

$(s, d, \varepsilon)$ -РАЗЛОЖЕНИЕ БУЛЕВЫХ ФУНКЦИЙ<sup>\*)</sup>

А. В. Чашкин

Рассматривается специальное  $(s, d, \varepsilon)$ -разложение произвольной булевой функции  $f$ , зависящей от  $n$  переменных. Элементами этого разложения являются  $s$ ,  $s < n$ , частичных функций, каждая из которых определена и совпадает с  $f$  на некоторой области мощности  $d$ , где минимально возможное  $d$  не более чем в  $n^3$  раз превосходит сложность реализации функции  $f$  схемами из функциональных элементов. Получены критерии существования  $(s, d, \varepsilon)$ -разложений.

Пусть  $f$  — полностью определенная булева функция от  $n$  переменных,  $L(f)$  — сложность минимальной схемы из функциональных элементов, реализующей в базисе из всех двуместных булевых функций булеву функцию  $f$ ,  $D \subseteq \{0, 1\}^n$ . Частичную булеву функцию  $f_D : D \rightarrow \{0, 1\}$  назовем *сужением* функции  $f$  на область  $D$ , если  $f_D(x) = f(x)$  для всех  $x \in D$  и  $L(f_D) = \min L(h)$ , где минимум берется по всем таким функциям  $h$ , что  $h(x) = f(x)$  при всех  $x \in D$ . Таким образом, в общем случае сужением булевой функции  $f$  на область  $D$  является некоторая частичная функция. Доопределим эту функцию до полностью определенной. Для этого линейно упорядочим все полностью определенные булевы функции, зависящие от  $n$  переменных. Сделаем это, сравнивая векторы значений булевых функций как целые числа, записанные в двоичной системе счисления. Каждой частичной булевой функции  $f : D \rightarrow \{0, 1\}$  поставим в соответствие полностью определенную булеву функцию  $h'$ , являющуюся минимальной (относительно указанного выше линейного порядка) среди таких функций  $h$ , что  $f = h_D$  и  $L(f) = L(h)$ . Функцию  $h'$  будем называть *продолжением* функции  $f$ . Продолжение функции  $f$  будем обозначать через  $\hat{f}$ .

---

<sup>\*)</sup> Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (код проекта 99-01-01175) и Федеральной целевой программы «Интеграция» (код проекта 1997-473).

Будем говорить, что для функции  $f$  имеет место  $(s, d, \varepsilon)$ -разложение, если при каждом  $x \in \{0, 1\}^n$  справедливо неравенство

$$\sum_{j=1}^s (f(x) \oplus \hat{f}_{D_j}(x)) < l,$$

где  $\varepsilon > 0$ , целые положительные  $s$  и  $l$  связаны соотношением  $l \leq (\frac{1}{2} - \varepsilon) s$  и  $|D_j| \leq d$  при каждом  $j \in \{1, 2, \dots, s\}$ . Величины  $s, d, \varepsilon$  будем называть *параметрами разложения*. Легко видеть, что если для функции  $f$  имеет место  $(s, d, \varepsilon)$ -разложение, то

$$f(x) = M(\hat{f}_{D_1}(x), \dots, \hat{f}_{D_s}(x)),$$

где  $M$  — функция голосования.

Основное свойство  $(s, d, \varepsilon)$ -разложений заключается в том, что значение любой булевой функции, зависящей от  $n$  переменных, на произвольном наборе из ее области определения однозначно определяется через значения  $s$ ,  $s < n$ , частичных функций, определенных на областях мощности  $d$ . Наибольший интерес рассматриваемые разложения представляют для функций небольшой сложности, например полиномиальной. В этом случае параметр  $d$  является полиномом от  $n$ . Часто более удобно рассматривать несколько функций с малыми областями определения вместо одной полностью определенной булевой функции. Примеры использования  $(s, d, \varepsilon)$ -разложений при решении различных задач можно найти в [5–7].

Далее полагаем, что  $n$  — число переменных рассматриваемых ниже функций всегда больше некоторого  $n_0$ .

Обозначим через  $N(L, n)$  число полностью определенных булевых функций от  $n$  переменных сложности не более  $L$ . Эта величина оценивается сверху числом различных схем, сложность которых не превосходит  $L$ . Из [2] следует, что

$$N(L, n) \leq (c_1(L + n))^L, \quad (1)$$

где  $c_1$  — константа.

Первая теорема, приводимая без доказательства, является простым следствием теоремы 1 из [4] и неравенства (1).

