

ЛОКАЛЬНАЯ СЛОЖНОСТЬ БУЛЕВЫХ ФУНКЦИЙ*)

А. В. Чашкин

Вводятся классы локально сложных и локально простых функций. Доказывается инвариантность этих классов относительно полиномиально эквивалентных мер сложности. Рассматривается связь между доказательством принадлежности функции классу локально сложных функций и доказательством нижних оценок сложности для схем из функциональных элементов, контактных схем, формул и параллельно-последовательных контактных схем.

Введение

Пусть f — произвольная вычислимая функция, определенная на всех двоичных последовательностях длины n , $n = 1, 2, \dots$, и принимающая значения 0 и 1. Далее такие функции будем называть *вычислимыми булевыми функциями*. Представим f в виде последовательности булевых функций $f_n : \{0, 1\}^n \rightarrow \{0, 1\}$. Пусть P_2 — множество всех полностью определенных булевых функций, $\mu : P_2 \rightarrow R^+$ — произвольная вычислимая положительная функция, определенная на множестве P_2 . Функцию μ будем называть *сложностью*. Распространим μ на булевы вычислимые функции. Пусть ϕ определена на множестве натуральных чисел и удовлетворяет равенству $\phi(n) = \mu(f_n)$. Положим $\mu(f) = \phi$, т. е. $\mu(f) = (\mu(f_1), \dots, \mu(f_i), \dots)$. Распространим μ на частичные булевы функции. Пусть $D \subseteq \{0, 1\}^n$ и $g : D \rightarrow \{0, 1\}$. Значение μ на функции g определим посредством равенства $\mu(g) = \min \mu(h)$, где минимум берется по всем функциям от n переменных, совпадающих на области D с g . Частичную функцию g , совпадающую на D с полностью определенной функцией h , будем обозначать через h_D .

Пусть $D \subset \{0, 1\}^n$ и $F : \{0, 1\}^n \rightarrow \{0, 1\}^m$. Будем говорить, что оператор F сжимает область D относительно функции f , если $F(x) \neq F(y)$ для любых $x, y \in D$ таких, что $f_n(x) \neq f_n(y)$. Определим частичную

*) Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (код проекта 96-01-01068).

функцию $f_{D,F} : \{0, 1\}^m \rightarrow \{0, 1\}$, положив $f_{D,F}(y) = f_n(x)$, если $y = F(x)$ при $x \in D$.

Локальной сложностью булевой функции f_n назовем функцию $\tilde{\mu}(f_n) = \max_D \min_F \mu(f_{D,F})$. Очевидно, что локальная сложность зависит от множества областей D и множества операторов \mathcal{F} , по которым вычисляются функции \max и \min . Распространим $\tilde{\mu}$ на вычислимые булевы функции, положив $\tilde{\mu}(f) = \phi$, где $\phi(n) = \tilde{\mu}(f_n)$ и при вычислении $\tilde{\mu}(f_n)$ максимум берется по всем областям D таким, что $|D| > n$. Легко видеть, что для вычислимых функций локальная сложность зависит только от множества сжимающих операторов, причем чем шире множество операторов, тем меньше как локальная сложность вычислимой функции, так и связь между ее локальной и обычной сложностью.

В этом можно убедиться, если рассмотреть предельный случай, когда отсутствуют какие-либо ограничения на сжимающие операторы, и в качестве одной из компонент сжимающего оператора взять саму функцию f_n . Поэтому изучение локальной сложности представляет тем больший интерес, чем меньше множество сжимающих операторов, т. е. в паре $\mathcal{F}, f_{D,F}$ основную информацию об исходной функции содержит функция $f_{D,F}$.

В работе рассматриваются два множества операторов: линейные операторы и линейные операторы, порожденные делением на неприводимые многочлены (далее такие операторы называются *линейными полиномиальными*). С одной стороны, эти множества достаточно узки, так как принадлежат классу линейных функций, и поэтому между функциями f_n и $f_{D,F}$ сохраняется достаточно сильная связь. С другой стороны, операторы из этих множеств позволяют достаточно сильно сжать любую область.

