ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Апрель—июнь 2005. Серия 1. Том 12, № 2, 56–72

УДК 519.71

О СЛОЖНОСТИ РЕАЛИЗАЦИИ БУЛЕВЫХ ФУНКЦИЙ ФОРМУЛАМИ*)

А. В. Чашкин

Рассматривается сложность вычисления частичных булевых функций данного веса формулами в базисе $\{\&, \vee, \neg\}$. Установлено асимптотически точное значение сложности минимальных формул, реализующих почти все n-местные частичные булевы функции данного веса в случае, когда логарифм размера области определения асимптотически равен n. Предложен новый метод реализации монотонных булевых функций формулами.

Введение

Весом частичной булевой функции называется число наборов в ее области определения, на которых значение функции равно единице. Сложностью $L(F)$ формулы F в базисе $\{\&, \vee, \neg\}$ называется число вхождений символов переменных в эту формулу. Сложностью $L(f)$ функции f называется сложность самой простой (имеющей минимальную сложность) формулы, реализующей f.

О. Б. Лупанов в [3] рассмотрел сложность реализации булевых функций формулами в произвольном полном конечном базисе B и установил асимптотически точную формулу для сложности $L_B(n)$ самой сложной n-местной булевой функции. Следствием этой формулы является асимптотически точная формула для величины $L(n)$ — сложности реализации самой сложной n-местной булевой функции формулами в базисе $\{\&, \vee, \neg\}$:

$$L(n) \sim \frac{2^n}{\log_2 n}. \tag{1}$$

Реализацию булевых функций малого веса формулами рассматривал Б. И. Финников, который, в частности, показал [7], что для любой

*)Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проект 02-01-00985), программы поддержки ведущих научных школ РФ (проект НШ-1807.2003.1) и программы "Университеты России"(проект УР 04.03.007/03).

n-местной булевой функции f веса k справедливо неравенство

$$L(f) \lesssim \frac{2kn}{\log_2 n},$$

если k по порядку величины больше чем $\log_2 n$. Сложность формул, приближенно реализующих частичные булевы функции, область определения и вес которых равны соответственно $d2^n$ и $pd2^n$, где p и d — константы, изучалась Н. Пиппенджером в [9]. Из его результатов, в частности, следует, что для сложности самой сложной n-местной булевой функции из рассматриваемого множества справедливо асимптотическое равенство

$$L(f) \sim \frac{\log_2 \binom{d2^n}{pd2^n}}{\log_2 n},$$

в котором при $d = 1$ и $p = \frac{1}{2}$ правая часть совпадает с правой частью (1). Сложность реализации формулами в произвольном полном конечном базисе n-местных полностью определенных булевых функций, вес k которых удовлетворяет условию $\log_2 k \sim \log_2(2^n - k) \sim n$, рассматривал А. Е. Андреев. В [2] он дал набросок доказательства асимптотически точной формулы сложности самой сложной функции f из этого множества. Для формул в базисе $\{\&, \vee, \neg\}$ его результат имеет следующий вид:

$$L(f) \sim \frac{\log_2 \binom{2^n}{k}}{\log_2 n}.$$

В своих работах Н. Пиппенджер и А. Е. Андреев существенным образом опирались на конструкцию О. Б. Лупанова из [3].

В настоящей работе изучается сложность реализации частичных булевых функций данного веса формулами в базисе $\{\&, \vee, \neg\}$. В первом разделе излагается новый эффективный метод реализации булевых функций малого веса. В рассматриваемом методе используется модификация конструкции Финникова из [7].

Во втором разделе рассматривается сложность реализации частичных булевых функций данного веса, определенных в областях больших размеров. Из доказанной в этом разделе теоремы 1 следует, что сложность почти всех n-местных частичных булевых функций веса k при их реализации формулами асимптотически равна $\binom{N}{k}/\log_2 n$ в том случае, когда логарифм размера области определения N асимптотически равен n, а для веса k справедливы неравенства $n^5 \leqslant k \leqslant 2^n - n^5$. В доказательстве теоремы 1 используется общий подход Нечипорука к реализации недоопределенных булевых матриц из [5].

В третьем разделе приводится новый метод реализации монотонных булевых функций формулами. Метод основан на сведéнии реализации n-местной монотонной функции к реализации двух $(n-2)$-местных монотонных функций и одной частичной функции, определенной в области, размер которой асимптотически не превосходит $\binom{n}{\lfloor n/2\rfloor}$. Сложность формул, построенных при помощи этого метода, асимптотически не превосходит

$$2\binom{n}{\lfloor n/2\rfloor}\Big/\log_2 n.$$

Ранее сложность реализации монотонных булевых функций формулами рассматривалась Н. П. Редькиным, который в [6] показал, что сложность реализации произвольной n-местной монотонной булевой функции не превосходит

$$O\left(\binom{n}{\lfloor n/2\rfloor}\Big/\log_2 n\right),$$

и А. Е. Андреевым, который в [1] сформулировал утверждение о том, что для сложности $L(f)$ самой сложной n-местной монотонной булевой функции f справедливо асимптотическое равенство

$$L(f)\sim\binom{n}{\lfloor n/2\rfloor}\Big/\log_2 n. \qquad (2)$$

Отметим, что приводимый в настоящей статье метод реализации монотонных булевых функций формулами не является наилучшим относительно сложности получаемых формул. С другой стороны, до настоящего времени более эффективный метод, по-видимому, опубликован не был, так как формула (2) приведена в [1] без доказательства.

1. Булевы функции с малым числом единиц

Лемма 1. *Пусть булева функция $f(x_1,\dots,x_n)$ равна единице ровно на k наборах одинакового веса. Тогда*

$$L(f(x_1,\dots,x_n))\leqslant\frac{kn}{\log_2 n}(1+o(1))+O(n^{4,62}).$$

Доказательство. Прежде всего заметим, что $L(f)=O(kn)$. Поэтому при $k=O(\log_2 n)$ утверждение леммы очевидно. Далее будем полагать, что $k\gg\log_2 n$. Множество M, состоящее из наборов, на которых функция f обращается в единицу, разобьем на $m=\lceil k/\lfloor\log_2 n-2\log_2\log_2 n\rfloor\rceil$ подмножеств M_p, каждое из которых, кроме быть может последнего, состоит из $q=\lfloor\log_2 n-2\log_2\log_2 n\rfloor$ наборов. Пусть f_p — функция, равная единице на наборах из M_p. Тогда $f=f_1\vee\dots\vee f_m$.