**Теорема 1.** Пусть  $f : \{0, 1\}^n \rightarrow \{0, 1\}$ ,  $\varepsilon$  и  $\delta$  — такие константы, что  $0 < \delta < \frac{1}{2}$  и  $0 < \varepsilon \leq \delta$ ,  $c_2, c_3$  — некоторые константы, зависящие от  $\varepsilon$ , и  $d_1 = c_2 n^2 L(f) \log_2 L(f)$ . Тогда при любых  $d, s$  таких, что

$$d \geq d_1, \quad s \leq \frac{c_3(n - \log_2 d_1 + 3 \log_2 n)}{\log_2 2d - \log_2 d_1},$$

для функции  $f$  имеет место  $(s, d, \varepsilon)$ -разложение.

Пусть  $f : \{0, 1\}^n \rightarrow \{0, 1\}$ . Величину  $w(f) = \sum_{x \in \{0, 1\}^n} f(x)$  назовем *весом* функции  $f$ .

**Теорема 2.** Пусть  $n^4 \leq L \leq 2^n/n^2$ ,  $0 < \varepsilon < \frac{1}{2}$ ,  $d_1 = n^2 L \log_2 L$ , и  $d \geq d_1$ . Тогда существует такая булева функция  $f : \{0, 1\}^n \rightarrow \{0, 1\}$ , что  $L(f) \lesssim L^*$  и для параметров любого  $(s, d, \varepsilon)$ -разложения функции  $f$  справедливо неравенство

$$s \geq \frac{c_4(n - \log_2 d_1 + 3 \log_2 n)}{\log_2 3d - \log_2 d_1 + 3 \log_2 n},$$

где  $c_4$  — константа.

**Доказательство.** Пусть целое число  $w$  таково, что при  $n \rightarrow \infty$

$$L \sim \frac{\log_2 \binom{2^n}{w}}{\log_2 \log_2 \binom{2^n}{w}}. \quad (2)$$

Легко видеть, что при  $n \rightarrow \infty$

$$\log_2 \binom{2^n}{w} = \log_2 \frac{2^n(2^n - 1) \dots (2^n - w + 1)}{w(w - 1) \dots 1} \geq w \log_2 \frac{2^n}{w}, \quad (3)$$

$$\log_2 \binom{2^n}{w} \leq \log_2 \frac{2^{nw}}{w!} \leq \log_2 \left( \frac{3 \cdot 2^n}{w} \right)^w \sim w \log_2 \frac{2^n}{w}. \quad (4)$$

Обозначим через  $M(n, w)$  множество, состоящее из всех булевых функций от  $n$  переменных веса  $w$ . Из [2, теорема 3] и (2) следует, что сложность любой функции из множества  $M(n, w)$  асимптотически не превосходит  $L$ . Тогда из определения  $M(n, w)$  и соотношений (3) и (4) имеем

$$\log_2 |M(n, w)| \sim w \log_2 \frac{2^n}{w}. \quad (5)$$

Допустим, что для каждой функции  $f$  из  $M(n, w)$  имеет место  $(s, d, \varepsilon)$ -разложение, где  $d$  — параметр из условий теоремы. Следовательно, для  $f$  найдутся такие области  $D_1, D_2, \dots, D_s$ , что  $|D_j| \leq d$ ,  $1 \leq j \leq s$ , и

$$f(x) = M(\hat{f}_{D_1}(x), \dots, \hat{f}_{D_s}(x)). \quad (6)$$

Из [3, лемма 6] следует, что

$$L(\hat{f}_{D_j}) \log_2 L(\hat{f}_{D_j}) \leq c_5 \log_2 \binom{d}{w} \leq c_5 \log_2 \frac{d^w}{w!} \leq c_5 w \log_2 \frac{3d}{w}, \quad (7)$$

---

<sup>\*</sup>  $\alpha(n) \lesssim \beta(n)$  означает, что  $\lim_{n \rightarrow \infty} \frac{\alpha(n)}{\beta(n)} \leq 1$  при  $n \rightarrow \infty$ ,  $\alpha(n) \sim \beta(n)$  означает, что  $\alpha(n) \lesssim \beta(n)$  и  $\alpha(n) \gtrsim \beta(n)$ .

