ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Январь—март 1997. Том 4, № 1, 60–78

УДК 519.7

О СРЕДНЕМ ВРЕМЕНИ ВЫЧИСЛЕНИЯ ЗНАЧЕНИЙ БУЛЕВЫХ ФУНКЦИЙ*)

А. В. Чашкин

Рассматривается задача о среднем времени вычисления булевых функций неветвящимися программами с условной остановкой, состоящими из операторов двух типов. Каждый оператор первого типа вычисляет значение некоторой двуместной булевой функции, аргументами которой могут быть либо величины, вычисленные предыдущими операторами, либо значения входных переменных. Каждый оператор второго типа либо прерывает работу программы, либо дает указание выполнять очередной оператор. Мерой сложности таких программ является среднее время работы относительно всех наборов значений входных переменных. Доказано, что сложность реализации почти всех всюду определенных и почти всех частично определенных булевых функций такими программами по порядку совпадает со сложностью обычных схем из функциональных элементов, а для почти всех n-местных булевых функций, принимающих значение 1 на n^c наборах, эти сложности с точностью до порядка различаются в n раз. Установлено существование булевых функций от n переменных, среднее время вычисления которых по порядку в $(2^n/n)^{1/2}$ раз меньше времени, необходимого для вычисления обычными неветвящимися программами.

Введение

В настоящей статье изучается сложность реализации булевых функций неветвящимися программами с условной остановкой. Исследуемые программы являются последовательностями операторов двух типов. Каждый оператор первого типа вычисляет значения некоторой двуместной булевой функции. Аргументами этой функции могут быть либо величины, вычисленные предыдущими операторами, либо значения входных переменных. Операторы второго типа могут прекращать выполнение программы. Результат работы оператора второго типа определяется значениями, вычисленными программой на некоторых двух

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

предыдущих шагах. Для каждого конкретного оператора номера этих шагов фиксированы и могут быть различными для различных операторов.

Если на первый вход выполняемого оператора второго типа поступает единица, то выполнение программы прекращается и значение переменной, которая поступает на второй вход оператора, объявляется значением булевой функции на вычисляемом наборе переменных. В противном случае выполняется следующий оператор. Если последним оператором какой-либо программы является оператор первого типа и выполнение этой программы на предыдущих шагах не было прервано, то результатом работы программы считается величина, вычисленная последним оператором. В отличие от обычных неветвящихся программ (схем), затрачивающих одинаковое число шагов для вычисления функции на различных аргументах, время работы рассматриваемых программ для разных аргументов может быть различным. Поэтому естественной мерой сложности таких программ является среднее время работы, взятое по всем возможным аргументам.

В статье для этой меры сложности установлены с точностью до порядка формулы для функции Шеннона в классе всех булевых функций, функций с полиномиальным числом единичных значений, а также частичных функций. Оказалось (теорема 1), что среднее время вычисления рассматриваемыми программами почти каждой булевой функции только в фиксированное число раз меньше времени, необходимого для вычисления обычными неветвящимися программами, т. е. возможность досрочной остановки вычислений позволяет уменьшить время работы в среднем не более чем в постоянное число раз. Аналогичный результат получен в теореме 5 для почти всех частичных функций. С другой стороны, установлено (теорема 2) существование функций от n переменных, среднее время вычисления которых по порядку в $(2^n/n)^{1/2}$ раз меньше времени, необходимого для вычисления обычными неветвящимися программами. Наконец, показано (теорема 4), что среди всех функций от n переменных, принимающих значение 1 на n^c наборах, среднее время вычисления почти всех функций почти в n раз меньше максимального времени.

1. Основные определения

Пусть $B' = \{f : \{0,1\}^2 \to \{0,1\}\}$ — множество всех одноместных и двуместных булевых функций, $\pi : \{0,1\}^2 \to \{0,1\}^2$ — тождественный двуместный булев оператор, $X = \{x_1, \dots, x_n\}$ — множество булевых переменных и $B = B' \cup \pi$. *Неветвящейся программой* с условной остановкой назовем последовательность $P = p_1 p_2 \dots p_s$, элементами которой являются операторы $p_i = f_i(p_{i,1}, p_{i,2})$, где $f_i \in B$, $p_{i,1} = p_k$, $p_{i,2} = p_l$, $f_k, f_l \in B' \cup X$ и $k, l < i$. Оператор p_i назовем *оператором первого типа*, или функциональным оператором, если $f_i \in B'$. Оператор p_i назовем *оператором второго типа*, или оператором остановки, если $f_i = \pi$. *Сложностью* $L(P)$ программы P назовем число операторов, входящих в P. Положим $n(p_i) = i$, т. е. $n(p)$ является номером оператора p в программе P. Для функциональных операторов программы P индуктивно определим их значения на произвольном наборе x. Для первого оператора положим $p_1(x) = f_1(x)$, а при любом $i > 1$ положим $p_i(x) = f_i(p_{i,1}(x), p_{i,2}(x))$. Пусть программа P содержит ровно k операторов второго типа. Через q_i обозначим i-й оператор второго типа программы P, а через $q_{i,1}$, $q_{i,2}$ — первый и второй аргументы этого оператора, т. е. операторы $p_{n(q_i),1}$ и $p_{n(q_i),2}$. Результат работы программы P на входном наборе x обозначим через $P(x)$ и определим следующим образом:

$$P(x) = q_{1,1}(x)q_{1,2}(x) \vee \overline{q}_{1,1}(x)(q_{2,1}(x)q_{2,2}(x) \vee \ldots \\ \vee \overline{q}_{k-1,1}(x)(q_{k,1}(x)q_{k,2}(x) \vee \overline{q}_{k,1}(x)p_{L(P)}(x)) \ldots).$$

