ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Январь—март 2007. Серия 1. Том 14, № 1. 45–69

УДК 519.7

О ГЛУБИНЕ БУЛЕВЫХ ФУНКЦИЙ НАД ПРОИЗВОЛЬНЫМ БЕСКОНЕЧНЫМ БАЗИСОМ*)

О. М. Касим-Заде

Рассматривается реализация булевых функций схемами из функциональных элементов над произвольным бесконечным полным базисом. Под глубиной схемы понимается наибольшее число функциональных элементов, составляющих ориентированную цепь, ведущую от входов схемы к её выходу. Вводится функция Шеннона глубины: при каждом натуральном n её значение $D_B(n)$ равно наименьшей глубине схем, достаточной для реализации над базисом B любой булевой функции от n переменных. Показано, что для любого бесконечного базиса B либо существует константа $\beta \geqslant 1$ такая, что $D_B(n) = \beta$ при всех достаточно больших n, либо существуют целочисленная константа $\gamma \geqslant 2$ и константа δ такие, что $\log_\gamma n \leqslant D_B(n) \leqslant \log_\gamma n + \delta$ при всех n.

Введение

Рассмотрим реализацию булевых функций схемами из функциональных элементов над произвольным фиксированным базисом B. Под *базисом* понимается любое функционально полное множество булевых функций, т. е. такое, что суперпозициями функций этого множества можно реализовать любую булеву функцию. *Глубиной схемы* над базисом B называется наибольшее число функциональных элементов, составляющих ориентированную цепь, ведущую от входов схемы к её выходу. Наименьшая глубина схем над базисом B, реализующих булеву функцию f, называется *глубиной функции* f над базисом B и обозначается через $D_B(f)$. Каждому базису B соответствует *функция Шеннона глубины* $D_B(n)$, определяемая при всех n соотношением $D_B(n) = \max_f D_B(f)$, где

*)Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проект 05–01–00994), программы поддержки ведущих научных школ РФ (проект НШ–5400.2006.1) и программы фундаментальных исследований Отделения математических наук РАН «Алгебраические и комбинаторные методы математической кибернетики» (проект «Синтез и сложность управляющих систем»).

максимум берётся по всем булевым функциям f от n переменных. Подробные определения этих и других используемых понятий см. в [9, 11].

Базис называется *конечным*, если число существенных переменных входящих в него функций ограничено, т. е. существует такое число m, что любая функция этого базиса существенно зависит не более чем от m переменных; в противном случае базис называется *бесконечным*.

Известно [9], что для любого конечного базиса B асимптотика функции Шеннона глубины при $n \to \infty$ имеет вид $D_B(n) = \alpha n + o(n)$, где $\alpha = (\log_2 m)^{-1}$ и m — наибольшее число существенных переменных у функций базиса B.

О поведении функции Шеннона глубины в случае бесконечных базисов до последнего времени было известно мало: асимптотики или порядки роста были установлены лишь для небольшого числа конкретных базисов. При этом во всех известных примерах порядки роста функции Шеннона глубины оказывались равными либо 1 (например, для базиса всех булевых функций или для базиса всех пороговых булевых функций [10]), либо $\log_2 n$ (например, для базиса, состоящего из всех линейных булевых функций и конъюнкции двух переменных [7]).

Вопрос об описании порядков роста функции Шеннона глубины для всех бесконечных базисов долгое время оставался открытым. Этот вопрос решен в [5], где показано, что для любого бесконечного базиса B порядок роста функции Шеннона глубины $D_B(n)$ при $n \to \infty$ равен либо 1, либо $\log_2 n$.

В данной статье этот результат усилен: доказано следующее утверждение.

Теорема 1. *Для любого бесконечного базиса B либо существует константа $\beta \geqslant 1$ такая, что $D_B(n) = \beta$ при всех достаточно больших n, либо существуют целочисленная константа $\gamma \geqslant 2$ и константа δ такие, что $\log_\gamma n \leqslant D_B(n) \leqslant \log_\gamma n + \delta$ при всех n.*

Доказательство теоремы 1 дано ниже в разделах 1–9.

Найдены необходимые и достаточные условия, позволяющие отнести заданный бесконечный базис к одному из двух случаев теоремы 1, и для базисов, относящихся ко второму случаю, указано в явном виде значение константы γ (раздел 9, теорема $1'$).

В разделе 10 рассмотрен вопрос о границах значений постоянной γ, в разделе 11 — вопрос о сравнении базисов с точки зрения глубины функций, в разделе 12 содержатся заключительные замечания.

1. D-функции и множество K

Согласно [4] *D-функцией* называется любая булева функция, принимающая на нулевом наборе значение 0, а на любом наборе, содержащем ровно одну единицу, — значение 1 (в остальном эта функция может быть произвольной).

Лемма 1.1 [4]. *При любом s из любой булевой функции, существенно зависящей от достаточно большого числа переменных, путём подстановки констант 0 и 1, замены некоторых переменных их отрицаниями и, возможно, самой функции её отрицанием, можно получить некоторую D-функцию от s переменных.*

Будем говорить, что множество (последовательность) булевых функций A *реализуется с ограниченной глубиной* над базисом B, если существует такое число d, что над базисом B любую функцию из A можно реализовать схемой глубины не более d.

Над любым базисом константы $0, 1$ и функция отрицания $\bar{x}$ реализуются с ограниченной глубиной. Отсюда следует

Лемма 1.2. *Пусть B — базис, A и C — два множества булевых функций такие, что A реализуется с ограниченной глубиной над B, и все функции множества C получаются из функций множества A путём подстановки констант $0, 1$, замены некоторых переменных их отрицаниями, и, возможно, самих функций их отрицаниями. Тогда C реализуется с ограниченной глубиной над B.*

Последовательность булевых функций $\{g_s\}_{s=1}^{\infty}$ назовём *правильной*, если для любого s функция g_s этой последовательности существенно зависит от s переменных.

При подстановке константы 0 в любую D-функцию от s, $s \geqslant 2$, переменных вместо любой переменной получается D-функция от $s-1$ переменных. Любая D-функция существенно зависит от всех своих переменных. Отсюда и из лемм 1.1 и 1.2 следует

Лемма 1.3. *Над любым бесконечным базисом реализуется с ограниченной глубиной некоторая бесконечная правильная последовательность D-функций.*

Пусть k_n обозначает конъюнкцию n переменных: $k_n = x_1 x_2 \dots x_n$. Через K обозначим множество всех функций k_n $(n = 1, 2, \dots)$.

Лемма 1.4. *Для любого бесконечного базиса B существует константа d_1 такая, что при любом n выполняются неравенства*

$$D_B(k_n) \leqslant D_B(n) \leqslant D_B(k_n) + d_1.$$

Доказательство. Левое неравенство очевидно. Докажем правое. По лемме 1.3 над базисом B реализуется с ограниченной глубиной некоторая правильная последовательность D-функций $\{G_s\}_{s=1}^{\infty}$.

Располагая D-функцией G_s от s переменных, любую булеву функцию f от n переменных, равную единице на s наборах, можно представить в виде $f(x_1,\dots,x_n) = G_s(x_1^{\sigma_{11}}x_2^{\sigma_{12}}\dots x_n^{\sigma_{1n}},\dots,x_1^{\sigma_{s1}}x_2^{\sigma_{s2}}\dots x_n^{\sigma_{sn}})$, где $x_1^{\sigma_{j1}}x_2^{\sigma_{j2}}\dots x_n^{\sigma_{jn}}$ — все различные элементарные конъюнкции, входящие в совершенную дизъюнктивную нормальную форму этой функции:

$$f(x_1,\dots,x_n) = \bigvee_{j=1}^{s} x_1^{\sigma_{j1}}x_2^{\sigma_{j2}}\dots x_n^{\sigma_{jn}},$$

$x^{\sigma} = \bar{x}$ при $\sigma = 0$, $x^{\sigma} = x$ при $\sigma = 1$.