где  $c_5 \geq 1$  — некоторая константа. Так как любую булеву функцию можно однозначно определить, задав реализующую ее схему, то, объединяя (1), (6) и (7), после несложных преобразований имеем

$$\log_2 |M(n, w)| \leq c_5 s w \log_2 \frac{3d}{w}. \quad (8)$$

Сравнивая (5) и (8) видим, что  $c_5 s w \log_2 \frac{3d}{w} \gtrsim w \log_2 \frac{2^n}{w}$ . Выделяя  $s$  и учитывая, что  $d_1 < w n^3$  и  $c_5 \geq 1$ , получаем

$$s \geq \frac{\log_2 \frac{2^n}{w}}{c_5 \log_2 \frac{3d}{w}} \gtrsim \frac{n - \log_2 d_1 + 3 \log_2 n}{c_5 (\log_2 3d - \log_2 d_1 + 3 \log_2 n)}.$$

Выберем константу  $c_4$  так, что  $c_4 c_5 < 1$ . Тогда среди функций из множества  $M(n, w)$  найдется такая функция  $f$ , что для параметров любого ее  $(s, d, \varepsilon)$ -разложения справедливо неравенство

$$s \geq \frac{c_4 (n - \log_2 d_1 + 3 \log_2 n)}{\log_2 3d - \log_2 d_1 + 3 \log_2 n}.$$

Теорема 2 доказана.

**Теорема 3.** Пусть  $f : \{0, 1\}^n \rightarrow \{0, 1\}$ ,  $L(f) \geq n^2$ ,  $\delta > 0$  — константа,  $\delta < \varepsilon < \frac{1}{2}$ . Тогда для параметров любого  $(s, d, \varepsilon)$ -разложения функции  $f$  справедливо неравенство

$$d > \frac{c_6 L(f) \log_2 L(f)}{n},$$

где  $c_6$  — положительная константа.

**Доказательство.** Допустим, существует функция  $f : \{0, 1\}^n \rightarrow \{0, 1\}$  такая, что при некотором  $d \leq \frac{c_6 L(f) \log_2 L(f)}{n}$  имеет место  $(s, d, \varepsilon)$ -разложение. Тогда существуют области  $D_1, D_2, \dots, D_s$ ,  $|D_j| \leq d$ ,  $1 \leq j \leq s$ , такие, что

$$\sum_{j=1}^s (f(x) \oplus \hat{f}_{D_j}(x)) \leq \left(\frac{1}{2} - \varepsilon\right) s, \quad (9)$$

где  $\varepsilon$  — некоторая положительная константа. Зафиксируем целое положительное  $l = 2l' + 1$ . Введем  $s^l$  функций

$$f_{i_1, \dots, i_l}(x) = M(\hat{f}_{D_{i_1}}(x), \dots, \hat{f}_{D_{i_l}}(x)), \quad (10)$$

где каждый индекс  $i_j$  независимо изменяется на множестве  $\{1, 2, \dots, s\}$ . При произвольном  $x \in \{0, 1\}^n$  оценим число функций  $f_{i_1, \dots, i_l}$ , значения

которых на наборе  $x$  не совпадают с  $f(x)$ . Пользуясь (9), получаем

$$\begin{aligned} \sum_{i_1, \dots, i_l} (f(x) \oplus f_{i_1, \dots, i_l}(x)) &\leq \sum_{j=l'+1}^l \binom{l}{j} \left( \left( \frac{1}{2} - \varepsilon \right) s \right)^j \left( \left( \frac{1}{2} + \varepsilon \right) s \right)^{l-j} \\ &= \left( \left( \frac{1}{2} + \varepsilon \right) s \right)^l \sum_{j=l'+1}^l \binom{l}{j} \left( \frac{1-2\varepsilon}{1+2\varepsilon} \right)^j < \left( \frac{s}{2} \right)^l (1+2\varepsilon)^l 2^{l-1} \sum_{j=l'+1}^{\infty} \left( \frac{1-2\varepsilon}{1+2\varepsilon} \right)^j \\ &\leq \frac{1}{2} s^l (1+2\varepsilon)^{2l'+1} \left( \frac{1-2\varepsilon}{1+2\varepsilon} \right)^{l'+1} \frac{1}{1 - \frac{1-2\varepsilon}{1+2\varepsilon}} = s^l \frac{(1-4\varepsilon^2)^{l'+1}}{8\varepsilon}. \quad (11) \end{aligned}$$

Выберем такое минимально возможное целое  $l'$ , что

$$\frac{(1-4\varepsilon^2)^{l'+1}}{8\varepsilon} < 2^{-n}. \quad (12)$$

Так как  $\varepsilon$  — константа, то после простых преобразований видим, что в этом случае справедливо неравенство

$$2l' + 1 \leq \frac{3 \log_2(2^n/8\varepsilon)}{\log_2(1/(1-4\varepsilon^2))} \leq c_7 n, \quad (13)$$

где  $c_7$  некоторая зависящая от  $\varepsilon$  константа. Подставляя выбранное значение  $l'$  в (11) и учитывая (12), имеем  $\sum_{x \in \{0,1\}^n} \sum_{i_1, \dots, i_l} (f(x) \oplus f_{i_1, \dots, i_l}(x)) < s^l$ .

