесконечны и изоморфны. Все интервалы множества $\mathscr{L}_L$, не содержащие наименьший элемент, конечны. Наконец, выше любого не наименьшего элемента в $\mathscr{L}_L$ расположено счетное число элементов.

§ 4. Класс конъюнкций, сохраняющих константы 0 и 1

Обозначим через K_{01} замкнутый класс, состоящий из всех конъюнкций, которые сохраняют константы 0 и 1 (см. [3]). Класс K_{01} состоит из всех функций $f(x_1, \ldots, x_n)$, которые представимы в виде

$$f(x_1, \ldots, x_n) = x_{i_1} \cdot \ldots \cdot x_{i_m},$$

где $1 \leqslant i_1 < i_2 < \ldots < i_m \leqslant n$ и $m \geqslant 1$.

Конъюнкцию $x_{i_1} \cdot \ldots \cdot x_{i_m}$ назовем нетривиальной, если $m \geqslant 2$.

Теорема 2. *Последовательность α сводится к себе нетривиальной конъюнкцией в том и только том случае, когда α — периодическая последовательность.*

Доказательство. Пусть α — периодическая последовательность с длиной периода d. Легко видеть, что α сводится к себе нетривиальной конъюнкцией $x_1 x_{d+1}$.

Обратно, предположим, что последовательность α сводится к себе нетривиальной конъюнкцией $x_{i_1} \cdot \ldots \cdot x_{i_m}$. Тогда согласно определению сводимости найдутся такие числа k, l из N, что для любого $j \geqslant 0$ выполняется равенство

$$\alpha_{k+j} = \alpha_{l+j+i_1-1} \cdot \ldots \cdot \alpha_{l+j+i_m-1}. \tag{11}$$

Можно предполагать, что последовательность α содержит бесконечное число единиц, поскольку в противном случае она является периодической. Далее рассмотрим две возможности.

1. $k < l + i_m - 1$.

Пусть h — наименьшее число, для которого $k < l + i_h - 1$. Положим

$$d_h = l + i_h - k - 1, \ldots, d_m = k + i_m - k - 1, \quad d = \text{НОД}(d_h, \ldots, d_m).$$

Если для некоторого j_0 выполняется равенство $\alpha_{k+j_0} = 1$, то из (11), в частности, следует, что

$$\alpha_{l+j_0+i_h-1} = \ldots = \alpha_{l+j_0+i_m-1} = 1. \tag{12}$$

С использованием обозначений $d_h, \ldots, d_m$ равенство (12) можно переписать в виде

$$\alpha_{k+j_0+d_h} = \ldots = \alpha_{k+j_0+d_m} = 1.$$

Применяя это рассуждение к величинам $\alpha_{k+j_0+d_h}, \ldots, \alpha_{k+j_0+d_m}$, равным 1, получим соотношения

$$\alpha_{k+j_0+d_h+d_h} = \alpha_{k+j_0+d_h+d_{h+1}} = \ldots = \alpha_{k+j_0+d_h+d_m} = 1, \ldots$$
$$\ldots, \alpha_{k+j_0+d_m+d_h} = \alpha_{k+j_0+d_m+d_{h+1}} = \ldots = \alpha_{k+j_0+d_m+d_m} = 1.$$

Вообще, рассуждая далее по индукции, придем к выводу, что из условия $\alpha_{k+j_0} = 1$ следует выполнимость равенства $\alpha_q = 1$ для всех q, имеющих вид

$$q = k + j_0 + a_h d_h + \ldots + a_m d_m,$$

где $a_h, \ldots, a_m$ — произвольные числа из N.

Из свойств линейных диофантовых уравнений следует, что суммами вида $a_h d_h + \ldots + a_m d_m$ можно представить, начиная с некоторого числа, все числа, кратные d. Таким образом, существует такое число b_0, что при любом $b \geqslant b_0$ все элементы α_{k+j_0+bd} последовательности α оказываются равными 1.

