

## НИЖНИЕ ОЦЕНКИ РАЗМЕРА СХЕМ ОГРАНИЧЕННОЙ ГЛУБИНЫ В ПОЛНОМ БАЗИСЕ, СОДЕРЖАЩЕМ ФУНКЦИЮ ЛОГИЧЕСКОГО СЛОЖЕНИЯ

А. А. Разборов

Одна из важнейших задач теории вычислительной сложности — получение хороших нижних оценок для схемной сложности булевых функций из  $NP$ -последовательностей. Несмотря на значительные усилия, прогресс в этой области весьма невелик — наилучшие известные оценки такого рода принадлежат Блюму [1] и составляют  $3n$  ( $n$  — число переменных).

За последние несколько лет удалось получить сверхполиномиальные нижние оценки размера схем, вычисляющих функции из  $NP$ -последовательностей, при различных ограничениях на схемы. В [2, 3] было доказано, что сложность реализации функции логического сложения по  $\text{mod } 2$  схемами ограниченной глубины в базисе  $\{\&, \vee\}$  растет сверхполиномиально от числа переменных. Независимо в [4] для той же задачи была получена более хорошая оценка.

В [5–7] содержатся экспоненциальные нижние оценки размера монотонных схем ограниченной глубины, вычисляющих различные функции. В [8] установлены экспоненциальные нижние оценки реализации функции логического сложения схемами ограниченной глубины в том же базисе  $\{\&, \vee\}$ . В [9] дано более простое доказательство аналогичных оценок.

Другой решенный случай — монотонные схемы в базисе  $\{\&, \vee\}$  (не обязательно ограниченной глубины).

Сверхполиномиальные нижние оценки монотонной сложности для функций из  $NP$ -последовательностей были получены автором в [10, 11]. А. Е. Андреев [12] перенес эти оценки на другие  $NP$ -последовательности с усилением их до экспоненциальных. В [13], независимо от Андреева, Алон и Боппана также усилили оценки из [10, 11] до экспоненциальных.

Рассматриваются схемы ограниченной глубины в базисе  $\{\&, \vee, \oplus\}$ . Так как функция  $x_1 \oplus x_2 \oplus \dots \oplus x_n$  имеет сверхполиномиальную сложность реализации схемами ограниченной глубины в базисе  $\{\&, \vee\}$  (см. [2—4, 8, 9]), то рассматриваемые в настоящей работе схемы являются более сильными вычислительными средствами, чем схемы в базисе  $\{\&, \vee\}$ . Наша цель — доказать экспоненциальную нижнюю оценку для сложности реализации функции голосования с помощью схем ограниченной глубины в базисе  $\{\&, \vee, \oplus\}$ . Вначале мы докажем аналогичную оценку для базиса  $\{\&, \oplus\}$ , а затем укажем, как она переносится на базис  $\{\&, \vee, \oplus\}$  (см. замечание в конце работы).

Метод доказательства в данной работе имеет много сходных черт с методом, используемым в [10—13]. Чтобы подчеркнуть эту аналогию, мы разбиваем настоящую работу на параграфы так же, как и [11]. В § 1 вводятся необходимые определения и доказывается теорема, позволяющая получать нижние оценки размера схем ограниченной глубины с помощью некоторой общей конструкции, которую автор назвал *правильной моделью*. В § 2 из булевых полиномов ограниченных степеней строится серия правильных моделей. Наконец, в § 3 построенные модели используются для того, чтобы доказать экспоненциальную нижнюю оценку сложности реализации функции голосования схемами ограниченной глубины в базисе  $\{\&, \oplus\}$ . Утверждения, которые, как нам кажется, могут быть полезны при оценке сложности других булевых функций, формулируются ниже в виде теорем; остальные — в виде лемм.