Пусть программа P работает на входном наборе x. Временем $T_P(x)$ работы P на x назовем минимальное $n(q_j)$, для которого $q_{j,1} = 1$. Легко видеть, что $P(x)$ не зависит от операторов с номерами, большими $n(q_j)$. Поэтому можно говорить, что после вычисления $n(q_j)$ программа P прекращает работу и $T_P(x)$ равно числу операторов, выполненных до остановки программы. Средним временем работы программы P назовем величину $T(P) = 2^{-n} \sum T_P(x)$, где суммирование осуществляется по всем двоичным наборам длины n. Если для некоторой булевой функции f и произвольного набора переменных x справедливо равенство $P(x) = f(x)$, то будем говорить, что программа P реализует (или вычисляет) функцию f. *Сложностью* $L(f)$ функции f назовем сложность самой простой программы, реализующей f. *Средним временем* реализации (или вычисления) функции f назовем величину $T(f) = \min T(P)$, где минимум берется по всем программам, реализующим функцию f. Пусть A — некоторое подмножество множества булевых функций. Величину $T_A(n) = \max T(f)$, где максимум берется по всем функциям из A, зависящим от n переменных, назовем функцией Шеннона на множестве A. Если A — множество всех булевых функций, то индекс A будем опускать.

Легко показать, что программы, состоящие только из операторов первого типа, изоморфны схемам из функциональных элементов. Поэтому все результаты, полученные для верхних оценок сложности схем из функциональных элементов, справедливы и для рассматриваемых программ. Более того, используя указанный изоморфизм в качестве отправной точки, легко получить ряд результатов, не являющихся прямым следствием этого изоморфизма.

Ниже предполагается, что число переменных рассматриваемых булевых функций достаточно велико. Через c и c_i, $i = 1, 2, \ldots$, обозначаются подходящие константы, а $\log$ обозначает логарифм по основанию 2.

2. Произвольные булевы функции

Обозначим через $N(L_1, L_2, n)$ число различных программ, реализующих булевы функции от n переменных, в каждой из которых содержится не более L_1 операторов первого типа и не более L_2 операторов второго типа. Далее, пусть $N(L, n)$ обозначает число различных схем из функциональных элементов, каждая из которых содержит не более L элементов, реализует булеву функцию от n переменных и построена над базисом, состоящим из всех двуместных функций.

Лемма 1. *При любых L_1, L_2 и n справедливо неравенство*

$$N(L_1, L_2, n) \leqslant N(L_1 + 3L_2, n).$$

Доказательство. Для доказательства леммы достаточно промоделировать программу схемой из функциональных элементов. Покажем, что это можно сделать так, что каждому оператору первого типа будет соответствовать один элемент, а каждому оператору второго типа — три элемента схемы.

Пусть $P = (p_1, \ldots, p_m)$ — программа, вычисляющая булеву функцию $f(x_1, \ldots, x_n)$. Эту программу разобьем на r подпрограмм $P_i = (p_{l_{i-1}+1}, \ldots, p_{l_i})$, $1 \leqslant i \leqslant r$, так, что последняя подпрограмма P_r будет содержать операторы только первого типа, а все остальные подпрограммы будут содержать ровно по одному оператору второго типа, причем этим оператором будет оператор $p_{l_i} = q_i$ — последний оператор каждой подпрограммы. Пусть работу операторов первого типа подпрограммы P_i моделирует схема S_i. При любом i, $1 \leqslant i \leqslant r-1$, схема S_i имеет два выхода — выходы элементов, соответствующих операторам $q_{i,1}$ и $q_{i,2}$, а схема S_r содержит один выход — выход элемента, соответствующего оператору $p_{l_r} = p_{L(P)}$. Построение схем S_i не представляет трудности вследствие упомянутого выше изоморфизма между программами, состоящими из операторов только первого типа, и схемами из функциональных элементов. Пусть S_{r+1} — схема, реализующая функцию

$$h = x_1 y_1 \vee \overline{y}_1 (x_2 y_2 \vee \ldots (x_{r-1} y_{r-1} \vee \overline{y}_{r-1} x_r) \ldots).$$

Присоединяя к входам схемы S_{r+1} выходы схем S_i, $1 \leqslant i \leqslant r$, получим схему, реализующую функцию $f(x_1, \ldots, x_n)$. Очевидно, что в базисе из всех двуместных булевых функций сложность схемы S_{r+1} не превосходит $3(r-1)$. Таким образом, описано моделирование программы P схемой из функциональных элементов, когда каждому оператору первого типа соответствует один элемент, а каждому оператору второго типа — три элемента схемы. Лемма 1 доказана.

