ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Апрель—июнь 2000. Серия 1. Том 7, № 2, 86–95

УДК 519.714

СВЕРХКВАДРАТИЧНЫЕ НИЖНИЕ ОЦЕНКИ СЛОЖНОСТИ ФОРМУЛ В НЕКОТОРЫХ БАЗИСАХ*)

Д. Ю. Черухин

Исследуется сложность булевых формул в полных базисах. В некоторых базисах получены нижние оценки сложности вида n^{2+c}, $c > 0$, для последовательности функций Андреева [1].

Одной из наиболее важных проблем дискретной математики является получение нижних оценок сложности функций в модельных классах схем [2, 6]. Первую нелинейную оценку такого рода получила Б. А. Субботовская. Она показала [8], что сложность линейной функции $x_1 \oplus \ldots \oplus x_n$ при реализации формулами в базисе $\text{Б}_0 = \{\&, \vee, \neg\}$ по порядку не меньше $n^{3/2}$. Затем Э. И. Нечипорук [5] получил оценки вида $n^{2-o(1)}$ для формул в произвольном конечном базисе и контактных схем. Нижнюю оценку вида n^2 для линейной функции в классе π-схем (формул в базисе Б_0) получил В. М. Храпченко в работе [9].

А. Е. Андреев, совместив в работе [1] идеи Субботовской и Нечипорука, для формул в базисе Б_0 получил оценку $n^{5/2-o(1)}$. Оценку сложности функции Андреева последовательно повышали Н. Нисан (N. Nisan) и Р. Импаглиассо (R. Impagliazzo), М. С. Патерсон (M. S. Paterson) и У. Звик (U. Zwick) (см. [11]). Наконец, Й. Хастад (J. Håstad) привлек идею Храпченко и в [11] довёл эту оценку до $n^{3-o(1)}$.

Б. А. Мучник (Субботовская) в [4] обобщила свой метод на формулы в «нелинейных» базисах, получив в них нижние оценки n^{1+c}, $c > 0$, для линейной функции. Н. А. Перязев [7] и автор [10] независимо друг от друга распространили результат из [4] на более широкий класс — формулы в обобщенно монотонных базисах. В данной статье, совместив технику [10] с техникой Андреева, мы получили оценки вида n^{2+c}, $c > 0$, для формул в обобщенно монотонных базисах.

---

*) Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (код проекта 99–01–01175) и Федеральной целевой программы «Интеграция» (проект 1997–473).

Введём необходимые понятия и обозначения. Пусть $X = \{x_1, x_2, \ldots\}$ — счётное множество *переменных*; $y_1, \ldots, y_k$ — попарно различные переменные из X; $c_1, \ldots, c_k$ — булевы константы, т. е. константы из множества $\{0, 1\}$. Множество пар $\{(y_1, c_1), \ldots, (y_k, c_k)\}$ назовём *подстановкой констант* и обозначим его $\{y_1 = c_1, \ldots, y_k = c_k\}$ (допустима пустая подстановка констант). Пусть $A = \{y_1 = c_1, \ldots, y_k = c_k\}$, $f : \{0,1\}^n \to \{0,1\}$ — булева функция от n переменных. Обозначим через $f|_A$ такую функцию от n переменных, для которой выполнено тождество

$$f|_A(x_1, \ldots, x_n) \equiv f(x_1, \ldots, c_1, \ldots, c_k, \ldots, x_n)$$

(здесь константы $c_1, \ldots, c_k$ расположены на местах переменных $y_1, \ldots, y_k$ соответственно; если какая-либо переменная y_j не входит в множество $\{x_1, \ldots, x_n\}$, то соответствующая ей константа c_j не используется). Далее, пусть $\{x_1, \ldots, x_n\} \setminus \{y_1, \ldots, y_k\} = \{x_{i_1}, \ldots, x_{i_s}\}$, $i_1 < \ldots < i_s$. Через $f|_A^*$ обозначим функцию от s переменных, полученную из $f|_A$ заменой переменных $x_{i_1}, \ldots, x_{i_s}$ на переменные $x_1, \ldots, x_s$ соответственно.