Если $j_1 \not\equiv j_0 \pmod{d}$ и $\alpha_{k+j_1} = 1$, то элемент α_{k+j_1} будет порождать другую подпоследовательность $\{\alpha_{k+j_1+bd}\}$ последовательности α, все элементы которой также равны 1. Значит, если имеется ровно $r+1$ чисел $j_0, j_1, \ldots, j_r$, попарно не сравнимых по модулю d, для которых

$$\alpha_{k+j_0} = \alpha_{k+j_1} = \ldots = \alpha_{k+j_r} = 1,$$

то, начиная с некоторого числа t, для элементов α_t последовательности α будет выполняться эквивалентность

$$(\alpha_t = 1) \Leftrightarrow (t \equiv k + j_0 \pmod{d} \vee \ldots \vee t \equiv k + j_r \pmod{d}).$$

Отсюда вытекает, что последовательность α является периодической.

2. $k \geqslant l + i_m - 1$.

Рассмотрим сначала случай, когда $k > l + i_m - 1$. Положим

$$d_1 = k - l - i_1 + 1, \ldots, d_m = k - l - i_m + 1, \quad d = \text{НОД}(d_1, \ldots, d_m).$$

Используя обозначения $d_1, \ldots, d_m$, перепишем равенство (11) в виде

$$\alpha_{k+j} = \alpha_{k+j-d_1} \cdot \ldots \cdot \alpha_{k+j-d_m}.$$

Из этого равенства вытекает, в частности, что при $\alpha_{k+j} = 1$ выполняются также равенства

$$\alpha_{k+j-d_1} = \ldots = \alpha_{k+j-d_m} = 1. \tag{13}$$

Применим теперь еще раз утверждение о представлении суммами вида $a_1 d_1 + \ldots + a_m d_m$ всех чисел из N, кратных d, начиная с некоторого. Из него следует, что для всякого $t \geqslant l + i_1 - 1$ найдется такое j_0, что при любом $j \geqslant j_0$ все числа из отрезка $[l + i_1 - 1, \ldots, t]$, сравнимые с $k + j$ по модулю d, представимы в форме

$$k + j - a_1 d_1 - \ldots - a_m d_m,$$

где $a_1, \ldots, a_m \in N$. Используя равенства (13), приходим далее к заключению, что из бесконечности множества единичных элементов α_{k+j}, имеющих сравнимые по модулю d индексы $k + j$, вытекает равенство $\alpha_{k+j} = 1$

для почти всех таких элементов α_{k+j} (т. е. для всех, начиная с некоторого элемента). Это означает, что последовательность α периодическая.

Случай $k = l + i_m - 1$ отличается от случая $k > l + i_m - 1$ тем, что рассматриваются только числа $d_1, \ldots, d_{m-1}$ и соответственно определяется число $d = \text{НОД}(d_1, \ldots, d_{m-1})$. Теорема доказана.

Следствие 1. *Пусть α — непериодическая последовательность. Тогда K_{01}-степень последовательности α состоит в точности из всех последовательностей вида $\beta_0\beta_1\ldots\beta_k(\alpha)_l$, где $k, l \in N$ и $\beta_0, \ldots, \beta_k \in \{0, 1\}$.*

Следствие 2. *Пусть непериодическая последовательность α K_{01}-сводится к последовательности β нетривиальной конъюнкцией. Тогда K_{01}-степени последовательностей α и β различны.*

Следствие 3. *Пусть $d \in N$ и α — непериодическая последовательность, которая обладает следующим свойством: существует такое число i_0, что при любом $i \geqslant i_0$ из соотношений $\alpha_i = 1$, $\alpha_{i+d+1} = 0$ следует, что $\alpha_{i+2d+2} = 0$. Тогда K_{01}-степень последовательности α не максимальна в $\mathscr{L}_{K_{01}}$.*

Доказательство. Заметим сначала, что из непериодичности последовательности α следует существование бесконечного числа значений i, для которых $\alpha_i = 1$ и $\alpha_{i+d+1} = 0$.

Пусть теперь последовательность β получается из последовательности α следующим образом: если $\alpha_i = 1$ и $\alpha_{i+d+1} = \alpha_{i+2d+2} = 0$, то полагаем $\beta_{i+d+1} = 1$. Во всех остальных случаях полагаем $\beta_i = \alpha_i$. Тогда, как нетрудно видеть, последовательность α будет сводиться к последовательности β нетривиальной конъюнкцией x_1x_{d+2}.