Лемма 2 [2]. *При любых L и n справедливо неравенство*

$$N(L,n) \leqslant (c_1(L+n))^{L+n+2}.$$

Из лемм 1 и 2 следует

Лемма 3. *При любых L_1, L_2 и n справедливо неравенство*

$$N(L_1,L_2,n) \leqslant (c_1(L_1+3L_2+n))^{L_1+3L_2+n+2}.$$

Пусть f — произвольная булева функция от n переменных, P — программа, реализующая функцию f. Каждому булеву набору x длины n, рассматриваемому как двоичная запись натурального числа, поставим в соответствие его номер $N_P(x)$ такой, что $1 \leqslant N_P(x) \leqslant 2^n$; $N_P(x) < N_P(y)$, если $T_P(x) < T_P(y)$; $N_P(x) < N_P(y)$, если $T_P(x) = T_P(y)$ и $x < y$.

Теорема 1. *Существуют константы c_2 и c_3 такие, что*

$$c_2\frac{2^n}{n} \leqslant T(n) \leqslant c_3\frac{2^n}{n}.$$

Доказательство. Верхняя оценка для $T(n)$ следует из верхней оценки для схем из функциональных элементов [2]. Нижнюю оценку докажем методом от противного. Пусть f — произвольная булева функция от n переменных. Тогда по предположению справедливо неравенство

$$T(f) \leqslant \frac{c_4 2^n}{n}, \qquad (1)$$

где c_4 — достаточно малая константа, которая будет указана позднее. Пусть P — программа, которая вычисляет f и для которой справедливо (1). Пусть x_0 такой, что $N_P(x_0) = 2^{n-1}$. Очевидно, что

$$T_P(x_0) < \frac{c_4 2^{n+1}}{n}, \qquad (2)$$

так как иначе

$$T_P(f) \geqslant \frac{1}{2^n} \sum_{x \mid N_P(x) \geqslant 2^{n-1}} T_P(x) > \frac{c_4 2^n}{n}.$$

Теперь оценим сверху число функций, для которых справедливо (1). Для этого покажем, как, используя программу P, однозначно определить любую такую функцию f. Пусть P' — начальная подпрограмма программы P, достаточная для вычисления значений f на наборах с номерами, не превосходящими 2^{n-1}. Очевидно, что P' определяет значения функции f на всех таких наборах. Так как остальные наборы однозначно определяются по P' и к тому же перенумерованы, то для окончательного определения f достаточно указать двоичный вектор длины 2^{n-1}, состоящий из значений функции f на этих наборах. Оценим сверху величину M, равную числу различных подпрограмм P'. Так как, начиная с некоторого n, справедливо неравенство $T_P(x_0) > n + 2$, то в силу леммы 3 и (2) имеем

$$M \leqslant (4c_1 T_P(x_0))^{4T_P(x_0)} \leqslant (4c_1 c_4 n^{-1} 2^{n+1})^{4c_4 n^{-1} 2^{n+1}} \leqslant 2^{c_4 c_5 2^n}.$$

Поэтому общее число функций, для которых справедливо неравенство (1), не превосходит величины $2^{c_4c_5 2^n} 2^{2^{n-1}}$. Взяв $c_4 < 1/(2c_5)$, получаем $2^{c_4c_5 2^n} 2^{2^{n-1}} < 2^{2^n}$. Это означает, что существует функция f, для которой не выполняется (1). Теорема 1 доказана.

Выясним, насколько сильно могут различаться среднее время вычисления конкретной булевой функции и ее сложность, т. е. время вычисления обычной неветвящейся программой. Пусть

$$m(n) = \max(L(f)/T(f)),$$

где максимум берется по всем булевым функциям от n переменных.

Теорема 2. *Существуют константы c_6 и c_7 такие, что*

$$c_6(2^n/n)^{1/2} \leqslant m(n) \leqslant c_7(2^n/n)^{1/2}.$$

Доказательство. Пусть $k = \lceil (n + \log n)/2 \rceil$ и g — самая сложная булева функция от k переменных, т. е. $L(g) = \Theta(2^n/n)^{1/2}$. Рассмотрим функцию $f(x_1, \ldots, x_n) = x_{k+1} \& \cdots \& x_n \& g(x_1, \ldots, x_k)$. Нетрудно видеть, что $L(f) = \Theta(2^n/n)^{1/2}$ и $T(f) = O(1)$. Следовательно, $m(n) \geqslant c_6(2^n/n)^{1/2}$.

Теперь покажем, что $m(n) \leqslant c_7(2^n/n)^{1/2}$. Пусть f — произвольная булева функция от n переменных, P — программа, которая вычисляет f, и среднее время ее работы минимально.

Положим $k = \lfloor (n + \log n)/2 \rfloor$. Рассмотрим набор x такой, что $N_P(x) = 2^n - 2^k$. Легко видеть, что

$$2^{k-n} T_P(x) < T(f). \tag{3}$$

Далее, пусть $\tilde{f}$ — частичная булева функция, определенная на всех таких наборах y_i, что $N_P(y_i) > N_P(x)$, и совпадающая на этих наборах с f. Так как $2^k = \Theta(2^n n)^{1/2}$, то из [1, 3] следует существование схемы S, реализующей $\tilde{f}$ и такой, что

$$|S| = O(2^n/n)^{1/2}. \tag{4}$$

Теперь опишем программу P', вычисляющую функцию f. Сначала воспользуемся программой P, которая за минимальное среднее время вычисляет f. С ее помощью будем вычислять значения функции f на наборах y таких, что $N_P(y) \leqslant N_P(x)$. Так как $2^{n-k} = O(2^n/n)^{1/2}$, то из (3) следует, что для вычисления функции f на этих наборах потребуется привлекать не более H_1 операторов, где

$$H_1 = O(2^n/n)^{1/2}T(f). \tag{5}$$

Для вычисления функции f на оставшихся наборах воспользуемся схемой, реализующей функцию $\tilde{f}$. Очевидно, что программа, моделирующая схему S, содержит не более H_2 операторов, где

$$H_2 = O(2^n/n)^{1/2}, \tag{6}$$

что следует из (4).

