

НИЖНИЕ ОЦЕНКИ СЛОЖНОСТИ РЕАЛИЗАЦИИ СИММЕТРИЧЕСКИХ БУЛЕВЫХ ФУНКЦИЙ КОНТАКТНО-ВЕНТИЛЬНЫМИ СХЕМАМИ

А. А. Разборов

Контактно-вентильными схемами называют электрические схемы, составленные из замыкающих и размыкающих контактов, а также вентилей (в англоязычной литературе контактно-вентильные схемы известны под названием *недетерминированных ветвящихся программ*). С теоретической точки зрения на сегодняшний день интерес представляют также следующие частные случаи этих схем: ветвящиеся программы и контактные (неупорядоченные) схемы. Ветвящиеся программы и контактные схемы в некотором строго уточняемом смысле (см., например, [1]) соответствуют детерминированным вычислениям с ограничениями на память, а контактно-вентильные схемы — недетерминированным. Поэтому контактно-вентильные схемы рассматриваются как по существу более сильная вычислительная модель, чем ветвящиеся программы и контактные схемы.

В настоящей статье мы доказываем нелинейные нижние оценки для сложности реализации ряда симметрических булевых функций произвольными контактно-вентильными схемами. На эту тему ранее были известны следующие результаты.

А. А. Марков [2] полностью решил рассматриваемую нами задачу в монотонном случае. Именно для всех монотонных симметрических булевых функций он точно вычислил сложность их реализации монотонными контактно-вентильными схемами. Она оказалась равной $k(n - k + 1)$ для пороговой функции $T_{k,n}$. Для сравнения отметим установленную О. Б. Лупановым в 1965 г. верхнюю оценку $O(n^{3/2})$ сложности реализации любой пороговой функции контактно-вентильными схемами (не обязательно монотонными).

Общий метод доказательства нелинейных нижних оценок сложности реализации, пригодный для контактных схем (и, следовательно, для ветвящихся программ, так как последние являются частным случаем контактных схем) был предложен Э. И. Нечипорук [3]. П. Пудлак [1] заметил, что метод Нечипорука позволяет получать нелинейные (но более слабые) нижние оценки

для произвольных контактно-вентильных схем. Однако метод Нечипорука неприменим к симметрическим булевым функциям.

В [4—6] были доказаны различные нелинейные нижние оценки для сложности реализации симметрических булевых функций ветвящимися программами ограниченной ширины. П. Пудлак [7] установил нижнюю оценку $\Omega(n \log \log n / \log \log \log n)$ для сложности реализации некоторых симметрических булевых функций ветвящимися программами общего вида. Другие оценки для ветвящихся программ ограниченной ширины можно найти в более поздних работах [8—10].

М. И. Гринчук [11] установил нелинейную нижнюю оценку $\Omega(n \log^{**} n)$ сложности реализации различных симметрических булевых функций (и, в частности, функции голосования) контактными схемами и полностью классифицировал симметрические булевы функции, имеющие нелинейную сложность реализации такими схемами.

В настоящей статье мы доказываем нижние оценки вида $\Omega(n \log \log \log^* n)$ для сложности реализации ряда симметрических булевых функций (включая функцию голосования) контактно-вентильными схемами общего вида. Отсюда вытекают аналогичные нижние оценки для более слабых моделей: ветвящихся программ и контактных схем. Эти оценки усиливают оценки Гринчука [11] для контактных схем, хотя и уступают оценкам Пудлака [7] для ветвящихся программ. Наш метод позволяет также в обширном классе симметрических функций полностью описать функции, имеющие нелинейную сложность реализации контактно-вентильными схемами.

Несколько слов о методе доказательства и строении работы. В [12] задача получения нижних оценок для сложности реализации булевых функций произвольными функциональными схемами была сведена к некоторой чисто комбинаторной задаче типа «МИНИМАЛЬНОЕ ПОКРЫТИЕ». В п. 1 настоящей работы мы устанавливаем аналогичную редукцию для контактно-вентильных схем (теорема 1). В этом же пункте формулируется основная комбинаторная лемма, оценивающая снизу минимальное число покрывающих множеств в задаче «МИНИМАЛЬНОЕ ПОКРЫТИЕ», полученной при применении теоремы 1 к симметрическим булевым функциям и на ее основе устанавливаются главные результаты работы. П.2 целиком посвящен доказательству Основной леммы, существенно опирающемуся на теорию Рамсея.

1. Редукция к задаче типа «МИНИМАЛЬНОЕ ПОКРЫТИЕ». На протяжении всей работы через B^n обозначается булев куб $\{0, 1\}^n$ размерности n , через F_n — семейство всех булевых функций от n переменных. Если $u \in B^n$, то u^i ($1 \leq i \leq n$) обозначает i -ю координату u . Пусть $X_i^\varepsilon \Leftrightarrow \{u \in B^n \mid u^i = \varepsilon\}$ ($1 \leq i \leq$

¹) Функция $\log^{**} n$ и функция $\log^* n$ из следующего абзаца — это медленно стремящиеся к бесконечности функции, точное определение которых мы приведем в п. 1.

$\leq n$, $\varepsilon \in \{0, 1\}$). Если $f \in F_n$, $U \subseteq B^n$, $\varepsilon \in \{0, 1\}$, то запись $\forall u \in U (f(u) = \varepsilon)$ будет сокращаться до $f(U) = \varepsilon$. \blacksquare

Как обычно, мы измеряем сложность с точностью до мультипликативной константы. Это соглашение позволяет нам принять следующее определение контактно-вентильных схем, эквивалентное обычному, но более удобное с технической точки зрения.