Базисом назовём произвольную конечную функционально полную систему булевых функций. Пусть Б — базис. Положим [Б] $= \{f|_A^*$, где $f \in$ Б, A— подстановка констант$\} \cup \{0, 1, \mathrm{Id}, \neg\}$ (здесь Id — тождественная функция, $\neg$ — отрицание). Тогда [Б] — базис и [[Б]] = [Б]. Базис Б назовём *нормальным*, если [Б] = Б. *Порядком* базиса Б назовём наибольшее число существенных переменных у функций из Б. Функцию f назовём *монотонной* по переменной y, если она либо возрастает, либо убывает по y (в естественном порядке на множестве $\{0,1\}$). Базис Б назовём *обобщенно монотонным*, если каждая функция из Б монотонна по всем своим переменным.

Формулами в базисе Б назовём переменные[*)] из X, а также выражения вида $f(F_1, \ldots, F_n)$ (f при $n = 0$), где f — n-местная функция, $f \in$ Б и $F_1, \ldots, F_n$ — формулы в Б. Формулу $\neg(F_1)$ обозначим через $\overline{F}_1$. Пусть F, G — формулы и $A = \{y_1 = c_1, \ldots, y_k = c_k\}$. *Подформулой* формулы F назовём часть формулы F, состоящую из подряд идущих символов и являющуюся формулой. Через $F \equiv G$ обозначим тождественное равенство формул F и G (т. е. совпадение их значений на всех наборах значений переменных), через $F \mathrel{\underline{\circ}} G$ обозначим графическое равенство формул (т. е. посимвольное их совпадение). Обозначим через $F|_A$ формулу, полученную из F заменой всех вхождений переменных $y_1, \ldots, y_k$ на константы $c_1, \ldots, c_k$ соответственно.

Пусть $y \in X$ и $Y \subseteq X$. Обозначим через $L_y(F)$ число вхождений в F переменной y. Положим $L_Y(F) = \sum\limits_{y \in Y} L_y(F)$ и $L(F) = L_X(F)$. Число

[*)] Для удобства переменные будем считать формулами; это не влияет на сложность функций в нормальном базисе.

$L(F)$ называется *сложностью* формулы F. *Вес* n-местной функции положим равным $\frac{n-2}{2}$ при $n \geqslant 2$ и равным 0 при $n \leqslant 1$. ***Весом формулы*** F (обозначение: $P(F)$) назовём сумму $L(F) + M(F)$, где $M(F)$ — сумма весов входящих в F функциональных символов с учётом кратности вхождений. Для каждой функции f и базиса Б положим $L_{\text{Б}}(f) = \min L(F)$, $P_{\text{Б}}(f) = \min P(F)$, где минимум берётся по всем формулам F в базисе Б, реализующим функцию f. Числа $L_{\text{Б}}(f)$ и $P_{\text{Б}}(f)$ называются соответственно *сложностью и весом функции* f в базисе Б. Формулу G назовём *упрощением* формулы F, если $G \equiv F$, $P(G) \leqslant P(F)$ и $L_y(G) \leqslant L_y(F)$ для любой переменной y.

Пусть F — формула в нормальном базисе Б. Построим следующую последовательность формул $F^0, \ldots, F^t$. Положим $F^0 = F$. Пусть формула F^j уже построена. Если существует подформула формулы F^j, к которой применимо хотя бы одно из преобразований a)–d) (определённых ниже), то применим его и полученную формулу обозначим через F^{j+1}; если же ни одно из преобразований a)–d) не применимо ни к одной из подформул формулы F^j, то положим $t = j$ и завершим построение (последовательность $F^0, \ldots, F^t$ строится, вообще говоря, не однозначно). Пусть G — подформула формулы F^j, причём $G \;\underline{\circ}\; f(F_1, \ldots, F_n)$, $f \in \text{Б}$, $F_1, \ldots, F_n$ — формулы; $y \in X$, $1 \leqslant i \leqslant n$. Тогда

