Math-Net.Ru
All Russian mathematical portal

A. V. Chashkin, On a decomposition of Boolean functions, *Diskr. Mat.*, 2000, Volume 12, Issue 3, 114–123

https://www.mathnet.ru/eng/dm338

Use of the all-Russian mathematical portal Math-Net.Ru implies that you have read and agreed to these terms of use
https://www.mathnet.ru/eng/agreement

Download details:
IP: 18.97.9.168
May 21, 2025, 01:29:07

Дискретная математика

том 12 выпуск 3 * 2000

УДК 519.7

Об одном разложении булевых функций

© 2000 г. А. В. Чашкин

Рассматривается специальное (s, d, ε)-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, ε)-разложений и изучены их свойства.

Работа выполнена при поддержке Российского фонда фундаментальных исследований, проект 99–01–01175, и ФЦП «Интеграция», проект 473.

1. Введение

Пусть $f\colon \{0,1\}^n \to \{0,1\}$, $L(f)$ — минимальная сложность реализации полностью определенной булевой функции f схемами в базисе из всех двуместных булевых функций, D — произвольная область в $\{0,1\}^n$. Частичную функцию $f_D\colon D \to \{0,1\}$ 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 функциям h, для которых $h(x) = f(x)$ при всех $x \in D$. Таким образом, в общем случае сужением булевой функции f на область D является некоторая частичная функция, то есть значения f_D вне области D определены неоднозначно. Избавимся от этой неопределенности. Для этого линейно упорядочим все полностью определенные булевы функции, зависящие от n аргументов. Сделать это можно разными способами, например, сравнивая векторы значений булевых функций как целые числа, записанные в двоичной системе счисления. Каждой частичной булевой функции $f\colon D \to \{0,1\}$ 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 $\hat{f}$.

Будем говорить, что для функции f имеет место (s, d, ε)-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 $l \leqslant (1/2-\varepsilon)s$ и $|D_j| \leqslant d$ при всех $j \in \{1, 2, \ldots, s\}$. Величины s, d, ε будем называть параметрами разложения. Легко видеть, что если для функции f имеет место (s, d, ε)-разложение, то

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

где M — функция голосования.

Главное свойство (s, d, ε)-разложений заключается в том, что значение любой булевой функции, зависящей от n переменных, на произвольном наборе из ее области определения однозначно определяется значениями s, $s < n$, частичных функций, определенных на областях мощности d. Наибольший интерес рассматриваемые разложения представляют в случае функций небольшой сложности, например полиномиальной. В этом случае параметр d будет полиномом от n. Часто более удобно рассматривать несколько функций с маленькой областью определения вместо одной полностью определенной булевой функции. Примеры использования (s, d, ε)-разложений при решении различных задач можно найти в [1–3].

В настоящей работе рассматриваются вопросы существования (s, d, ε)-разложений для произвольных булевых функций. Найдены соотношения, связывающие параметры разложения и сложность функции. Показано, что для достаточно широкого множества значений параметров разложения установленные соотношения являются точными по порядку. Установлены оценки минимально возможных значений параметров s и d, при которых рассматриваемые разложения существуют. В частности, показано, что сложность функции не может превышать величину параметра d более чем в n раз (теорема 4), то есть знание сужений булевой функции даже на достаточно большое число областей маленького размера не позволяет вычислить ее значение на произвольном наборе.

Далее полагаем, что n — число переменных рассматриваемых ниже функций, всегда больше некоторой положительной постоянной.

2. Условия существования разложений

Обозначим через $N(L, n)$ число полностью определенных булевых функций от n переменных, сложность которых не превосходит L. Эта величина оценивается сверху через число различных схем, сложность которых не превосходит L. Из [4] следует, что

$$N(L, n) \leqslant (c(L+n))^L, \tag{1}$$

где c — постоянная.

Первая теорема, приводимая без доказательства, является простым следствием теоремы 1 из [5] и неравенства (1).

Теорема 1. *Пусть L, d, d_1 — положительные числа, p, $p \geqslant 2$, — целое число, $f\colon \{0,1\}^n \to \{0,1\}$, $d_1 = 16(pn)^2 L \log_2 L$, $d \geqslant d_1$.*

Далее, пусть для любой области D такой, что $D \subset \{0,1\}^n$ и $|D| \leqslant d$, справедливо неравенство $L(f_D) \leqslant L$.