Следовательно, среди  $s^l$  функций  $f_{i_1, \dots, i_l}(x)$  имеется функция  $f_{\alpha_1, \dots, \alpha_l}(x)$  такая, что сумма  $\sum_{x \in \{0,1\}^n} (f(x) \oplus f_{\alpha_1, \dots, \alpha_l}(x))$  не превосходит среднее по всем функциям значение, т. е. строго меньше единицы. Так как значение рассматриваемой суммы является целым числом, то  $\sum_{x \in \{0,1\}^n} (f(x) \oplus f_{\alpha_1, \dots, \alpha_l}(x)) = 0$ , т. е.  $f_{\alpha_1, \dots, \alpha_l}(x)$  совпадает с  $f(x)$  при каждом  $x$  из  $\{0,1\}^n$ . Из [1, 8] и условий теоремы для каждой области  $D_j$  из (9) имеем

$$L(\hat{f}_{D_j}) \lesssim \frac{d}{\log_2 d} \leq \frac{2c_6 L(f) \log_2 L(f)}{n \log_2 L(f)} = \frac{2c_6 L(f)}{n}.$$

Учитывая, что функция голосования имеет линейную сложность, из (10), (13), условий теоремы и предыдущего неравенства получаем

$$L(f) \leq L(f_{\alpha_1, \dots, \alpha_l}) \leq \frac{2c_6(2l'+1)L(f)}{n} + \mathcal{O}(l') \lesssim 2c_6 c_7 L(f).$$

При  $2c_6 c_7 < 1$  приходим к противоречию. Теорема 3 доказана.

В следующей теореме устанавливается существование функций, для которых нижняя оценка минимально возможного значения параметра  $d$  выше, чем в общем случае.

**Теорема 4.** Пусть  $n^2 \leq L \leq 2^n/n$ ,  $\delta > 0$  — константа и  $\varepsilon$  таково, что  $\delta < \varepsilon < \frac{1}{2}$ . Существует такая булева функция  $f : \{0, 1\}^n \rightarrow \{0, 1\}$ , что  $L(f) \sim L$  и для параметров любого  $(s, d, \varepsilon)$ -разложения функции  $f$  справедливо неравенство

$$d > c_8 L(f) \log_2 L(f),$$

где  $c_8$  — положительная константа.

**ДОКАЗАТЕЛЬСТВО.** Пусть область  $D \subseteq \{0, 1\}^n$  и частичная функция  $f' : D \rightarrow \{0, 1\}$  такие, что  $|D| \sim L \log_2 L$  и  $L(f') \sim L$ . Рассмотрим функцию  $f$  — продолжение функции  $f'$ , т. е.  $f = \hat{f}'$ . Допустим, что существует  $(s, d, \varepsilon)$ -разложение функции  $f$  такое, что  $d \leq c_8 L(f) \log_2 L(f)$ . Тогда существуют области  $D_1, D_2, \dots, D_s$ ,  $|D_j| \leq d$ , такие, что  $\sum_{j=1}^s (f(x) \oplus \hat{f}_{D_j}(x)) \leq (\frac{1}{2} - \varepsilon) s$ . Зафиксируем целое положительное  $l = 2l' + 1$ . Введем  $s^l$  функций

$$f_{i_1, \dots, i_l}(x) = M(\hat{f}_{D_{i_1}}(x), \dots, \hat{f}_{D_{i_l}}(x)), \quad (14)$$

где каждый индекс  $i_j$  независимо изменяется на множестве  $\{1, 2, \dots, s\}$ . Для произвольного  $x \in D$  оценим число функций  $f_{i_1, \dots, i_l}$ , значения которых на наборе  $x$  не совпадают с  $f(x)$ . Выберем такое минимально возможное целое  $l'$ , что

$$\frac{(1 - 4\varepsilon^2)^{l'+1}}{8\varepsilon} < c_9, \quad (15)$$

где  $c_9$  — константа, определяемая ниже. Так как  $\varepsilon$  — константа, то легко видеть, что в этом случае

$$2l' + 1 \leq c_{10}, \quad (16)$$

где  $c_{10}$  — константа, зависящая от  $\varepsilon$  и  $c_9$ . Объединяя (11) и (15), получаем, что  $\sum_{x \in D} \sum_{i_1, \dots, i_l} (f(x) \oplus f_{i_1, \dots, i_l}(x)) < c_9 s^l |D|$ . Следовательно, среди функций  $f_{i_1, \dots, i_l}(x)$  найдется функция  $f_{\alpha_1, \dots, \alpha_l}(x)$  такая, что

$$\sum_{x \in D} (f(x) \oplus f_{\alpha_1, \dots, \alpha_l}(x)) < c_9 |D|. \quad (17)$$