§ 1. Схемы ограниченной глубины и правильные модели. Мы будем рассматривать булевы функции от  $n$  переменных  $x_1, x_2, \dots, x_n$ ; число  $n$  считается фиксированным до леммы 6 включительно. Пусть  $B_n \cong \{0, 1\}^n$ ;  $G_n \cong \{0, 1\}^{B_n}$  — семейство всех  $n$ -местных булевых функций. Существует естественное взаимно-однозначное соответствие между  $G_n$  и  $F_2[x_1, \dots, x_n]$  (при этом, разуме-

ется, для полиномов над полем  $F_2$  мы предполагаем  $x_i^2 = x_i$ ); мы будем отождествлять булеву функцию и полином, который ее изображает. Операция сложения в поле  $F_2$  обозначается через  $\oplus$ .

В определении схемы глубины  $k$  в базисе  $\{\&, \oplus\}$  (в дальнейшем — просто схемы глубины  $k$ ) мы, с очевидными изменениями, следуем [3]. Определение дается индукцией по  $k$ .

Схема глубины 0 есть элемент множества  $\{x_1, x_1 \oplus 1, x_2, x_2 \oplus 1, \dots, x_n, x_n \oplus 1\}$ . Схема глубины  $k$  есть непустое множество схем глубины  $(k - 1)$ . Схему глубины  $k$  будем называть  $\oplus$ -схемой, если  $k$  нечетно и  $\&$ -схемой, если  $k$  четно.

Определим теперь для схемы  $C$  глубины  $k$  булеву функцию  $f_C \in G_n$ , которую она вычисляет. Для схем глубины 0 положим  $f_C \Leftrightarrow C$ . Функция  $f_C$ , которая вычисляется  $\oplus$ -схемой ( $\&$ -схемой)  $C$  ненулевой глубины есть  $\bigoplus_{B \in C} f_B$  (соответственно,  $\&_{B \in C} f_B$ ).

Бинарное отношение  $\rightarrow$  для схем определяется как рефлексивное транзитивное замыкание отношения принадлежности. Размером  $s(C)$  схемы  $C$  называется  $|\{B \mid B \rightarrow C\}|$ . Наконец, положим для  $f \in G_n$

$$L_k(f) \Leftrightarrow \min \{s(C) \mid C \text{ — схема глубины } k, f_C = f\}.$$

Для  $f \in G_n$  обозначим  $\|f\| \Leftrightarrow |\{\varepsilon \in B_n \mid f(\varepsilon) = 1\}|$ . Если  $\mathfrak{A} \subseteq G_n$  — семейство булевых функций и  $f \in G_n$ , то

$$\rho(f, \mathfrak{A}) \Leftrightarrow \min \{\|f \oplus g\| \mid g \in \mathfrak{A}\}. \quad (1)$$

Правильной моделью  $\mathfrak{M}$  глубины  $k$  назовем кортеж

$$\mathfrak{M} = \langle \mathfrak{M}_0, \mathfrak{M}_1, \dots, \mathfrak{M}_k, \pi_1, \dots, \pi_k \rangle, \quad (2)$$

где  $\mathfrak{M}_i \subseteq G_n$  ( $0 \leq i \leq k$ );  $\{x_1, x_1 \oplus 1, x_2, x_2 \oplus 1, \dots, x_n \oplus 1\} \subseteq \mathfrak{M}_0$ ;  $\pi_i$  — некоторое отображение вида  $\pi_i: \mathcal{P}(\mathfrak{M}_{i-1}) \rightarrow \mathfrak{M}_i$ . Если  $H \subseteq \mathfrak{M}_{i-1}$ , то положим

$$\delta(H, i) \Leftrightarrow \min_{f \in H} \|\pi_i(H) \oplus * f\|, \quad (3)$$

где  $*$  обозначает  $\oplus$ , если  $i$  нечетно и  $\&$ , если  $i$  четно. Дефектом  $\delta(\mathfrak{M})$  модели (2) назовем число

$$\delta(\mathfrak{M}) \Leftrightarrow \max_{1 \leq i \leq k} \max_{H \subseteq \mathfrak{M}_{i-1}} \delta(H, i);$$

верхним слоем модели  $\mathfrak{M}$  назовем семейство булевых функций  $\mathfrak{M}_k$ .