Из наборов множества M_p составим матрицу $T_p = (t_p(i,j))$ размера $q \times n$, в которой столбцы соответствуют переменным, а строки — наборам. В этой матрице $t_p(i,j)$ равно j-у разряду i-го набора множества M_p. Легко видеть, что в матрице T_p найдется не более $n/\log_2^2 n$ различных видов столбцов. Множество переменных $x_1, \ldots, x_n$ разобьем на подмножества R_{pj} так, что $x_i \in R_{pj}$ в том случае, если i-й столбец матрицы T_p является двоичным представлением числа j. Пусть i_j — такой минимальный индекс, что $x_{i_j} \in R_{pj}$. Из переменных с такими индексами i_j образуем множество R_p. Например, если матрица T_p имеет вид

$$\begin{pmatrix} 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \end{pmatrix},$$

то $R_{p1} = \{x_1\}$, $R_{p2} = \varnothing$, $R_{p3} = \{x_4, x_8\}$, $R_{p4} = \{x_2, x_7\}$, $R_{p5} = \varnothing$, $R_{p6} = \{x_5\}$, $R_{p7} = \{x_3, x_6, x_9\}$, $i_1 = 1$, $i_3 = 4$, $i_4 = 2$, $i_6 = 5$, $i_7 = 3$, а индексы i_2 и i_5 не определены, так как соответствующие множества пусты. Следовательно, $R_p = \{x_1, x_2, x_3, x_4, x_5\}$.

Пусть вес наборов из M равен r. Через $h_r(x_1, \ldots, x_n)$ обозначим симметрическую булеву функцию, равную единице на наборах веса r. Введем вспомогательную функцию

$$g_p(x_1, \ldots, x_n) = \bigvee_{i=1}^{q} \Big(\bigwedge_{j=1}^{n} x_j^{t_p(i,j)} \Big), \tag{3}$$

где $x^1 = x$ и $x^0 = 1$.

Ясно, что последняя формула получается из совершенной дизъюнктивной нормальной формы функции f_p удалением из элементарных конъюнкций всех переменных, входящих в конъюнкции с отрицаниями. Поэтому

$$f_p(x_1, \ldots, x_n) = g_p(x_1, \ldots, x_n) \cdot h_r(x_1, \ldots, x_n). \tag{4}$$

Используя g_p, образуем новую функцию g_{p1}, удалив из функции (3) все переменные кроме переменных из R_p. Нетрудно видеть, что

$$g_{p1}(x_1, \ldots, x_n) = \bigvee_{i=1}^{q} \Big(\bigwedge_{\substack{j \in \{1, \ldots, n\} \\ x_j \in R_p}} x_j^{t_p(i,j)} \Big). \tag{5}$$

Наконец, положим

$$g_{p2}(x_1, \ldots, x_n) = \bigwedge_{j=1}^{2^q} \Big(\Big(\bigwedge_{x_i \in R_{pj}} x_i \Big) \vee \bar{x}_{i_j} \Big). \tag{6}$$

Нетрудно видеть, что после раскрытия скобок в произведении $g_{p1} \cdot g_{p2}$ будут получаться либо конъюнкции функции g_p, либо конъюнкции функции g_p, умноженные на отрицания переменных, либо конъюнкции, в которые входит более чем r переменных без отрицаний. Поэтому, учитывая (4), имеем

$$f_p(x_1, \ldots, x_n) = g_{p1}(x_1, \ldots, x_n) \cdot g_{p2}(x_1, \ldots, x_n) \cdot h_r(x_1, \ldots, x_n).$$

Следовательно,

$$f(x_1, \ldots, x_n) = h_r(x_1, \ldots, x_n)\Big(\bigvee_{p=1}^{m} g_{p1}(x_1, \ldots, x_n) \cdot g_{p2}(x_1, \ldots, x_n)\Big). \qquad (7)$$

Из (5) и (6) легко видеть, что

$$L(g_{p1}) \leqslant 2^q q, \qquad L(g_{p2}) \leqslant 2^q + n.$$

Кроме того, известно [8], что $L(h_r(x_1, \ldots, x_n) = O(n^{4,62})$. Поэтому из (7) и условий леммы получаем

$$\begin{aligned} L(f) &\leqslant \sum_{p=1}^{m} L(f_p) \leqslant m(2^q q + 2^q + n) + O(n^{4,62}) \\ &\leqslant \frac{k}{\log_2 n}\Big(\frac{n}{\log_2 n} + n\Big)\Big(1 + O\Big(\frac{\log_2 \log_2 n}{\log_2 n}\Big)\Big) + O(n^{4,62}) \\ &\leqslant \frac{kn}{\log_2 n}(1 + o(1)) + O(n^{4,62}). \end{aligned}$$

Лемма 1 доказана.

Из леммы 1 вытекает следующее утверждение, которое приведем без доказательства.

Лемма 2. *Пусть булева функция $f(x_1, \ldots, x_n)$ равна единице ровно на k наборах. Тогда при $n \to \infty$*

$$L(f(x_1, \ldots, x_n)) \leqslant \frac{kn}{\log_2 n}(1 + o(1)) + O(n^{5,62}).$$

В следующей лемме уточним оценку из леммы 2 для таких k, когда $\log_2 k$ сравним по порядку с n.

Лемма 3. *Пусть булева функция $f(x_1, \ldots, x_n)$ равна единице ровно на k наборах, причем $2n^6 \leqslant k \leqslant 2^{n-1}$. Тогда при $n \to \infty$*

$$L(f(x_1, \ldots, x_n)) \leqslant \frac{k(n - \log_2 k)}{\log_2(n - \log_2 k)}(1 + o(1)).$$

Доказательство. Функцию f разложим по первым m переменным:

$$f(x_1,\dots,x_n)=\bigvee_{\sigma_1,\dots,\sigma_m} x_1^{\sigma_1}\cdot\ldots\cdot x_m^{\sigma_m}\cdot f(\sigma_1,\dots,\sigma_m,x_{m+1},\dots,x_n), \qquad (8)$$

где $x^1=x$ и $x^0=\overline{x}$.