a) если $G \equiv 0$ $(1,\ y,\ \bar{y})$ и G не равна графически формуле 0 $(1,\ y,\ \bar{y})$, то G заменим формулой 0 $(1,\ y,\ \bar{y})$ соответственно;

b) если $F_i \;\underline{\circ}\; b$, $b \in \{0, 1\}$, то G заменим формулой $f|^*_{\{x_i = b\}}(F_1, \ldots, F_{i-1}, F_{i+1}, \ldots, F_n)$;

c) если $n \geqslant 2$ и $G \equiv F_i$ $(\overline{F}_i)$, то G заменим формулой F_i $(\overline{F}_i)$ соответственно;

d) если φ — двуместная нелинейная функция, $G \equiv \varphi(y, F_i)$, $L_y(F_i) > 0$, c — такая константа, что функция $\varphi(c, z)$ не зависит существенно от z, то F_i заменим формулой $F_i|_{\{y = \bar{c}\}}$.

Через конечное число шагов ни одно из этих преобразований не будет применимо. Полученная при этом формула F^t является упрощением формулы F в базисе Б и обладает следующими свойствами (i)–(iv). Пусть G, H — подформулы формулы F^t, причём $G \;\underline{\circ}\; f(F_1, \ldots, F_n)$, $f \in \text{Б}$, $F_1, \ldots, F_n$ — формулы; $y \in X$, $1 \leqslant i \leqslant n$. Тогда

(i) если $H \equiv 0$ $(1,\ y,\ \bar{y})$, то $H \;\underline{\circ}\; 0$ $(1,\ y,\ \bar{y})$ соответственно;

(ii) либо H — константа, либо H не содержит констант;

(iii) если $n \geqslant 2$, то $G \not\equiv F_i$ и $G \not\equiv \overline{F}_i$;

(iv) если φ — нелинейная функция и $G \equiv \varphi(y, F_i)$, то $L_y(F_i) = 0$.

Произвольную формулу, подформулы которой обладают свойствами (i)–(iv), назовём *приведенной.*

Лемма 1. *Пусть Б — нормальный базис порядка k и F — приведённая формула в Б. Тогда*

$$L(F) \geqslant \frac{2k-2}{3k-4}P(F). \tag{1}$$

Доказательство. Если F — константа, то неравенство (1) выполнено. Если F отлична от константы, то индукцией по построению F докажем неравенство

$$L(F) \geqslant \frac{2k-2}{3k-4}P(F) + \frac{k-2}{3k-4}. \tag{2}$$

Тем самым лемма будет доказана.

Базис индукции: F — переменная. Тогда

$$L(F) = 1 = \frac{2k-2}{3k-4} + \frac{k-2}{3k-4} = \frac{2k-2}{3k-4}P(F) + \frac{k-2}{3k-4}.$$

Индуктивный переход: $F \mathrel{\underline{\circ}} f(F_1, \ldots, F_n)$, где f — функция и $F_1, \ldots, F_n$ — формулы. Формулы $F_1, \ldots, F_n$ являются приведёнными в Б. В силу свойства (ii) приведённых формул (для $H = F$) каждая из формул $F_1, \ldots, F_n$ отлична от констант. По предположению индукции имеем

$$L(F_i) \geqslant \frac{2k-2}{3k-4}P(F_i) + \frac{k-2}{3k-4}, \quad i = 1, \ldots, n. \tag{3}$$

Если $n = 1$, то $L(F) = L(F_1)$ и $P(F) = P(F_1)$. Поэтому из (3) следует (2). Пусть теперь $n \geqslant 2$. Тогда

$$L(F) = \sum_{i=1}^{n} L(F_i), \qquad P(F) = \sum_{i=1}^{n} P(F_i) + \frac{n-2}{2}.$$