**ТЕОРЕМА 1.** Допустим, что существует правильная модель глубины  $k$ , дефекта  $\delta$  с верхним слоем  $\mathfrak{M}$ . Тогда для любой булевой функции  $f$  справедливо неравенство

$$L_k(f) \geq \rho(f, \mathfrak{M}) \cdot \delta^{-1}.$$

**Доказательство.** Пусть  $\mathfrak{M} = \langle \mathfrak{M}_0, \mathfrak{M}_1, \dots, \mathfrak{M}_k, \pi_1, \dots, \pi_k \rangle$  — модель, существование которой утверждается в условии теоремы. Определим для любой схемы  $C$  глубины  $i \leq k$  булеву функцию  $f_C^{\mathfrak{M}} \in \mathfrak{M}_i$  индукцией по  $i$ .

Если схема  $C$  имеет глубину 0, то  $f_C \in \mathfrak{M}_0$  в силу определения правильной модели, и мы положим  $f_C^{\mathfrak{M}} \equiv f_C$ . Если схема  $C$  имеет глубину  $i > 0$ , то положим

$$f_C^{\mathfrak{M}} \equiv \pi_i(\{f_B^{\mathfrak{M}} \mid B \in C\}), \quad (4)$$

воспользовавшись тем, что  $f_B^{\mathfrak{M}}$  уже определены. Простая индукция по глубине показывает, что

$$f_C^{\mathfrak{M}} \oplus f_C \leq \bigvee \{ \pi_j(\{f_B^{\mathfrak{M}} \mid B \in D\}) \oplus *_{B \in D} f_B^{\mathfrak{M}} \mid D \rightarrow C \}, \quad (5)$$

где  $*$  обозначает  $\oplus$ , если глубина  $j$  схемы  $D$  нечетна и  $\&$ , если она четна. Из (5), определения дефекта и (3) вытекает

$$\|f_C^{\mathfrak{M}} \oplus f_C\| \leq \delta(\mathfrak{M}) \cdot s(C). \quad (6)$$

Если некоторая схема  $C$  глубины  $k$  вычисляет функцию  $f_C$ , то из (6) и (1) с учетом  $f_C^{\mathfrak{M}} \in \mathfrak{M}$  получаем  $\rho(f_C, \mathfrak{M}) \leq \delta \cdot s(C)$ , что доказывает теорему 1.

**§ 2. Построение правильной модели.** Через  $P(d)$  будем обозначать линейное подпространство в  $G_n$ , образованное всеми полиномами, степень которых не превышает  $d$ . Зафиксируем натуральное  $l$  и положим

$$\mathfrak{M}_{2j} = \mathfrak{M}_{2j+1} \equiv P(l^j) \quad (j \geq 0). \quad (7)$$

Наша ближайшая цель — так определить отображения  $\pi_i: \mathcal{P}(\mathfrak{M}_{i-1}) \rightarrow \mathfrak{M}_i$ , чтобы кортеж  $\langle \mathfrak{M}_0, \mathfrak{M}_1, \dots, \mathfrak{M}_k, \pi_1, \dots, \pi_k \rangle$  превратился в правильную модель дефекта, не превосходящего  $2^{n-l}$ .

Если  $i$  нечетно, то мы, воспользовавшись тем, что  $\mathfrak{M}_{i-1} = \mathfrak{M}_i$  — линейное подпространство в  $G_n$ , просто полагаем  $\pi_i(H) \equiv \bigoplus_{f \in Hf}$  и получаем

$$\delta(H, i) = 0 \quad (i \text{ нечетно}). \quad (8)$$

Для четных  $i$  возможность выбора  $\pi_i$  так, чтобы  $\delta(H, i) \leq 2^{n-i}$  для всех  $H$  составляет утверждение следующей леммы (которая является ключевым моментом доказательства).

**ЛЕММА 1.** Если  $H \subseteq P(d)$ , то существует  $g \in P(dl)$  такое, что  $\|(\&_{f \in Hf}) \oplus g\| \leq 2^{n-l}$ .