Из [1, 8], условий теоремы и сделанного предположения о величине  $d$  следует, что для каждой области  $D_j$  справедливо неравенство

$$L(\hat{f}_{D_j}) \lesssim \frac{d}{\log_2 d} \leq \frac{c_8 L(f) \log_2 L(f)}{\log_2 L(f)} = c_8 L(f).$$

Учитывая, что функция голосования имеет линейную сложность, из (14), (16), условий теоремы и предыдущего неравенства получаем

$$\begin{aligned} L(f_{\alpha_1, \dots, \alpha_l}) &\leq c_8(2l' + 1)L(f) + \mathcal{O}(l') \lesssim c_8 c_{10} L(f), \\ L(f_{\alpha_1, \dots, \alpha_l}) \log_2 L(f_{\alpha_1, \dots, \alpha_l}) &\lesssim c_8 c_{10} L(f) \log_2 L(f). \end{aligned} \quad (18)$$

Из (7), (17) и [3, лемма 6] следует, что

$$\begin{aligned} L(f \oplus f_{\alpha_1, \dots, \alpha_l}) \log_2 (L(f \oplus f_{\alpha_1, \dots, \alpha_l})) &\leq c_5 \log_2 \left( \frac{|D|}{c_9 |D|} \right) \\ &\leq c_5 \log_2 \frac{(|D|)^{c_9 |D|}}{(c_9 |D|)!} \leq c_5 c_9 |D| \log_2 \left( \frac{3}{c_9} \right). \end{aligned} \quad (19)$$

Так как  $L(f) \leq L(f_{\alpha_1, \dots, \alpha_l}) + L(f \oplus f_{\alpha_1, \dots, \alpha_l}) + 1$ , то из (18) и (19) после несложных преобразований получаем

$$L(f) \log_2 L(f) \leq 2L(f) \log_2 L(f) (c_8 c_{10} + c_5 c_9 \log_2(3/c_9)).$$

Выбирая константы  $c_8$  и  $c_9$  достаточно малыми так, чтобы выполнялось неравенство

$$2(c_8 c_{10} + c_5 c_9 \log_2(3/c_9)) < 1,$$

приходим к противоречию. Теорема 4 доказана.

## ЛИТЕРАТУРА

1. Андреев А. Е. О сложности реализации частичных булевых функций схемами из функциональных элементов // Дискрет. математика. 1989. Т. 1, вып. 4. С. 36–45.
2. Лупанов О. Б. Об одном подходе к синтезу управляющих систем — принципе локального кодирования // Проблемы кибернетики. М.: Наука, 1965. Вып. 14. С. 31–110.
3. Чашкин А. В. О среднем времени вычисления значений булевых функций // Дискрет. анализ и исслед. операций. Сер. 1. 1997. Т. 4, № 1. С. 60–78.
4. Чашкин А. В. Нижние оценки сложности сужений булевых функций // Дискрет. анализ и исслед. операций. Сер. 1. 1997. Т. 4, № 2. С. 75–111.
5. Чашкин А. В. О вычислении булевых функций вероятностными программами // Дискрет. анализ и исслед. операций. Сер. 1. 1997. Т. 4, № 3. С. 49–68.
6. Чашкин А. В. Локальная сложность булевых функций // Дискрет. анализ и исслед. операций. Сер. 1. 1997. Т. 4, № 3. С. 69–80.

7. **Чашкин А. В.** Самокорректирующиеся схемы для функций полиномиального веса // Вестн. Моск. ун-та. Сер. 1. Математика. Механика. 1997. № 5. С. 64–66.
8. **Шоломов Л. А.** О реализации недоопределенных булевых функций схемами из функциональных элементов // Проблемы кибернетики. М.: Наука, 1969. Вып. 21. С. 215–226.

Адрес автора:

МГУ, мех.-мат. факультет,  
Воробьевы горы,  
119899 Москва, Россия.  
E-mail: chash@glasnet.ru

Статья поступила

2 декабря 1999 г.