Контактно-вентильной схемой (или *недетерминированной ветвящейся программой*) с n переменными называется четверка $\langle G, s, t, \mu \rangle$, где G — ориентированный граф (W, E) с двумя выделенными вершинами s и t , а μ — функция, ставящая в соответствие каждому ребру $e \in E$ метку $\mu(e) \in \{X_i^\varepsilon \mid 1 \leq i \leq n, \varepsilon \in \{0, 1\}\} \cup \{B^n\}$. Схема $\langle G, s, t, \mu \rangle$ реализует (или вычисляет) булеву функцию f , определенную следующим образом: для $u \in B^n$ полагаем $f(u) = 1$, если и только если существует ориентированный путь $e_1 e_2 \dots e_l$ из s в t такой, что $u \in \bigcap \{\mu(e_j) \mid 1 \leq j \leq l\}$. *Размером* схемы $\langle G, s, t, \mu \rangle$ называется число тех ребер $e \in E$, метки которых отличны от B^n . Соответствующую меру сложности мы будем обозначать через $RS(f)$.

Пример 1. Пусть для каждого ребра в E существует ребро с той же меткой и соединяющее те же пары вершин, но противоположно ориентированное. Тогда мы можем стереть ориентацию всех ребер и получить определение неупорядоченной *контактной схемы*. Соответствующая мера сложности обозначается через $S(f)$; мы таким образом, установили, что $S(f) \geq \Omega(RS(f))$.

Пример 2 [1]. Рассмотрим теперь в некотором смысле противоположное ограничение, состоящее в требовании ацикличности графа G . Мы получим определение *упорядоченной контактной схемы*. Соответствующая мера сложности обозначается через $DS(f)$ ¹⁾; таким образом, $DS(f) \geq \Omega(RS(f))$.

Пример 3. Рассмотрим теперь частный случай упорядоченных контактных схем, наложив на них следующее дополнительное ограничение. Из всякой вершины $w \in W$ выходит либо 0 либо 2 ребра, причем в последнем случае их метки имеют вид X_i^0 и X_i^1 (в частности, не существует ребер с меткой B^n). Мы получим определение *ветвящейся программы* (обозначение меры сложности — $BP(f)$). Таким образом, $BP(f) \geq \Omega(DS(f))$ ($\geq \Omega(RS(f))$).

Зафиксируем теперь два произвольных непересекающихся подмножества $U, V \subseteq B^n$. Обозначим через \mathcal{F} семейство всех монотонных функционалов $F: \mathcal{P}(U) \rightarrow \{0, 1\}$, не равных тождественно константе. Для $1 \leq i \leq n$, $\varepsilon \in \{0, 1\}$, $A \subseteq U$ полагаем

$$\delta_{i, \varepsilon}(A) \Leftrightarrow \{ (F, v) \in \mathcal{F} \times V \mid v^i = \varepsilon, F(A) = 1, F(A \cap X_i^\varepsilon) = 0 \}. \quad (1)$$

¹⁾ В определении Пудлака [1] размер упорядоченной контактной схемы определяется числом *всех* ребер в графе G , в том числе и ребер с тривиальной меткой B^n . Все наши результаты остаются в силе для модифицированной в соответствии с этим меры DS .

Пусть, далее,

$$\Delta \ni \{\delta_{i, \varepsilon}(A) \mid 1 \leq i \leq n, \varepsilon \in \{0, 1\}, A \subseteq U\}.$$

Мы будем говорить об элементах множества $\mathcal{F} \times V$ как о *точках*, а об элементах множества Δ — как о *покрывающих множествах*. Обозначим через $\tau(U, V)$ наименьшее число множеств, покрывающих все точки из $\mathcal{F} \times V$. Следующая теорема является переносом результатов из § 4 работы [12] на случай контактно-вентильных схем.

ТЕОРЕМА 1. Пусть $U, V \subseteq B^n$; $U \cap V = \emptyset$. Тогда $\tau(U, V) = \min \{RS(f) \mid f \in F_n, f(U) = 0, f(V) = 1\}$.

Доказательство. а) Пусть $\langle G, s, t, \mu \rangle$ — контактно-вентильная схема, вычисляющая некоторую функцию f такую, что $f(U) = 0, f(V) = 1$, причем размер схемы $\langle G, s, t, \mu \rangle$ равен $RS(f)$. Для каждой вершины w графа $G = (W, E)$ через f_{sw} обозначим функцию, реализуемую схемой $\langle G, s, w, \mu \rangle$. Очевидно, $f_{ss} = 1$ и $f_{st} = f$. Для всякого ребра $e = \langle w, w' \rangle$ с меткой $\mu(e) = X_i^{\varepsilon}$ введем в рассмотрение множество $\delta(e) \ni \delta_{i, \varepsilon}(U \cap f_{sw}^{-1}(1))$. Утверждается, что $RS(f)$ множеств $\{\delta(e) \mid \mu(e) \neq B^n\}$ покрывает все точки из $\mathcal{F} \times V$.