**Доказательство.** Пусть  $h = \&_{f \in Hf}$ . Положим  $\text{Ann}(h) \Leftrightarrow \{f \in P(d) \mid f \& h = 0\}$ . Тогда  $\text{Ann}(h)$  является линейным подпространством в  $P(d)$ . Покажем, что можно выбрать последовательность

$$f_1, f_2, \dots, f_t, \dots \quad (9)$$

элементов из  $\text{Ann}(h)$  такую, что  $\|h \oplus (\&_{i=1}^t (f_i \oplus 1))\| \leq 2^{n-t}$ . Последовательность (9) будем строить индукцией по  $t$ .

**База индукции**,  $t = 0$  очевидна:  $\|h\| \leq 2^n$ .

**Шаг индукции.** Пусть многочлены  $f_1, f_2, \dots, f_t$  уже построены:  $\Delta_t \Leftrightarrow \{\varepsilon \mid h(\varepsilon) \neq (\&_{i=1}^t (f_i \oplus 1))(\varepsilon)\}$ ;  $|\Delta_t| \leq 2^{n-t}$ . Так как  $f_i \in \text{Ann}(h)$  ( $1 \leq i \leq t$ ), то  $h \leq f_i \oplus 1$  и, значит,  $h \leq \&_{i=1}^t (f_i \oplus 1)$ . Поэтому, если  $\varepsilon \in \Delta_t$ , то  $h(\varepsilon) = 0$ ;  $(\&_{i=1}^t (f_i \oplus 1))(\varepsilon) = 1$ . Так как  $h = \&_{f \in Hf}$ , то  $\exists (f_0 \in H)$  ( $h \leq f_0$ ;  $f_0(\varepsilon) = 0$ ). Элемент  $1 \oplus f_0$  лежит в  $\text{Ann}(h)$  и  $(1 \oplus f_0)(\varepsilon) = 1$ .

Введем в рассмотрение для каждого  $\varepsilon \in \Delta_t$  линейный функционал  $p_\varepsilon$  на  $\text{Ann}(h)$ , заданный правилом  $p_\varepsilon(f) \Leftrightarrow f(\varepsilon)$ . Предыдущие рассуждения показывают, что для любого  $\varepsilon \in \Delta_t$  функционал  $p_\varepsilon$  невырожден. Пусть  $f$  — случайная величина, равномерно распределенная на  $\text{Ann}(h)$ . Тогда для любого  $\varepsilon \in \Delta_t$  мы получаем  $P[f(\varepsilon) = 1] = 1/2$  и, значит,  $M[|\{\varepsilon \in \Delta_t \mid f(\varepsilon) = 1\}|] = 1/2 |\Delta_t|$ . Выберем в качестве  $f_{t+1}$  такой элемент из  $\text{Ann}(h)$ , для которого  $|\{\varepsilon \in \Delta_t \mid f_{t+1}(\varepsilon) = 1\}| \geq 1/2 |\Delta_t|$ . После этого оказывается  $|\Delta_{t+1}| \leq 1/2 |\Delta_t| \leq 2^{n-t-1}$ , что завершает шаг индукции.

Итак, последовательность (9) построена. Положив  $g = \&_{i=1}^l (f_i \oplus 1)$ , мы получим элемент с требуемыми в лемме 1 свойствами. Лемма 1 доказана.

Итак, мы доказали, что для любого натурального  $l$  существует правильная модель глубины  $k$  с верхним слоем  $P(U^{[k/2]})$  и дефектом, не превосходящим  $2^{n-l}$ . На основании теоремы 1 получаем следующий результат:

**ТЕОРЕМА 2.**  $L_k(f) \geq \rho(f, P(U^{[k/2]})) \cdot 2^{l-n}$ .

§ 3. Нижние оценки для функции голосования. Функцией голосования называется следующая булева функция из  $G_n$ :  $\text{MAJ}(n)(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n) = 1 \Leftrightarrow$  среди  $\varepsilon_1, \dots, \varepsilon_n$  содержится  $\geq n/2$  единиц.

Вместо того, чтобы оценивать величину  $\rho(\text{MAJ}(n), P(d))$  (для некоторого  $d$ ), мы вначале попробуем решить ту же задачу для какой-нибудь симметрической функции  $f$ . Для этого нам понадобится идея, которая уже по крайней мере один раз встречалась в литературе (см. [14, § 11]). Нам кажется, что метод, о котором идет речь, заслуживает того, чтобы быть сформулированным в полной общности.