Любая элементарная конъюнкция n переменных получается из конъюнкции k_n заменой некоторых переменных их отрицаниями и потому реализуется схемой глубины не более $D_B(k_n) + D_B(\bar{x})$. Отсюда $D_B(f) \leqslant D_B(k_n) + D_B(\bar{x}) + D_B(G_s)$. Величины $D_B(\bar{x})$ и $D_B(G_s)$ ограничены сверху зависящими только от базиса константами. Следовательно, для любой булевой функции f от n переменных имеем $D_B(f) \leqslant D_B(k_n)+d_1$, где d_1 — некоторая константа, зависящая только от базиса (следует еще учесть, что при $s = 0$ функция f равна константе 0). Лемма 1.4 доказана.

Из последнего утверждения вытекает

Лемма 1.5. *Множество всех булевых функций реализуется с ограниченной глубиной над базисом B тогда и только тогда, когда множество K реализуется с ограниченной глубиной над B.*

Замечание. Из леммы 1.4 вытекает установленная в [5] грубая верхняя оценка функции Шеннона глубины: для любого бесконечного базиса B при $n \to \infty$ выполняется соотношение $D_B(n) = O(\log_2 n)$ (достаточно заметить, что $D_B(k_n) \leqslant D_B(k_2)\lceil \log_2 n \rceil$). Лучшая оценка следует из теоремы 1: для любого бесконечного базиса B существует такая константа δ, что $D_B(n) \leqslant \log_2 n + \delta$ при всех n. При условии сохранения общности результата эта оценка является неулучшаемой с точностью до ограниченного сверху слагаемого.

2. Получение правильной последовательности симметрических D-функций ограниченной глубины

Булева функция называется *симметрической*, если её значение не изменяется при любой перестановке переменных. На всех наборах с одина-

ковым числом единиц симметрическая функция принимает одинаковые значения.

В дальнейшем потребуются два известных утверждения.

Лемма 2.1 [15]. *При любом m из любой булевой функции от достаточно большого числа переменных путём подстановки константы* 0 *вместо некоторых переменных можно получить некоторую симметрическую функцию от m переменных.*

Доказательство этого утверждения см. также в [12].

Следующее утверждение иногда называют леммой Кёнига (оно известно также под названиями: теорема о бесконечном дереве, теорема о веерах, «Endlichkeitslemma»).

Лемма 2.2 [6]. *В любом бесконечном корневом дереве с конечными степенями всех вершин, в котором все дуги ориентированы по направлению к корню, существует хотя бы одна входящая в корень бесконечная ориентированная цепь.*

С использованием этих утверждений устанавливается

Лемма 2.3. *Над любым бесконечным базисом B реализуется с ограниченной глубиной некоторая правильная последовательность симметрических D-функций $\{g_s\}_{s=1}^{\infty}$ такая, что при любом s функция g_s получается из g_{s+1} путём подстановки константы* 0 *вместо последней переменной.*

Доказательство. В соответствии с леммой 1.3 над базисом B реализуется с ограниченной глубиной некоторая бесконечная правильная последовательность D-функций. В силу леммы 2.1 при любом m из подходящей функции этой последовательности путём подстановки константы 0 вместо некоторых переменных можно получить некоторую симметрическую функцию от m переменных. При подстановке константы 0 в любую D-функцию от двух или более переменных снова получается D-функция. Поэтому над B реализуется с ограниченной глубиной некоторая бесконечная правильная последовательность симметрических D-функций.

К множеству функций этой последовательности добавим все функции, получающиеся из функций этой последовательности путём подстановки константы 0 вместо одной или нескольких последних переменных. Среди этих функций есть константа 0. Отбросим её. Полученное множество функций обозначим через H. Множество H бесконечно и состоит только из симметрических D-функций.

На множестве H, как на множестве вершин, построим бесконечный

ориентированный граф, соединяя вершины h' и h'' из H ориентированной от h' к h'' дугой тогда и только тогда, когда функция h'' получается из h' подстановкой константы 0 вместо последней переменной.

Множество H содержит единственную D-функцию от одной переменной: тождественную функцию $g_1 = x$. Из каждой вершины построенного графа, кроме g_1, исходит ровно одна дуга. Поэтому рассматриваемый граф есть дерево с корнем в вершине g_1, в котором все дуги ориентированы по направлению к корню.

В каждую вершину построенного дерева входит не более двух дуг. По лемме 2.2 в этом дереве существует хотя бы одна входящая в корень бесконечная ориентированная цепь. Вершины этой цепи $g_1, g_2, \ldots$, занумерованные в порядке удаления от корня, образуют правильную последовательность симметрических D-функций $\{g_s\}_{s=1}^{\infty}$, в которой при любом s функция g_s получается из g_{s+1} путём подстановки константы 0 вместо последней переменной. По лемме 1.2 эта последовательность реализуется с ограниченной глубиной над базисом B. Лемма 2.3 доказана.

3. Получение множеств K и L_p

Любой симметрической булевой функции g от n переменных соответствует *характеристическое слово* (его называют также *характеристической последовательностью*) этой функции: двоичное слово $\tilde{\pi} = \pi_0\pi_1 \ldots \pi_n$ длины $n+1$, в котором разряд π_i равен значению функции g на наборах с i единицами, $0 \leqslant i \leqslant n$ [8].

Например, если $g = x_1 \oplus x_2 \oplus x_3$, то $\tilde{\pi} = 0101$. Характеристическое слово конъюнкции n переменных k_n имеет вид $\underbrace{0\ldots0}_{n}1$, характеристическое слово конъюнкции отрицаний n переменных $\bar{x}_1 \ldots \bar{x}_n$ имеет вид $1\underbrace{0\ldots0}_{n}$.

Симметрическая функция однозначно определяется своим характеристическим словом. Любое двоичное слово длины $n+1$ является характеристическим словом некоторой симметрической функции от n переменных.

Операциям над симметрическими функциями соответствуют операции над их характеристическими словами.

Если функция g' получена из функции g путём подстановки константы 0 (соответственно 1) вместо последней (или любой другой) переменной, то характеристическое слово $\tilde{\pi}'$ функции g' получается из характеристического слова $\tilde{\pi} = \pi_0\pi_1 \ldots \pi_n$ функции g путём отбрасывания последнего (соответственно начального) разряда, т. е. имеет вид $\tilde{\pi}' = \pi_0\pi_1 \ldots \pi_{n-1}$ (соответственно $\tilde{\pi}' = \pi_1\pi_2 \ldots \pi_n$).

Если функция $g = \varphi(g_1, \ldots, g_m)$ получена из симметрических функций $g_1, \ldots, g_m$ от одних и тех же n переменных путём подстановки этих функций в произвольную функцию φ от m переменных, то функция g также является симметрической и её характеристическое слово $\tilde{\pi} = \pi_0\pi_1 \ldots \pi_n$ получается из характеристических слов $\tilde{\pi}_j = \pi_{j0}\pi_{j1} \ldots \pi_{jn}$ функций g_j, $1 \leqslant j \leqslant m$, путём поразрядного применения функции φ, т. е. при любом i имеет место равенство $\pi_i = \varphi(\pi_{1i}, \pi_{2i}, \ldots, \pi_{mi})$.

Наоборот, выполнение описанных операций над словами приводит к соответствующим операциям над функциями.

При любых n, p, a, где $n \geqslant 1$, p — простое и $0 \leqslant a \leqslant p-1$, обозначим через $l_n^{p,a}$ булеву функцию от n переменных, определяемую соотношением

$$l_n^{p,a}(x_1, \ldots, x_n) = \begin{cases} 1, & \text{если } x_1 + \ldots + x_n \equiv a \,(\mathrm{mod}\ p), \\ 0 & \text{в противном случае,} \end{cases}$$

— *элементарную периодическую* симметрическую функцию с периодом p и начальным сдвигом a (см. [8]). Характеристическое слово функции $l_n^{p,a}$ имеет вид

$$\underbrace{0\ldots0}_{a}1\underbrace{0\ldots0}_{p-1}1\underbrace{0\ldots0}_{p-1}1\ldots\underbrace{0\ldots0}_{p-1}1\underbrace{0\ldots0}_{b},$$

где $b = n - a - p\lfloor (n-a)/p \rfloor$.

Множество всех функций $l_n^{p,a}$ при фиксированном p и всевозможных n, a обозначим через L_p.