В самом деле, пусть (F, v) — произвольная точка. Рассмотрим некоторый путь $s = w_0, w_1, \dots, w_l = t$, соответствующий вычислению $f_{st}(v) = 1$. Так как F не равен тождественно константе, то $F(U) = 1, F(\emptyset) = 0$. Следовательно, существует j ($0 \leq j \leq l - 1$) такое, что

$$F(U \cap f_{sw_j}^{-1}(1)) = 1, \quad (2)$$

$$F(U \cap f_{sw_{j+1}}^{-1}(1)) = 0. \quad (3)$$

Заметим, что $\mu(\langle w_j, w_{j+1} \rangle) \neq B^n$, так как в противном случае было бы $f_{sw_{j+1}} \geq f_{sw_j}$ и, в силу монотонности, $F[U \cap f_{sw_{j+1}}^{-1}(1)] \geq F[U \cap f_{sw_j}^{-1}(1)]$ вопреки (2), (3). Утверждается, что $\delta(\langle w_j, w_{j+1} \rangle)$ покрывает (F, v) .

В самом деле, пусть $\mu(\langle w_j, w_{j+1} \rangle) = X_i^{\varepsilon}, A = U \cap f_{sw_j}^{-1}(1)$. По определению пути $w_0, w_1, \dots, w_l, v^i = \varepsilon$, что доказывает первое условие в (1). Формула (2) в точности означает второе условие в (1). Наконец, $A \cap X_i^{\varepsilon} \subseteq U \cap f_{sw_{j+1}}^{-1}(1)$, поэтому последнее условие в (1) вытекает из (3) и монотонности функционала F .

б) Пусть теперь $\Delta_0 \subseteq \Delta$ покрывает все точки из $\mathcal{F} \times V$; $|\Delta_0| = \tau(U, V)$. Построим следующую контактно-вентильную схему $\langle G, s, t, \mu \rangle$. В качестве G возьмем граф с множеством вершин $\mathcal{P}(U)$ и следующим множеством ребер. Для каждой пары A, B ($A \subseteq B \subseteq U$) введем ребро $\langle A, B \rangle$ с меткой B^n . Для каждого элемента $\delta_{i, \varepsilon}(A) \in \Delta_0$ введем ребро $\langle A, A \cap X_i^{\varepsilon} \rangle$ с меткой X_i^{ε} . Положим $s \ni U, t \ni \emptyset$. Легко видеть (ср. с доказательством теоремы 2.6 в [12]), что эта схема имеет размер $|\Delta_0| =$

$= \tau(U, V)$ и реализует булеву функцию f такую, что $f(U) = 0$, $f(V) = 1$. ■

З а м е ч а н и е 1. Для лучшего понимания поведения величины $\tau(U, V)$ сформулируем еще одно ее свойство.

П р е д л о ж е н и е 1. Существует вероятностное распределение на Δ , относительно которого каждая точка покрывается с вероятностью $\geq \Omega(1/n)$.

Это предложение доказывается аналогично лемме 3.1 из работы [12] и не используется в дальнейшем, поэтому мы опускаем его доказательство. ■

Из предложения 1, в частности, вытекает, что прямые вероятностные методы непригодны для получения нелинейных нижних оценок для величины $\tau(U, V)$.

Напомним некоторые общепринятые теоретико-множественные обозначения: $[n] \doteq \{1, 2, \dots, n\}$, $[A]^s \doteq \{B \in \mathcal{P}(A) \mid |B| = s\}$. Элементы $[A]^s$ также называются s -подмножествами. $[[n]]^s$ сокращается до $[n]^s$. В дальнейшем нам будет удобно отождествлять B^n с $\mathcal{P}([n])$.

Через $t(x, y)$ обозначается «функция башни» двух натуральных аргументов x и y , определяемая следующей рекурсией:

$$t(0, y) \doteq y,$$

$$t(x+1, y) \doteq 2^{t(x, y)}.$$

Положим $\log^* n \doteq \max \{x \mid t(x, 1) \leq n\}$. Обозначим через $t'(x)$ итерацию функции $t(x, 1)$:

$$t'(0) \doteq 1;$$

$$t'(x+1) \doteq t(t'(x), 1).$$

Функция $\log^{**} n$ определяется следующим образом: $\log^{**} n \doteq \max \{x \mid t'(x) \leq n\}$.

ОСНОВНАЯ ЛЕММА. Существует $\varepsilon > 0$ такое, что при любых n, q, d, s , для которых выполняются условия

$$\left. \begin{aligned} & \text{Н. О. К. } (1, \dots, q) \mid d, \\ & dq^{2/\varepsilon} \leq s \leq \varepsilon (\log^* n)^{1/2}, \end{aligned} \right\} \quad (4)$$

справедлива оценка $\tau([n]^{s-d}, [n]^s) \geq \Omega(n \log q)$.

Доказательству Основной леммы посвящен весь следующий пункт. Сейчас же мы приведем один пример, демонстрирующий важность первого условия в (4).

П р и м е р 4. Пусть d нечетно, так что первое условие в (4) заведомо невыполнено (при $q \geq 3$). Тогда $[n]^{s-d}$ и $[n]^s$ отделяются функцией $x_1 \oplus \dots \oplus x_n$ сложения по модулю 2. Эта функция вычисляется очевидной ветвящейся программой размера $O(n)$. Поэтому в силу теоремы 1 $\tau([n]^{s-d}, [n]^s) \leq O(n)$. Выпишем соответствующее покрытие в явном виде. Оно состоит из всех элементов вида $\delta_{i, \varepsilon}(A_{i, \nu})$, где $i \in [n]$; $\varepsilon, \nu \in \{0, 1\}$ и $A_{i, \nu} \doteq \{u \in$

$\in [n]^{s-d} \mid u \cap [i-1] \mid \equiv v \pmod{2}$). Мы еще вернемся к этому примеру в следующем пункте.