Затем, применяя лемму 2, оценим сложность функции f через сложность формулы, стоящей в правой части (8). Нетрудно видеть, что

$$L(f(x_1,...,x_n))\leqslant\sum_{\sigma_1,\dots,\sigma_m}(L(x_1^{\sigma_1}\cdot...\cdot x_m^{\sigma_m})+L(f(\sigma_1,...,\sigma_m,x_{m+1},...,x_n)))$$

$$\leqslant 2^m m+O(2^m(n-m)^{5{,}62})+\frac{k(n-m)}{\log_2(n-m)}(1+o(1)). \qquad (9)$$

Положим $m=\lfloor\log_2 k-6\log_2 n\rfloor$. В этом случае

$$2^m m\leqslant k, \qquad 2^m(n-m)^{5{,}62}\leqslant k, \qquad n-m\sim n-\log_2 k. \qquad (10)$$

Подставив оценки (10) в (9), получаем требуемую оценку сложности функции f. Лемма 3 доказана.

2. Частичные булевы функции

Теорема 1. *Пусть $D\subseteq\{0,1\}^n$ состоит из N наборов, $\log_2 N\sim n$, булева функция f определена в D и равна единице ровно на k наборах из D. Тогда*

$$L(f(x_1,\dots,x_n))\leqslant\frac{\log_2\binom{N}{k}}{\log_2 n}(1+o(1))+O(n^{5{,}62}).$$

Для почти каждой функции f, определенной в D и равной единице ровно на k наборах из D,

$$L(f(x_1,\dots,x_n))\geqslant\frac{\log_2\binom{N}{k}}{\log_2 n}.$$

В этом разделе доказывается первое неравенство теоремы 1. Второе неравенство оставим без доказательства, которое легко может быть получено стандартным мощностным методом (см., например, [4]).

Введем необходимые определения. Набор $\alpha\in\{0,1\}^m$ назовем *доопределением набора* $\beta\in\{0,1,*\}^m$, если $\alpha_i=\beta_i$ для всех таких i, что $\beta_i\in\{0,1\}$. Множество $B\subseteq\{0,1\}^m$ назовем *доопределением множества* $A\subseteq\{0,1,*\}^m$, если для каждого элемента α из A в B найдется элемент

β, являющийся доопределением набора α.

Лемма 4. *Пусть A — множество наборов из $\{0,1,*\}^m$, в каждом из которых содержится t единиц и $s-t$ нулей. Тогда существует доопределение множества A, состоящее не более чем из $2m^2\binom{s}{t}$ наборов.*

Доказательство. Пусть $B(m,k)$ — множество всех двоичных наборов длины m с k единицами. Допустим, что любое N-элементное подмножество множества $B(m,k)$ не является доопределением множества A. Тогда для каждого такого подмножества можно указать хотя бы один набор из A, для которого в этом подмножестве нет доопределения. Поэтому число таких пар (α,B), где $\alpha\in A$, а B является N-элементным подмножеством множества $B(m,k)$, что в B нет допределения набора α, не меньше чем $\binom{\binom{m}{k}}{N}$. Так как A состоит из $\binom{m}{s}\binom{s}{t}$ элементов, то в A найдется такой набор α, что по крайней мере $\binom{\binom{m}{k}}{N}\Big/\binom{m}{s}\binom{s}{t}$ N-элементных подмножеств множества $B(m,k)$ не содержат доопределение набора α. С другой стороны, легко видеть, что для любого набора из A ровно $\binom{\binom{m}{k}-\binom{m-s}{k-t}}{N}$ N-элементных подмножеств множества $B(m,k)$ не содержат его доопределения. Поэтому должно выполняться неравенство

$$\binom{\binom{m}{k}}{N}\Big/\binom{m}{s}\binom{s}{t}\leqslant\binom{\binom{m}{k}-\binom{m-s}{k-t}}{N}. \tag{11}$$

Определим максимальное N, при котором это возможно. Для этого оценим снизу величину $\binom{\binom{m}{k}}{N}\Big/\binom{\binom{m}{k}-\binom{m-s}{k-t}}{N}$. Так как $\frac{X-k}{X-Y-k}\geqslant\frac{X}{X-Y}$ при $X-Y-k>0$ и $\left(1+\frac{1}{x}\right)^x\geqslant 2$ при $x\geqslant 1$, то

$$\binom{X}{N}\Big/\binom{X-Y}{N}=\prod_{k=0}^{N-1}\frac{X-k}{X-Y-k}\geqslant\left(\frac{X}{X-Y}\right)^N$$
$$\geqslant\left(1+\frac{Y}{X-Y}\right)^N\geqslant\left(1+\frac{Y}{X}\right)^{X/Y(NY/X)}\geqslant 2^{NY/X}.$$

Объединяя полученную оценку и неравенство (11), имеем

$$2^{N\binom{m-s}{k-t}/\binom{m}{k}}\leqslant\binom{\binom{m}{k}}{N}\Big/\binom{\binom{m}{k}-\binom{m-s}{k-t}}{N}\leqslant\binom{m}{s}\binom{s}{t}.$$

Так как $\binom{m}{s}\binom{s}{t}<3^m$, то вычисляя двоичные логарифмы от левой и правой частей получившегося неравенства видим, что

$$N<\log_2 3\cdot m\binom{m}{k}\Big/\binom{m-s}{k-t}. \tag{12}$$

Далее рассмотрим равенство $\binom{m}{k} = \sum\limits_{i=0}^{k} \binom{s}{i}\binom{m-s}{k-i}$. Покажем, что при фиксированных m, k и s произведения под знаком суммы возрастают вместе с i до некоторого максимального значения, а затем начинают убывать. Для этого рассмотрим отношение двух соседних произведений и выясним, когда оно не превосходит единицы:

$$\binom{s}{i-1}\binom{m-s}{k-i+1}\Big/\binom{s}{i}\binom{m-s}{k-i}$$
$$= \frac{s!(m-s)!i!(s-i)!(k-i)!(m-s-k+i)!}{(i-1)!(s-i+1)!(k-i+1)!(m-s-k+i-1)!s!(m-s)!}$$
$$= \frac{i(m-s-k+i)}{(s-i+1)(k-i+1)} \leqslant 1.$$