Доказательство утверждения 7 аналогично доказательству утверждения 1.

Утверждение 7. *Пусть β — периодическая последовательность с периодом $b_1 = \beta_j\beta_{j+1}\ldots\beta_{j+d-1}$ и*

$$b_2 = \beta_{j+1}\ldots\beta_{j+d-1}\beta_j, \ldots, b_d = \beta_{j+d-1}\beta_j\ldots\beta_{j+d-2}.$$

Тогда последовательность α K_{01}-сводится к последовательности β в том и только том случае, когда α — периодическая последовательность, период которой получается покомпонентной конъюнкцией некоторых из слов $b_1, \ldots, b_d$.

Из утверждения 7 вытекает, например, что при любом $d \geqslant 1$ к периодической последовательности, имеющей период 01^d, K_{01}-сводится любая периодическая последовательность, у которой период имеет длину $d + 1$ и содержит хотя бы один нуль. Кроме того, так же, как в следствии 1 из теоремы 2, для любой периодической последовательности α ее K_{01}-степень состоит в точности из всех (периодических) последовательностей вида $\beta_0\ldots\beta_k(\alpha)_l$, где $k, l \in N$ и $\beta_0, \ldots, \beta_k \in \{0, 1\}$. В самом деле, если b_1 — период последовательности α и слова $b_2, \ldots, b_d$ получены из слова b_1, как это указано в утверждении 7, то, очевидно, $b_2, \ldots, b_d$ — также периоды последовательности α. Период b произвольной последовательности β из $[\alpha]_{K_{01}}$ получается в виде покомпонентной конъюнкции некоторых из слов $b_1, \ldots, b_d$. Если период b отличен от слов $b_1, \ldots, b_d$, то он, в частности, содержит большее число нулей, чем каждое из слов $b_1, \ldots, b_d$. Поэтому из K_{01}-сводимости последовательности α к последовательности β следовало бы, что период последовательности α содержит большее число нулей, чем слово b_1. Противоречие показывает, что любая последовательность из $[\alpha]_{K_{01}}$ является периодической с периодом b_1.

Утверждение 8. *Пусть α — периодическая последовательность, содержащая бесконечное число нулей, Q — замкнутый класс бу-*

левых функций и $K_{01} \subseteq Q$. Тогда в частично упорядоченном множестве $\mathcal{L}_Q$ выше элемента $[\alpha]_Q$ расположено континуальное множество элементов. В частности, элемент $[\alpha]_Q$ не максимален в $\mathcal{L}_Q$.

Доказательство. Будем предполагать, что α — чисто периодическая последовательность с периодом $\alpha_0\alpha_1 \ldots \alpha_{d-1}$ и, например, $\alpha_0 = 0$. Рассмотрим последовательность β, которая получается из α заменой некоторых нулевых элементов α_{2id} единицами. Тогда последовательность α будет сводиться к последовательности β конъюнкцией $x_1 x_{d+1}$. Так как последовательностей β с указанным свойством существует континуальное число, а каждая Q-степень состоит из счетного числа последовательностей, приходим к выводу, что в частично упорядоченном множестве $\mathcal{L}_Q$ над элементом $[\alpha]_Q$ имеется еще континуальное множество элементов. Утверждение доказано.

Утверждение 9. *Элементы $[\mathbf{0}]_{K_{01}}$ и $[\mathbf{1}]_{K_{01}}$ являются единственными минимальными элементами в частично упорядоченном множестве $\mathcal{L}_{K_{01}}$.*

Доказательство. Согласно [4, предложение 5] элементы $[\mathbf{0}]_{K_{01}}$ и $[\mathbf{1}]_{K_{01}}$ минимальны в $\mathcal{L}_{K_{01}}$. Если последовательность α содержит конечное число нулей, то, очевидно, $[\alpha]_{K_{01}} = [\mathbf{1}]_{K_{01}}$. Пусть для некоторого m в последовательность α не входит слово 1^m (в этом случае, разумеется, последовательность α содержит бесконечное число нулей). Тогда последовательность $\mathbf{0}$ сводится к последовательности α конъюнкцией $x_1 \cdot \ldots \cdot x_m$. Если же последовательность α содержит бесконечное число нулей и для всякого $m \geqslant 1$ в последовательность α входит слово 1^m, то конъюнкция $x_1 x_2$ сводит к последовательности α такую последовательность с бесконечным числом нулей и бесконечным числом единиц, которая в силу теоремы 2 не может иметь ту же K_{01}-степень, что и последовательность α. Утверждение доказано.