На множестве булевых вычислимых функций выделяются классы локально сложных и локально простых функций. Доказывается инвариантность этих классов относительно полиномиально эквивалентных мер сложности. Рассматривается связь между доказательством принадлежности функции классу локально сложных функций и доказательством нижних оценок сложности для схем из функциональных элементов, контактных схем, формул и π -схем, т. е. параллельно-последовательных контактных схем. Вопросы, в некотором смысле близкие к рассматриваемым, изучались ранее в [4]. Как обычно, сложностью булевой функции f в каждом из этих классов управляющих систем называется сложность минимальной системы (схемы, контактной схемы, формулы, π -схемы), реализующей функцию f . Сложность функции f в классе схем из функциональных элементов в базисе из всех двуместных булевых функций обозначается через $L(f)$, в классе контактных схем — через

$L_k(f)$, в классе формул в базисе из всех двуместных булевых функций — через $L_\phi(f)$, в классе π -схем — через $L_\pi(f)$.

Обозначая булевы функции, будем, как правило, опускать индексы, указывающие число переменных. Предполагается, что параметр n всегда больше некоторой положительной константы. Понятия, используемые без определений, можно найти в [2, 5]. Через c и c_i , $i = 0, 1, \dots$, обозначаются подходящие константы. Всюду в этой статье \log обозначает логарифм по основанию 2.

1. Операторы сжатия

Рассматриваются возможности линейных и полиномиальных линейных операторов, используемых для сжатия областей.

Лемма 1. Пусть $D \subset \{0, 1\}^n$ и $m = \lfloor 2 \log |D| \rfloor$. Тогда существует линейный оператор $F : \{0, 1\}^n \rightarrow \{0, 1\}^m$ такой, что $F(x) \neq F(y)$ для любых $x, y \in D$.

ДОКАЗАТЕЛЬСТВО. Воспользуемся методом от противного. Предположим, что для некоторой области D при $m = \lfloor 2 \log |D| \rfloor$ требуемый линейный оператор не существует. Тогда для каждого линейного оператора $F : \{0, 1\}^n \rightarrow \{0, 1\}^m$ найдутся по крайней мере два набора $x, y \in D$ таких, что $F(x) = F(y)$. Так как существует 2^{mn} различных линейных операторов из $\{0, 1\}^n$ в $\{0, 1\}^m$, каждый из которых переводит нулевой набор в нулевой, и $|D|(|D| - 1)/2$ пар наборов из D , то для некоторых двух наборов x и y из D найдется не менее $2^{mn+1}/|D|(|D| - 1) > 2^{mn+1}/|D|^2$ различных операторов, отображающих x и y в один и тот же набор. Следовательно, каждый такой оператор отображает $x \oplus y$ в нулевой набор. С другой стороны, легко видеть, что ядра не более $2^{(n-1)m}$ линейных операторов могут иметь общий ненулевой набор. Поэтому необходимо, чтобы $2^{mn+1}/|D|^2 < 2^{(n-1)m}$, т. е. $2^{m+1} < |D|^2$. Последнее неравенство противоречит равенству $m = \lfloor 2 \log |D| \rfloor$. Лемма 1 доказана.

Установим соответствие между двоичными наборами длины n и многочленами степени $n - 1$ с двоичными коэффициентами. Многочлену $g(t) = \sum_{i=0}^{n-1} g_i t^i$ поставим в соответствие набор $x_g = (g_0, \dots, g_{n-1})$,

а набору $x = (x_0, \dots, x_{n-1})$ — многочлен $g_x(t) = \sum_{i=0}^{n-1} x_i t^i$. Каждому числу n и многочлену g степени m поставим в соответствие такой линейный оператор $F_g : \{0, 1\}^n \rightarrow \{0, 1\}^m$, что $F_g(x) = y$, если $g_y(t)$ — остаток от деления $g_x(t)$ на $g(t)$. Будем говорить, что многочлен g порождает оператор F_g .

Справедливо следующее утверждение.

Лемма 2. Пусть $D \subset \{0, 1\}^n$ и $m = \lfloor 2 \log |D| + \log n \rfloor$. Тогда имеются неприводимый многочлен g и порожденный этим многочленом полиномиальный линейный оператор $F_g : \{0, 1\}^n \rightarrow \{0, 1\}^m$ такие, что $F_g(x) \neq F_g(y)$ при любых $x, y \in D$.