Продолжая преобразования видим, что

$$0 \geqslant i(m-s-k+i) - (s-i+1)(k-i+1)$$
$$= i^2 + i(m-s-k) - i^2 + i(s+k+2) - (s+1)(k+1)$$
$$= i(m+2) - (s+1)(k+1).$$

Таким образом, при $i \leqslant \frac{(s+1)(k+1)}{m+2}$ значения произведений возрастают, при $i > \frac{(s+1)(k+1)}{m+2}$ — убывают и, следовательно, произведение максимально при

$$i = \Big\lfloor \frac{(s+1)(k+1)}{m+2} \Big\rfloor. \tag{13}$$

Рассматривая правую часть в (13) как функцию от k, легко видеть, при возрастании k от нуля до m ее значение так же возрастает, пробегая все целые числа между нулем и s, принимая, в частности, значение t. Пусть далее k такое, при котором максимум произведений $\binom{s}{i}\binom{m-s}{k-i}$ достигается при $i = t$. Из неравенства (12) при таком k имеем

$$N < \log_2 3 \cdot m\Big(\sum_{i=0}^{k} \binom{s}{i}\binom{m-s}{k-i}\Big)\Big/\binom{m-s}{k-t} \leqslant 2m^2\binom{s}{t}.$$

Таким образом, из предположения, что любое N-элементное подмножество множества $B(m,k)$ не является доопределением множества A, следует неравенство $N < 2m^2\binom{s}{t}$. Поэтому при N, не меньших $2m^2\binom{s}{t}$, среди N-элементных подмножеств множества $B(m,k)$ найдется хотя бы одно доопределение множества A. Лемма 4 доказана.

На множестве наборов с компонентами из $\{0,1,*\}$ определим функцию I. Если набор α из $\{0,1,*\}^m$ содержит s булевых компонент, среди которых t компонент равны единице, то положим $I(\alpha) = \log_2 \binom{s}{t}$.

Лемма 5. *Пусть $A = \{\alpha\}$ — множество наборов из $\{0,1,*\}^m$ таких, что $I(\alpha') < R$, где набор α' получается из α заменой последней булевой компоненты символом $*$. Тогда существует доопределение множества A, состоящее не более чем из $2m^5 2^R$ наборов.*

Доказательство. Множество A разобьем на непересекающиеся классы, поместив в класс $A(s,t)$, $t \leqslant s$, все наборы с s булевыми компонентами, среди которых t компонент равны единице. Из леммы 4 следует, что для множества $A(s,t)$ существует доопределение $B(s,t)$, состоящее не более чем из $2m^2\binom{s}{t}$ наборов. Пусть $\alpha \in A(s,t)$. Тогда $I(\alpha) = \log_2 \binom{s}{t}$. Так как $\binom{s}{t} \leqslant m\binom{s-1}{t}$, $\binom{s}{t} \leqslant m\binom{s-1}{t-1}$ и по условию леммы $I(\alpha') < R$, то $\binom{s}{t} < m \cdot 2^R$.

Так как общее число классов (число возможных значений параметров s и t) не превосходит m^2, то множество $\bigcup\limits_{s,t} B(s,t)$ состоит не более чем из $2m^5 2^R$ наборов и по построению является доопределением множества A. Лемма 5 доказана.

Лемма 6. *Пусть булева функция f определена в области $D \subseteq \{0,1\}^n$, состоящей из N наборов, и равна единице ровно на k наборах этой области. Если $\log_2 \log_2 \binom{N}{k} \sim n$ и $k \leqslant \frac{1}{2}N$, то*

$$L(f(x_1,\ldots,x_n)) \leqslant \frac{\log_2 \binom{N}{k}}{\log_2 n}(1+o(1)).$$

Доказательство. Введем параметры R и r, значения которых определим позднее. Значения частичной n-местной булевой функции f запишем в таблице T_f, состоящей из 2^r столбцов и 2^{n-r} строк, поставив в соответствие i-му столбцу таблицы набор $(\sigma_1,\ldots,\sigma_r)$, являющийся двоичным представлением числа $i-1$, а j-й строке — набор $(\sigma_{r+1},\ldots,\sigma_n)$, являющийся двоичным представлением числа $j-1$. На пересечении i-го столбца и j-й строки таблицы поставим значение $f(\sigma_1,\ldots,\sigma_r,\sigma_{r+1},\ldots,\sigma_n)$. Каждую строку таблицы представим в виде следующих друг за другом элементарных наборов α, для каждого из которых, кроме быть может последнего, справедливы неравенства $I(\alpha) \geqslant R$ и $I(\alpha') < R$. Множество таких наборов разобьем на классы, поместив в класс P_{ij} наборы, начинающиеся в i-й и заканчивающиеся в j-й позициях. Нетрудно видеть, что число различных классов не превосходит 2^{2r-1}.

Из леммы 5 следует, что для множества элементарных наборов класса P_{ij} существует множество их доопределений, состоящее не более чем из $2^{5r+1}2^R$ наборов длины 2^r, в каждом из которых первые $i-1$ и последние $2^r - j$ компонент равны нулю. Следовательно, для множества всех элементарных наборов существует множество их доопределений $H = \{h_i\}$, которое состоит не более чем из $2^{7r}2^R$ наборов h_i длины 2^r.