Утверждение 10. *Пусть в последовательность α входит любое двоичное слово. Тогда элемент $[\alpha]_{K_{01}}$ максимален в $\mathcal{L}_{K_{01}}$.*

Доказательство. Рассмотрим нетривиальную конъюнкцию

$$K = x_{i_1} \cdot \ldots \cdot x_{i_m},$$

где $1 \leqslant i_1 < i_2 < \ldots < i_m$ и $m \geqslant 2$. Предположим, что последовательность α стандартно сводится к последовательности β конъюнкцией K. Пусть далее $\alpha_j = 1$. Тогда по условиям сводимости должно быть

$$\beta_{j+i_1-1} = \ldots = \beta_{j+i_m-1} = 1.$$

Если теперь предположить, что $\alpha_{j+i_2-i_1} = 0$, то хотя бы один из элементов

$$\beta_{j+i_2-1}, \beta_{j+i_2+i_2-i_1-1}, \ldots, \beta_{j+i_m+i_2-i_1-1}$$

должен быть равен нулю. Однако $\beta_{j+i_2-1} = 1$. Значит, нулю должен быть равен один из элементов

$$\beta_{j+i_2+i_2-i_1-1}, \ldots, \beta_{j+i_m+i_2-i_1-1}.$$

Исходя из этого, заключаем, что для опровержения (не обязательно стандартной) сводимости последовательности α к какой-либо последовательности β конъюнкцией K достаточно, чтобы в последовательности α содержалось бесконечное число подслов вида

$$1\gamma_1 \ldots \gamma_{i_2-i_1-1} 0 1^{i_m-i_1},$$

где $\gamma_1, \ldots, \gamma_{i_2 - i_1 - 1} \in \{0, 1\}$. Это условие будет заведомо выполнено, если в последовательность α входит любое двоичное слово. Утверждение доказано.

Следствие. *В частично упорядоченном множестве $\mathscr{L}_{K_{01}}$ имеется континуальное число максимальных элементов.*

Утверждение 11. *Пусть последовательность α сводится нетривиальной конъюнкцией к последовательности β, содержащей бесконечное число нулей. Тогда для некоторого $t \in N$ последовательность α содержит бесконечное число слов 01^t0.*

Доказательство. Пусть последовательность α сводится к последовательности β конъюнкцией $x_{i_1} \cdot \ldots \cdot x_{i_m}$, где $1 \leqslant i_1 < i_2 < \ldots < i_m$ и $m \geqslant 2$. Тогда существуют такие $k, l \in N$, что для любого $i \in N$ выполняется равенство

$$\alpha_{k+i} = \beta_{l+i+i_1-1} \cdot \ldots \cdot \beta_{l+i+i_m-1}. \tag{14}$$

Предположим, что $j \geqslant i_m - 1$ и $\beta_{l+j} = 0$. Тогда из (14) следует, что

$$\alpha_{k+j-i_m+1} = \alpha_{k+j-i_{m-1}+1} = \ldots = \alpha_{k+j-i_1+1} = 0.$$

Поскольку $m \geqslant 2$, это означает, что для некоторого

$$t \leqslant \max\,(i_2 - i_1 - 1, i_3 - i_2 - 1, \ldots, i_m - i_{m-1} - 1)$$

в слово

$$\alpha_{k+j-i_m+1}\alpha_{k+j-i_m} \ldots \alpha_{k+j-i_1+1}$$

входит подслово 01^t0. Учитывая теперь, что последовательность β содержит бесконечное число нулей, приходим к заключению, что последовательность α будет содержать бесконечное число слов 01^t0. Утверждение доказано.