Доказательство. Воспользуемся методом от противного. Пусть $G = \{g_i\}$ — множество всех неприводимых многочленов степени m . Предположим, что для некоторой области D при $m = \lfloor 2 \log |D| + \log n \rfloor$ требуемые многочлен и линейный оператор не существуют. Тогда для каждого многочлена $g_i \in G$ и линейного оператора $F_{g_i} : \{0, 1\}^n \rightarrow \{0, 1\}^m$ найдутся по крайней мере два набора x и y из D таких, что $F_{g_i}(x) = F_{g_i}(y)$. Известно [2], что $|G| > 2^m/m$. Так как имеется ровно $|D|(|D| - 1)/2$ неупорядоченных пар различных наборов из D , то для некоторой пары наборов (x, y) , где $x, y \in D$, найдется не менее $2^{m+1}/m|D|(|D| - 1) > 2^{m+1}/m|D|^2$ различных линейных полиномиальных операторов, отображающих x и y в один и тот же набор $x \oplus y$. Следовательно, каждый такой оператор F_{g_i} отображает $x \oplus y$ в нулевой набор. Это означает, что многочлен $g_{x \oplus y}$ делится без остатка на неприводимый многочлен g_i . Так как все многочлены g_i взаимно просты, то многочлен $g_{x \oplus y}$ делится на их произведение. Следовательно, степень многочлена $g_{x \oplus y}$ не меньше степени этого произведения, т. е. не меньше $2^{m+1}/|D|^2$. Поэтому должно выполняться неравенство $2^{m+1}|D|^{-2} < n - 1$, т. е. $m < 2 \log |D| + \log n$. Последнее неравенство противоречит равенству $m = \lfloor 2 \log |D| + \log n \rfloor$. Лемма 2 доказана.

Следующие две леммы приведем без доказательств. Доказательства результатов, аналогичных утверждению первой леммы, можно найти во многих работах, например в [3]. Вторая лемма является очевидным следствием теоремы 8.10 из [1].

Лемма 3. Пусть $m \leq n$ и $F : \{0, 1\}^n \rightarrow \{0, 1\}^m$ — произвольный линейный оператор. Тогда справедливо неравенство

$$L(F) \leq \frac{2mn}{\log n}.$$

Лемма 4. Пусть $m \leq n$, g_1, \dots, g_k — многочлены степени m , $mk \leq 2n$, и $F_{g_i} : \{0, 1\}^n \rightarrow \{0, 1\}^m$ — полиномиальный линейный оператор, порожденный многочленом g_i . Тогда справедливо неравенство

$$L(F_{g_1}, \dots, F_{g_k}) \leq c_0 n (\log n)^2.$$

Далее множество линейных операторов будем обозначать через $\widehat{\mathcal{L}}$, а множество линейных операторов, каждый из которых соответствует некоторому многочлену, — через $\widetilde{\mathcal{L}}$.

2. Локально сложные функции

Положим $\mu(m) = \max \mu(f)$, где максимум берется по всем булевым функциям от m переменных.

Вычислимую булеву функцию f назовем *локально сложной* относительно функции μ и множества операторов \mathcal{F} , если существуют константа $c_1 < 1$ и натуральное N такие, что при любом $n \geq N$ имеется такая область $D \subseteq \{0, 1\}^n$, $|D| > n$, что для любого целого m и любого оператора $F' : \{0, 1\}^n \rightarrow \{0, 1\}^m$, принадлежащего \mathcal{F} и сжимающего D относительно f , имеет место неравенство

$$\log \mu(f_{D, F'}) \geq c_1 \log \mu(m).$$

Множество функций, локально сложных относительно μ и \mathcal{F} , обозначим через $LC(\mu, \mathcal{F})$.

Функции μ_1 и μ_2 назовем *полиномиально эквивалентными с показателем c* , если для любой вычислимой функции f справедливы неравенства

$$\mu_1(f) \leq (\mu_2(f))^c, \quad \mu_2(f) \leq (\mu_1(f))^c.$$

Функции μ_1 и μ_2 назовем *полиномиально эквивалентными*, если существует такая константа c , что функции μ_1 и μ_2 полиномиально эквивалентны с показателем c .

Ясно, что если функции μ_1 и μ_2 полиномиально эквивалентны с показателем c , то для любых двух вычислимых булевых функций f и g справедливы неравенства

$$\mu_1(f_n) \leq (\mu_2(g_n))^c, \quad \mu_2(g_n) \leq (\mu_1(f_n))^c.$$

Имеет место следующая

Лемма 5. Пусть функции μ_1 и μ_2 полиномиально эквивалентны с показателем c . Тогда

$$\mu_1(m) \leq (\mu_2(m))^c, \quad \mu_2(m) \leq (\mu_1(m))^c.$$

Справедливость леммы 5 следует из неравенств

$$\mu_1(m) = \mu_1(g) \leq (\mu_2(g))^c \leq (\mu_2(m))^c,$$

где функция g такова, что $\mu_1(g) = \mu_1(m)$.