Теорема 1 и Основная лемма позволяют доказать нелинейные нижние оценки для сложности реализации контактно-вентильными схемами многих симметрических булевых функций. Мы рассмотрим в качестве примеров следующие наиболее часто встречающиеся в литературе функции $E_{k,n}$, $T_{k,n}$, $MAJORITY_n$, $MOD_{k,n}$ ($k \leq n$):

$$E_{k,n}(u) = 1 \Leftrightarrow |u| = k,$$

$$T_{k,n}(u) = 1 \Leftrightarrow |u| \geq k,$$

$$MAJORITY_n \Leftrightarrow T_{n/2,n},$$

$$MOD_{k,n}(u) = 1 \Leftrightarrow k \mid |u|.$$

ТЕОРЕМА 2. Пусть H обозначает любую из трех функций E , T , MOD . Тогда $RS(H_{k,n}) \geq \Omega((n-k) \cdot \log \log \min(k, \log^* n))$. В частности, $RS(MAJORITY_n) \geq \Omega(n \cdot \log \log \log^* n)$.

Доказательство. При $n-k \leq n^{1/2}$ доказываемая оценка становится тривиальной, поэтому мы можем считать, что $n-k > n^{1/2}$ и, следовательно, $\log^*(n-k) \geq \Omega(\log^* n)$. Положим $s \Leftrightarrow \min(k, \varepsilon (\log^*(n-k))^{1/2})$ (ε — константа из Основной леммы). Выберем q так, чтобы $q! \cdot q^2 / \varepsilon \leq s$ и $q \geq \Omega(\log s / \log \log s)$ и положим $d \Leftrightarrow q!$. Подставив в $H_{k,n}$ вместо $k-s$ переменных единицы, мы получим (симметрическую) булеву функцию f от $n-k+s$ переменных такую, что $f([n-k+s]^{s-d}) = 0$, $f([n-k+s]^s) = 1$. Применяв теорему 1 и Основную лемму, мы, с учетом отмеченного выше факта $\log^*(n-k) \geq \Omega(\log^* n)$, докажем искомую оценку для f . Однако $RS(H_{k,n}) \geq RS(f)$, так как f получена из $H_{k,n}$ подстановкой констант вместо некоторых переменных. ■

З а м е ч а н и е 2. Ввиду отмеченных выше примеров 1–3 те же оценки справедливы для любой из трех сложностных мер S , DS , BP . В частности, для контактных схем мы имеем $S(MAJORITY_n) \geq \Omega(n \cdot \log \log \log^* n)$, что является усилением результата Гринчука $S(MAJORITY_n) \geq \Omega(n \cdot \log^{**} n)$ из [11].

С л е д с т в и е. Пусть $k(n) \leq n/2$ — произвольная функция и H — любая из трех булевых функций E , T , MOD . $RS(H_{k(n),n})$ линейна по n тогда и только тогда, когда $k(n) \leq O(1)$.

Доказательство. Часть «только тогда» вытекает из теоремы 2. Если же $k(n) \leq O(1)$, то можно считать $k(n) = k$ ($= \text{const}$) и в этом случае $H_{k,n}$ вычисляется очевидной ветвящейся программой линейного по n размера. ■

З а м е ч а н и е 3. Легко видеть, что ветвящиеся программы являются частным случаем не только упорядоченных контактных схем (как мы уже убедились в примере 3), но и неупорядоченных. Поэтому сформулированное следствие так же, как и теорема 2, остается справедливым при замене RS на любую из трех мер BP , S , DS . Следует, впрочем, отметить, что для мер BP и S этот ре-

зультат вытекает уже из классификации симметрических функций, имеющих нелинейную сложность реализации контактными неупорядоченными схемами, данной Гринчуком [11].

2. Нижние оценки для числа покрывающих множеств. Этот пункт целиком посвящен доказательству Основной леммы. Пусть n, q, d, s выбраны так, что выполняются условия (4). Положим $U \doteq [n]^{s-d}, V = [n]^s$.

Среди совершенно необозримого множества точек $\mathcal{F} \times V$ мы выделим некоторое разумное подмножество и покажем, что даже для покрытия этого подмножества требуется $\Omega(n \log q)$ покрывающих множеств. Для этого для каждого $v \in V$ положим

$$C_v \doteq \{ \chi: v \rightarrow \{0, 1, 2, 3\} \mid |\chi^{-1}(1)| = |\chi^{-1}(2)| = \\ = |\chi^{-1}(3)| = d \}$$

и для $\chi \in C_v$ обозначим

$$\text{supp}(\chi) \doteq \{v - \chi^{-1}(1), v - \chi^{-1}(2), v - \chi^{-1}(3)\}; \\ \text{supp}(\chi) \subseteq U.$$

Далее, для $\chi \in C_v$ введем в рассмотрение следующий нетривиальный монотонный функционал $F_{v, \chi}: \mathcal{P}(U) \rightarrow \{0, 1\}$:

$$F_{v, \chi}(A) = 1 \Leftrightarrow |A \cap \text{supp}(\chi)| \geq 2.$$

Мы собираемся доказать, что если $\Delta_0 \subseteq \Delta$ покрывает все точки вида $(F_{v, \chi}, v)$, то $|\Delta_0| \geq \Omega(n \log q)$. Фиксируем произвольное Δ_0 , покрывающее все точки рассматриваемого вида. Легко видеть, что если $\delta_{i, \varepsilon}(A)$ покрывает точку $(F_{v, \chi}, v)$, то $\varepsilon = 1, i \in v, \chi(i) \neq 0$ и ровно один из двух элементов множества $\text{supp}(\chi)$, отличных от $v - \chi^{-1}(\chi(i))$, принадлежит A . В частности, можно считать, что Δ_0 содержит лишь множества вида $\delta_{i, 1}(A)$.