Преобразуем таблицу T_f, заменив в ней каждый элементарный набор каким-либо его доопределением из H. Нетрудно видеть, что преобразованная таблица будет таблицей значений некоторой n-местной булевой функции h, являющейся доопределением функции f. Из номеров тех наборов h_i, которые входят в j-ю строку преобразованной таблицы, составим множество A_j. Каждый набор h_i из H будем рассматривать как вектор значений r-местной булевой функции g_i, зависящей от переменных $x_1, \ldots, x_r$. Очевидно, что множество G, состоящее из функций g_i, содержит не более чем $2^{7r}2^R$ элементов и функция h может быть выражена через функции из G следующим образом:

$$h(x_1, \ldots, x_n) = \bigvee_{\sigma=(\sigma_{r+1},\ldots,\sigma_n)} \Bigl(\bigvee_{g\in A_j} g(x_1, \ldots, x_r)\Bigr) x_{r+1}^{\sigma_{r+1}} \cdot \ldots \cdot x_n^{\sigma_n}, \tag{14}$$

где $j = \sum\limits_{i=1}^{n-r} \sigma_{r+i}2^{i-1}$.

Оценим сверху число вхождений функций g в правую часть (14). Прежде всего заметим, что число функций, соответствующих наборам α с $I(\alpha) < R$, не превосходит числа строк таблицы, т. е. не больше 2^{n-r}. Число остальных функций обозначим через p. Соответствующие этим функциям элементарные наборы перенумеруем числами от 1 до p. Пусть s_i и t_i — число булевых и число единичных компонент в i-м элементарном наборе. Так как $\sum\limits_{i=1}^{p} s_i \leqslant N$, $\sum\limits_{i=1}^{p} t_i \leqslant k$ и по условию леммы $k \leqslant \frac{1}{2}N$, то

$$\log_2 \binom{N}{k} \geqslant \log_2 \binom{\sum s_i}{\sum t_i} \geqslant \log_2 \prod_{i=1}^{p} \binom{s_i}{t_i} = \sum_{i=1}^{p} \log_2 \binom{s_i}{t_i} \geqslant p \cdot R.$$

Таким образом, общее число элементарных наборов в T_f, а следовательно, и число вхождений функций g в (14), не превосходит

$$\log_2 \binom{N}{k} \Big/ R + 2^{n-r}. \tag{15}$$

Преобразуем равенство (14), поменяв порядок выполнения дизъюнкций: сначала будем выполнять дизъюнкции по функциям из G, а затем по элементарным конъюнкциям последних $n-r$ переменных, на которые эти функции умножаются. В результате получим равенство

$$h(x_1,\ldots,x_n)=\underbrace{\bigvee_{g\in G} g(x_1,\ldots,x_r)}_{A}\underbrace{\Bigl(\bigvee_{\sigma_{r+1},\ldots,\sigma_n} x_{r+1}^{\sigma_{r+1}}\cdot\ldots\cdot x_n^{\sigma_n}\Bigr)}_{B},\tag{16}$$

в котором число внутренних дизъюнкций (в подформулах B) как и в (14) не превосходит величины из (15). Так как $|G|\leqslant 2^{7r}2^R$ и каждая функция из G является дизъюнкцией не более чем 2^r элементарных конъюнкций, то сложность подформул из части A не превосходит

$$O(r2^r2^{7r}2^R).\tag{17}$$

Часть B состоит не более чем из $2^{7r}2^R$ дизъюнкций, в которых общее число элементарных конъюнкций не превосходит величины из (15). Поэтому в силу леммы 2 сложность подформул из части B не превосходит

$$O(r2^r2^{7r}2^Rn^{5,62})+\frac{n\bigl(\log_2\binom{N}{k}\big/R+2^{n-r}\bigr)}{\log_2 n}(1+o(1)).\tag{18}$$

Очевидно, что сложность формулы (16) и, следовательно, функции f не превосходит суммы величин (17) и (18), т. е.

$$L(f(x_1,\ldots,x_n))\leqslant O(2^{8r+R}n^{6,62})+\frac{n\bigl(\log_2\binom{N}{k}\big/R+2^{n-r}\bigr)}{\log_2 n}(1+o(1)).\tag{19}$$

Положим

$$r=\Bigl\lceil n-\log_2\log_2\binom{N}{k}+2\log_2 n\Bigr\rceil,$$
$$R=\Bigl\lfloor\log_2\log_2\binom{N}{k}-8r-8\log_2 n\Bigr\rfloor.$$

Тогда, учитывая условие $\log_2\log_2\binom{N}{k}\sim n$, имеем

$$\begin{aligned}R&\sim\log_2\log_2\binom{N}{k}\sim n,\\ R+8r&\leqslant\log_2\log_2\binom{N}{k}-8\log_2 n,\\ n-r&\leqslant\log_2\log_2\binom{N}{k}-2\log_2 n.\end{aligned}\tag{20}$$

Подставляя оценки (20) в (19), получаем требуемую оценку сложности функции f. Лемма 6 доказана.

Доказательство теоремы 1. Без ограничения общности будем полагать, что $k \leqslant \frac{1}{2}N$. Так как по условию теоремы $\log_2 N \sim n$, то $\log_2 N$ можно представить в виде $\log_2 N = (1-\delta)n$, где $\delta \to 0$ при $n \to \infty$. Введем параметр ε_0, положив $\varepsilon_0 = \frac{1}{\log_2 n} - \frac{1}{\log_2 \delta}$. Рассмотрим два случая: $\log_2 k \leqslant (1-\varepsilon_0)\log_2 N$ и $\log_2 k > (1-\varepsilon_0)\log_2 N$.

Если $\log_2 k \leqslant (1-\varepsilon_0)\log_2 N$, то $\log_2 k$ можно представить в виде $\log_2 k = (1-\varepsilon)\log_2 N$, где $\varepsilon_0 \leqslant \varepsilon < 1$. Так как $\varepsilon \geqslant -\frac{1}{\log_2 \delta}$ и $\varepsilon \geqslant \frac{1}{\log_2 n}$, то легко видеть, что $\delta = o(\varepsilon)$ и $|\log_2 \varepsilon| = o(\log_2 n)$. Из леммы 3 следует, что

$$L(f) \lesssim \frac{k(n-\log_2 k)}{\log_2(n-\log_2 k)} = \frac{kn(\varepsilon+\delta-\varepsilon\delta)}{\log_2(n(\varepsilon+\delta-\varepsilon\delta))} = \frac{kn(\varepsilon+o(\varepsilon))}{\log_2 n + o(\log_2 n)}.$$

С другой стороны,

$$\log_2 \binom{N}{k} \geqslant k\log_2 \frac{N}{k} = k\log_2 2^{\varepsilon(1-\delta)n} = kn\varepsilon(1+o(1)).$$

Объединяя получившиеся неравенства, получаем

$$L(f) \leqslant \frac{\log_2 \binom{N}{k}}{\log_2 n}(1+o(1)).$$

Если $\log_2 k > (1-\varepsilon_0)\log_2 N$, то $\log_2\log_2\binom{N}{k} \sim \log_2 k \sim n$. В этом случае утверждение теоремы следует из леммы 6. Теорема 1 доказана.