Лемма 3.1. *Над любым бесконечным базисом B реализуется с ограниченной глубиной или множество K, или хотя бы одно из множеств L_p (возможно, одновременно).*

Доказательство. В соответствии с леммой 2.3 над базисом B реализуется с ограниченной глубиной некоторая правильная последовательность симметрических D-функций $\{g_s\}_{s=1}^{\infty}$, в которой при любом s функция g_s получается из g_{s+1} путём подстановки константы 0 вместо последней переменной. Фиксируем такую последовательность.

Каждой функции g_s соответствует характеристическое слово $\omega_0\omega_1 \ldots \omega_s$ длины $s+1$. При этом $\omega_0 = 0$, $\omega_1 = 1$ и при любом s слово, соответствующее g_s, служит началом слова, соответствующего g_{s+1}.

Для любого $a \leqslant s$ обозначим через g_s^a функцию от $s-a$ переменных, полученную из g_s путём подстановки константы 1 вместо последних a переменных ($g_s^0 = g_s$). Характеристическое слово функции g_s^a имеет вид $\omega_a\omega_{a+1} \ldots \omega_s$.

Рассмотрим бесконечное слово $\tilde{\omega} = \omega_0\omega_1\omega_2\ldots$ и его бесконечные подслова $\tilde{\omega}^a = \omega_a\omega_{a+1}\omega_{a+2}\ldots$ при всевозможных $a \geqslant 0$ (при этом $\tilde{\omega}^0 = \tilde{\omega}$). Слово $\tilde{\omega}^a$ получается из слова $\tilde{\omega}$ путём отбрасывания a начальных разрядов, т. е. сдвигом влево на a позиций.

Возможны три взаимно исключающих случая:

1. Слово $\tilde{\omega}$ *апериодическое,* т. е. $\tilde{\omega}^a \neq \tilde{\omega}^b$ при любых a и b, $a \neq b$.

При любом n найдутся такие a и b, $a < b$, что в слове $\tilde{\omega}$ подслова $\omega_a\omega_{a+1}\ldots\omega_{a+n-1}$ и $\omega_b\omega_{b+1}\ldots\omega_{b+n-1}$ одинаковой длины n совпадают.

Существует m такое, что $\omega_{a+m} \neq \omega_{b+m}$. Пусть m — наименьшее положительное число с таким свойством. Тогда $m \geqslant n$ и слова $\omega_a\omega_{a+1}\ldots\omega_{a+m}$, $\omega_b\omega_{b+1}\ldots\omega_{b+m}$ длины $m+1$ совпадают во всех разрядах, кроме последнего. Их подслова $\omega_{a+m-n}\omega_{a+m-n+1}\ldots\omega_{a+m}$ и $\omega_{b+m-n}\omega_{b+m-n+1}\ldots\omega_{b+m}$ длины $n+1$ также совпадают во всех разрядах, кроме последнего. Поэтому $g_{a+m}^{a+m-n} \oplus g_{b+m}^{b+m-n} = k_n$.

Число n выбирается произвольно. Отсюда следует, что в рассматриваемом случае над базисом B множество K реализуется с ограниченной глубиной.

2. Слово $\tilde{\omega}$ *периодическое с периодом* 1, т. е. $\tilde{\omega}^a = \tilde{\omega}^{a+1}$ при некотором a. Пусть a — наименьшее число с таким свойством. Тогда $a \geqslant 1$ и слова $\omega_{a-1}\omega_a\ldots\omega_{n+a-1}$, $\omega_a\omega_{a+1}\ldots\omega_{n+a}$ длины $n+1$ совпадают во всех разрядах, кроме первого. Поэтому $g_{a+n-1}^{a-1} \oplus g_{a+n}^{a} = \bar{x}_1\ldots\bar{x}_n$. Таким образом, в рассматриваемом случае над базисом B множество всех функций вида $\bar{x}_1\ldots\bar{x}_n$ реализуется с ограниченной глубиной. Отсюда в силу леммы 1.2 следует, что и множество K реализуется с ограниченной глубиной над базисом B.

3. Слово $\tilde{\omega}$ *периодическое с минимальным положительным периодом* T, $T \geqslant 2$, т. е. $\tilde{\omega}^a = \tilde{\omega}^{a+T}$ при некотором a и не существуют такие b и T', что $\tilde{\omega}^b = \tilde{\omega}^{b+T'}$ и $1 \leqslant T' \leqslant T-1$.

Фиксируем произвольную булеву функцию φ от T переменных и применим её поразрядно к словам $\tilde{\omega}^a, \tilde{\omega}^{a+1}, \ldots, \tilde{\omega}^{a+T-1}$, т. е. образуем бесконечное слово $\tilde{\pi} = \pi_0\pi_1\pi_2\ldots$, полагая $\pi_j = \varphi(\omega_{j+a}, \omega_{j+a+1}, \ldots, \omega_{j+a+T-1})$ при любом j.

Слово $\tilde{\pi}$ — *чисто периодическое с периодом* T, т. е. $\pi_i = \pi_{i+T}$ при любом i, и поэтому однозначно определяется своими T начальными разрядами $\pi_0, \pi_1, \ldots, \pi_{T-1}$. Эти разряды являются значениями функции φ на T наборах значений её переменных:

$$\begin{aligned} \pi_0 &= \varphi(\omega_a, \omega_{a+1}, \omega_{a+2}, \ldots, \omega_{a+T-1}), \\ \pi_1 &= \varphi(\omega_{a+1}, \omega_{a+2}, \ldots, \omega_{a+T-1}, \omega_a), \end{aligned}$$

$$\begin{array}{rcl} & \dots & \\ \pi_{T-1} & = & \varphi(\omega_{a+T-1}, \omega_a, \omega_{a+1}, \dots, \omega_{a+T-2}) \end{array}$$

(слово $\tilde{\omega}^a$ является чисто периодическим с периодом T; поэтому все T наборов получаются из первого путём последовательного циклического сдвига на одну позицию влево). Равенство каких-либо двух таких наборов повлекло бы равенство слов $\tilde{\omega}^{a+j}$ и $\tilde{\omega}^{a+k}$ при некоторых j и k, $0 \leqslant j < k \leqslant T-1$, т. е. равенство $\tilde{\omega}^{a+j} = \tilde{\omega}^{a+j+(k-j)}$, где $1 \leqslant k-j \leqslant T-1$. Но это невозможно. Следовательно, все указанные наборы попарно различны. Поэтому при подходящем выборе функции φ разрядам $\pi_0, \pi_1, \dots, \pi_{T-1}$ можно придать любые наперёд заданные значения.

Фиксируем любой простой делитель p числа T и возьмём функцию φ такую, что $\pi_i = 1$ при $i \equiv 0 \,(\mathrm{mod}\, p)$ и $\pi_i = 0$ в противном случае. Тогда $\tilde{\pi} = 1\underbrace{0\dots0}_{p-1}1\underbrace{0\dots0}_{p-1}\dots$ — чисто периодическое слово с периодом p. Отсюда следует, что при любом n имеет место равенство $\varphi(g^a_{n+a}, g^{a+1}_{n+a+1}, \dots, g^{a+T-1}_{n+a+T-1}) = l^{p,0}_n$.

Функция φ фиксирована, её глубина над базисом B не зависит от n. Множество всех функций g^c_s при любых s и c над базисом B реализуется с ограниченной глубиной. Поэтому множество всех функций $l^{p,0}_n$ также реализуется с ограниченной глубиной над B.

Из функций $l^{p,0}_n$ путём подстановки константы 1 получаются все функции множества L_p. Поэтому в силу леммы 1.2 множество L_p реализуется над B с ограниченной глубиной. Лемма 3.1 доказана.

Если над некоторым базисом множество K реализуется с ограниченной глубиной, то в силу леммы 1.5 и множество L_p при любом p реализуется над тем же базисом с ограниченной глубиной. Поэтому из леммы 3.1 вытекает

Лемма 3.2. *Над любым бесконечным базисом B реализуется с ограниченной глубиной хотя бы одно из множеств L_p.*

4. Представление булевых функций многочленами по простому модулю

Обозначим через F_p поле классов вычетов по простому модулю p, т. е. $F_p = \{0, 1, \dots, p-1\}$. Будем рассматривать функции, переменные которых принимают значения в подмножестве $\{0, 1\}$ множества F_p, а сами функции — значения из множества F_p, т. е. функции f вида $f\colon \{0,1\}^n \to F_p$, где n обозначает число переменных функции f. Множество всех таких функций обозначим через R^n_p. Число функций в этом множестве равно p^{2^n}.