Изложим теперь общую стратегию доказательства. Вернемся для этого вначале к примеру 4.

П р и м е р 4 (продолжение). То же самое семейство покрывающих множеств $\{\delta_{i, \varepsilon}(A_{i, v}) \mid i \in [n]; \varepsilon, v \in \{0, 1\}\}$ может быть рассмотрено и при четных d . Однако на этот раз существуют точки вида $(F_{v, \chi}, v)$, не покрытые этим семейством. Действительно, выберем произвольное $v \in [n]^s$. Выберем функцию $\chi \in C_v$ так, что она принимает нетривиальные значения 1, 2, 3 в следующем порядке (v читается слева направо): $\dots 1 \dots 1 \dots 3 \dots 3 \dots$
 $\dots 2 \dots 2 \dots 1 \dots 1 \dots 3 \dots 3 \dots 2 \dots 2 \dots$. Легко видеть, что $(F_{v, \chi}, v)$ не покрывается рассматриваемой системой. Аналогичная конструкция возможна и для любого q_0 такого, что $q_0 \mid d$ (рассмотренный случай соответствует $q_0 = 2$).

План доказательства состоит в следующем. Прежде всего, используя рамсеевские аргументы, мы найдем $(2s + 1)$ -подмножество в $[n]$, внутри которого система покрывающих множеств Δ_0 ведет себя достаточно регулярным образом. После этого мы докажем, что, если бы Δ_0 содержала менее $\Omega(n \log q)$ элементов, то хотя бы для одного $q_0 \in [q]$ изложенную выше в примере 4 кон-

струкцию можно было бы использовать для построения точки, не покрытой системой Δ_0 .

Шаг 1. Редуцируем нашу задачу к доказательству того, что хотя бы для одного i семейство Δ_0 содержит $\Omega(\log q)$ элементов вида $\delta_{i,1}(A)$. В самом деле, если t_i — число множеств вида $\delta_{i,1}(A)$ в Δ_0 , то $\sum_{i=1}^n t_i = |\Delta_0|$ и, значит, существует $\geq n/2$ индексов i , для которых $t_i \leq 2|\Delta_0|/n$. Удаляя из $[n]$ все остальные индексы, мы можем предполагать с самого начала, что вместо $|\Delta_0| \geq \Omega(n \log q)$ требуется доказать более слабый факт $\max_{i=1}^n t_i \geq \Omega(\log q)$.

Прежде чем двигаться дальше, напомним некоторые сведения из теории Рамсея (см., например, [13]). Классическая теорема Рамсея утверждает, что для любых k, l, r существует n такое, что если все k -подмножества в $[n]$ раскрашены в r цветов, то некоторое l -подмножество из $[n]$ имеет все k -подмножества одного цвета. Наименьшее такое n обозначается через $R(k, l, r)$ и называется (классическим) числом Рамсея. Следующую (рекурсивную) верхнюю оценку для $R(k, l, r)$ можно найти в [13, с. 7—9]:

$$R(1, l, r) \leq lr + 1 - r,$$

$$R(k+1, l, r) \leq 2r^c, \quad \text{где } c = \sum_{i=k-1}^{R(k, l, r)-1} \binom{i+1}{k-1}.$$

Отсюда вытекает (чрезвычайно грубая!) верхняя оценка для $R(k, l, r)$ в терминах введенной в предыдущем параграфе функции башни:

$$R(k, l, r) \leq t(O(k), lr). \quad (5)$$

Двудольный вариант теоремы Рамсея [13, с. 97] утверждает, что если n достаточно велико по сравнению с k_1, k_2, l, r и $[n]^{k_1} \times [n]^{k_2}$ раскрашено в r цветов, то существуют два l -подмножества $I_1, I_2 \subseteq [n]$ такие, что $[I_1]^{k_1} \times [I_2]^{k_2}$ монохроматично. Обозначим через $R(k_1, k_2, l, r)$ соответствующее число Рамсея. Приведенное в [13] доказательство существования чисел $R(k_1, k_2, l, r)$ дает следующую оценку:

$$R(k_1, k_2, l, r) \leq R(k_2, l, r^c), \quad \text{где } c = \binom{R(k_1, l, r)}{k_1},$$

откуда с учетом (5) получается аналогичная (5) оценка для двудольных чисел Рамсея:

$$R(k_1, k_2, l, r) \leq t(O(k_1 + k_2), lr). \quad (6)$$

Вернемся теперь к доказательству Основной леммы. Положим

$$\left. \begin{aligned} n_0 &\Leftarrow s, \\ n_{j+1} &\Leftarrow R(j, s-d-1-j, n_j, q-1) \quad (0 \leq j \leq s-d-1), \\ n' &\Leftarrow 2n_{s-d} + 1, \\ n'' &\Leftarrow R(s, n', s^{(s')}). \end{aligned} \right\} \quad (7)$$

Так как в силу (4) $q \leq s$, то, применяя оценки (5—6), мы видим, что $n'' \leq t(O(s^2), 1)$. Итак, если константа ε в формулировке Основной леммы достаточно мала, то

$$n'' \leq n. \quad (8)$$

Шаг 2. Для каждого $v \in V$ множество C_v покрашено в s цветов в соответствии с тем, для какого именно $i \in v$ в Δ_0 существует множество вида $\delta_{i,1}(A)$, покрывающее данную точку (F_v, χ, v) , $\chi \in C_v$. Линейная упорядоченность всех v позволяет рассматривать такие раскраски «однородным» по v образом. Шаг 2 состоит в выборе n' -подмножества, для которого раскраски, ассоциированные со всеми v , лежащими внутри этого подмножества, совпадают.