Тогда среди областей D имеются области $D_1, \ldots, D_s$ такие, что

$$\sum_{j=1}^{s} (f(x) \oplus \hat{f}_{D_j}(x)) \leqslant l, \qquad f(x) = M(\hat{f}_{D_1}(x), \ldots, \hat{f}_{D_s}(x)),$$

где

$$l \leqslant \left\lceil \frac{n - \log_2 d_1 + 3\log_2 n}{\log_2 2d - \log_2 d_1} \right\rceil, \qquad s = pl + p - 1.$$

Следующая теорема, являющаяся следствием теоремы 1, устанавливает достаточные условия существования (s, d, ε)-разложения для произвольной булевой функции f.

Теорема 2. *Пусть $f\colon \{0,1\}^n \to \{0,1\}$, ε и δ — такие постоянные, что $0 < \delta < 1/2$ и $0 < \varepsilon \leqslant \delta$, c_1, c_2 — некоторые постоянные, зависящие от ε, $d_1 = c_1 n^2 L(f) \log_2 L(f)$.*

Тогда при любых d, s таких, что

$$d \geqslant d_1, \qquad s \leqslant \frac{c_2(n - \log_2 d_1 + 3\log_2 n)}{\log_2 2d - \log_2 d_1)},$$

для функции f имеет место (s, d, ε)-разложение.

Доказательство. Положим $p = \lceil 2/(1-2\varepsilon) \rceil$. Очевидно, что $p \geqslant 2$. При $s = pl + p - 1$

$$\left(\frac{1}{2} - \varepsilon\right) s \geqslant \left(\frac{1}{2} - \varepsilon\right)\left(\frac{2}{1-2\varepsilon} l + \frac{2}{1-2\varepsilon} - 1\right) = l + 1 - \frac{1-2\varepsilon}{2} > l.$$

Так как $\varepsilon \leqslant \delta < 1/2$ и δ — константа, p также является константой. Выберем

$$d_2 = 16(pn)^2 L(f) \log_2 L(f).$$

Так как для любой функции $f\colon \{0,1\}^n \to \{0,1\}$ и любой области $D \subseteq \{0,1\}^n$ справедливо неравенство $L(f_D) \leqslant L(f)$, при $d \geqslant d_2$ из теоремы 1 следует существование таких областей

$$D_1, \ldots, D_s, \quad |D_j| \leqslant d, \quad 1 \leqslant j \leqslant s,$$

что

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

где

$$l \leqslant \left\lceil \frac{n - \log_2 d_1 + 3\log_2 n}{\log_2 2d - \log_2 d_1} \right\rceil, \qquad s = p(l+1) - 1.$$

Положим $c_1 = 16p^2$. Тогда $d_2 = d_1$. После несложных преобразований получаем, что

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

где c_3 — подходящая постоянная, зависящая от p. Полагая $c_2 = c_3$, получаем утверждение теоремы.

Пусть $f\colon \{0,1\}^n \to \{0,1\}$. Величину

$$w(f) = \sum_{x \in \{0,1\}^n} f(x)$$

назовем весом функции f.

Теорема 3. *Пусть*

$$n^2 \leqslant L \leqslant 2^n/n^2, \quad 0 < \varepsilon < 1/2, \quad d_1 = n^2 L \log_2 L, \quad d \geqslant d_1.$$

Тогда существует такая булева функция $f\colon \{0,1\}^n \to \{0,1\}$, *что* $L(f) \lesssim L$ *и для параметров любого* (s,d,ε)*-разложения функции* f *справедливо неравенство*

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

где c_4 *— постоянная.*

Доказательство. Пусть целое число w такое, что при $n \to \infty$ справедливо асимптотическое равенство

$$L \sim \frac{\log_2 \binom{2^n}{w}}{\log_2 \log_2 \binom{2^n}{w}}. \tag{2}$$

Легко видеть, что при $n \to \infty$

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

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

Рассмотрим множество $M(n,w)$, состоящее из всех булевых функций от n переменных веса w. Из теоремы 3 в [4] и соотношения (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) следует, что

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

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

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

Из леммы 6 в [6] следует, что

$$L(\hat f_{D_j}) \log_2 L(\hat f_{D_j}) \leqslant c_5 \log_2 \binom{d}{w} \leqslant c_5 \log_2 \frac{d^w}{w!} \leqslant c_5 w \log_2 \frac{3d}{w}, \tag{7}$$

где $c_5 \geqslant 1$ — некоторая постоянная. Так как любую булеву функцию можно однозначно определить, задав реализующую ее схему, объединяя (1), (6) и (7), после несложных преобразований находим, что

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

Сравнивая (5) и (8) видим, что

$$c_5 sw \log_2 \frac{3d}{w} \gtrsim w \log_2 \frac{2^n}{w}.$$

Выделяя s и учитывая, что $d_1 < wn^3$ и $c_5 \geqslant 1$, получаем, что

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

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

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

Теорема 3 доказана.