Теорема 1. Пусть \mathcal{F} — некоторое множество операторов, а функции μ_1 и μ_2 полиномиально эквивалентны. Тогда

$$LC(\mu_1, \mathcal{F}) = LC(\mu_2, \mathcal{F}).$$

Доказательство. Пусть функции μ_1 и μ_2 полиномиально эквивалентны с показателем c . Предположим, что утверждение теоремы

неверно. Тогда существует такая функция f , что $f \in LC(\mu_1, \mathcal{F})$ и $f \notin LC(\mu_2, \mathcal{F})$, т. е. для некоторой константы c_2 , любой константы c_3 и любого фиксированного N найдутся $n > N$, область $D \subseteq \{0, 1\}^n$ и оператор $F_1 : \{0, 1\}^n \rightarrow \{0, 1\}^m$, сжимающий D относительно f , такие, что

$$\begin{aligned} \log \mu_1(f_{D, F'}) &\geq c_2 \log \mu_1(m), \\ \log \mu_2(f_{D, F_1}) &< c_3 \log \mu_2(m), \end{aligned} \quad (1)$$

где $F' : \{0, 1\}^n \rightarrow \{0, 1\}^m$ — произвольный оператор, сжимающий D относительно f . Из (1) легко следует, что

$$\log \mu_1(f_{D, F_1}) \geq c_2 \log \mu_1(m).$$

Так как $\mu_1(f_{D, F_1}) \leq (\mu_2(f_{D, F_1}))^c$, а из леммы 5 следует, что $\mu_2(m) \leq (\mu_1(m))^c$, то

$$\log \mu_1(f_{D, F_1}) \leq \log(\mu_2(f_{D, F_1}))^c \leq cc_3 \log \mu_2(m) \leq c^2 c_3 \log \mu_1(m).$$

Поскольку константа c_3 может быть сколь угодно малой, при $c^2 c_3 < c_2$ приходим к противоречию. Теорема 1 доказана.

Теорема 2. Пусть f — вычислимая булева функция такая, что $L(f) \geq c_4 n^2 / \log n$. Тогда $f \in LC(L, \widehat{\mathcal{L}})$.

Доказательство. Из [5, теорема 4] следует существование такой области $D \subseteq \{0, 1\}^n$, что $|D| = \lceil L(f) \log L(f) \rceil$ и

$$L(f_D) \geq L(f) \frac{c_5 \log n}{n}. \quad (2)$$

Из лемм 1 и 3 следует, что при $m = \lfloor 2 \log |D| \rfloor$ сложность любого линейного оператора $F : \{0, 1\}^n \rightarrow \{0, 1\}^m$, сжимающего D относительно f , удовлетворяет неравенству $L(F) \leq \frac{5n \log |D|}{\log n}$. Если $L(f) \leq n^3$, то $L(F) \leq 20n$, а так как $L(f) \geq c_4 n^2 / \log n$, то из (2) следует неравенство $L(f_D) \geq c_4 c_5 n$. Так как $f_D(x) = f_{D, F}(F(x))$, то $L(f_{D, F}) \geq L(f_D) - L(F) \geq (c_4 c_5 - 20)n$. Поэтому $L(f_{D, F}) \geq n$ при $c_4 c_5 \geq 21$. Так как $|D| = \lceil L(f) \log L(f) \rceil$, то $\log |D| \leq 2 \log L(f) \leq 6 \log n$. Так как $m = \lfloor 2 \log |D| \rfloor \leq 3 \log |D|$, то

$$L(f_{D, F}) \geq 2^{(\log |D|)/6} > 2^{m/20}. \quad (3)$$

Если $L(f) > n^3$, то $L(F) \leq n^2$, и из (2) следует неравенство $L(f_D) > 2n^2$. Поэтому

$$L(f_{D, F}) \geq L(f_D) - L(F) \geq L(f_D)/2 \geq (L(f))^{2/3}.$$

Учитывая неравенства $|D| \leq L(f) \log L(f)$ и $m \leq 2 \log |D|$, получаем

$$L(f_{D, F}) \geq (L(f))^{2/3} \geq |D|^{1/3} \geq 2^{m/6}. \quad (4)$$

Из неравенств (3) и (4) следует справедливость утверждения теоремы 2.