Отсюда, использовав (3), получаем

$$\begin{aligned}
L(F) &= \sum_{i=1}^{n} L(F_i) \geqslant \sum_{i=1}^{n} \left(\frac{2k-2}{3k-4}P(F_i) + \frac{k-2}{3k-4}\right) \\
&= \frac{2k-2}{3k-4}\sum_{i=1}^{n} P(F_i) + \frac{n(k-2)}{3k-4} \\
&= \frac{2k-2}{3k-4}\left(\sum_{i=1}^{n} P(F_i) + \frac{n-2}{2}\right) - \frac{(n-2)(k-1)}{3k-4} + \frac{n(k-2)}{3k-4} \\
&= \frac{2k-2}{3k-4}P(F) + \frac{-nk+n+2k-2+nk-2n}{3k-4} \\
&= \frac{2k-2}{3k-4}P(F) + \frac{2k-n-2}{3k-4} \geqslant \text{(ибо } n \leqslant k) \geqslant \frac{2k-2}{3k-4}P(F) + \frac{k-2}{3k-4}.
\end{aligned}$$

Тем самым справедливость неравенство (2) установлена. Лемма 1 доказана.

Лемма 2. *Пусть Б — нормальный обобщенно монотонный базис, y — переменная и F — приведённая формула в Б, отличная от y и $\bar{y}$. Тогда существуют такая константа σ и формула F' в Б, являющаяся упрощением формулы $F|_{\{y=\sigma\}}$, что выполнено неравенство*

$$P(F) - P(F') \geqslant \frac{3}{2} L_y(F). \tag{4}$$

Доказательство. Индукцией по построению формулы F докажем, что существуют такие формулы F^0 и F^1 в Б, являющиеся упрощениями формул $F|_{\{y=0\}}$ и $F|_{\{y=1\}}$ соответственно, что выполнено неравенство

$$P(F) - \frac{P(F^0) + P(F^1)}{2} \geqslant \frac{3}{2} L_y(F). \tag{5}$$

Отсюда, выбрав в качестве σ такую константу, что выполнено неравенство $P(F^\sigma) \leqslant P(F^{\bar{\sigma}})$, и положив $F' = F^\sigma$, получим (4). Тем самым лемма будет доказана.

Базис индукции: либо F — переменная, отличная от y, либо F — константа. Положим $F^0 = F^1 = F$. Тогда в силу равенства $L_y(F) = 0$ неравенство (5) выполнено.

Индуктивный переход: $F \overset{\circ}{=} f(F_1, \ldots, F_n)$, где f — функция и $F_1, \ldots, F_n$ — формулы. Не ограничивая общности будем считать, что $F_1 \overset{\circ}{=} \ldots \overset{\circ}{=} F_s \overset{\circ}{=} y$, $F_{s+1} \overset{\circ}{=} \ldots \overset{\circ}{=} F_t \overset{\circ}{=} \bar{y}$, а каждая формула $F_{t+1}, \ldots, F_n$ отлична от y и $\bar{y}$. Формулы $F_{t+1}, \ldots, F_n$ являются приведёнными. Применим к ним предположение индукции. Существуют такие формулы F_i^0 и F_i^1 в Б, являющиеся упрощениями формул $F_i|_{\{y=0\}}$ и $F_i|_{\{y=1\}}$ соответственно, что выполнено неравенство

$$P(F_i) - \frac{P(F_i^0) + P(F_i^1)}{2} \geqslant \frac{3}{2} L_y(F_i), \quad i = t+1, \ldots, n. \tag{6}$$

Если $n = t$, то формула F реализует одну из функций 0, 1, y, $\bar{y}$. Тогда в силу свойства (i) приведённых формул F графически равна одной из формул 0, 1, y, $\bar{y}$. Случаи $F \overset{\circ}{=} y$ и $F \overset{\circ}{=} \bar{y}$ невозможны по условию леммы, а случаи $F \overset{\circ}{=} 0$ и $F \overset{\circ}{=} 1$ не удовлетворяют условию индуктивного перехода. Таким образом, $n > t$. Рассмотрим два случая: $n = t + 1$ и $n > t + 1$.