Таким образом, из (5) и (6) следует, что сложность $L(P')$ программы P' по порядку не превосходит величины

$$(2^n/n)^{1/2}T(f) + (2^n/n)^{1/2} \leqslant 2(2^n/n)^{1/2}T(f).$$

Так как $L(f) \leqslant L(P')$, то найдется константа c_7 такая, что

$$L(f)/T(f) \leqslant c_7(2^n/n)^{1/2}.$$

Теорема 2 доказана.

Теорема 3. *Для любой булевой функции f найдется вычисляющая ее программа P такая, что*

$$c_8T(f)L(f) \leqslant T(P)L(P) \leqslant c_9T(f)L(f).$$

Доказательство. Пусть P — программа, вычисляющая функцию f за минимальное среднее время. Пусть x — набор с минимальным номером такой, что $T_P(x) \geqslant 2L(f)$ (если такого набора нет, то утверждение теоремы тривиально, так как тогда $T(f) = T(P) \leqslant L(P) \leqslant 2L(f)$). Ясно, что $T_P(x) \leqslant 3L(f)$, поскольку невыполнение этого неравенства влечет существование в программе P расположенных друг за другом $L(f)+1$ операторов первого типа, что противоречит минимальности программы P. Среднее время работы программы P можно представить следующим образом:

$$\begin{aligned} T(P) = 2^{-n}\Big(\sum_{N_P(y)<N_P(x)} T_P(y) + \sum_{N_P(y)\geqslant N_P(x)} T_P(y)\Big) \\ = T_1 + T_2 \geqslant T_1 + 2L(f)(2^n - N_P(x)+1)2^{-n}. \end{aligned}$$

Преобразуем программу P, заменив операторы с номерами большими $T_P(x)$ программой, моделирующей минимальную схему. Для сложности и среднего времени работы новой программы P' справедливы следующие неравенства:

$$L(P') \leqslant T_P(x) + L(f) \leqslant 4L(f),$$

$$\begin{aligned} T(P') &\leqslant 2^{-n}\Big(\sum_{N_P(y)<N_P(x)} T_{P'}(y) + \sum_{N_P(y)\geqslant N_P(x)} T'_P(y)\Big) \\ &= T'_1 + T'_2 \leqslant T'_1 + 4L(f)(2^n - N_P(x) + 1)2^{-n} \\ &\leqslant 2T'_1 + 4L(f)(2^n - N_P(x) + 1)2^{-n}. \end{aligned}$$

Так как $T'_1 = T_1$, то $T(P') \leqslant 2T(P)$. Теорема 3 доказана.

3. Функции с малым числом единиц

Далее рассматриваются булевы функции от n переменных, принимающие значения 1 не более чем на n^c наборах, где $c \geqslant 3$. Пусть

$$T_c(n) = \max T(f),$$

где максимум берется по всем булевым функциям от n переменных, каждая из которых принимает значения 1 ровно на n^c наборах (полагаем, что n^c целое). При реализации таких функций схемами из функциональных элементов функция Шеннона $L_c(n)$ согласно [2] удовлетворяет соотношению

$$L_c(n) = \Theta\left(\frac{n^{c+1}}{\log n}\right). \qquad (7)$$

В доказанной ниже теореме 4 устанавливается порядок функции $T_c(n)$. Сравнение (7) и теоремы 4 показывает, что при вычислении значений некоторых функций из рассматриваемого класса среднее и максимальное время могут различаться по порядку в n раз.

Лемма 4. *Пусть $D_1 \subset D_2 \subset \{0,1\}^n$ и $m = \lfloor \log|D_2| + 2 \rfloor$. Тогда существует линейный оператор $F : D_2 \to \{0,1\}^m$ такой, что*

$$|\{(x,y)|x \in D_1, y \in D_2 \setminus D_1, F(x) = F(y)\} \leqslant |D_1|/2.$$

Доказательство. Обозначим через $F(n,m)$ множество всех линейных операторов $F : \{0,1\}^n \to \{0,1\}^m$. Очевидно, что $F(n,m) = 2^{nm}$. Нетрудно видеть, что для любых различных наборов x, y из $\{0,1\}^n$ имеется 2^{n-1} линейных функций f таких, что $f(x) = f(y)$. Поэтому в $F(n,m)$ имеется 2^{nm-m} различных операторов F таких, что $F(x) = F(y)$. Из этого факта следует, что величина

$$2^{-nm} \sum_{x\in D_1, y\in D_2\setminus D_1} 2^{nm-m} = 2^{-m}|D_1||D_2 \setminus D_1|$$

является средним значением для числа таких пар (x, y), на которых значения оператора из $F(n, m)$ одинаковы. Следовательно, в $F(n, m)$ имеется оператор F такой, что $F(x) = F(y)$ не более чем на

$$2^{-m}|D_1||D_2 \setminus D_1| < \frac{1}{2|D_2|}|D_1||D_2 \setminus D_1| < \frac{1}{2}|D_1|$$

парах (x, y), $x \in D_1$, $y \in D_2 \setminus D_1$. Лемма 4 доказана.