Теорема 3. Пусть f — вычислимая булева функция и $L_k(f) \geq n^{2+\varepsilon}$, где ε — сколь угодно малая положительная константа. Тогда $f \in LC(L_k, \widehat{\mathcal{L}})$.

ДОКАЗАТЕЛЬСТВО. Из [5, теорема 7] следует существование такой области $D \subseteq \{0, 1\}^n$, что $|D| = \lceil L_k(f) \log L_k(f) \rceil$ и

$$L_k(f_D) \geq L_k(f)/S\left(\frac{c_6 n}{\log n}\right), \quad (5)$$

где $S(x) = x(\ln x)^4/(\ln \ln x)^2$. Далее из леммы 1 следует, что существует линейный оператор $F : \{0, 1\}^n \rightarrow \{0, 1\}^m$, $m = \lfloor 2 \log |D| \rfloor$, сжимающий область D относительно f . Известно, что $L_k(\bigoplus_{i=1}^n x_i) = 4n - 2$. Пусть S' — контактная схема, реализующая функцию $f_{D,F}(z_1, \dots, z_m)$, а $l_i(x_1, \dots, x_n)$ — i -я функция оператора F . Каждый контакт вида $z_i^{\sigma_i}$ в схеме S' заменим на контактную схему, реализующую функцию $l_i^{\sigma_i}(x_1, \dots, x_n)$. Так как $f_D(x) = f_{D,F}(F(x))$, то очевидно, что новая схема S реализует функцию f_D . Таким образом, $L_k(f_{D,F}) > L_k(f_D)/4n$. Отсюда и из (5) следует, что

$$L_k(f) \leq n(\ln n)^4 L_k(f_D) \leq 4n^2(\ln n)^4 L_k(f_{D,F}) \leq n^{2+\varepsilon/4} L_k(f_{D,F}).$$

Так как $L_k(f) \geq n^{2+\varepsilon}$ и при $\varepsilon < 1$ справедливо неравенство $(2 + \varepsilon)(1 - \varepsilon/4) > 2 + \varepsilon/4$, то

$$L_k(f) \leq n^{2+\varepsilon/4} L_k(f_{D,F}) \leq n^{(2+\varepsilon)(1-\varepsilon/4)} L_k(f_{D,F}) \leq (L_k(f))^{1-\varepsilon/4} L_k(f_{D,F}).$$

Поэтому

$$L_k(f_{D,F}) \geq (L_k(f))^{\varepsilon/4}. \quad (6)$$

Так как $|D| \leq L_k(f) \log L_k(f)$, то

$$|D| < (L_k(f))^2 \leq L_k(f_{D,F})^{\varepsilon/8}.$$

Объединяя последнее неравенство и (6) и пользуясь неравенством $m = \lfloor 2 \log |D| \rfloor \leq 3 \log |D|$, получаем

$$L_k(f_{D,F}) > |D|^{\varepsilon/8} = 2^{(\varepsilon \log |D|)/8} > 2^{\varepsilon m/16}.$$

Теорема 3 доказана.

Теорема 4. Пусть f — вычислимая булева функция такая, что $L_\phi(f) \geq n^{3+\varepsilon}$, где ε — сколь угодно малая положительная константа. Тогда $f \in LC(L_\phi, \widehat{\mathcal{L}})$.

ДОКАЗАТЕЛЬСТВО теоремы 4 почти дословно совпадает с доказательством теоремы 3. Основное отличие состоит в использовании теоремы 4 из [6] вместо теоремы 4 из [5]. Из [6, теорема 4] следует существование такой области $D \subseteq \{0, 1\}^n$, что $|D| = \lceil L_\phi(f) \log n \rceil$ и

$$L_\phi(f_D) \geq L_\phi(f) \left(\frac{c_7 \log n}{n} \right)^2. \quad (7)$$

Теорема 5. Пусть f — вычислимая булева функция такая, что $L_\pi(f) \geq n^{4+\varepsilon}$, где ε — сколь угодно малая положительная константа. Тогда $f \in LC(L_\pi, \widehat{\mathcal{L}})$.

Доказательство теоремы 5 почти дословно совпадает с доказательством теоремы 4. Единственное отличие заключается в том, что сложность реализации линейной функции π -схемами квадратична, а не линейна, как в случае реализации этой функции формулами в базисе из всех двуместных функций.