Пусть $L(n,N) = \max L(f)$, где максимум берется по всем n-местным частичным булевым функциям, определенным в областях из N наборов. Из теоремы 1 легко извлекается следующее утверждение о сложности частичных функций, которое приведем без доказательства.

Теорема 2. *Пусть $\log_2 N \sim n$. Тогда*

$$L(n,N) \sim \frac{N}{\log_2 n}.$$

3. Монотонные булевы функции

Теорема 3. *Для любой монотонной n-местной булевой функции существует реализующая эту функцию формула F такая, что*

$$L(F) \lesssim \frac{2^{n+1}}{\sqrt{\pi n/2}\cdot\log_2 n}. \tag{21}$$

Так как $\frac{2^n}{\sqrt{\pi n/2}} \sim \binom{n}{\lfloor n/2 \rfloor}$, то неравенство (21) можно переписать в виде

$$L(F) \lesssim \frac{2\binom{n}{\lfloor n/2 \rfloor}}{\log_2 n}.$$

Учитывая, что логарифм числа n-местных монотонных булевых функций не меньше чем $\binom{n}{\lfloor n/2 \rfloor}$, нетрудно видеть, что правая часть неравенства (21) превосходит нижнюю мощностную оценку сложности монотонных функций ровно в два раза.

Пара вершин n-мерного булева куба $\{0,1\}^n$ называется ребром, если эти вершины различаются ровно в одном разряде. Последовательность вершин $\boldsymbol{\alpha} = (\alpha_0, \ldots, \alpha_n)$ такую, что $\alpha_0 \prec \cdots \prec \alpha_n$, будем называть *максимальной цепью* n-мерного булева куба. Будем говорить, что цепь $\boldsymbol{\alpha}$ проходит через ребро (γ, δ) если вершины γ и δ принадлежат $\boldsymbol{\alpha}$. Ребра (α, β) и (γ, δ) назовем *несравнимыми,* если никакая максимальная цепь не проходит одновременно через них.

Следующая лемма является реберным аналогом известной оценки числа элементов антицепи в булевом кубе.

Лемма 7. *Любое множество попарно несравнимых ребер n-мерного булева куба состоит не более чем из $\lceil \frac{n}{2} \rceil \binom{n}{\lfloor n/2 \rfloor}$ элементов.*

Доказательство. Пусть $\mathcal{N}$ — произвольное множество попарно несравнимых ребер n-мерного булева куба, а $\mathcal{N}_k$ — его подмножество, состоящее из всех тех ребер множества $\mathcal{N}$, которые в булевом кубе соединяют вершины k-го и $(k+1)$-го слоев. Если $(\alpha, \beta) \in \mathcal{N}_k$, то через это ребро проходит $k!(n-k-1)!$ максимальных цепей. Так как каждая максимальная цепь проходит только через одно ребро множества $\mathcal{N}$, то через все ребра множества $\mathcal{N}$ проходит $\sum\limits_{k=0}^{n-1} k!(n-k-1)!|\mathcal{N}_k|$ максимальных цепей. Так как в n-мерном булевом кубе существует $n!$ различных максимальных цепей, то

$$n! \geqslant \sum_{k=0}^{n-1} k!(n-k-1)!|\mathcal{N}_k| = (n-1)! \sum_{k=0}^{n-1} |\mathcal{N}_k| \Big/ \binom{n-1}{k}$$
$$\geqslant (n-1)! \Big(\sum_{k=0}^{n-1} |\mathcal{N}_k| \Big) \Big/ \binom{n-1}{\lceil \frac{n-1}{2} \rceil} = (n-1)! |\mathcal{N}| \Big/ \binom{n-1}{\lceil \frac{n-1}{2} \rceil}.$$

Так как $\lceil \frac{n}{2} \rceil = \lfloor \frac{n+1}{2} \rfloor$, то, преобразуя предыдущее неравенство, получаем требуемую оценку:

$$|\mathcal{N}| \leqslant n\binom{n-1}{\lceil\frac{n-1}{2}\rceil} \leqslant \frac{n\cdot(n-1)!}{\lfloor\frac{n-1}{2}\rfloor!\lceil\frac{n-1}{2}\rceil!}$$
$$= \frac{n!}{\lceil\frac{n-2}{2}\rceil!\lceil\frac{n-1}{2}\rceil!} = \frac{\lceil\frac{n}{2}\rceil\cdot n!}{\lceil\frac{n}{2}\rceil\cdot\lceil\frac{n-2}{2}\rceil!\lceil\frac{n-1}{2}\rceil!} = \frac{\lceil\frac{n}{2}\rceil\cdot n!}{\lceil\frac{n}{2}\rceil!\lfloor\frac{n}{2}\rfloor!} = \left\lceil\frac{n}{2}\right\rceil\binom{n}{\lfloor\frac{n}{2}\rfloor}.$$

Лемма 7 доказана.

Пусть f — монотонная булева функция. Ребро (α,β) назовем непостоянным, если $f(\alpha) \neq f(\beta)$. Так как любые два непостоянных ребра несравнимы, то из леммы 7 вытекает следующее утверждение.

Лемма 8. *Число непостоянных ребер любой n-местной монотонной булевой функции не превосходит $\lceil\frac{n}{2}\rceil\binom{n}{\lfloor n/2\rfloor}$.*

Будем говорить, что ребро (α,β) проходит в i-м направлении, если наборы α и β различаются в i-м разряде.