Случай 1. Если $t = 0$, то положим $F^0 = f(F_1^0)$ и $F^1 = f(F_1^1)$. Тогда из (6) и равенств $L_y(F) = L_y(F_1)$, $P(F) = P(F_1)$, $P(F^\tau) = P(F_1^\tau)$ $(\tau = 0, 1)$ следует неравенство (5). В случае $t > 0$ рассмотрим функцию

$$\varphi(y, z) = f(y, \ldots, y, \bar{y}, \ldots, \bar{y}, z)$$

(здесь y повторяется s раз, $\bar{y}$ повторяется $t-s$ раз). Из свойства (iii) приведённых формул следует, что функция $\varphi(y,z)$ существенно зависит от переменных y и z. В силу обобщенной монотонности базиса Б функция f монотонна по последней переменной. Поэтому функция $\varphi(y,z)$ монотонна по z. Следовательно, функция $\varphi(y,z)$ нелинейна. Тогда существуют такие булевы константы b, c и d, что $\varphi(c,z)\equiv b$ и $\varphi(\bar{c},z)\equiv z\oplus d$. Положим $F^c=b$, $F^{\bar{c}}=F_n$ при $d=0$ и $F^{\bar{c}}=\bar{F}_n$ при $d=1$.

Формула F^c является упрощением формулы $F|_{\{y=c\}}$. Далее в силу тождества $F\equiv\varphi(y,F_n)$ и свойства (iv) приведённых формул формула F_n не содержит вхождений переменной y. Поэтому формула $F^{\bar{c}}$ является упрощением формулы $F|_{\{y=\bar{c}\}}$. По свойству (ii) приведённых формул F_n отлична от константы, а значит, $P(F_n)\geqslant 1$. Отсюда следует, что

$$\begin{aligned}P(F)-\frac{P(F^0)+P(F^1)}{2}&=\frac{n-2}{2}+t+P(F_n)-\frac{P(F_n)+0}{2}\\&=\frac{t-1}{2}+t+\frac{1}{2}P(F_n)\geqslant\frac{3}{2}t=\frac{3}{2}L_y(F).\end{aligned}$$

Случай 1 рассмотрен.

Случай 2. Для каждой константы τ положим

$$f^\tau=f|^*_{\{x_1=\tau,\dots,x_s=\tau,x_{s+1}=\bar{\tau},\dots,x_t=\bar{\tau}\}},\qquad F^\tau=f^\tau(F^\tau_{t+1},\dots,F^\tau_n).$$

Формула F^τ является упрощением формулы $F|_{\{y=\tau\}}$ в базисе Б. Имеем

$$\begin{aligned}P(F)-\frac{P(F^0)+P(F^1)}{2}&=\frac{n-2}{2}+t+\sum_{i=t+1}^{n}P(F_i)\\&\quad-\frac{(n-t-2)+\sum\limits_{i=t+1}^{n}\left(P(F_i^0)+P(F_i^1)\right)}{2}\\&=\frac{3}{2}t+\sum_{i=t+1}^{n}\left(P(F_i)-\frac{P(F_i^0)+P(F_i^1)}{2}\right)\\&\geqslant\text{ (см. (6)) }\geqslant\frac{3}{2}t+\frac{3}{2}\sum_{i=t+1}^{n}L_y(F_i)=\frac{3}{2}L_y(F).\end{aligned}$$

Случай 2 рассмотрен. Неравенство (5) установлено. Лемма 2 доказана.

Лемма 3. *Пусть Б — нормальный обобщенно монотонный базис, F — формула в базисе Б и $Y_1,\dots,Y_s$ — попарно не пересекающиеся множества переменных мощности l, $s\geqslant 0, l\geqslant 1$. Тогда существуют такая подстановка констант A_s, где $A_s=\{y_1=\sigma_1,\dots,y_s=\sigma_s\}$*

и $y_1 \in Y_1, \ldots, y_s \in Y_s$, *и такая приведённая формула* F_s *в базисе* Б, $F_s \equiv F|_{A_s}$, *что выполнено неравенство*

$$P(F) - P(F_s) \geqslant \frac{3}{2l} L_{Y_1 \cup \ldots \cup Y_s}(F_s). \tag{7}$$

Доказательство. Проведём индукцию по s.