Допустим на время, что  $k$  — произвольное поле;  $V$  — конечномерное векторное пространство над  $k$ ;  $X \subseteq V$  — множество, порождающее  $V$  как векторное пространство. Тогда для любого  $v \in V$  определена величина  $L^X(v) \Leftrightarrow \Leftrightarrow \min \{ \|X_0\| \mid X_0 \subseteq X \text{ и } v \text{ лежит в линейной оболочке множества } X_0 \}$ . Рассматриваемый метод предназначен для оценки снизу величины  $L^X(v)$  и состоит в следующем. Пусть  $A: V \rightarrow M$  — некоторый линейный оператор ( $M$  — пространство матриц некоторого размера над полем  $k$ ). Положим  $r = \max \{ \text{rg}(A(x)) \mid x \in X \}$ . Тогда для любого  $v \in V$  имеет место оценка  $L^X(v) \geq r^{-1} \cdot \text{rg}(A(v))$ .

Вернемся теперь к нашей задаче. Для любых  $d', d''$  таких, что  $d' + d'' \leq n$ , построим линейный оператор  $A_{d', d''}: G_n \rightarrow M \left( \binom{n}{d'} \times \binom{n}{d''} \right)$  (через  $M(p \times q)$  здесь и далее обозначается пространство матриц размера  $p \times q$  над полем  $F_2$ ). Мы предполагаем, что строки матриц из  $M \left( \binom{n}{d'} \times \binom{n}{d''} \right)$  занумерованы  $d'$  — элементными подмножествами  $I$  множества  $\{1, 2, \dots, n\}$ , а столбцы —  $d''$  — элементными подмножествами  $J$ . Для любого  $K \subseteq \subseteq \{1, 2, \dots, n\}$  введем обозначение

$$B_n(K) \Leftrightarrow \{ \varepsilon = (\varepsilon_1, \dots, \varepsilon_n) \in B_n \mid \forall (i \in K)(\varepsilon_i = 0) \}.$$

Отметим, что

$$B_n(K_1 \cup K_2) = B_n(K_1) \cap B_n(K_2). \quad (10)$$

В этих обозначениях оператор  $A_{d', d''}$  задается формулой:

$$A_{d', d''}: f \mapsto A, \text{ где } a_{IJ} \Leftrightarrow \bigoplus_{\varepsilon \in B_n(I \cup J)} f(\varepsilon). \quad (11)$$

ЛЕММА 2. а) если  $d' + d'' + d < n$  и  $f \in P(d)$ , то  $A_{d', d''}(f) = 0$ ; б) если  $\|f\| = 1$ , то  $\text{rg}(A_{d', d''}(f)) \leq 1$ .

**Доказательство.** а) в силу линейности достаточно рассмотреть случай, когда  $f$  — одночлен. Пусть  $f = \sum_{i \in K} x_i$ ;  $|K| \leq d$ ;  $A_{d', d''}(f) = A$ . Тогда  $a_{IJ} = \sum_{e \in V_n(I \cup J)} \sum_{i \in K} \varepsilon_i$ . Так как  $|I \cup J \cup K| < n$ , то  $a_{IJ}$  равно сумме четного числа единиц (в частности, если  $K \cap (I \cup J) \neq \emptyset$ , то это число единиц равно нулю) и, стало быть, нулю в поле  $F_2$ ; б) из (10) и (11) следует равенство  $A_{d', d''}(f) = A_{d', 0}(f) \cdot A_{0, d''}(f)$ , истинное при условии  $\|f\| = 1$ . Отсюда непосредственно вытекает пункт б).

**ЛЕММА 3.** Если  $d' + d'' + d < n$ , то  $\rho(f, P(d)) \geq \text{rg}(A_{d', d''}(f))$ .

**Доказательство.** Выберем на основании (1) полином  $g \in P(d)$  такой, что  $\|f \oplus g\| = \rho(f, P(d))$ . Тогда  $\text{rg}(A_{d', d''}(f)) \leq \text{rg}(A_{d', d''}(f \oplus g)) + \text{rg}(A_{d', d''}(g))$ . Первое слагаемое не превосходит  $\|f \oplus g\|$  по лемме 2б), а второе равно нулю на основании пункта а) той же леммы. Лемма 3 доказана.