Сравнивая утверждения теоремы 2 и теоремы 3, видим, что при $d \geqslant d_1^{1+\delta}$, где δ — произвольная положительная постоянная, оценки сверху и снизу для параметра s отличаются только постоянным множителем. Следовательно, при $d \geqslant d_1^{1+\delta}$, параметр s в этих теоремах не может быть улучшен более, чем в постоянное число раз.

В следующей теореме для (s,d,ε)-разложений при постоянной ε устанавливаются ограничения на параметр d. Показано, что d не может быть слишком маленьким.

Теорема 4. *Пусть $f\colon \{0,1\}^n \to \{0,1\}$, $L(f) \geqslant n^2$, δ — положительная постоянная, $\delta < \varepsilon < 1/2$. Тогда для параметров любого (s,d,ε)-разложения функции f справедливо неравенство*

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

где c_6 — положительная постоянная.

Доказательство. Теорему докажем методом от противного. Допустим, что существует функция $f\colon \{0,1\}^n \to \{0,1\}$, для которой (s,d,ε)-разложение имеет место при некотором $d \leqslant (c_6 L(f) \log_2 L(f))/n$. Следовательно, существуют области

$$D_1, D_2, \ldots, D_s, \quad |D_j| \leqslant d, \quad 1 \leqslant j \leqslant s,$$

для которых

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

где ε — некоторая положительная постоянная. Зафиксируем целое положительное $l = 2l' + 1$. Введем s^l функций

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

где каждый индекс i_j независимо изменяется на множестве $\{1,2,\ldots,s\}$. Для произвольного $x \in \{0,1\}^n$ оценим число функций $f_{i_1,\ldots,i_l}$, значения которых на наборе x не совпадают с $f(x)$. Из (9) следует, что

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

Выберем такое минимально возможное целое l', что

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

Так как ε — постоянная, после простых преобразований видим, что в этом случае справедливо неравенство

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

где c_7 — некоторая постоянная, зависящая от ε. Подставляя выбранное значение l' в (11) и учитывая (12), находим, что

$$\sum_{x\in\{0,1\}^n} \sum_{i_1,\ldots,i_l} (f(x) \oplus f_{i_1,\ldots,i_l}(x)) < s^l.$$

Следовательно, среди s^l функций $f_{i_1,\ldots,i_l}(x)$ найдется функция $f_{\alpha_1,\ldots,\alpha_l}(x)$ для которой сумма

$$\sum_{x\in\{0,1\}^n} (f(x) \oplus f_{\alpha_1,\ldots,\alpha_l}(x))$$

не превосходит среднее по всем функциям значение, то есть эта сумма строго меньше единицы. Так как значение рассматриваемой суммы является целым числом,

$$\sum_{x\in\{0,1\}^n} (f(x) \oplus f_{\alpha_1,\ldots,\alpha_l}(x)) = 0,$$

то есть $f_{\alpha_1,\ldots,\alpha_l}(x)$ совпадает с $f(x)$ при всех x из $\{0,1\}^n$. Из [7, 8], сделанного предположения о величине d и условий теоремы для каждой области D_j, представленной в (9), справедливы соотношения

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

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

$$L(f) \leqslant L(f_{\alpha_1,\ldots,\alpha_l}) \leqslant \frac{2c_6(2l'+1)L(f)}{n} + O(l') \lesssim 2c_6c_7L(f).$$

При $2c_6c_7 < 1$ приходим к противоречию. Теорема 4 доказана.

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

Теорема 5. *Пусть $n^2 \leqslant L \leqslant 2^n/n$, δ, $\delta > 0$, — постоянная, $\delta < \varepsilon < 1/2$. Тогда существует такая булева функция $f\colon \{0,1\}^n \to \{0,1\}$, что $L(f) \sim L$ и для параметров любого (s, d, ε)-разложения функции f справедливо неравенство*

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

где c_8 — положительная постоянная.