Множество R_p^n можно рассматривать как линейное пространство над полем F_p относительно операций сложения функций и умножения функций на элементы поля: для любых функций $f_1, f_2 \in R_p^n$ и любых элементов $a_1, a_2 \in F_p$ функция f, определяемая соотношением

$$f(x_1, \ldots, x_n) \equiv a_1 f_1(x_1, \ldots, x_n) + a_2 f_2(x_1, \ldots, x_n) (\mathrm{mod}\, p)$$

при любых $x_1, \ldots, x_n \in \{0, 1\}$, также принадлежит R_p^n. Размерность линейного пространства R_p^n равна 2^n.

Любая функция f из R_p^n, принимающая значения в множестве $\{0, 1\}$, может рассматриваться как булева функция. В дальнейшем будем считать, что множество всех булевых функций от n переменных погружено описанным образом в R_p^n. Это позволяет ввести для булевых функций каноническое представление в виде многочленов по модулю p с булевыми переменными.

Лемма 4.1 [16]. *При любом простом p любую булеву функцию f от n переменных можно представить, и притом единственным образом, в виде многочлена*

$$f(x_1, \ldots, x_n) \equiv a_0 + \sum_{s=1}^{n} \sum_{1 \leqslant i_1 < \ldots < i_s \leqslant n} a_{i_1 \ldots i_s} x_{i_1} \ldots x_{i_s} \pmod{p} \qquad (1)$$

с коэффициентами a_0, $a_{i_1 \ldots i_s}$ из F_p.

Доказательство. Докажем более сильное утверждение: любую функцию из R_p^n можно представить в указанном виде и притом единственным образом. Для этого достаточно доказать, что система функций 1, $x_{i_1} \ldots x_{i_s}$, где $1 \leqslant s \leqslant n$, $1 \leqslant i_1 < \ldots < i_s \leqslant n$, является базисом линейного пространства R_p^n (здесь понятие базиса употребляется в смысле линейной алгебры).

Число функций в рассматриваемой системе равно 2^n, т. е. совпадает с размерностью пространства R_p^n. Поэтому достаточно доказать, что эта система функций линейно независима в R_p^n.

Рассмотрим произвольную линейную комбинацию

$$a_0 + \sum_{s=1}^{n} \sum_{1 \leqslant i_1 < \ldots < i_s \leqslant n} a_{i_1 \ldots i_s} x_{i_1} \ldots x_{i_s} \pmod{p}$$

с коэффициентами a_0, $a_{i_1 \ldots i_s}$ из F_p, среди которых хотя бы один отличен от нуля. При $x_1 = \ldots = x_n = 0$ рассматриваемая линейная комбинация принимает значение a_0. Поэтому если $a_0 \neq 0$, то линейная комбинация

выражает ненулевую функцию. Если $a_0 = 0$, то среди чисел $s \geqslant 1$ таких, что некоторый коэффициент $a_{i_1 \ldots i_s} \neq 0$, возьмём наименьшее и положим $x_i = 1$ при $i \in \{i_1, \ldots, i_s\}$ и $x_i = 0$ при остальных i. На этом наборе рассматриваемая линейная комбинация принимает значение $a_{i_1 \ldots i_s}$, и следовательно, выражает ненулевую функцию. Таким образом, функции, входящие в рассматриваемую систему, линейно независимы. Лемма 4.1 доказана.

Представление булевой функции f в виде (1) будем называть *p-представлением*.

Для получения p-представления булевой функции достаточно заменить в её совершенной дизъюнктивной нормальной форме все булевы операции арифметическими: дизъюнкцию — сложением, конъюнкцию — умножением, отрицание $\bar{x}$ — арифметической операцией $1 - x$, затем раскрыть скобки и привести подобные члены по модулю p.

Например, сумма по модулю 2 двух переменных $x_1 \oplus x_2$ имеет p-представление $x_1 + x_2 + (p-2)x_1x_2 \pmod p$ при любом p; дизъюнкция двух переменных $x_1 \vee x_2$ имеет p-представление $x_1 + x_2 + (p-1)x_1x_2 \pmod p$ при любом p. Конъюнкция n переменных k_n при любых n и p имеет p-представление $x_1x_2 \ldots x_n \pmod p$.

Для любого простого p назовём *p-степенью* булевой функции f и обозначим через $\deg_p f$ наибольшее число s такое, что в p-представлении функции f хотя бы один из коэфициентов $a_{i_1 \ldots i_s}$ отличен от нуля; если все такие коэффициенты равны нулю, то положим $\deg_p f = 0$.

Величина p-степени булевой функции, вообще говоря, зависит от p. Например, если $f = x_1 \oplus x_2$, то $\deg_2 f = 1$, в то время как $\deg_p f = 2$ при любом $p \geqslant 3$. С другой стороны, существуют функции, p-степень которых не зависит от p. Например, для конъюнкции n переменных k_n при любых n и p имеем $\deg_p k_n = n$.

5. Нижние оценки глубины над базисами ограниченной степени

При любом простом p для любого множества A булевых функций обозначим через $\deg_p A$ наибольшую из p-степеней входящих в A функций; если A содержит функции сколь угодно большой p-степени, то положим $\deg_p A = \infty$. (Для указания на первый случай будет использоваться обозначение $\deg_p A < \infty$.)

Величину $\deg_p A$ будем называть *p-степенью множества A*; если $\deg_p A = \infty$, то будем говорить, что p-степень множества A *бесконечна*.

Лемма 5.1. *Если базис B при некотором p удовлетворяет условию*

$\deg_p B < \infty$, *то для любой булевой функции* f *выполняется неравенство* $\deg_p f \leqslant (\deg_p B)^{D_B(f)}$.

Доказательство проводится индукцией по глубине функций. Базис индукции: функции глубины 0. Глубину 0 имеют тождественные функции x_i и только они. Для них $\deg_p x_i = 1$ и $(\deg_p B)^{D_B(x_i)} = 1$. Базис индукции установлен.

Индуктивный переход: пусть $D_B(f) \geqslant 1$ и пусть утверждение доказано для всех функций глубины не более $D_B(f) - 1$. Докажем его для функции f. Рассмотрим реализующую f схему глубины $D_B(f)$ над базисом B. Функция f реализуется в этой схеме на выходе некоторого функционального элемента. Этому элементу приписана некоторая базисная функция φ от m переменных, на его входы поступают некоторые функции $f_1, \ldots, f_m$, и $f = \varphi(f_1, \ldots, f_m)$. Отсюда следует, что

$$\deg_p f \leqslant \deg_p \varphi \max_{1 \leqslant i \leqslant m} \deg_p f_i \leqslant \deg_p B \max_{1 \leqslant i \leqslant m} \deg_p f_i.$$

При любом i имеем $D_B(f_i) \leqslant D_B(f) - 1$. Поэтому в соответствии с предположением индукции $\deg_p f_i \leqslant (\deg_p B)^{D_B(f_i)} \leqslant (\deg_p B)^{D_B(f)-1}$. Следовательно, $\deg_p f \leqslant (\deg_p B)^{D_B(f)}$. Индуктивный переход обоснован. Лемма 5.1 доказана.

Лемма 5.2. *Для любого базиса* B, *удовлетворяющего при некотором* p *условию* $\deg_p B < \infty$, *выполняется неравенство* $\deg_p B \geqslant 2$.

Доказательство. Действительно, в противном случае, т. е. при $\deg_p B \leqslant 1$, для любой булевой функции f имело бы место неравенство $\deg_p f \leqslant 1$, что, очевидно, неверно. Лемма 5.2 доказана.

Из леммы 5.1 с учётом леммы 5.2 следует

Лемма 5.3. *Если базис* B *при некотором* p *удовлетворяет условию* $\deg_p B < \infty$, *то для любой булевой функции* f, *отличной от констант, выполняется неравенство* $D_B(f) \geqslant \log_\gamma \deg_p f$, *где* $\gamma = \deg_p B$.

6. Классификация бесконечных базисов

Лемма 6.1. *Если множество функций* A *реализуется над базисом* B *с ограниченной глубиной и* $\deg_p A = \infty$, *то* $\deg_p B = \infty$.