Теорема 6. Пусть f — вычислимая булева функция такая, что $L(f) \geq n^{1+\varepsilon}$, где ε — сколь угодно малая положительная константа. Тогда $f \in LC(L, \widetilde{\mathcal{L}})$.

Перед доказательством теоремы введем ряд необходимых понятий. В [5] было дано следующее определение.

Пусть $D_1 \subseteq D_2 \subseteq \{0, 1\}^n$, P_2^n — множество всех полностью определенных булевых функций от n переменных, $P_2^n(D_1)$ — множество всех частичных булевых функций от n переменных, определенных в области D_1 и $F : P_2^n(D_1) \rightarrow P_2^n$ такая функция, что для любой $f \in P_2^n(D_1)$ справедливо равенство $(F(f))_{D_1} = f$. Функцию $F(f)$ назовем *продолжением* функции f на область D_2 .

Введенное понятие позволяет для каждой функции $f \in P_2^n(D_1)$ и каждого x из D_2 однозначно определить значение $f(x)$. Пусть $D \subseteq \{0, 1\}^n$ и $f \in P_2^n(D)$. Определим конкретную функцию F . Пусть $m = \lfloor 2 \log |D| + \log n \rfloor$, $\mathcal{F}(n, m) = \{F : \{0, 1\}^n \rightarrow \{0, 1\}^m\}$ и $\mathcal{L}^m = \widetilde{\mathcal{L}} \cap \left(\bigcup_{i=1}^m \mathcal{F}(n, i) \right)$. Рассмотрим множество $H_{D,f} = \{h_i\}$, состоящее из таких булевых функций h_i , зависящих не более чем от m переменных, что $h_i(y) = f(x)$, если $x \in D$, $y = L_i(x)$, L_i сжимает D относительно f и $L_i \in \mathcal{L}^m$. Пусть функция $h'_{D,f}$ такова, что

$$L(h'_{D,f}) = \min_{h_i \in H_{D,f}} L(h_i) \quad (8)$$

и $L_{D,f}$ — соответствующий сжимающий линейный полиномиальный оператор, т. е. $L_{D,f} \in \mathcal{L}^m$ и $h'_{D,f}(L_{D,f}(x)) = f(x)$ при $x \in D$. Положим $h_{D,f}(x) = h'_{D,f}(L_{D,f}(x))$ и $F(f) = h_{D,f}$. Функция F определена, ее существование следует из леммы 2. Следующая лемма является простым следствием теоремы 1, теоремы 2 и следствия из теоремы 2 [5].

Лемма 6. Пусть функция $f : \{0, 1\}^n \rightarrow \{0, 1\}$ такая, что $L(f) < n^3$, а M — функция голосования. Тогда существуют области D_1, \dots, D_s , где $s \leq 2 \lceil n / \log n \rceil$ и $|D_i| < n^7$ такие, что $f = M(f_{D_1}, \dots, f_{D_s})$.

Доказательство теоремы 6. Если $L(f) \geq n^{2+\varepsilon}$, то утверждение теоремы следует из теоремы 2. Рассмотрим случай $L(f) < n^{2+\varepsilon}$.

Предположим, что утверждение теоремы неверно. Тогда для любой области D , $n < |D| < n^7$, найдутся целое m , $\log n \leq m \leq 16 \log n$, и оператор $L_D \in \widetilde{\mathcal{L}}$, $L_D : \{0, 1\}^n \rightarrow \{0, 1\}^m$, такие, что $L(f_{D, L_D}) \leq 2^{m\delta}$, где δ — произвольная константа. Положим $\delta = \varepsilon/32$. Тогда

$$L(f_{D, L_D}) \leq 2^{m\varepsilon/32} \leq 2^{16 \log(n) \cdot \varepsilon/32} = n^{\varepsilon/2}. \quad (9)$$

Воспользуемся леммой 6. В силу этой леммы найдутся такие области D_1, \dots, D_s , где $s \leq 2 \lceil n / \log n \rceil$, $|D_i| < n^7$, и полиномиальные линейные операторы L'_{D_i} , что

$$f = M(f_{D_1}, \dots, f_{D_s}), \quad (10)$$

где $f_{D_i} = h_{D_i, f} = h'_{D_i, f}(L_{D_i, f})$. Из лемм 2 и 4 легко следует неравенство

$$L(L_{D_1, f}, \dots, L_{D_s, f}) \leq n(\log n)^3. \quad (11)$$

Согласно определению (8) имеем $L(f_{D_i, L_{D_i}}) \geq L(h'_{D_i, f})$. Поэтому в силу (9) справедливо неравенство

$$L(h'_{D_i, f}) \leq n^{\varepsilon/2}. \quad (12)$$

Объединяя (10), (11) и (12), получаем

$$\begin{aligned} L(f) &\leq L(M) + \sum_{i=1}^s L(h'_{D_i, f}) + L(L_{D_1}, \dots, L_{D_s}) \\ &\leq n + n(\log n)^3 + n \cdot n^{\varepsilon/2} < n^{1+\varepsilon}. \end{aligned}$$

Противоречие. Теорема 6 доказана.