Более формально, определим следующую раскраску V в $\leq s^{(4^s)}$ цветов. Прежде всего положим

$$\begin{aligned} \bar{C} \ni \{\bar{\chi}: [s] \rightarrow \{0, 1, 2, 3\} \mid |\bar{\chi}^{-1}(1)| = \\ = |\bar{\chi}^{-1}(2)| = |\bar{\chi}^{-1}(3)| = d\} \end{aligned}$$

и для каждого $v = \{i_1, \dots, i_s\} \in V$ ($i_1 < \dots < i_s$) и $\bar{\chi} \in \bar{C}$ определим следующим образом функцию $\chi \in C_v$:

$$\chi(i_j) \ni \bar{\chi}(j) \quad (1 \leq j \leq s). \quad (9)$$

Соответствующая точка (F_v, χ, v) покрывается некоторым $\delta_{i_j,1}(A)$ с $1 \leq j \leq s$. Ставя в соответствие элементу $\bar{\chi} \in \bar{C}$ найденное таким образом $j \in [s]$, мы получим некоторое, ассоциированное с v , отображение $\bar{C} \rightarrow [s]$. Число таких отображений равно $s^{|\bar{C}|} \leq s^{(4^s)}$, и мы раскрашиваем v в соответствии с ассоциированным с ним отображением. В силу (8), (7) существует n' -подмножество $\{i_1, i_2, \dots, i_{2n_s-d+1}\}$, монохроматичное относительно этой раскраски.

Положим

$$i_{\text{med}} \ni i_{n_s-d+1}.$$

Нам достаточно показать, что

$$t_{i_{\text{med}}} \geq \log_2 q.$$

Предположим противное.

Пусть $\delta_{i_{\text{med}},1}(A_1), \delta_{i_{\text{med}},1}(A_2), \dots, \delta_{i_{\text{med}},1}(A_h)$ ($h < \log_2 q$) — полный список покрывающих множеств из Δ_0 вида $\delta_{i_{\text{med}},1}(A)$. Пусть \approx — отношение эквивалентности на U , определенное системой множеств $\{A_1, A_2, \dots, A_h\}$. \approx содержит не более $2^h \leq q - 1$ классов. Роль отношения \approx состоит в том, что если точка (F_v, χ, v) покрывается некоторым $\delta_{i_{\text{med}},1}(A_i)$, то A_i разделяет те два элемента из $\text{supp}(\chi)$, которые отличны от v — $\chi^{-1}(\chi(i_{\text{med}}))$ и, следовательно, эти элементы принадлежат разным

классам отношения \approx . Этого свойства отношения \approx нам будет достаточно для вывода противоречия.

Шаг 3. Множество U раскрашено в соответствии с отношением \approx . Мы хотим выбрать в уже построенном множестве $\{i_1, i_2, \dots, i_{2n_s-d+1}\}$ достаточно большое однородное относительно этой раскраски подмножество. При этом нас интересуют только те $u \in U$, которые содержат i_{med} . Эта задача заведомо невыполнима в полном объеме, так как класс эквивалентности элемента u , содержащего i_{med} , может определяться мощностью части u , лежащей левее i_{med} (как, скажем, в примере 4). Однако двудольная теорема Рамсея показывает, что на самом деле это *единственное* препятствие к осуществлению нашего плана и мы можем добиться того, что класс эквивалентности элемента u будет зависеть *только* от этой мощности.

Более точно, отношение \approx для каждого j ($0 \leq j \leq s-d-1$) индуцирует раскраску множества $\{\{i_1, i_2, \dots, i_{n_s-d}\}\}^j \times \{\{i_{n_s-d+2}, \dots, i_{2n_s-d+1}\}\}^{s-d-1-j} \in \leq (q-1)$ цветов, при которой цвет пары подмножеств (u', u'') ($u' \in \{\{i_1, i_2, \dots, i_{n_s-d}\}\}^j$, $u'' \in \{\{i_{n_s-d+2}, \dots, i_{2n_s-d+1}\}\}^{s-d-1-j}$) определяется классом эквивалентности элемента $u' \cup \{i_{med}\} \cup u''$. Применив $s-d$ раз двудольный вариант теоремы Рамсея, мы с учетом (7) отыщем в итоге $(2s+1)$ -подмножество $\{i'_1, i'_2, \dots, i'_{2s+1}\} \subseteq \{i_1, i_2, \dots, i_{2n_s-d+1}\}$ обладающее следующими тремя свойствами:

а) существует функция $j: \bar{C} \rightarrow [s]$, $\bar{\chi} \mapsto j(\bar{\chi})$ такая, что для любых $v = \{i''_1, \dots, i''_s\} \subseteq \{i'_1, i'_2, \dots, i'_{2s+1}\}$ ($i''_1 < \dots < i''_s$) и $\bar{\chi} \in \bar{C}$ точка (F_v, χ, v) (где $\chi \in C_v$ определена посредством (9)) покрывается одним из множеств вида $\delta_{i'_{j(\bar{\chi})}, 1}(A) \in \Delta_0$;

б) $i'_{s+1} = i_{med}$;

в) для любого j ($0 \leq j \leq s-d-1$) все $u \in U$ такие, что $u = \{i''_1, \dots, i''_{s-d}\} \subseteq \{i'_1, i'_2, \dots, i'_{2s+1}\}$ ($i''_1 < \dots < i''_{s-d}$) и $i''_{j+1} = i_{med}$, принадлежат одному и тому же классу эквивалентности отношения \approx , который мы обозначим через R_j .