Весом $w(f)$ функции $f : D \to \{0,1\}$ назовем число наборов в D, на которых f равна 1.

Лемма 5. *Пусть $c \geqslant 2$, $D \subset \{0,1\}^n$, $|D| \geqslant 10n^c$, а функция $f : D \to \{0,1\}$ такова, что $n^c \leqslant w(f) \leqslant \frac{1}{10}|D|$. Тогда существует функция $g : D \to \{0,1\}$ такая, что*

(a) $g \geqslant f$;

(b) $w(g) \leqslant \frac{3}{2}w(f)$;

(c) $L(g) \leqslant \frac{\log\binom{4|D|}{w(g)}}{\log\log\binom{4|D|}{w(g)}}(1 + o(1))$.

Доказательство. Положим $D_2 = D$ и $D_1 = \{x \in D_2 \mid f(x) = 1\}$. Пусть F — линейный оператор из леммы 4. Введем функцию $g' : \{0,1\}^m \to \{0,1\}$ такую, что $g'(x) = \max f(y)$, где максимум берется по всем $y \in D_2$, для которых $x = F(y)$, и функцию $g : D \to \{0,1\}$ такую, что $g(x) = \max f(y)$, где максимум берется по всем $y \in D_2$ таким, что $F(x) = F(y)$. Очевидно, что $g(x) = g'(F(x))$ и $g \geqslant f$, т. е. справедливы (a) и (b). Поэтому $L(g) \geqslant L(g') + L(F)$. В силу известного результата О. Б. Лупанова [2] о сложности реализации функций с малым числом единиц схемами из функциональных элементов имеем

$$L(g') \leqslant \frac{\log\binom{4|D|}{w(g)}}{\log\log\binom{4|D|}{w(g)}}(1 + o(1))$$

и, кроме того, $L(F) \leqslant O\left(\frac{n\log|D_2|}{\log n}\right)$. Отсюда следует, что если $n^c \leqslant w(f) \leqslant \frac{1}{10}|D|$, где $c \geqslant 2$, то справедливо (c).

Из определения функции g следует, что

$$w(g) = \sum_{x\in D_2} \max_{F(x)=F(y)} f(y) = \sum_{x\in D_1} f(x) + \sum_{x\in D_2\setminus D_1} \max_{F(x)=F(y)} f(y)$$
$$\leqslant w(f) + |\{(x, y) | x \in D_1, y \in D_2 \setminus D_1, F(x) = F(y)\}| \leqslant \frac{3}{2}|D_1|.$$

Лемма 5 доказана.

Лемма 6. *Пусть $c \geqslant 3$ и $D \geqslant 10n^c$. Тогда для любой функции $f : D \to \{0,1\}$ такой, что $n^c \leqslant w(f) < |D|/10$, справедливо неравенство*

$$L(f) \leqslant \frac{4\log\binom{4|D|}{\lfloor 3w(f)/2\rfloor}}{\log\log\binom{4|D|}{\lfloor 3w(f)/2\rfloor}}(1+o(1)).$$

Доказательство. Пусть f_1 — функция из леммы 5. Тогда имеем

$$w(f_1) \leqslant \frac{3}{2}w(f), \tag{8}$$

$$f_1 \geqslant f, \tag{9}$$

$$L(f_1) \leqslant \frac{\log\binom{4|D|}{w(f_1)}}{\log\log\binom{4|D|}{w(f_1)}}(1+o(1)). \tag{10}$$

Из (8) и (9) следует, что

$$w(f \oplus f_1) \leqslant \frac{1}{2}w(f). \tag{11}$$

Если $w(f \oplus f_1) > n^{c-1}$, то, применяя к функции $f \oplus f_1$ лемму 5, получим новую функцию f_2 такую, что

$$f_2 \geqslant f \oplus f_1, \tag{12}$$

$$w(f_2) \leqslant \frac{3}{2}w(f \oplus f_1), \tag{13}$$

$$L(f_2) \leqslant \frac{\log\binom{4|D|}{w(f_2)}}{\log\log\binom{4|D|}{w(f_2)}}(1+o(1)). \tag{14}$$

Из (12), (13) и (11) следует, что

$$w(f \oplus f_1 \oplus f_2) \leqslant \frac{1}{2}w(f \oplus f_1) \leqslant \frac{1}{4}w(f).$$

Используя (13) и (11), получаем

$$w(f_2) \leqslant \frac{3}{2}w(f \oplus f_1) \leqslant \frac{3}{4}w(f).$$

Повторим эту процедуру s раз. В результате получим последовательность функций f_i, $2 \leqslant i \leqslant s$, такую, что

$$f_i \geqslant f \oplus \left(\bigoplus_{j=1}^{i-1} f_j\right), \tag{15}$$

$$w(f_i) \leqslant \frac{3}{2}w\left(f \oplus \left(\bigoplus_{j=1}^{i-1} f_j\right)\right), \tag{16}$$