Лемма 9. *Для любой n-местной монотонной булевой функции найдутся такие направления i и j, что число непостоянных ребер, проходящих в этих направлениях, не превосходит $\frac{n+1}{n}\binom{n}{\lfloor n/2\rfloor}$.*

Доказательство. Допустим, что в любых двух направлениях i и j проходит в совокупности больше чем $\frac{n+1}{n}\binom{n}{\lfloor n/2\rfloor}$ непостоянных ребер. Тогда сумма S числа непостоянных ребер, взятых по всем парам направлений, больше $\frac{n+1}{n}\binom{n}{\lfloor n/2\rfloor}\binom{n}{2}$. При этом каждое непостоянное ребро любого направления будет подсчитано ровно $n-1$ раз. Поэтому в силу леммы 8 сумма S не превосходит величины $(n-1)\lceil\frac{n}{2}\rceil\binom{n}{\lfloor n/2\rfloor}$. Таким образом

$$\frac{n+1}{n}\binom{n}{\lfloor n/2\rfloor}\binom{n}{2} < S \leqslant (n-1)\left\lceil\frac{n}{2}\right\rceil\binom{n}{\lfloor n/2\rfloor}.$$

Перенося множитель $\binom{n}{2}$ из левой части полученного неравенства в правую, получим противоречие. Лемма 9 доказана.

Символом $f_{ij}^{\alpha\beta}(\boldsymbol{x})$ обозначим $(n-2)$-местную функцию, получающуюся из n-местной булевой функции f подстановкой констант α и β вместо ее i-го и j-го аргументов, а символом $\boldsymbol{x}_{ij}^{\alpha\beta}$ — булев набор длины n, в котором i-й и j-й разряды равны α и β и который после удаления этих разрядов превращается в булев набор $\boldsymbol{x}$ длины $n-2$.

Лемма 10. *Для любой n-местной монотонной булевой функции f найдутся такие i и j, что $f_{ij}^{11}(\boldsymbol{x}) \neq f_{ij}^{00}(\boldsymbol{x})$ не более чем для $\frac{n+1}{2n}\binom{n}{\lfloor n/2\rfloor}$ различных наборов $\boldsymbol{x}$ длины $n-2$.*

Доказательство. Рассмотрим такие i и j, что функция f в i-м и

j-м направлениях в совокупности имеет не более $\frac{n+1}{n}\binom{n}{\lfloor n/2\rfloor}$ непостоянных ребер. Если $f_{ij}^{11}(\boldsymbol{x}) \neq f_{ij}^{00}(\boldsymbol{x})$, то $f_{ij}^{11}(\boldsymbol{x}) = 1$ и $f_{ij}^{00}(\boldsymbol{x}) = 0$ и, следовательно, одно из ребер $(\boldsymbol{x}_{ij}^{00}, \boldsymbol{x}_{ij}^{01})$ или $(\boldsymbol{x}_{ij}^{01}, \boldsymbol{x}_{ij}^{11})$ будет непостоянным. Точно также непостоянным будет одно из ребер $(\boldsymbol{x}_{ij}^{00}, \boldsymbol{x}_{ij}^{10})$ или $(\boldsymbol{x}_{ij}^{10}, \boldsymbol{x}_{ij}^{11})$. Поэтому каждому неравенству $f_{ij}^{11}(\boldsymbol{x}) \neq f_{ij}^{00}(\boldsymbol{x})$ соответствует пара непостоянных ребер, каждое из которых может быть как ребром i-го, так и j-го направления. Так как число непостоянных ребер i-го и j-го направлений в два раза больше числа наборов $\boldsymbol{x}$, на которых $f_{ij}^{11}(\boldsymbol{x}) \neq f_{ij}^{00}(\boldsymbol{x})$, то утверждение леммы следует из выбора i и j. Лемма 10 доказана.

Символом $\boldsymbol{x}_{ij}$ обозначим булев набор длины $n-2$, получающийся из булева набора $\boldsymbol{x}$ длины n удалением i-го и j-го разрядов.

Лемма 11. *Для любой n-местной монотонной булевой функции f найдутся такие целые i и j, $(n-2)$-местные монотонные функции p и q и область $D \subseteq \{0,1\}^n$, что $|D| \leqslant \frac{n+1}{n}\binom{n}{\lfloor n/2\rfloor}$ и*

$$f(\boldsymbol{x}) = p(\boldsymbol{x}_{ij}) \vee q(\boldsymbol{x}_{ij})(f_D(\boldsymbol{x})(x_i \vee x_j) \vee x_i x_j). \tag{22}$$

Доказательство. Пусть i и j такие, как в лемме 10. В $\{0,1\}^n$ определим множество $D = \{\boldsymbol{x} \mid \Big(f_{ij}^{11}(\boldsymbol{x}_{ij}) \neq f_{ij}^{00}(\boldsymbol{x}_{ij})\Big) \,\&\, (x_i \neq x_j)\}$. Из леммы 10 следует, что это множество состоит не более чем из $\frac{n+1}{n}\binom{n}{\lfloor n/2\rfloor}$ элементов. Покажем, что формула

$$f_{ij}^{11}(\boldsymbol{x}_{ij})f_{ij}^{00}(\boldsymbol{x}_{ij}) \vee \big(f_{ij}^{11}(\boldsymbol{x}_{ij}) \vee f_{ij}^{00}(\boldsymbol{x}_{ij})\big)\big(f_D(\boldsymbol{x})(x_i \vee x_j) \vee x_i x_j\big) \tag{23}$$