Функция j и система классов $\{R_j\}$ описывают поведение покрытия Δ_0 по отношению к точкам (F_v, χ, v) , содержащимся в $\{i'_1, i'_2, \dots, i'_{2s+1}\}$. Вообще говоря, мы ничего не знаем про j и $\{R_j\}$. Сейчас мы, однако, покажем, что для любого выбора j и $\{R_j\}$ существует $q_0 \in [q]$ и точка рассмотренного в примере 4 вида, не покрытая системой Δ_0 . Тем самым будет получено искомое противоречие с предположением $t_{i_{med}} < \log_2 q$.

Если константа ϵ в формулировке Основной леммы достаточно мала, то на интервале $(1, \dots, s)$ можно выделить dq попарно непересекающихся интервалов J_1, \dots, J_{dq} (занумерованных слева направо) так, что $|J_k| = q$ ($1 \leq k \leq dq$), расстояние между двумя соседними интервалами больше q , а расстояние между J_{dq} и s больше $q + d + 1$. Для каждого k ($1 \leq k \leq dq$) среди q

классов эквивалентности $\{R_j \mid j \in J_k\}$ есть по крайней мере два совпадающих (так как вообще число классов эквивалентности не превосходит $q - 1$). Пусть $R_{j_1(k)} = R_{j_2(k)}$, где $j_1(k) < j_2(k)$; $j_1(k), j_2(k) \in J_k$. Положим $q(k) \Leftrightarrow j_2(k) - j_1(k)$. Отметим, что $1 \leq q(k) \leq q - 1$.

Среди $\{q(k) \mid 1 \leq k \leq dq\}$ имеется по крайней мере d одинаковых значений. Пусть, например, значение q_0 ($1 \leq q_0 \leq q - 1$) встречается по меньшей мере d раз, а именно $q(k_1) = q(k_2) = \dots = q(k_d) = q_0$ ($k_1 < k_2 < \dots < k_d$). Отметим, что по построению

$$\left. \begin{aligned} j_1(k_l) - j_1(k_{l-1}) &> q > q_0 & (2 \leq l \leq d), \\ s - j_1(k_d) &> q_0 + d + 1. \end{aligned} \right\} \quad (10)$$

Мы утверждаем, что существует функция $\bar{\chi}_0 \in \bar{C}$, обладающая следующими двумя свойствами:

а) для любого $j \in [s]$, если $\bar{\chi}_0(j) \in \{1, 2\}$ и $\{1, 2, 3\} = \{\bar{\chi}_0(j), \pi, \pi'\}$, то $|\{1, 2, \dots, j - 1\} \setminus \bar{\chi}_0^{-1}(\pi)| = |\{1, 2, \dots, j - 1\} \setminus \bar{\chi}_0^{-1}(\pi')|$,

б) если $j_1 < j_2 < \dots < j_d$ — полный список элементов $j \in [s]$ таких, что $\bar{\chi}_0(j) = 3$, то $|\{1, 2, \dots, j_l - 1\} \setminus \bar{\chi}_0^{-1}(1)| = = j_1(k_l)$ и $|\{1, 2, \dots, j_l - 1\} \setminus \bar{\chi}_0^{-1}(2)| = j_2(k_l)$ ($1 \leq l \leq d$).

Для построения такой $\bar{\chi}_0$ положим вначале

$$j_l = 1 + \lfloor l/q_0 \rfloor \cdot q_0 + j_1(k_l) \quad (1 \leq l \leq d),$$

где $\lfloor x \rfloor$ — наименьшее целое a такое, что $a \geq x$, и определим $\bar{\chi}_0(j_l) = 3$ ($1 \leq l \leq d$). Отметим, что в силу (10) $j_1 > q_0$, $j_{q_0 \alpha + 1} - j_{q_0 \alpha} > 2q_0$ ($1 \leq \alpha \leq d/q_0 - 1$) и $s - j_d > q_0$. Пусть функция χ_0 принимает q_0 значений 1 в интервале $\{1, \dots, j_1 - 1\}$ (произвольным образом), по q_0 значений 1 и q_0 значений 2 в каждом из интервалов $\{j_{q_0 \alpha} + 1, \dots, j_{q_0 \alpha + 1}\}$ ($1 \leq \alpha \leq d/q_0 - 1$) так, что в каждом из этих интервалов все 2-значения лежат левее всех 1-значений и, наконец, q_0 значений 2 в интервале $\{j_d + 1, \dots, s\}$. Для всех остальных j полагаем $\bar{\chi}_0(j) = 0$. Непосредственно проверяется, что функция $\bar{\chi}_0$ обладает сформулированными выше свойствами а), б) (единственное нетривиальное равенство $|\{1, 2, \dots, j_l - 1\} \setminus \bar{\chi}_0^{-1}(2)| = j_2(k_l)$ вытекает из $|\{1, 2, \dots, j_l - 1\} \setminus \bar{\chi}_0^{-1}(1)| = j_1(k_l)$, свойства $j_2(k_l) - j_1(k_l) = = q(k_l) = q_0$ и выполняющегося по построению соотношения $|\{1, 2, \dots, j_l - 1\} \cap \bar{\chi}_0^{-1}(1)| = |\{1, 2, \dots, j_l - 1\} \cap \bar{\chi}_0^{-1}(2)| + q_0$).