Доказательство. Доказательство во многом аналогично доказательству предыдущей теоремы. Рассмотрим область $D \subseteq \{0,1\}^n$ и частичную функцию $f'\colon D \to \{0,1\}$ такие, что $|D| \sim L\log_2 L$ и $L(f') \sim L$. Далее рассматриваем функцию f, являющуюся продолжением функции f', то есть $f = \hat{f}'$. Допустим, что существует (s, d, ε)-разложение функции f, у которого $d \leqslant c_8 L(f) \log_2 L(f)$. Тогда, существуют области

$$D_1, D_2, \ldots, D_s, \qquad |D_j| \leqslant d,$$

для которых

$$\sum_{j=1}^{s} (f(x) \oplus \hat{f}_{D_j}(x)) \leqslant (1/2 - \varepsilon)s.$$

Зафиксируем целое положительное $l = 2l' + 1$. Введем s^l функций

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

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

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

где c_9 — постоянная, определяемая ниже. Так как ε — постоянная, легко видеть, что в этом случае

$$2l' + 1 \leqslant c_{10}, \tag{16}$$

где c_{10} — постоянная, зависящая от ε и c_9. Из (11) и (15) следует, что

$$\sum_{x\in D} \sum_{i_1,\ldots,i_l} (f(x) \oplus f_{i_1,\ldots,i_l}(x)) < c_9 s^l |D|.$$

Следовательно, среди функций $f_{i_1,\dots,i_l}(x)$ найдется функция $f_{\alpha_1,\dots,\alpha_l}(x)$ такая, что

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

Из [7, 8], условий теоремы и сделанного предположения о величине d, заключаем, что для каждой области D_j справедливо неравенство

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

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

$$\begin{gathered} L(f_{\alpha_1,\dots,\alpha_l}) \leqslant (2l'+1)L(f) + O(l') \lesssim c_8c_{10}L(f),\\ L(f_{\alpha_1,\dots,\alpha_l})\log_2 L(f_{\alpha_1,\dots,\alpha_l}) \lesssim c_8c_{10}L(f)\log_2 L(f). \end{gathered} \qquad (18)$$

Из (17) и леммы 6 в [6] следует, что (см. (7))

$$\begin{aligned} &L(f\oplus f_{\alpha_1,\dots,\alpha_l})\log_2(L(f\oplus f_{\alpha_1,\dots,\alpha_l}))\\ &\qquad\leqslant c_5\log_2\binom{|D|}{c_9|D|} \lll c_5\log_2\frac{(|D|)^{c_9|D|}}{(c_9|D|)!} \leqslant c_5c_9|D|\log_2\left(\frac{3}{c_9}\right). \end{aligned} \qquad (19)$$

Так как

$$L(f) \leqslant L(f_{\alpha_1,\dots,\alpha_l}) + L(f\oplus f_{\alpha_1,\dots,\alpha_l}),$$

из (18) и (19) после несложных преобразований получаем, что

$$L(f)\log_2 L(f) \leqslant 2L(f)\log_2 L(f)(c_8c_{10} + c_5c_9\log_2(3/c_9)).$$

Выбирая постоянные c_8 и c_9 достаточно малыми так, чтобы

$$2(c_8c_{10} + c_5c_9\log_2(3/c_9)) < 1,$$

приходим к противоречию. Теорема 5 доказана.

3. Сложность разложений

Введем функцию, количественно характеризующую (s,d,ε)-разложения булевых функций. Естественно полагать, что (s,d,ε)-разложение тем проще, чем меньше величины s и d. В качестве меры сложности (s,d,ε)-разложения рассмотрим величину d^s. Сложность самого простого (s,d,ε)-разложения функции f определим посредством функции

$$\lambda(f,\varepsilon) = \min d^s,$$

где минимум берется по всем возможным (s,d,ε)-разложениям функции f. Далее изучается функция $\lambda(f,\varepsilon)$. В двух последних теоремах устанавливается связь между величиной $\lambda(f,\varepsilon)$ и сложностью $L(f)$ функции f.

Теорема 6. *Пусть* $f\colon \{0,1\}^n \to \{0,1\}$, $L(f) \geqslant n\varphi(n)$, *где* $\varphi(n)\to\infty$ *при* $n\to\infty$, $0<\varepsilon<1/2$. *Тогда*

$$L(f)\log_2 L(f) \lesssim \lambda(f,\varepsilon) \leqslant 2^n.$$

Доказательство. Очевидно, что каждая функция f при любом положительном ε сама является своим $(1, 2^n, \varepsilon)$-разложением. Поэтому справедливо неравенство

$$\lambda(f, \varepsilon) \leqslant 2^n.$$

Если для функции f имеет место (s, d, ε)-разложение и $L(f) \geqslant n\varphi(n)$, где $\varphi(n) \to \infty$ при $n \to \infty$, то из [7, 8] и теоремы 2 следует, что