Доказательство. Допустим, что, напротив, $\deg_p B < \infty$. Тогда по лемме 5.1 для любой функции f из множества A выполняется неравенство $\deg_p f \leqslant (\deg_p B)^{D_B(f)}$. Но это невозможно, ибо по условию величина $\deg_p f$ может принимать сколь угодно большие значения, в то время как величина $D_B(f)$ ограничена сверху. Лемма 6.1 доказана.

Лемма 6.2. *При любых простых p и q, $p \neq q$, выполняется соотношение* $\deg_q L_p = \infty$.

Доказательство. Рассмотрим функцию $l_n^{p,0}$ при произвольном n. Эта функция симметрическая. Поэтому её q-представление приводится к виду

$$l_n^{p,0}(x_1, \ldots, x_n) \equiv a_0 + \sum_{s=1}^{n} a_s \sum_{1 \leqslant i_1 < \ldots < i_s \leqslant n} x_{i_1} \ldots x_{i_s} \,(\mathrm{mod}\ q)$$

с коэффициентами a_0, a_s из F_q. Полагая $x_1 = \ldots = x_n = 1$, имеем

$$l_n^{p,0}(1, \ldots, 1) \equiv \sum_{s=0}^{n} a_s \binom{n}{s} \,(\mathrm{mod}\ q).$$

Положим $n = q^m$, где m — любое фиксированное натуральное число. Известно (см., например, [3, 6]), что

$$\binom{q^m}{s} \equiv \begin{cases} 1 \,(\mathrm{mod}\ q) & \text{при } s = 0 \text{ и } s = q^m, \\ 0 \,(\mathrm{mod}\ q) & \text{при остальных } s. \end{cases}$$

Отсюда следует, что $l_n^{p,0}(1, \ldots, 1) \equiv a_0 + a_n \,(\mathrm{mod}\ q)$. При этом $a_0 = l_n^{p,0}(0, \ldots, 0) = 1$ и $l_n^{p,0}(1, \ldots, 1) = 0$, ибо $n \not\equiv 0 \,(\mathrm{mod}\ p)$. Следовательно, $a_n \equiv -1 \,(\mathrm{mod}\ q)$, а это означает, что $\deg_q l_n^{p,0} = n$.

Число m выбирается произвольно, поэтому число $n = q^m$ может быть сделано сколь угодно большим. Отсюда вытекает, что в множестве L_p имеются функции сколь угодно большой q-степени, т. е. $\deg_q L_p = \infty$. Лемма 6.2 доказана.

Лемма 6.3. *Если базис B бесконечный, то либо* $\deg_q B = \infty$ *при любом q, либо существует единственное p такое, что* $\deg_p B < \infty$.

Доказательство. В соответствии с леммой 3.2 над базисом B реализуется с ограниченной глубиной множество L_p при некотором p. В силу леммы 6.2 при любом $q \neq p$ выполняется соотношение $\deg_q L_p = \infty$, а потому в силу леммы 6.1 и $\deg_q B = \infty$. Если при этом $\deg_p B = \infty$, то $\deg_q B = \infty$ при любом q. Если же $\deg_p B < \infty$, то такое p единственно. Лемма 6.3 доказана.

Если бесконечный базис B при некотором (и, следовательно, единственном) p удовлетворяет условию $\deg_p B < \infty$, то будем говорить, что B есть базис *конечной характеристики p*. Если $\deg_q B = \infty$ при любом q, то будем говорить, что B — базис *бесконечной характеристики*.

Приведём примеры соответствующих базисов. Добавив к множеству K функцию отрицания $\bar{x}$, получаем пример базиса бесконечной характеристики. Добавив к множеству L_2, состоящему из всех линейных булевых функций, конъюнкцию двух переменных, получаем пример базиса характеристики 2.

При любом $p \geqslant 3$ множество L_p является функционально полным, ибо уже одна функция $l_2^{p,0} = \bar{x}_1\bar{x}_2$ составляет функционально полную систему.

Лемма 6.4. *Равенство* $\deg_p L_p = p - 1$ *справедливо при любом простом* p.

Доказательство. В соответствии с малой теоремой Ферма (см., например, [2]) при любом целом x выполняется соотношение

$$x^{p-1} \equiv \begin{cases} 0 \pmod p, & \text{если } x \equiv 0 \pmod p, \\ 1 \pmod p, & \text{если } x \not\equiv 0 \pmod p. \end{cases}$$

Используя это соотношение, при любых n и a, $0 \leqslant a \leqslant p-1$, функцию $l_n^{p,a}$ можно представить в виде

$$l_n^{p,a}(x_1, \ldots, x_n) \equiv 1 - (x_1 + \ldots + x_n - a)^{p-1} \pmod p.$$

Отсюда вытекает, что $\deg_p l_n^{p,a} \leqslant p-1$. Следовательно, $\deg_p L_p \leqslant p-1$.

При $n = p-1$, $a = 0$ имеем $l_{p-1}^{p,0} = \bar{x}_1\bar{x}_2 \ldots \bar{x}_{p-1}$ и $\deg_p l_{p-1}^{p,0} = p-1$. Поэтому $\deg_p L_p = p-1$. Лемма 6.4 доказана.

Таким образом, при любом $p \geqslant 3$ множество L_p даёт пример базиса характеристики p.

Из доказательства леммы 6.3 вытекает

Лемма 6.5. *Над любым бесконечным базисом характеристики* p *реализуется с ограниченной глубиной множество* L_p *и не реализуется с ограниченной глубиной ни одно из множеств* L_q *при* $q \neq p$.

7. Главные функции и их свойства

Назовём булеву функцию *p-главной*, если p-степень этой функции равна числу её существенных переменных. В дальнейшем, говоря о p-главной функции p-степени s, для краткости будем называть её p-главной функцией *степени* s.

Лемма 7.1. *Пусть* $k \leqslant n$ *и* $\psi_1, \psi_2, \ldots, \psi_k$ *— произвольные фиксированные* p*-главные функции соответственно степени* $1, 2, \ldots, k$. *Тогда*

любую булеву функцию f от n переменных p-степени $\deg_p f \leqslant k$ можно представить единственным образом в виде

$$f(x_1,\ldots,x_n) \equiv b_0 + \sum_{s=1}^{k} \sum_{1\leqslant i_1<\ldots<i_s\leqslant n} b_{i_1\ldots i_s}\psi_s(x_{i_1},\ldots,x_{i_s}) \pmod p \qquad (2)$$

с коэффициентами b_0, $b_{i_1\ldots i_s}$ из F_p.

Доказательство. Обозначим через $R_p^{n,k}$ множество всех булевых функции p-степени не более k от переменных $x_1,\ldots,x_n$. Множество $R_p^{n,k}$ замкнуто относительно сложения и умножения функций на элементы поля F_p, т. е. является линейным подпространством пространства R_p^n. Размерность подпространства $R_p^{n,k}$ равна $\binom{n}{0}+\binom{n}{1}+\ldots+\binom{n}{k}$.

Аналогично тому, как было сделано при доказательстве леммы 4.1, достаточно показать, что система функций 1, $\psi_s(x_{i_1}\ldots x_{i_s})$, где $1\leqslant s\leqslant k$, $1 \leqslant i_1 < \ldots < i_s \leqslant n$, является базисом линейного пространства $R_p^{n,k}$. Число этих функций совпадает с размерностью пространства $R_p^{n,k}$. Поэтому достаточно доказать их линейную независимость в R_p^n.

Рассмотрим произвольную линейную комбинацию

$$b_0 + \sum_{s=1}^{k} \sum_{1\leqslant i_1<\ldots<i_s\leqslant n} b_{i_1\ldots i_s}\psi_s(x_{i_1},\ldots,x_{i_s}) \pmod p$$

с коэффициентами b_0, $b_{i_1\ldots i_s}$ из поля F_p, среди которых хотя бы один отличен от нуля.

Если только один коэффициент b_0 не равен нулю, то рассматриваемая линейная комбинация равна константе b_0 и, следовательно, выражает ненулевую функцию.