Следствие. *Пусть для любого $t \in N$ в последовательность α входит лишь конечное число слов 01^t0. Тогда элемент $[\alpha]_{K_{01}}$ максимален в частично упорядоченном множестве $\mathscr{L}_{K_{01}}$.*

Нетрудно видеть, что в $\mathscr{L}_{K_{01}}$ имеется континуальное число максимальных элементов, определяемых последовательностями α с указанным в следствии свойством.

Подведем итоги исследования частично упорядоченного множества $\mathscr{L}_{K_{01}}$. Множество $\mathscr{L}_{K_{01}}$ имеет только два минимальных элемента, $[\mathbf{0}]_{K_{01}}$ и $[\mathbf{1}]_{K_{01}}$. Элемент $[\mathbf{1}]_{K_{01}}$, как нетрудно видеть, является также и максимальным в $\mathscr{L}_{K_{01}}$. Над элементом $[\mathbf{0}]_{K_{01}}$ в $\mathscr{L}_{K_{01}}$ расположены все элементы $[\alpha]_{K_{01}}$, где для некоторого m последовательность α не содержит слово 1^m. Вместе с тем верхний конус, определяемый элементом $[\mathbf{0}]_{K_{01}}$ в множестве $\mathscr{L}_{K_{01}}$, состоит только из таких элементов. Чтобы убедиться в этом, достаточно заметить, что для последовательности α, содержащей сколь угодно большие слова, составленные только из единиц, всякая K_{01}-сводящаяся к ней последовательность непременно содержит бесконечное число единиц. Таким образом, максимальные элементы, даваемые утверждением 10, лежат вне упомянутого конуса. Следствия из утверждений 10 и 11 гарантируют существование в множестве $\mathscr{L}_{K_{01}}$ континуального числа максимальных элементов двух различных типов.

В заключение скажем несколько слов о перенесении результатов, полученных в параграфе 4, на другие замкнутые классы булевых функций. Обозначим через K_0, K_1, K замкнутые классы, которые получаются из класса K_{01} добавлением соответственно константы 0, константы 1 и обеих констант 0,1 (см. [3]). Основные результаты данного параграфа без труда переносятся на частично упорядоченные множества $\mathscr{L}_{K_0}$, $\mathscr{L}_{K_1}$ и $\mathscr{L}_K$. Главное отличие состоит в том, что согласно [4] в частично упорядоченных множествах $\mathscr{L}_{K_0}$, $\mathscr{L}_{K_1}$, $\mathscr{L}_K$ появляются наименьшие элементы. Это суть соответственно $[\mathbf{0}]_{K_0}$, $[\mathbf{1}]_{K_1}$ и $[\{\mathbf{0},\mathbf{1}\}]_K$.

По принципу двойственности аналогичные результаты имеют место для замкнутых классов дизъюнкций D_{01}, D_0, D_1 и D.

СПИСОК ЛИТЕРАТУРЫ

1. Байрашева В. Р. Структурные свойства автоматных преобразований // Известия вузов. Математика. — 1988. — № 7. — С. 34–39.
2. Марченков С. С. Конечные начальные сегменты верхней полурешетки конечно-автоматных степеней // Дискретная математика. — 1989. — Т. 1, вып. 3. — С. 96–103.
3. Марченков С. С. Замкнутые классы булевых функций. — М.: Физматлит, 2000.
4. Марченков С. С. Булева сводимость // Дискретная математика. — 2003. — Т. 15, вып. 3. — С. 40–53.
5. Рейна Г. Степени автоматных преобразований // Кибернетический сборник. — 1977. — Вып. 14. — С. 95–106.
6. Роджерс Х. Теория рекурсивных функций и эффективная вычислимость. — М.: Мир, 1972.
7. Соловьев В. Д. Структура распределения информации в бесконечной последовательности // Дискретная математика. — 1996. — Т. 8, вып. 2. — С. 97–107.
8. Gordon H. G. Complete degrees of finite-state transformability // Information and Control. — 1976. — V. 32. — P. 169–187.
9. Soare R. I. Recursively enumerable sets and degrees. — Berlin: Springer-Verlag, 1987.

Поступило в редакцию 22 III 2005