$$L(f) \log_2 L(f) \lesssim sd. \tag{20}$$

Предположим, что

$$d^s \lesssim (1 - \delta) L(f) \log_2 L(f),$$

где δ — положительная постоянная. Тогда из (20) следует, что

$$d^s \lesssim (1 - \delta) L(f) \log_2 L(f) \lesssim (1 - \delta) ds.$$

Так как s — целое положительное число, пришли к противоречию. Следовательно, $d^s \gtrsim L(f) \log_2 L(f)$. Таким образом,

$$L(f) \log_2 L(f) \lesssim \lambda(f, \varepsilon) \leqslant 2^n.$$

Теорема 6 доказана.

Очевидно, что существуют функции, на которых достигается верхняя граница теоремы 6. Более того, для почти всех булевых функций n переменных

$$\lambda(f, \varepsilon) \sim 2^n.$$

Это следует из сравнения числа всех булевых функций n переменны и числа функций, для которых $\lambda(f, \varepsilon) = o(2^n)$. В следующей теореме показано, что нижняя граница теоремы 6 также достигается, и кроме того, при любом $L > n^2$ существуют функции сложности L, для которых логарифм λ равен по порядку n, то есть в некотором смысле верхняя граница теоремы 6 достигается на достаточно простых функциях.

Теорема 7. *Пусть $n^2 \leqslant L \leqslant 2^n/n$, $0 < \varepsilon < 1/2$. Тогда существуют такие булевы функции n переменных f_1, f_2, что $L(f_1), L(f_2) \lesssim L$ и*

$$\lambda(f_1, \varepsilon) \sim L \log_2 L,$$
$$\log_2 \lambda(f_2, \varepsilon) \asymp n.$$

Доказательство. Пусть $D \subseteq \{0,1\}^n$, $|D| = d$, $f\colon D \to \{0,1\}$ — такая частичная функция, что $L(\hat{f}) \sim d/\log_2 d \sim L$. Очевидно, что для $\hat{f}$ имеет место $(1, d, \varepsilon)$-разложение. Следовательно, для $f_1 = \hat{f}$ справедливо неравенство

$$\lambda(f_1, \varepsilon) \lesssim d \sim L \log_2 L,$$

которое вместе с теоремой 6 доказывает первое утверждение теоремы.

Если $\log_2 L \asymp n$, то второе утверждение следует из первого. Поэтому далее полагаем, что $\log_2 L = o(n)$. Воспользуемся теоремой 3. Пусть f_2 — функция, существование которой гарантирует теорема 3. Для параметров любого (s, d, ε)-разложения функции f_2 справедливо неравенство

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

где $d_1 = n^2 L \log_2 L$. Если $d \leqslant d_1^2$, то легко видеть, что $(\log_2 2d - \log_2 d_1 + 3\log_2 n)$ не меньше $\log_2 n$, и так как $d > n$, то

$$s \log_2 d \gtrsim n.$$

Если $d > d_1^2$, то

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

Два последних соотношения вместе с теоремой 6 доказывают второе утверждение теоремы 7. Теорема 7 доказана.

Список литературы

1. Чашкин А. В., О вычислении булевых функций вероятностными программами. *Дискретный анализ и исследование операций* (1997) **4**, №3, 49–68.

2. Чашкин А. В., Локальная сложность булевых функций. *Дискретный анализ и исследование операций* (1997) **4**, №3, 69–80.

3. Чашкин А. В., Самокорректирующиеся схемы для функций полиномиального веса. *Вестн. Моск. унив., Сер 1: Математика, Механика* (1997) №5, 64–66.

4. Лупанов О. Б., Об одном подходе к синтезу управляющих систем — принципе локального кодирования. *Пробл. кибернетики* (1965) **14**, 31–110.

5. Чашкин А. В., Нижние оценки сложности сужений булевых функций. *Дискретный анализ и исследование операций* (1997) **4**, №2, 75–111.

6. Чашкин А. В., О среднем времени вычисления значений булевых функций. *Дискретный анализ и исследование операций* (1997) **4**, №1, 60–78.

7. Шоломов Л. А., О реализации недоопределенных булевых функций схемами из функциональных элементов. *Пробл. кибернетики* (1969) **21**, 215–226.

8. Андреев А. Е., О сложности реализации частичных булевых функций схемами из функциональных элементов. *Дискретная математика* (1989) **1**, №4, 36–45.

Статья поступила 14.07.1999.