а при $w(f_i) > n^{c-1}$

$$L(f_i) \leqslant \frac{\log \binom{4|D|}{w(f_i)}}{\log\log \binom{4|D|}{w(f_i)}}(1 + o(1)). \tag{17}$$

Из (15) и (16) имеем

$$w\left(f \oplus \left(\bigoplus_{j=1}^{i} f_j\right)\right) \leqslant \frac{1}{2} w\left(f \oplus \left(\bigoplus_{j=1}^{i-1} f_j\right)\right). \tag{18}$$

Используя (18) и (16), индукцией по i легко получаем следующие неравенства:

$$w\left(f \oplus \left(\bigoplus_{j=1}^{i} f_j\right)\right) \leqslant \frac{1}{2} w\left(f \oplus \left(\bigoplus_{j=1}^{i-1} f_j\right)\right) \leqslant \frac{1}{2^i} w(f),$$

$$w(f_i) \leqslant \frac{3}{2} w\left(f \oplus \left(\bigoplus_{j=1}^{i-1} f_j\right)\right) \leqslant \frac{3}{2^i} w(f). \tag{19}$$

Параметр s выбирается таким, чтобы f_s оказалась первой функцией, для которой выполняется неравенство

$$w\left(f \oplus \left(\bigoplus_{i=1}^{s} f_i\right)\right) \leqslant w(f)/n.$$

Пользуясь (19), имеем $s < \log n + 2$.

Убедимся в том, что

$$L\left(f \oplus \left(\bigoplus_{i=1}^{s} f_i\right)\right) \leqslant \frac{w(f)}{\log w(f)}(1 + o(1)). \tag{20}$$

Действительно, в силу упомянутого выше результата О. Б. Лупанова справедливо неравенство

$$L\left(f \oplus \left(\bigoplus_{i=1}^{s} f_i\right)\right) \leqslant \frac{\log \binom{2^n}{\lfloor w(f)/n \rfloor}}{\log\log \binom{2^n}{\lfloor w(f)/n \rfloor}}(1 + o(1)). \tag{21}$$

Так как $w(f) \geqslant n^c$, где $c \geqslant 3$, то

$$\binom{2^n}{\lfloor w(f)/n \rfloor} \leqslant (3n2^n/w(f))^{w(f)/n} \leqslant 2^{w(f)}. \tag{22}$$

Подставляя (22) в (21), получаем (20). Вместе с тем при $w(f) < \frac{1}{10}|D| < 2^n$ справедливо неравенство

$$w(f) < \log \binom{4|D|}{w(f)}. \tag{23}$$

Положим
$$f \oplus \left(\bigoplus_{i=1}^{s} f_i \right) = f'.$$
Тогда имеем
$$f = f' \oplus \left(\bigoplus_{i=1}^{s} f_i \right)$$
и
$$L(f) \leqslant L(f') + \sum_{i=1}^{s} L(f_i) + s + 1. \tag{24}$$

Поскольку $w(f') \leqslant w(f)/n$, то согласно [2] получаем
$$L(f') < \log \binom{2^n}{\lfloor w(f)/n \rfloor} \Big/ \log\log \binom{2^n}{\lfloor w(f)/n \rfloor} (1 + o(1)) \leqslant (\text{см. } (21))$$
$$< \frac{w(f)}{\log w(f)} (1 + o(1)) \leqslant (\text{см. } (23)) < \log \binom{4|D|}{w(f)} \Big/ \log\log \binom{4|D|}{w(f)} (1 + o(1)). \tag{25}$$

Пользуясь (19), возрастанием функции $\varphi(x) = x/\log x$ при $x > e$, а также тем, что $i \leqslant s \leqslant \log n + 2$ и
$$L(f_i) \leqslant (1 + o(1)) \log \binom{4|D|}{w(f_i)} \Big/ \log\log \binom{4|D|}{w(f_i)},$$
получаем
$$L(f_i) \leqslant (1 + o(1)) \log \binom{4|D|}{\lfloor 3 \cdot 2^{-i} w(f) \rfloor} \Big/ \log\log \binom{4|D|}{\lfloor 3 \cdot 2^{-i} w(f) \rfloor}$$
$$< \frac{(1 + o(1)) \log (4|D| 2^i / w(f))^{3 \cdot 2^{-i} w(f)}}{\log\log (4|D| / w(f))^{3 \cdot 2^{-i} w(f)}}$$
$$= \frac{(1 + o(1)) 3 \cdot 2^{-i} w(f) \log (4|D| 2^i / w(f))}{\log (2^{-i} w(f))}. \tag{26}$$

Из (26) следует, что
$$\sum_{i=1}^{s} L(f_i) < 3(1 + o(1)) w(f) \sum_{i=1}^{s} \frac{2^{-i} \log (4|D| 2^i / w(f))}{\log (2^{-i} w(f))}$$
$$= 3(1 + o(1)) w(f) \left\{ \sum_{i=1}^{s} \frac{2^{-i} \log (4|D| / w(f))}{\log (2^{-i} w(f))} + \sum_{i=1}^{s} \frac{i\, 2^{-i}}{\log (2^{-i} w(f))} \right\}$$
$$= \frac{3(1 + o(1)) w(f) \log (4|D| / w(f))}{\log w(f)}$$
$$\leqslant 3(1 + o(1)) \log \binom{4|D|}{w(f)} \Big/ \log\log \binom{4|D|}{w(f)}. \tag{27}$$

Подставляя (25) и (27) в (24), убеждаемся в справедливости леммы 6.