**ТЕОРЕМА 3.** Для любых  $d', d''$  таких, что  $d' + d'' < n$ , имеем  $L_k(f) \geq \exp_2((n - d' - d'' - 1)^{2/k} - n) \text{rg}(A_{d', d''}(f))$ .

**Доказательство.** Теорема непосредственно вытекает из теоремы 2 и леммы 3, если положить  $l = (n - d' - d'' - 1)^{2/k}$ ;  $d = n - d' - d'' - 1$ .

Введем теперь в рассмотрение специальные матрицы пересечений  $P_{d', d''}$  размера  $\binom{n}{d'} \times \binom{n}{d''}$ , которые имеют следующее определение:

$$P_{IJ} = \begin{cases} 0, & \text{если } I \cap J \neq \emptyset, \\ 1, & \text{если } I \cap J = \emptyset. \end{cases} \quad (12)$$

**ЛЕММА 4.** Пусть  $d < n/2$ . Рассмотрим матрицу  $P_d = (P_{d,0}; P_{d,1}; \dots; P_{d,d})$ , полученную записыванием матриц пересечений  $P_{d,0}; P_{d,1}; \dots; P_{d,d}$  в одну линию (с соблюдением нумерации строк). Тогда  $\text{rg}(P_d) = \binom{n}{d}$ .

**Доказательство.** Нам надо показать, что строки матрицы  $P_d$  линейно независимы, т. е. для любой ненулевой матрицы  $H \in M\left(1 \times \binom{n}{d}\right)$  имеем  $HP_d \neq 0$ . Для этого рассмотрим полином  $f_H = \sum_{|I|=d} h_{1,I} \sum_{i \in I} x_i$ . Выберем  $I_0$  такое, что  $h_{1,I_0} \neq 0$  и осуществим в полиноме  $f_H$  подстановку  $\{x_i \mapsto 1 \mid i \notin I_0\}$ . После этой подстановки получится ненулевой полином от переменных  $\{x_i \mid i \in I_0\}$ , так как член  $\sum_{i \in I_0} x_i$  остался нетронутым. Следовательно, полученный после подстановки полином обращается в

единицу при некотором распределении переменных  $\{\varepsilon_i \mid i \in I_0\}$ . Полагая остальные позиции равными единице, мы найдем в итоге  $\varepsilon \in B_n$ , содержащий не более  $d$  нулей и такой, что  $f_H(\varepsilon) = 1$ .

Пусть  $J = \{i \mid \varepsilon_i = 0\}$ ;  $|J| \leq d$ . Тогда  $1 = f_H(\varepsilon) = \bigoplus_{|I|=d} h_{1,I} \&_{i \in I} \varepsilon_i$ . Заметим, что  $\&_{i \in I} \varepsilon_i = p_{IJ}$ . Отсюда  $\bigoplus_{|I|=d} h_{1,I} p_{IJ} = 1$  и, значит,  $HP_d \neq 0$ . Лемма 4 доказана.

Следствие.  $\forall \left(d' < \frac{n}{2}\right) \exists (d'' \leq d') \left(\text{rg}(P_{d', d''}) \geq \frac{1}{n} \binom{n}{d'}\right)$ .

Доказательство очевидно.

Теперь мы докажем, что  $P_{d', d''} = A_{d', d''}(f)$  для некоторой симметрической булевой функции  $f$ .

ЛЕММА 5. Пусть  $d' + d'' < n$ . Тогда существует симметрическая функция  $f$  такая, что  $A_{d', d''}(f) = P_{d', d''}$ .