Пусть теперь $j_0 \Leftrightarrow j(\bar{\chi}_0)$. Определим $v_0 = \{i_1, \dots, i_s\} \subseteq \subseteq \{i_1, i_2, \dots, i_{2s+1}\}$ ($i_1 < \dots < i_s$) так, чтобы $i_{j_s} = i_{\text{med}}$ (возможность такого выбора обеспечивается свойством б)). Пусть $\chi_0 \in C_{v_0}$ определена по $\bar{\chi}_0$ в соответствии с правилом (9). Тогда в силу свойства а) точка (F_{v_0, χ_0}, v_0) покрывается хотя бы одним из множеств $\delta_{i_{\text{med}}, 1}(A) \in \Delta_0$. Покажем, что это невозможно.

Напомним, что если $\delta_{i,1}(A)$ покрывает точку $(F_{v,\chi}, v)$, то $i \in v$, $\chi(i) \neq 0$ и ровно один из двух элементов множества $\text{supp}(\chi)$, отличных от $v - \chi^{-1}(\chi(i))$, принадлежит A . Обозначим $u_\pi \Leftrightarrow v_0 - \chi_0^{-1}(\pi)$ ($\pi \in \{1, 2, 3\}$).

Если $\chi_0(i_{\text{med}}) (= \bar{\chi}_0(j_0)) \in \{1, 2\}$ и $\{1, 2, 3\} = \{\chi_0(i_{\text{med}}), \pi, \pi'\}$, то, в силу свойств ϑ , ϱ , u_π и $u_{\pi'}$ принадлежат одному и тому же классу эквивалентности отношения \approx , а именно, классу R_j , где $j = |\{1, 2, \dots, j_0 - 1\} \setminus \bar{\chi}_0^{-1}(\pi)| (= |\{1, 2, \dots, j_0 - 1\} \setminus \bar{\chi}_0^{-1}(\pi')|)$. По определению отношения \approx это означает, что ни одно A такое, что $\delta_{i_{\text{med}},1}(A) \in \Delta_0$, не может содержать ровно один из двух элементов u_π и $u_{\pi'}$. Если же $\chi_0(i_{\text{med}}) = 3$, т. е. $j_0 = j_l$ для некоторого l ($1 \leq l \leq d$), то, в силу свойств ϑ , $\bar{\vartheta}$, u_1 и u_2 принадлежат классам $R_{j_l(k_l)}$ и $R_{j_l(k_l)}$ соответственно. Однако эти классы совпадают по построению, так что и в этом случае ни одно A такое, что $\delta_{i_{\text{med}},1}(A) \in \Delta_0$, не может содержать ровно один из двух элементов u_1 и u_2 .

Таким образом, мы получили противоречие с предположением $t_{i_{\text{med}}} < \log_2 q$. Доказательство Основной леммы завершено. ■

Математический институт
им. В. А. Стеклова АН СССР

Поступило
07.12.89

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

- [1] Pudlák P. The hierarchy of Boolean circuits // Computers and Artificial Intelligence. 1987. V. 6, N 5. P. 449—468.
- [2] Марков А. А. О минимальных контактно-вентильных двухполюсниках для монотонных симметрических функций // Проблемы кибернетики. 1962. Вып. 8. С. 117—121.
- [3] Нечипорук Э. И. Об одной булевой функции // ДАН СССР. 1966. Т. 169, № 4. С. 765—766.
- [4] Bogodin A., Dolev D., Fich F. E., Paul W. Bounds for width 2 branching programs // Proc. 15th ACM STOC. 1983. P. 87—93.
- [5] Chandra A. K., Furst M. L., Lipton R. J. Multiparty protocols // Proc. 15th ACM STOC. 1983. P. 94—99.
- [6] Yao A. C. Lower Bounds by Probabilistic Arguments // Proc. 24th IEEE FOCS. 1983. P. 420—428.
- [7] Pudlák P. A lower bound on complexity of branching programs // Proceedings of the 11th Symposium on Mathematical Foundations of Computer Science (1984). Lecture Notes in Computer Science. 1984. V. 176.
- [8] Ajtai M., Babai L., Hajnal P., Komlos J., Pudlák P., Rödl V., Szemerédi E., Turan Gy. Two lower bounds for branching programs // Proc. 18th ACM STOC. 1986. P. 30—38.
- [9] Alon N., Maass W. Meanders, Ramsey Theory and lower bounds for branching programs // Proc. 27th IEEE FOCS. 1986. P. 410—417.
- [10] Babai L., Pudlák P., Rödl V., Szemerédi E. Lower bounds to the complexity of symmetric Boolean functions. Prepr.
- [11] Гринчук М. И. О сложности реализации симметрических булевых функций контактными схемами: Дис. ... канд. физ.-мат. наук. М., 1989.
- [12] Razborov A. A. On the method of approximations // Proc. 21st ACM STOC. 1989. P. 167—176.
- [13] Graham R. L., Rothschild B. L., Spencer J. H. Ramsey Theory. N. Y.: John Wiley & Sons, 1980.