Теорема 4. *Пусть $c > 3$ и n достаточно велико. Тогда существуют константы c_{10} и c_{11} такие, что*

$$c_{10}\frac{n^c}{\log n} \leqslant T_c(n) \leqslant c_{11}\frac{n^c}{\log n}.$$

Доказательство. Нижняя оценка. Предположим, что нижняя оценка теоремы неверна, т. е. при $c > 3$

$$T_c(n) = o\left(\frac{n^c}{\log n}\right).$$

Это означает, что для любой булевой функции f от n переменных, принимающей значение 1 на n^c наборах, при достаточно малой константе c_{12} справедливо неравенство

$$T(f) < c_{12}\frac{n^c}{\log n}. \tag{28}$$

Пусть P — программа, которая вычисляет функцию f и для которой справедлива оценка (28). Пусть P' — начальная подпрограмма программы P, достаточная для вычисления значений функции f на всех наборах с номерами, не превосходящими 2^{n-1}. Из леммы 3 и (28) следует, что число различных подпрограмм P' не больше чем $2^{c_{12}c_{13}n^c}$. Поэтому число рассматриваемых функций не превосходит величины

$$2^{c_{12}c_{13}n^c}\sum_{i=0}^{n^c}\binom{2^{n-1}}{i} < 2^{c_{12}c_{14}n^c}\binom{2^{n-1}}{n^c} < 2^{c_{12}c_{14}n^c-n^c}\binom{2^n}{n^c}.$$

Так как число булевых функций, которые принимают значение 1 на n^c наборах, равно $\binom{2^n}{n^c}$, то должно выполняться неравенство $2^{c_{12}c_{14}n^c-n^c} \geqslant 1$. Однако при $c_{12} < \frac{1}{2c_{14}}$ последнее неравенство нарушается. Противоречие. Следовательно, $T_c(n) > c_{10}n^c/\log n$.

Верхняя оценка. Пусть f — произвольная булева функция от n переменных, принимающая значение 1 на n^c наборах, $c \geqslant 3$, и D — область, состоящая из наборов, на которых f равна единице. В $\{0,1\}^n$ рассмотрим множество всех областей

$$M_1 = \{W_i \mid D \subset W_i, |W_i| = 25|D|\}$$

и частичные булевы функции $f_i : W_i \to \{0,1\}$ такие, что $f_i(x) = f(x)$ при $x \in W_i$, т. е. $f_i(x) = 1$ при $x \in D$ и $f_i(x) = 0$ при $x \in W\backslash D$.

В силу леммы 6 имеем

$$L(f_i) \leqslant \frac{4\log\binom{100|D|}{\lfloor 3w(f)/2\rfloor}}{\log\log\binom{100|D|}{\lfloor 3w(f)/2\rfloor}}(1+o(1)) < \frac{45n^c}{c\log n}. \tag{29}$$

Из леммы 2 и (29) следует, что имеется множество, состоящее не более чем из $\binom{100|D|}{\lfloor 3w(f)/2\rfloor}^{4(1+o(1))} = \binom{100|D|}{\lfloor 3|D|/2\rfloor}^{4(1+o(1))}$ схем сложности не более $4\log\binom{100|D|}{\lfloor 3|D|/2\rfloor}(1+o(1))$, и в этом множестве для каждой функции f_i найдется схема, реализующая эту функцию. Так как число различных функций f_i равно $\binom{2^n-|D|}{24|D|}$, то существует схема S_1, одновременно реализующая не менее $\binom{2^n-|D|}{24|D|}/\binom{100|D|}{\lfloor 3|D|/2\rfloor}^{4(1+o(1))}$ различных функций f_i, т. е. функция h_1, реализуемая схемой S_1, совпадает с f по крайней мере на $\binom{2^n-|D|}{24|D|}/\binom{100|D|}{\lfloor 3|D|/2\rfloor}^{4(1+o(1))}$ областях из M_1. Совокупность наборов, принадлежащих объединению этих областей и не входящих в D, обозначим через U_1 и положим $q_i = |U_1|$. Ясно, что $h_1(x) = 0$ при любом $x \in U_1$. Так как в U_1 содержится не менее $\binom{2^n-|D|}{24|D|}/\binom{100|D|}{\lfloor 3|D|/2\rfloor}^{4(1+o(1))}$ подмножеств мощности $24|D|$, то должно выполняться неравенство

$$\binom{2^n-|D|}{24|D|}\bigg/\binom{100|D|}{\lfloor 3|D|/2\rfloor}^{4(1+o(1))} \leqslant \binom{q_1}{24|D|},$$

т. е.

$$\frac{\binom{2^n-|D|}{24|D|}}{\binom{100|D|}{\lfloor 3|D|/2\rfloor}^{4(1+0(1))}\binom{q_1}{24|D|}} < 1. \tag{30}$$