Доказательство. Запишем искомую функцию  $f$  в виде

$$f = \bigoplus_{d=0}^{d'+d''} \lambda_d T_{n-d, n},$$

где  $T_{s, n} = \bigoplus_{|I|=s} \&_{i \in I} x_i$  — однородный симметрический полином степени  $s$ , а  $\lambda_d \in F_2$  — неизвестные пока коэффициенты. Пусть  $A = A_{d', d''}(f)$ ;  $|I| = d'$ ;  $|J| = d''$ ;  $K = I \cup J$ ;  $|K| = u$ ; тогда  $a_{IJ} = \bigoplus_{\varepsilon \in B_n(K)} \bigoplus_{d=0}^{d'+d''} \lambda_d T_{n-d, n}(\varepsilon) = \bigoplus_{d=0}^{d'+d''} \lambda_d \left(\bigoplus_{\varepsilon \in B_n(K)} T_{n-d, n}(\varepsilon)\right)$ . Обозначим  $\bigoplus_{\varepsilon \in B_n(K)} T_{n-d, n}(\varepsilon)$  через  $\varphi(n, d, u)$ ; тогда  $\varphi(n, d, u) = \bigoplus_{\varepsilon \in B_n(K)} T_{n-d, n}(\varepsilon) = \bigoplus_{i=0}^{n-u} \binom{n-u}{i} \binom{i}{n-d}$  (где  $\binom{p}{q}$  равно по определению нулю, если  $p < q$ ). Отсюда непосредственно видно, что  $\varphi(n, u, u) = 1$ ;  $\varphi(n, d, u) = 0$ , если  $u > d$ .

Искомое условие  $A = P_{d', d''}$  в силу (12) эквивалентно системе

$$\left\{ \bigoplus_{d=0}^{d'+d''} \lambda_d \varphi(n, d, u) = \delta_{u, d'+d''} \right\}_{u=\max(d', d'')},$$

где  $\delta$  — символ Кронекера. В силу сказанного выше, эта система имеет треугольный вид и, стало быть, существует ее решение  $\lambda_0, \lambda_1, \dots, \lambda_{d'+d''}$ , которое и доставляет нам требуемую симметрическую функцию  $f$ . Лемма 5 доказана.

Теперь мы в состоянии оценить  $L_k(f)$  для какой-нибудь симметрической функции  $f$ .

ЛЕММА 6. Для любого  $k$  существует симметрическая функция  $f$  такая, что  $L_k(f) \geq \frac{1}{70n^2} \exp_2(n^{1/k})$ .



Доказательство. Положим  $d' = \lfloor n/2 - \sqrt{n} \rfloor$  и применим следствие к лемме 4. Мы найдем  $d'' \leq d'$  такое, что  $\text{rg}(P_{d', d''}) \geq \frac{1}{n} \binom{n}{n/2 - \sqrt{n}} \geq \frac{2^n}{70n^2}$ . На основании леммы 5, для некоторой симметрической функции  $f$  имеем  $A_{d', d''}(f) = P_{d', d''}$ . Лемма 6 для этой функции  $f$  непосредственно следует из теоремы 3.

Докажем, наконец, наш основной результат.

**ТЕОРЕМА 4.** Для любого фиксированного  $k$  справедливо

$$L_k^{\&, \oplus}(\text{MAJ}(n)) = \exp(\Omega(n^{1/k+1})),$$

где  $L_k^{\&, \oplus}$  обозначает сложность реализации схемами глубины  $k$  в базисе  $\{\&, \oplus\}$ .

Доказательство. Любая симметрическая функция  $f(x_1, \dots, x_n)$  допускает представление в виде  $f(x_1, \dots, x_n) = \bigoplus_{i=0}^n \lambda_i \text{MAJ}(2n)(x_1, \dots, x_n, 1^i, 0^{n-i})$ , где  $\lambda_i \in \mathbb{F}_2$ . Отсюда вытекает  $L_{k+1}(f) \leq n L_k(\text{MAJ}(2n))$  для любой симметрической функции  $f(x_1, \dots, x_n)$ . Выбирая в качестве  $f$  функцию, существование которой утверждается в лемме 6, мы получим

$$L_k(\text{MAJ}(2n)) \geq \frac{1}{70n^2} \exp_2(n^{1/k+1}). \quad (13)$$

Из (13) вытекает теорема 4.