Рассмотрим случай, когда хотя бы один из остальных коэффициентов ненулевой. Возьмём наибольшее число $r \geqslant 1$ такое, что некоторый коэффициент $b_{j_1\ldots j_r} \neq 0$. Функция $\psi_r(x_{j_1},\ldots,x_{j_r})$ является p-главной. Поэтому её p-представление имеет вид $\psi_r(x_{j_1},\ldots,x_{j_r}) = ax_{j_1}\ldots x_{j_r} + H$, где a — некоторый элемент из F_p, $a \neq 0$, а H обозначает сумму некоторых одночленов степени не выше $r-1$ (возможно, пустую).

В рассматриваемой линейной комбинации каждую функцию $\psi_s(x_{i_1},\ldots,x_{i_s})$ заменим её p-представлением, раскроем скобки и приведём подобные члены. Получится p-представление функции, выражаемой рассматриваемой линейной комбинацией. Это p-представление содержит одночлен $b_{j_1\ldots j_r}ax_{j_1}\ldots x_{j_r}$ с ненулевым коэффициентом $b_{j_1\ldots j_r}a$

(сократиться с другими одночленами он не может: последние имеют либо меньшую степень, либо, при той же степени, являются произведениями других подмножеств переменных). Следовательно, по лемме 4.1 это p-представление выражает ненулевую функцию. Лемма 7.1 доказана.

Покажем, что из произвольной булевой функции любой данной p-степени подстановкой констант можно получить p-главную функцию той же или любой меньшей степени.

Лемма 7.2. *Если функция p-степени $r \geqslant 2$ не является p-главной, то из неё путём подстановки константы* 0 *вместо некоторых переменных можно получить p-главную функцию степени r.*

Доказательство. Если φ — функция p-степени r, то её p-представление содержит хотя бы один одночлен вида $ax_{i_1} \dots x_{i_r}$, $a \neq 0$. Фиксируем такой одночлен и подставим в функцию φ константу 0 вместо всех переменных x_i при $i \notin \{i_1, \dots, i_r\}$. Тогда φ переходит в p-главную функцию степени r от оставшихся переменных. Лемма 7.2 доказана.

Лемма 7.3. *Из любой p-главной функции степени $r \geqslant 2$ путём подстановки константы* 0 *или* 1 *вместо некоторой переменной можно получить p-главную функцию степени $r - 1$.*

Доказательство. Любая p-главная функция φ степени r имеет p-представление вида

$$\varphi(x_1, \dots, x_n) \equiv ax_1 \dots x_r + a_1 x_2 \dots x_r + \dots + a_i x_1 \dots x_{i-1} x_{i+1} \dots x_r + a_r x_1 \dots x_{r-1} + H \pmod p,$$

где a, $a_1, \dots, a_r$ — некоторые элементы из F_p, причём $a \neq 0$, а H — сумма (возможно, пустая) одночленов степени не выше $r - 2$. Если найдётся i такое, что $a_i \neq 0$, то при подстановке $x_i = 0$ функция φ переходит в p-главную функцию степени $r - 1$ от оставшихся переменных. Если же $a_i = 0$ при всех i, то φ переходит в p-главную функцию степени $r - 1$ при подстановке $x_r = 1$. Лемма 7.3 доказана.

Из лемм 7.2 и 7.3 вытекает

Лемма 7.4. *Из любой булевой функции p-степени $r \geqslant 2$ путём подстановки констант* 0, 1 *вместо некоторых переменных можно получить p-главную функцию любой степени s, $1 \leqslant s \leqslant r - 1$.*

Лемма 7.5. *Если при некотором p множество L_p реализуется с ограниченной глубиной над базисом B, то существует такая константа d_2, что для любых булевых функций f и ψ, удовлетворяющих условию $\deg_p f \leqslant \deg_p \psi$, выполняется неравенство $D_B(f) \leqslant D_B(\psi) + d_2$.*

Доказательство. Для сокращения записи введём обозначение $k = \deg_p f$. Опираясь на лемму 7.4, подстановкой констант 0, 1 из функции ψ получим p-главные функции $\psi_1, \psi_2, \ldots, \psi_k$ соответственно степени $1, 2, \ldots, k$. Используя эти функции, с помощью леммы 7.1 представим функцию f в виде (2).

Обозначим через M сумму всех коэффициентов b_0, $b_{i_1 \ldots i_s}$ в этом представлении, рассматриваемых как целые числа. Возьмём функцию $l_M^{p,1}$ и подставим в неё константу 1 в количестве b_0 экземпляров и всевозможные функции $\psi_s(x_{i_1}, \ldots, x_{i_s})$ из (2) в количестве $b_{i_1 \ldots i_s}$ экземпляров соответственно. Тогда функция f представляется в виде

$$f(x_1, \ldots, x_n) = l_M^{p,1}(1, \ldots, \psi_s(x_{i_1}, \ldots, x_{i_s}), \ldots), \tag{3}$$

где правая часть обозначает результат описанной подстановки (по существу (3) есть лишь другая форма записи (2)).

Глубина над базисом B каждой функции ψ_s не превосходит величины $D_B(\psi) + d_0$, где d_0 обозначает глубину, достаточную для реализации над базисом B констант 0, 1. Отсюда в соответствии с (3) имеем $D_B(f) \leqslant D_B(\psi) + d_0 + D_B(l_M^{p,1})$. Над базисом B множество L_p реализуется с ограниченной глубиной. Поэтому $D_B(f) \leqslant D_B(\psi) + d_2$, где d_2 — некоторая константа, зависящая только от базиса. Лемма 7.5 доказана.

8. Базисы бесконечной характеристики

Теорема 2. *Для любого базиса B бесконечной характеристики существует константа $\beta \geqslant 1$ такая, что $D_B(n) = \beta$ при всех достаточно больших n.*

Доказательство. В силу леммы 3.2 над базисом B реализуется с ограниченной глубиной множество L_p при некотором p. По условию $\deg_p B = \infty$, т. е. базис B содержит функции сколь угодно большой p-степени. Поэтому для любой булевой функции f в базисе найдётся функция ψ, удовлетворяющая условию $\deg_p f \leqslant \deg_p \psi$. В соответствии с леммой 7.5 $D_B(f) \leqslant D_B(\psi) + d_2$, где d_2 — константа, зависящая только от базиса. Учитывая, что $D_B(\psi) = 1$, приходим к заключению, что множество всех булевых функций реализуется над базисом B с ограниченной глубиной.

Таким образом, функция Шеннона глубины $D_B(n)$ при всех n ограничена сверху некоторой константой. Эта функция монотонно неубывающая. Следовательно, при достаточно больших n её значения стабилизируются, т. е. существуют такие константы n_0 и $\beta \geqslant 1$, что $D_B(n) = \beta$ при всех $n \geqslant n_0$. Теорема 2 доказана.

Замечание. Из теоремы 2 и леммы 1.5 вытекает, что над базисом B множество всех булевых функций реализуется с ограниченной глубиной тогда и только тогда, когда B есть базис бесконечной характеристики.

9. Базисы конечной характеристики. Завершение доказательства теоремы 1

Легко проверить, что при бесповторной суперпозиции p-главных функций снова получается p-главная функция. Иными словами, имеет место следующее утверждение.

Лемма 9.1. *Пусть g и h — p-главные булевы функции соответственно степени $r+1$ и k, и пусть функция f от $r+k$ переменных определена соотношением*

$$f = g(h(x_1, \ldots, x_k), x_{k+1}, \ldots, x_{k+r}).$$

Тогда f есть p-главная функция степени $r+k$.

Лемма 9.2. *Пусть g и h — p-главные булевы функции соответственно степени l и k, и пусть функция f от lk переменных определена соотношением*

$$f = g(h(x_1, \ldots, x_k), h(x_{k+1}, \ldots, x_{2k}), \ldots, h(x_{(l-1)k+1}, \ldots, x_{lk})).$$

Тогда f есть p-главная функция степени lk.

Лемма 9.3. *Для любого базиса B характеристики p существует такая константа δ, что для любой булевой функции f, отличной от констант, выполняется неравенство $D_B(f) \leqslant \log_\gamma \deg_p f + \delta$, где $\gamma = \deg_p B$.*

Доказательство. Фиксируем любую функцию ξ p-степени γ из базиса B. Используя лемму 7.4, из функции ξ путём подстановки констант 0, 1 вместо некоторых переменных получим p-главную функцию ξ_1 степени γ.