Из сравнения утверждений теорем 3–6 с известными в настоящее время максимальными нижними оценками сложности булевых функций следует, что, во-первых, ни для одной конкретной функции не доказана нижняя оценка сложности, позволяющая утверждать, что эта функция локально сложная, а во-вторых, правые части неравенств из теорем (равные по порядку $n^{1+\varepsilon}$ для схем из функциональных элементов, $n^{2+\varepsilon}$ для контактных схем, $n^{3+\varepsilon}$ для формул и $n^{4+\varepsilon}$ для π -схем) задают тот же порядок на множестве управляющих систем, что и известные нижние оценки сложности (не превосходящие по порядку n для схем из функциональных элементов, n^2 для контактных схем, n^2 для формул и n^3 для π -схем).

Сопоставление этих двух фактов позволяет высказать предположение о существовании значительных препятствий, затрудняющих доказательство принадлежности конкретных булевых функций классам локально сложных функций. Принятие этого предположения позволяет не только на качественном, но и на количественном уровне ответить

на вопрос, почему максимальные в настоящее время нижние оценки сложности конкретных булевых функций для различных управляющих систем различны.

В заключение отметим, что распространение понятия локально сложной функции на булевы вектор-функции не представляет интереса. Это связано с тем, что возможна ситуация, когда каждая компонента вектор-функции не является локально сложной функцией, однако общий для всех компонент вектор-функции сжимающий оператор, обеспечивающий простоту индуцированных функций от меньшего числа переменных, не существует.

3. Локально простые функции

Вычислимую булеву функцию f назовем *локально простой* относительно функции μ и множества операторов \mathcal{F} , если для любой константы $c_8 < 1$ существуют функция $d(n)$ и положительные константы c_9 , N такие, что при любом $n > N$

$$(a) \ n^2 \leq d(n) \leq n^{c_9};$$

(b) для любой области $D \subseteq \{0, 1\}^n$ мощности $d(n)$ найдутся целое m и оператор $F' : \{0, 1\}^n \rightarrow \{0, 1\}^m$ из \mathcal{F} такие, что \mathcal{F}' сжимает D относительно f и справедливо неравенство

$$\log \mu(f_{D, F'}) \leq c_8 \log \mu(m).$$

Множество функций, локально простых относительно μ и \mathcal{F} , обозначим через $LS(\mu, \mathcal{F})$.

Теорема 7. Пусть \mathcal{F} — множество операторов, а функции μ_1 и μ_2 полиномиально эквивалентны. Тогда

$$LS(\mu_1, \mathcal{F}) = LS(\mu_2, \mathcal{F}).$$

Доказательство. Пусть функции μ_1 и μ_2 полиномиально эквивалентны с показателем c . Предположим, что утверждение теоремы неверно. Тогда существует такая функция f , что $f \in LS(\mu_1, \mathcal{F})$ и $f \notin LS(\mu_2, \mathcal{F})$. Так как $f \notin LS(\mu_2, \mathcal{F})$, то существует такая константа $c_{10} < 1$, что для любой функции $d(n)$ и любых положительных констант c_{11} , N таких, что для некоторого $n > N$

$$(a) \ n^2 \leq d(n) \leq n^{c_{11}};$$

(b) существует такая область $D \subseteq \{0, 1\}^n$ мощности $d(n)$, что для любого целого m и любого оператора $F' : \{0, 1\}^n \rightarrow \{0, 1\}^m$ из \mathcal{F} , сжимающего D относительно f , справедливо неравенство

$$\log \mu_2(f_{D, F'}) > c_{10} \log \mu_2(m). \quad (13)$$

С другой стороны, $f \in LS(\mu_1, \mathcal{F})$. Поэтому существует такой оператор $F'' : \{0, 1\}^n \rightarrow \{0, 1\}^m$ из \mathcal{F} , сжимающий D относительно f , что справедливо неравенство

$$\log \mu_1(f_{D, F''}) \leq c_{10} c^{-2} \log \mu_1(m). \quad (14)$$

Объединяя (13), (14) и используя лемму 5, получаем неравенства

$$\begin{aligned} c_{10} \log \mu_2(m) &< \log \mu_2(f_{D, F''}) \\ &\leq c \log \mu_1(f_{D, F''}) \leq c_{10} c^{-1} \log \mu_1(m) \leq c_{10} \log \mu_2(m). \end{aligned}$$

Противоречие. Теорема 7 доказана.