Базис индукции: $s = 0$. Положим $A_s = \varnothing$, а в качестве F_s возьмём приведённую формулу в базисе Б, являющуюся упрощением формулы F. Тогда (7) выполнено.

Индуктивный переход: $s \geqslant 1$. Применим предположение индукции к множествам $Y_1, \ldots, Y_{s-1}$. Существует такая подстановка констант A_{s-1}, где $A_{s-1} = \{y_1 = \sigma_1, \ldots, y_{s-1} = \sigma_{s-1}\}$ и $y_1 \in Y_1, \ldots, y_{s-1} \in Y_{s-1}$, и такая приведённая формула F_{s-1} в базисе Б, $F_{s-1} \equiv F|_{A_{s-1}}$, что выполнено неравенство

$$P(F) - P(F_{s-1}) \geqslant \frac{3}{2l} L_{Y_1 \cup \ldots \cup Y_{s-1}}(F_{s-1}). \tag{8}$$

В качестве y_s возьмём такую переменную из множества Y_s, которая входит в формулу F_{s-1} наибольшее число раз (среди всех переменных из множества Y_s). Тогда

$$L_{y_s}(F_{s-1}) \geqslant \frac{1}{l} L_{Y_s}(F_{s-1}). \tag{9}$$

Если формула F_{s-1} графически равна y_s или $\bar{y}_s$, то положим $A_s = A_{s-1} \cup \{y_s = 0\}$ и $F_s = F_{s-1}|_{\{y_s=0\}}$. Тогда $F_s \equiv F|_{A_s}$. Кроме того, $P(F_s) = 0$, $L_{Y_1 \cup \ldots \cup Y_s}(F_s) = 0$, следовательно, (7) выполнено.

Теперь рассмотрим случай, когда формула F_{s-1} графически не равна ни y_s, ни $\bar{y}_s$. По лемме 2 существуют такая константа σ_s и формула F' в базисе Б, являющаяся упрощением формулы $F_{s-1}|_{\{y_s=\sigma_s\}}$, что выполнено неравенство

$$P(F_{s-1}) - P(F') \geqslant \frac{3}{2} L_{y_s}(F_{s-1}). \tag{10}$$

Положим $A_s = A_{s-1} \cup \{y_s = \sigma_s\}$. В качестве F_s возьмём приведённую формулу в базисе Б, являющуюся упрощением формулы F'. Тогда $F_s \equiv F' \equiv F_{s-1}|_{\{y_s=\sigma_s\}} \equiv F|_{A_s}$. Из (8), (10) и (9) следует, что

$$\begin{aligned} P(F) - P(F_s) &\geqslant P(F) - P(F') = P(F) - P(F_{s-1}) + P(F_{s-1}) - P(F') \\ &\geqslant \frac{3}{2l} L_{Y_1 \cup \ldots \cup Y_{s-1}}(F_{s-1}) + \frac{3}{2} L_{y_s}(F_{s-1}) \geqslant \frac{3}{2l} L_{Y_1 \cup \ldots \cup Y_{s-1}}(F_{s-1}) + \frac{3}{2l} L_{Y_s}(F_{s-1}) \\ &\geqslant \frac{3}{2l} L_{Y_1 \cup \ldots \cup Y_s}(F_s). \end{aligned}$$

Лемма 3 доказана.

Следствие. *Пусть Б — нормальный обобщенно монотонный базис порядка k, $Y_1, \ldots, Y_s$ — попарно не пересекающиеся множества переменных мощности l, $s \geqslant 0$, $l \geqslant 1$ и f — функция, у которой каждая существенная переменная принадлежит одному из множеств $Y_1, \ldots, Y_s$. Тогда существует такая подстановка констант A_s, где $A_s = \{y_1 = \sigma_1, \ldots, y_s = \sigma_s\}$ и $y_1 \in Y_1, \ldots, y_s \in Y_s$, что выполнено неравенство*

$$P_{\text{Б}}(f) \geqslant P_{\text{Б}}(f|_{A_s})\Big(1 + \frac{c_k}{l}\Big), \tag{11}$$

где $c_k = \frac{3k-3}{3k-4}$.