Замечание 1. Так как  $\bigvee_{i=1}^t f_i = 1 \oplus \&_{i=1}^t (f_i \oplus 1)$ , то  $L_k^{\&, \vee} = \Omega(L_{2k}^{\&, \oplus})$ , где  $L_k^{\&, \vee}$  — сложность реализации схемами глубины  $k$  в базисе  $\{\&, \vee, \oplus\}$  (при этом порядок, в котором применяются операции, может быть любым). Отсюда вытекает анонсированная в [15] оценка

$$L_k^{\&, \vee}(\text{MAJ}(n)) = \exp(\Omega(n^{1/2k+2})). \quad (14)$$

(14), в свою очередь, влечет предположение из работы [3] о том, что неверно  $\text{majority} \leq_{\text{ср}} \text{parity}$  (все необходимые определения см. там же).

Замечание 2. Пока статья находилась в печати, автору стало известно о новых результатах в этой области [16, 17]. В частности, в [16] доказано обобщение теоремы 4 с заменой в ней  $\oplus$  на  $\text{MOD } q$ , где  $q$  — степень простого числа. В [17] упрощены рассуждения § 3 и усилена оценка теоремы 4.

## СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

- [1] Blum N. A Boolean function requiring  $3n$  network size // Theoretical Computer Science. 1984. V. 28. P. 337—345.
- [2] Furst M., Saxe J. B., Sipser M. Parity, circuits and the polynomial time hierarchy // Proceedings 22nd Ann. IEEE Symp. on Foundations of Computer Science. 1981. P. 260—270.
- [3] Furst M., Saxe J. B., Sipser M. Parity, circuits and the polynomial time hierarchy // Math. Syst. Theory. 1984. V. 17. P. 13—27.
- [4] Ajtai M.  $\sum_1^1$  formulas on finite structures // Ann. of Pure and Applied Logic. 1983. V. 24. P. 1—48.
- [5] Valiant L. G. Exponential lower bounds for restricted monotone circuits // Proc. 15th Ann ACM Symp. on Theory of Comp. 1983. P. 110—187.
- [6] Borraja R. Threshold functions and bounded depth monotone circuits // Proc. 16th Ann. ACM Symp. on Theory of Comp. 1984. P. 475—479.
- [7] Klawe M., Paul W., Pippenger N., Yannakakis M. On monotone formulas with restricted depth // там же. P. 480—487.
- [8] Yao A. Separating the Polynomial-Time Hierarchy by Oracles // Proc. 26th Ann. IEEE Symp. on Found. of Comp. Science, 1985. P. 1—10.
- [9] Hastad J. Almost Optimal Lower Bounds for Small Depth Circuits // Preprint, 1985.
- [10] Разборов А. А. Нижние оценки монотонной сложности некоторых булевых функций // ДАН СССР. 1985. Т. 281, № 4. С. 798—801.
- [11] Разборов А. А. Нижние оценки монотонной сложности логического перманента // Математические заметки. 1985. Т. 37, вып. 6. С. 887—900.
- [12] Андреев А. Е. Об одном методе получения нижних оценок сложности индивидуальных монотонных функций // ДАН СССР. 1985. Т. 282, № 5. С. 1033—1037.
- [13] Alon N., Borraja R. B. The monotone circuit complexity of Boolean functions // Preprint, 1985.
- [14] Григорьев Д. Ю. Нижние оценки в алгебраической сложности вычислений // Теория сложности вычислений. I. (Зап. научн. семин. ЛОМИ, т. 118) / Л.: Наука, 1982.
- [15] Разборов А. А. Нижние оценки размера схем ограниченной глубины в базисе  $\{\&, \vee, \oplus\}$  // Успехи мат. наук. 1986. Т. 41, вып. 4. С. 219—220.
- [16] Smolensky R. Algebraic methods in the theory of Lower bounds for Boolean circuit complexity // Preprint. Berkeley: University of California. 1986.
- [17] Paterson M. Bounded depth circuits over  $\{\oplus, \wedge\}$  // Preprint. University of Warwick, 1986.