Следующая лемма является тривиальным следствием теоремы 1 из [5].

Лемма 7. Пусть $f : \{0, 1\}^n \rightarrow \{0, 1\}$ и d таково, что $n^3 \leq d \leq n^{c_{12}}$. Далее, пусть для любой области $D \subseteq \{0, 1\}^n$, $|D| = d$, справедливо неравенство $L(f_D) \leq d^{1/2}$. Тогда среди областей D найдутся такие области D_1, \dots, D_s , что

$$f = M(f_{D_1}, \dots, f_{D_s}),$$

где $s < n$.

Будем говорить, что функция $f_n \in NC$, если f_n может быть реализована схемой глубины $(\log n)^{O(1)}$.

Теорема 8. Если $f \in LS(L, \widehat{\mathcal{L}})$, то $f \in NC$.

Доказательство. Если $f \in LS(L, \widehat{\mathcal{L}})$, то для любой постоянной $c_{13} < 1$ существуют функция $d(n)$ и положительные постоянные c_{14} , N такие, что для любого $n > N$

(а) $n^2 \leq d(n) \leq n^{c_{14}}$;

(б) для любой области $D \subseteq \{0, 1\}^n$ мощности $d(n)$ найдутся такие целое m и оператор $L_D : \{0, 1\}^n \rightarrow \{0, 1\}^m$, принадлежащий $\widehat{\mathcal{L}}$ и сжимающий D относительно f , что справедливо неравенство

$$\log L(f_{D, L_D}) < c_{13} \log L(m).$$

Положим $c_{13} = 1/9$. Тогда

$$L(f_D) \leq L(L_D) + 2^{c_{13}m} \leq n(\log n)^2 + 2^{m/9} \leq |D|^{1/2}.$$

Следовательно, можно воспользоваться леммой 7. Из этой леммы следует существование таких областей D_1, \dots, D_s , $s < n$, что $f = M(f_{D_1}, \dots, f_{D_s})$, где $f_{D_i} = h_{D_i, f} = h'_{D_i, f}(L_{D_i, f})$. Так как каждая функция $h'_{D_i, f}$ зависит не более чем от m переменных и $m < 5 \log |D| \leq 5c_{14} \log n$, то каждая функция $h'_{D_i, f}$ может быть реализована схемой, глубина которой

по порядку равна $\log n$. Очевидно также, что любой линейный оператор может быть реализован схемой логарифмической глубины. Поэтому глубина каждой функции f_{D_i} по порядку не превышает $\log n$. Наконец, заметим, что функция голосования тоже имеет логарифмическую глубину. Следовательно, $f \in NC$. Теорема 8 доказана.

Автор благодарен профессору О. Б. Лупанову за внимание к работе.

ЛИТЕРАТУРА

1. Ахо А., Хопкрофт Дж., Ульман Дж. Построение и анализ вычислительных алгоритмов. М.: Мир, 1979.
2. Лидл Р., Нидеррайтер Г. Конечные поля. М.: Мир, 1988. Т. 1.
3. Лупанов О. Б. Асимптотические оценки сложности управляющих систем. М.: Изд-во МГУ, 1984.
4. Нигматуллин Р. Г. Нижние оценки сложности и сложность универсальных схем. Казань: Изд-во Казан. ун-та, 1990.
5. Чашкин А. В. Нижние оценки сложности сужений булевых функций // Дискрет. анализ и исслед. операций. Сер. 1. 1997. Т. 4, № 2. С. 75–111.
6. Чашкин А. В. О сложности сужений булевых функций // Дискрет. математика. 1996. Вып. 2. С. 133–150.

Адрес автора:

МГУ, мех.-мат. факультет,
Воробьевы горы,
119899 Москва,
Россия

Статья поступила

28 апреля 1997 г.