Доказательство. Пусть F — формула в базисе Б, реализующая функцию f, причём $P(F) = P_{\text{Б}}(f)$. По лемме 3 существует такая подстановка констант A_s, где $A_s = \{y_1 = \sigma_1, \ldots, y_s = \sigma_s\}$ и $y_1 \in Y_1, \ldots, y_s \in Y_s$, и приведённая формула F_s в базисе Б, $F_s \equiv F|_{A_s}$, что выполнено (7). Из (7), равенства $L_{Y_1 \cup \ldots \cup Y_s}(F_s) = L(F_s)$ и (1) следует, что

$$\begin{aligned} P_{\text{Б}}(f) &= P(F) = P(F) - P(F_s) + P(F_s) \geqslant \frac{3}{2l} L(F_s) + P(F_s) \\ &\geqslant \frac{3}{2l} \cdot \frac{2k-2}{3k-4} P(F_s) + P(F_s) = P(F_s)\Big(1 + \frac{c_k}{l}\Big) \geqslant P_{\text{Б}}(f|_{A_s})\Big(1 + \frac{c_k}{l}\Big). \end{aligned}$$

Тем самым справедливость неравенства (11) установлена. Следствие доказано.

Пусть s — натуральное число, $n = 2^s$, $l = \lceil \frac{n}{s} \rceil$, $\widetilde{\sigma} = (\sigma_1, \ldots, \sigma_s)$ и $|\widetilde{\sigma}| = \sum_{i=1}^{s} 2^{s-i} \cdot \sigma_i$. Положим

$$\mathscr{A}_n = \bigvee_{\widetilde{\sigma} \in \{0,1\}^s} \Big(x_{|\widetilde{\sigma}| + ls + 1} \bigwedge_{i=1}^{s} (x_{l(i-1)+1} \oplus \ldots \oplus x_{li} \oplus \sigma_i) \Big).$$

Функция $\mathscr{A}_n$ была введена А. Е. Андреевым [1]. Она существенно зависит от $n + ls$ аргументов, причём $n + ls \sim 2n$.

Теорема. *Пусть Б — произвольный нормальный обобщенно монотонный базис порядка k. Тогда при $n \to \infty$*

$$L_{\text{Б}}(\mathscr{A}_n) \succcurlyeq \frac{n^{2+\varepsilon_k}}{\log_2^{c_k} n \log_2 \log_2 n}, \tag{12}$$

где $\varepsilon_k = \frac{1}{3k-4}$ *и* $c_k = \frac{3k-3}{3k-4}$.

Доказательство. Пусть f_s — самая сложная функция от s переменных в классе формул в базисе Б. Тогда согласно [3] имеем

$$L_{\text{Б}}(f_s) \sim \frac{2^s}{\log_2 s} = \frac{n}{\log_2 \log_2 n}. \tag{13}$$

Рассмотрим подстановку констант

$$B = \{x_{sl+1} = f_s(0, \dots, 0), x_{sl+2} = f_s(0, \dots, 0, 1), \dots, x_{sl+n} = f_s(1, \dots, 1)\}.$$

К функции $\mathscr{A}_n|_B$ применим $l-1$ раз следствие из леммы 3. На каждом шаге в качестве $Y_1, \dots, Y_s$ будем брать множества, полученные из множеств $\{x_1, \dots, x_l\}, \dots, \{x_{l(s-1)+1}, \dots, x_{ls}\}$ удалением тех переменных, вместо которых подставлялись константы на предыдущих шагах. После $(l-1)$-й подстановки констант будет получена функция, отличающаяся от f_s биективной заменой переменных и, быть может, навешиванием отрицаний на некоторые переменные. Тогда из (11) следует, что при $l \to \infty$

$$P_{\text{Б}}(\mathscr{A}_n|_B) \geqslant P_{\text{Б}}(f_s) \prod_{i=2}^{l} \left(1 + \frac{c_k}{i}\right) \geqslant P_{\text{Б}}(f_s) \exp\left\{\sum_{i=2}^{l} \ln\left(1 + \frac{c_k}{i}\right)\right\}$$

$$= P_{\text{Б}}(f_s) \exp\left\{\sum_{i=2}^{l} \frac{c_k}{i} + \sum_{j=2}^{\infty} O\left(\frac{c_k^2}{j^2}\right)\right\}$$

$$= P_{\text{Б}}(f_s) \exp\left\{\sum_{i=2}^{l} \frac{c_k}{i} + O(1)\right\} \asymp P_{\text{Б}}(f_s) \exp(c_k \ln l) = P_{\text{Б}}(f_s) l^{c_k}.$$