Построим последовательно функции ξ_t от γ^t переменных, полагая

$$\xi_t = \xi_{t-1}(\xi_1(x_1, \ldots, x_\gamma), \ldots, \xi_1(x_{\gamma^t-\gamma+1}, \ldots, x_{\gamma^t}))$$

при $t = 2, 3, \ldots$ (говоря содержательно, функция ξ_t есть равномерная по глубине бесповторная суперпозиция функций ξ_1 глубины t).

Из леммы 9.2 следует, что при любом t функция ξ_t является p-главной степени γ^t. Кроме того, из построения функций ξ_t видно, что при всех t выполняется соотношение $D_B(\xi_t) \leqslant t + d_0$, где d_0 — глубина, достаточная для реализации над базисом B констант 0, 1.

Положим $t = \lceil \log_\gamma \deg_p f \rceil$. Тогда $\deg_p f \leqslant \deg_p \xi_t$. Воспользуемся леммой 7.5, полагая в ней $\psi = \xi_t$. В соответствии с этой леммой существует зависящая только от базиса константа d_2 такая, что $D_B(f) \leqslant D_B(\xi_t) + d_2$. Отсюда вытекает, что $D_B(f) \leqslant \log_\gamma \deg_p f + \delta$, где δ — некоторая константа, зависящая только от базиса. Лемма 9.3 доказана.

Из лемм 5.3 и 9.3 следует

Теорема 3. *Для любого базиса B характеристики p существует такая константа δ, что для любой булевой функции f, отличной от констант, выполняются неравенства*

$$\log_\gamma \deg_p f \leqslant D_B(f) \leqslant \log_\gamma \deg_p f + \delta,$$

где $\gamma = \deg_p B$.

Теорема 4. *Для любого базиса B характеристики p существует такая константа δ, что при любом n выполняются неравенства*

$$\log_\gamma n \leqslant D_B(n) \leqslant \log_\gamma n + \delta,$$

где $\gamma = \deg_p B$.

Доказательство. Требуемые оценки вытекают из теоремы 3. Верхняя оценка есть следствие очевидного неравенства $\deg_p f \leqslant n$, справедливого при любом p для любой функции f от n переменных (если f — константа, то её глубина над B не превосходит некоторой константы). Для получения нижней оценки в качестве f достаточно взять конъюнкцию n переменных k_n, ибо $\deg_p k_n = n$ при любых p и n. Теорема 4 доказана.

Завершение доказательства теоремы 1. Справедливость утверждения теоремы 1 вытекает непосредственно из теорем 2 и 4 с учётом неравенства $\deg_p B \geqslant 2$, выполненного для любого базиса B характеристики p (лемма 5.2). Теорема 1 доказана.

В действительности доказано даже более сильное утверждение.

Теорема 1′. *Для любого бесконечного базиса B либо существует константа $\beta \geqslant 1$ такая, что $D_B(n) = \beta$ при всех достаточно больших n, либо существуют целочисленная константа $\gamma \geqslant 2$ и константа δ такие, что $\log_\gamma n \leqslant D_B(n) \leqslant \log_\gamma n + \delta$ при всех n. Первый случай имеет место тогда и только тогда, когда B есть базис бесконечной характеристики; второй — когда B есть базис конечной характеристики, причём в последнем случае $\gamma = \deg_p B$, где p — характеристика базиса B.*

10. Границы значений постоянной γ

В соответствии с теоремой $1'$ поведение функции Шеннона глубины $D_B(n)$, отвечающей базису B конечной характеристики, в основном определяется величиной параметра $\gamma = \deg_p B$, где p — характеристика базиса. Возникает вопрос: какие значения может принимать величина γ для базисов характеристики p?

Для базиса B характеристики $p = 2$ величина $\gamma = \deg_2 B$ есть наибольшая из степеней многочленов Жегалкина входящих в этот базис функций. В частности, при любом $m \geqslant 2$ для базиса $L_2 \cup \{k_m\}$ характеристики 2, состоящего из всех линейных булевых функций и конъюнкции m переменных имеет место равенство $\gamma = m$. Отсюда видно, что для базисов характеристики 2 величина γ принимает все значения, удовлетворяющие условию $\gamma \geqslant 2$.

Рассмотрим случай базисов характеристики $p \geqslant 3$. Ответу на поставленный вопрос предпошлём следующее вспомогательное утверждение.

Лемма 10.1. *При любом простом p любая симметрическая булева функция от $p-1$ переменных p-степени не выше $p-2$ равна константе.*

Доказательство. Пусть φ — симметрическая функция от $p-1$ переменных. Приведём её p-представление к виду

$$\varphi(x_1, \ldots, x_{p-1}) \equiv a_0 + \sum_{s=1}^{p-1} a_s \sum_{1 \leqslant i_1 < \ldots < i_s \leqslant p-1} x_{i_1} \ldots x_{i_s} \pmod p$$

с коэффициентами a_0, a_s из F_p. Разряды характеристического слова $\tilde{\pi} = \pi_0 \pi_1 \ldots \pi_{p-1}$ функции φ связаны с коэффициентами её p-представления соотношениями

$$\pi_m \equiv \sum_{s=0}^{m} a_s \binom{m}{s} \pmod p$$

при всех m, $0 \leqslant m \leqslant p-1$.

Покажем, что $\pi_0 + \pi_1 + \ldots + \pi_{p-1} \equiv a_{p-1} \pmod p$. Действительно,

$$\sum_{m=0}^{p-1} \sum_{s=0}^{m} a_s \binom{m}{s} = \sum_{s=0}^{p-1} a_s \sum_{m=s}^{p-1} \binom{m}{s} = \sum_{s=0}^{p-1} a_s \binom{p}{s+1}$$

в силу известного тождества $\sum\limits_{m=s}^{r} \binom{m}{s} = \binom{r+1}{s+1}$, справедливого при любых r и s, $r \geqslant s$ [13]. Остаётся учесть, что $\binom{p}{s+1} \equiv 0 \pmod p$ при $0 \leqslant s \leqslant p-2$ и $\binom{p}{s+1} = 1$ при $s = p-1$.

Если $\deg_p\varphi \leqslant p-2$, то $a_{p-1} \equiv 0 \pmod p$ и, следовательно, $\pi_0 + \pi_1 + \ldots + \pi_{p-1} \equiv 0 \pmod p$. Каждый из разрядов $\pi_0, \pi_1, \ldots, \pi_{p-1}$ равен 0 или 1. Поэтому сумма этих разрядов делится на p тогда и только тогда, когда все они одновременно равны 0 или 1. Но это означает, что функция φ — константа. Лемма 10.1 доказана.

Лемма 10.2. *Для любого базиса B характеристики p выполняется неравенство* $\deg_p B \geqslant p-1$.

Доказательство. Из доказательств лемм 1.3 и 2.3 вытекает, что из некоторой функции базиса B путём подстановки констант $0, 1$, замены некоторых переменных их отрицаниями, и, возможно, самой функции её отрицанием, можно получить симметрическую D-функцию φ от $p-1$ переменных. Так как указанные операции не увеличивают p-степень функции, то $\deg_p\varphi \leqslant \deg_p B$. Функция φ не равна константе. Поэтому в силу леммы 10.1 $\deg_p\varphi \geqslant p-1$. Следовательно, $\deg_p B \geqslant p-1$. Лемма 10.2 доказана.

Из леммы 10.2 следует, что при любом простом $p \geqslant 3$ для любого базиса характеристики p выполняется неравенство $\gamma \geqslant p-1$. Легко проверить, что при любом $m \geqslant p-1$ для базиса $L_p \cup \{k_m\}$ характеристики p имеет место равенство $\gamma = m$. Таким образом, для базисов характеристики $p \geqslant 3$ величина γ принимает все значения, удовлетворяющие условию $\gamma \geqslant p-1$.

Суммируем сказанное выше в виде следующего утверждения.

Теорема 5. *При любом простом p для любого базиса B характеристики p константа $\gamma = deg_p B$ удовлетворяет неравенству* $\gamma \geqslant \max(2, p-1)$, *причём для любого числа m такого, что $m \geqslant \max(2, p-1)$, существует базис характеристики p, для которого имеет место равенство $\gamma = m$.*

11. Сравнение базисов

Базисы B_1 и B_2 назовём *эквивалентными* по глубине, если существуют константы $c_1, c_2 > 0$ такие, что для всех булевых функций f выполняются неравенства $c_2 D_{B_1}(f) \leqslant D_{B_2}(f) \leqslant c_1 D_{B_1}(f)$.