реализует функцию f. Действительно, если $f_{ij}^{11}(\boldsymbol{x}_{ij}) = f_{ij}^{00}(\boldsymbol{x}_{ij}) = 0$, то $f(\boldsymbol{x}) = 0$ в силу монотонности независимо от значений x_i и x_j. Легко видеть, что в этом случае значение функции из (23) также равно нулю. Аналогичным образом убеждаемся, что если $f_{ij}^{11}(\boldsymbol{x}_{ij}) = f_{ij}^{00}(\boldsymbol{x}_{ij}) = 1$, то $f(\boldsymbol{x})$ и функция из (23) равны единице. Если же $f_{ij}^{11}(\boldsymbol{x}_{ij}) \neq f_{ij}^{00}(\boldsymbol{x}_{ij})$, то $f(\boldsymbol{x}) = 0$ при $x_i = x_j = 0$, $f(\boldsymbol{x}) = 1$ при $x_i = x_j = 1$ и $f(\boldsymbol{x}) = f_D(\boldsymbol{x})$ при $x_i \neq x_j$. С другой стороны, в рассматриваемом случае формула из (23) превращается в формулу $f_D(\boldsymbol{x})(x_i \vee x_j) \vee x_i x_j$. Поэтому легко видеть, что значение этой формулы равно нулю при $x_i = x_j = 0$, равно единице при $x_i = x_j = 1$ и совпадает с значением $f_D(\boldsymbol{x})$ при $x_i \neq x_j$. Положив $p(\boldsymbol{x}_{ij}) = f_{ij}^{11}(\boldsymbol{x}_{ij})f_{ij}^{00}(\boldsymbol{x}_{ij})$ и $q(\boldsymbol{x}_{ij}) = f_{ij}^{11}(\boldsymbol{x}_{ij}) \vee f_{ij}^{00}(\boldsymbol{x}_{ij})$, получим равенство (22). Лемма 11 доказана.

Из леммы 11 следует, что вычисление значения n-местной монотонной функции можно свести к вычислению значений двух $(n-2)$-местных монотонных функций и одной n-местной частичной функции, определенной в области, состоящей не более чем из $\frac{n+1}{n}\binom{n}{\lfloor n/2\rfloor}$ наборов.

Допустим, что любая n-местная монотонная булева функция может быть реализована формулой, сложность которой не превосходит $L_M(n)$. Пусть, кроме того, любая n-местная частичная булева функция, определенная в области размера d, может быть реализована формулой сложности не более $L_d(n)$. Тогда из леммы 11 следует, что для величины $L_M(n)$ справедливо рекуррентное неравенство

$$L_M(n) \leqslant 2L_M(n-2) + L_d(n) + 4, \tag{24}$$

где $d \leqslant \frac{n+1}{n}\binom{n}{\lfloor n/2 \rfloor}$. Положим $k = \lceil \log_2 n \rceil$. Для оценки сверху величины $L_M(n)$ применим k раз соответствующее неравенство из (24). Оценивая появляющиеся при этом величины L_d при помощи теоремы 2 и учитывая, что $\frac{n+1}{n}\binom{n}{\lfloor n/2 \rfloor} \sim \frac{2^n}{\sqrt{\pi n/2}}$, имеем

$$\begin{aligned}
L_M(n) &\lesssim 2L_M(n-2) + \frac{2^n}{\sqrt{\pi n/2}\cdot\log_2 n} \\
&\lesssim 4L_M(n-4) + \frac{2\cdot 2^{n-2}}{\sqrt{\pi(n-2)/2}\cdot\log_2(n-2)} + \frac{2^n}{\sqrt{\pi n/2}\cdot\log_2 n} \lesssim \dots \\
&\lesssim 2^k L_M(n-2k) + \frac{2^n}{\sqrt{\pi n/2}\cdot\log_2 n}\sum_{i=1}^{k}\frac{1}{2^{i-1}} \\
&\lesssim 2^k L_M(n-2k) + \frac{2\cdot 2^n}{\sqrt{\pi n/2}\cdot\log_2 n}.
\end{aligned}$$

Очевидно, что величина $L_M(n-2k)$ не превосходит сложности произвольной $(n-2k)$-местной булевой функции. Поэтому из (1), последнего неравенства и теоремы 2 следует, что

$$\begin{aligned}
L_M(n) &\lesssim \frac{2^k\cdot 2^{n-2k}}{\log_2(n-2k)} + \frac{2\cdot 2^n}{\sqrt{\pi n/2}\cdot\log_2 n} \\
&\lesssim \frac{2^n}{n\log_2 n} + \frac{2\cdot 2^n}{\sqrt{\pi n/2}\cdot\log_2 n} \sim \frac{2\cdot 2^n}{\sqrt{\pi n/2}\cdot\log_2 n}.
\end{aligned}$$

Теорема 3 доказана.

Заметим, что рассмотренный метод реализации монотонных булевых функций применим и для схем из функциональных элементов. Нетрудно видеть, что он позволяет строить схемы, сложность которых асимптотически не превосходит $\frac{2\cdot 2^n}{n\sqrt{\pi n/2}}$.

ЛИТЕРАТУРА

1. **Андреев А. Е.** О сложности монотонных функций // Вест. Моск. ун-та. Сер. 1. Математика. Механика. 1985. № 4. С. 83–87.
2. **Андреев А. Е.** Об одном методе синтеза формул // Вест. Моск. ун-та. Сер. 1. Математика. Механика. 1994. № 6. С. 23–27.
3. **Лупанов О. Б.** О сложности реализации функций алгебры логики формулами // Проблемы кибернетики. Вып. 3. М.: Физматгиз, 1960. С. 61–80.
4. **Лупанов О. Б.** О синтезе некоторых классов управляющих систем // Проблемы кибернетики. Вып. 10. М.: Физматгиз, 1963. С. 63–98.
5. **Нечипорук Э. И.** О сложности вентильных схем, реализующих булевские матрицы с неопределенными элементами // Докл. АН СССР. 1965. Т. 163, № 1. С. 40–42.
6. **Редькин Н. П.** О реализации монотонных булевых функций контактными схемами // Проблемы кибернетики. Вып. 35. М.: Наука, 1979. С. 87–110.
7. **Финников Б. И.** Об одном семействе классов функций алгебры логики и их реализации в классе π-схем // Докл. АН СССР. 1957. Т. 115, № 2. С. 247–248.
8. **Храпченко В. М.** О сложности реализации симметрических функций формулами // Матем. заметки. 1972. Т. 11, вып. 1. С. 109–120.
9. **Pippenger N.** Information theory and the complexity of Boolean functions // Math. System Theory. 1976/77. V. 10, N 2. P. 129–167.

Адрес автора:

МГУ, мех.-мат. факультет,
Воробьевы горы,
119992 Москва, Россия.
E-mail: chash@online.ru

Статья поступила
10 декабря 2004 г.