Поскольку $l = \lceil \frac{n}{s} \rceil$ и $2^s = n$, то, воспользовавшись (13), получаем

$$P_{\text{Б}}(\mathscr{A}_n|_B) \succcurlyeq \frac{n}{\log_2 \log_2 n} \cdot \frac{n^{c_k}}{\log_2^{c_k} n} = \frac{n^{2+\varepsilon_k}}{\log_2^{c_k} n \log_2 \log_2 n}.$$

Отсюда и из соотношений $L_{\text{Б}}(\mathscr{A}_n) \asymp P_{\text{Б}}(\mathscr{A}_n) \geqslant P_{\text{Б}}(\mathscr{A}_n|_B)$ следует (12). Теорема доказана.

Заметим, что если Б — произвольный обобщенно монотонный базис, то оценка (12) также справедлива (достаточно применить теорему к базису [Б]). Если же Б — не обобщенно монотонный базис, то согласно [7, 10] $L_{\text{Б}}(x_1 \oplus \dots \oplus x_n) \asymp n$. Следовательно, $L_{\text{Б}}(\mathscr{A}_n) \preccurlyeq n^2$.

Автор выражает благодарность своему научному руководителю О. Б. Лупанову.

ЛИТЕРАТУРА

1. **Андреев А. Е.** Об одном методе получения более чем квадратичных эффективных нижних оценок сложности π-схем // Вестн. МГУ. Сер. 1. Математика. Механика. 1987. № 1. С. 70–73.

2. **Лупанов О. Б.** О методах получения оценок сложности и вычисления индивидуальных функций // Дискретный анализ: Сб. науч. тр. Новосибирск: Ин-т математики СО АН СССР, 1974. Вып. 25. С. 3–18.

3. **Лупанов О. Б.** Асимптотические оценки сложности управляющих систем. М.: Изд-во МГУ, 1984.
4. **Мучник Б. А. (Субботовская Б. А.)** Оценка сложности реализации линейной функции в некоторых базисах // Кибернетика. 1970. № 4. С. 29–38.
5. **Нечипорук Э. И.** Об одной булевской функции // Докл. АН СССР. 1966. Т. 169, № 4. С. 765–766.
6. **Нигматуллин Р. Г.** Сложность булевых функций. М.: Наука, 1991.
7. **Перязев Н. А.** Сложность представлений булевых функций формулами в немонолинейных базисах. Иркутск: Изд-во Иркут. ун-та, 1995. (Сер.: Дискретная математика и информатика; Вып. 2).
8. **Субботовская Б. А.** О реализации линейных функций формулами в базисе $\vee, \&, ^{-}$ // Докл. АН СССР. 1961. Т. 136, № 3. С. 553–555.
9. **Храпченко В. М.** О сложности реализации линейной функции в классе π-схем // Мат. заметки. 1971. Т. 9, № 1. С. 35–40.
10. **Черухин Д. Ю.** О сложности реализации линейной функции формулами в конечных булевых базисах // Дискрет. математика. 2000. Т. 12, вып. 1. С. 135–144.
11. **Håstad J.** The shrinkage exponent is 2 // 34th Annual symp. on foundations of comput. sci. Proc. Los Alamitos: IEEE Comput. Soc. Press, 1993. P. 114–123.

Адрес автора:

МГУ, мех.-мат. факультет,
Воробьевы горы,
119899 Москва, Россия.
E-mail:
dyucher@mech.math.msu.su

Статья поступила
20 марта 2000 г.