Будем говорить, что базис B_1 *слабее* по глубине базиса B_2, если существует такая константа c_3, что для любой булевой функции f выполняется нервенство $D_{B_2}(f) \leqslant c_3 D_{B_1}(f)$, и базисы B_1 и B_2 не эквивалентны по глубине.

Нетрудно показать, что базисы эквивалентны по глубине тогда и только тогда, когда каждый из них реализуется над другим с ограниченной глубиной. Аналогичным образом, базис B_1 слабее по глубине базиса B_2, если B_1 реализуется над B_2 с ограниченной глубиной, но не наоборот.

Два базиса называются *сравнимыми* по глубине, если они эквивалентны или один из них слабее другого по глубине. В противном случае базисы называются *несравнимыми* по глубине.

Известно [9, 11], что все конечные базисы эквивалентны по глубине. Из теоремы 2 следует, что все бесконечные базисы бесконечной характеристики эквивалентны по глубине. Из теоремы 3 вытекает, что все бесконечные базисы одинаковой конечной характеристики p также эквивалентны по глубине.

Нетрудно показать, что любой конечный базис слабее по глубине любого бесконечного базиса, и что среди бесконечных базисов любой базис конечной характеристики слабее любого базиса бесконечной характеристики.

Лемма 11.1. *При любых простых p и q, $p \neq q$, базисы характеристик p и q несравнимы по глубине.*

Доказательство. Пусть B_1 и B_2 — базисы соответственно характеристик p и q. В соответствии с леммой 6.5 множество L_p реализуется с ограниченной глубиной над базисом B_1, но не реализуется с ограниченной глубиной над B_2. Отсюда вытекает, что базис B_1 не слабее базиса B_2 и не эквивалентен ему по глубине. Аналогичным образом, B_2 не слабее B_1. Следовательно, эти базисы несравнимы по глубине. Лемма 11.1 доказана.

Из сказанного выше и леммы 11.1 вытекает

Теорема 6. *Бесконечные базисы эквивалентны по глубине тогда и только тогда, когда их характеристики одинаковы.*

В разделе 6 указаны примеры бесконечных базисов любой возможной характеристики: базис $K \cup \{\bar{x}\}$ бесконечной характеристики, базис $L_2 \cup \{k_2\}$ характеристики 2, базис L_p характеристики p при произвольном простом $p \geqslant 3$. Добавим к ним конечный базис $\{k_2, \bar{x}\}$. Из теоремы 6 следует

Теорема 7. *Любой базис эквивалентен по глубине одному из счётного числа следующих попарно не эквивалентных базисов*: $\{k_2, \bar{x}\}$, $K \cup \{\bar{x}\}$, $L_2 \cup \{k_2\}$, L_p *при всевозможных простых* $p \geqslant 3$.

Из теоремы 6 и леммы 11.1 вытекает также следующее утверждение, суммирующее большинство результатов данного раздела (по поводу используемых начальных понятий теории решёток см., например, [1]).

Теорема 8. *Отношение эквивалентности базисов по глубине определяет разбиение всей совокупности базисов на следующие классы эквива-*

лентности: *класс* E_0 *всех конечных базисов, класс* E_∞ *всех бесконечных базисов бесконечной характеристики, и для каждого простого числа* p, $p \geqslant 2$, *класс* E_p *всех бесконечных базисов характеристики* p. *Число этих классов счётно. Множество всех классов эквивалентности базисов частично упорядочено по отношению «слабее по глубине»*; *более того, это множество является полной решёткой* (*структурой*) *с наименьшим элементом* E_0, *наибольшим элементом* E_∞ *и счётным множеством заключённых строго между ними попарно не сравнимых элементов* E_p *при всевозможных простых* $p \geqslant 2$.

Описанная в теореме 8 решётка классов эквивалентности базисов по глубине в некотором смысле представляет собой простейшую счётную полную решётку: каждый отличный от минимального и максимального элемент этой решётки является в ней одновременно атомом и коатомом.

12. Заключительные замечания

Рассматриваемая в данной статье задача о глубине булевых функций над бесконечными базисами связана с другими задачами, в частности с задачей о реализации булевых функций схемами над конечными базисами, содержащими элементы с нулевой задержкой [7]. Из результатов работы [7] можно извлечь ряд фактов, касающихся поведения функции Шеннона глубины для бесконечных базисов специального вида, связанных с замкнутыми классами булевых функций. На примере таких базисов уже просматривается общая закономерность: наличие для бесконечных базисов лишь двух различных порядков роста функции Шеннона глубины — константного и логарифмического. Это обстоятельство помогло сформулировать теорему 1. Некоторые вспомогательные утверждения данной статьи, в том числе леммы 5.1, 5.3, 7.1–7.5, 9.2, 9.3, имеют аналоги в [7].

Важные для данной статьи понятия p-представления и p-степени булевой функции введены под другими названиями в работе [16] (см. также [14]) при изучении сложности реализации булевых функций схемами ограниченной глубины над некоторыми специальными бесконечными базисами. Отвлекаясь от несущественных деталей и пользуясь обозначениями данной статьи можно сказать, что фактически в [16] рассматривается реализация функций из множества L_p схемами ограниченной глубины над базисом $K \cup \{\bar{x}\} \cup L_q$ при $q \neq p$. Хотя указанная задача достаточно далека от рассматриваемой в данной статье, знакомство с [16] оказалось полезным.

Выражаю глубокую благодарность В. В. Кочергину, внимательно прочитавшему работу и высказавшему ряд замечаний, способствовавших

улучшению изложения.

ЛИТЕРАТУРА

1. **Биркгоф Г.** Теория решеток. М.: Наука, 1984.
2. **Виноградов И. М.** Основы теории чисел. М.: Наука, 1972.
3. **Гашков С. Б., Чубариков В. Н.** Арифметика. Алгоритмы. Сложность вычислений. М.: Высш. шк., 2000.
4. **Касим-Заде О. М.** Общая верхняя оценка сложности схем в произвольном бесконечном полном базисе // Вестник Московского университета. Серия 1. Математика. Механика. 1997. № 4. С. 59–61.
5. **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.
6. **Кнут Д. Э.** Искусство программирования, том 1. Основные алгоритмы. М.: Издательский дом «Вильямс», 2000.
7. **Ложкин С. А.** Асимптотическое поведение функций Шеннона для задержек схем из функциональных элементов // Математические заметки. 1976. Т. 19, № 6. С. 939–951.
8. **Лупанов О. Б.** К вопросу о реализации симметрических функций алгебры логики контактными схемами // Проблемы кибернетики. Вып. 15. М.: Наука, 1965. С. 85–99.
9. **Лупанов О. Б.** О схемах из функциональных элементов с задержками // Проблемы кибернетики. Вып. 23. М.: Наука, 1970. С. 43–81.
10. **Лупанов О. Б.** О синтезе схем из пороговых элементов // Проблемы кибернетики. Вып. 26. М.: Наука, 1973. С. 109–140.
11. **Сэведж Дж. Э.** Сложность вычислений. М.: Изд-во «Факториал», 1998.
12. **Таранников Ю. В.** О критериях бесконечности инвариантных классов дискретных функций // Математические вопросы кибернетики. Вып. 9. М.: Физматлит, 2000. С. 59–78.
13. **Холл М.** Комбинаторика. М.: Мир, 1970.
14. **Boppana R. B., Sipser M.** The complexity of finite functions // Handbook of Theoretical Computer Science. Vol. A. Algoritms and complexity. Amsterdam: Elsevier, 1990. P. 757–804.
15. **Nešetřil J.** Some nonstandard Ramsey-like applications // Theoret. Computer Science. 1984. V. 34, N 1–2. P. 3–15.

16. Smolensky R. Algebraic methods in the theory of lower bounds for Boolean circuit complexity // Proc. of the 19th Annual ACM Symposium on Theory of Computing (1987). New York: ACM, 1987. P. 77–82.

Адрес автора:

МГУ, мех.-мат. факультет,
Воробьёвы горы,
119992 Москва,
Россия.
E-mail: kasimz@mech.math.msu.su

Статья поступила
5 февраля 2007 г.