Убедимся в том, что неравенство (30) может выполняться только при $q_1 > 2^{n-2}$. Действительно, при любом $q \leqslant 2^{n-2}$ имеем

$$\frac{\binom{2^n-|D|}{24|D|}}{\binom{100|D|}{\lfloor 3|D|/2\rfloor}^{4(1+o(1))}\binom{q_1}{24|D|}} > \frac{\binom{2^n-|D|}{24|D|}}{\binom{100|D|}{\lfloor 3|D|/2\rfloor}^{4(1+o(1))}\binom{2^{n-2}}{24|D|}}$$
$$> \frac{4^{24|D|}}{\binom{100|D|}{\lfloor 3|D|/2\rfloor}^{4(1+o(1))}} > 4^{24|D|}\left(\frac{\lfloor 3|D|/2\rfloor!}{(100|D|)^{\lfloor 3|D|/2\rfloor}}\right)^{4(1+o(1))}$$
$$> \left(\text{ибо } r! > \left(\frac{r}{e}\right)^r\right) > \frac{4^{24|D|}}{200^{6|D|(1+o(1))}} > 1,$$

что противоречит неравенству (30). Следовательно, $q_1 > 2^{n-2}$.

Обозначим через R_1 множество наборов из $\{0,1\}^n \setminus D$, на которых функция h_1 равна 1. Рассмотрим множество областей

$$M_2 = \{W_i \subset (R_i \cup D) \mid D \subset W_i,\ |W_i| = 25|D|\}$$

и частичные булевы функции $f_i : W_i \to \{0,1\}$ такие, что $f_i(x) = f(x)$ при $x \in W_i$. Как и в предыдущем случае, убеждаемся в том, что найдется схема S_2, реализующая булеву функцию h_2, такая, что

(a) S_2 одновременно реализует не менее $\binom{R}{24|D|}/\binom{100|D|}{\lfloor 3|D|/2\rfloor}^{4(1+o(1))}$ различных функций f_i;

(b) совокупность наборов, которые принадлежат объединению этих областей, но не входят в D, не меньше $\frac{1}{4}|R_1|$;

(c) $L(h_2) < 45n^c/c\log n$.

Далее, множество наборов $x \in R_1$ таких, что $h_2(x) = 1$, обозначим через R_2. Если $|R_2| > 2^n/n$, то рассматривается множество областей

$$M_3 = \{W_i \subset (R_2 \cup D) \mid D \subset W_i,\ |W_i| = 25|D|\}$$

и частичные функции $f_i : W_i \to \{0,1\}$ такие, что $f_i(x) = f(x)$ при $x \in W_i$. Как и в первом случае, убеждаемся в существовании множества R_3 и функции h_3, обладающих свойствами (a)–(c).

Порождение областей $R_1, R_2, \ldots$ таких, что $R_1 \supset R_2 \supset \ldots$ и $|R_i| \leqslant \frac{3}{4}|R_{i-1}|$, продолжается до тех пор, пока впервые не возникнет такая область R_s, что $|R_s| < 2^n/n$. В результате появится последовательность функций $h_1, h_2, \ldots, h_{s-1}$ таких, что при любом i, $1 \leqslant i \leqslant s-1$, справедливо неравенство

$$L(h_i) < \frac{45n^c}{c\log n}. \tag{31}$$

Теперь опишем программу P, вычисляющую значение функции f на произвольном наборе y. Эта программа строится на основе схем из функциональных элементов, реализующих функции f и h_i, и работает следующим образом. Сначала вычисляется значение $h_1(y)$. Если $h_1(y) = 0$, то программа останавливается и полагается, что $f(y) = 0$. Если $h_1(y) = 1$, то вычисляется значение $h_2(y)$. Если $h_2(y) = 0$, то программа останавливается и полагается, что $f(y) = 0$. Если $h_2(y) = 1$, то вычисляется значение $h_3(y)$ и т. д. Если $h_{s-1}(y) = 1$, то $f(y)$ вычисляется программой, которая ставится в соответствие схеме из [1], предназначенной для реализации функции f с заданным числом единиц.

Оценим сверху среднее время работы программы P. Используя (31), получаем

$$T(P) \leqslant \frac{1}{2^n}\left(\sum_{i=1}^{s-1} L(h_i)2^n\left(\frac{3}{4}\right)^{i-1} + L(f)2^n n^{-1}\right) \leqslant O\left(\frac{n^c}{\log n}\right).$$

Теорема 4 доказана.

4. Частичные булевы функции

Ниже рассматриваются частичные булевы функции от n переменных, определенные в областях фиксированной мощности. Среднее время вычисления таких функций определяется так же, как и для полностью определенных булевых функций — осреднением по всем 2^n наборам.

Пусть $T(n, d) = \max T(f)$, где максимум берется по всем частичным булевым функциям от n переменных, определенных в областях мощности d.

Теорема 5. *Если* $d > n \log n$, *то*

$$c_{15}\frac{d}{\log d} \leqslant T(n, d) \leqslant c_{16}\frac{d}{\log d}.$$

Доказательство. Верхняя оценка следует из соответствующих результатов для схем из функциональных элементов [1, 3]. Докажем нижнюю оценку. Рассмотрим два случая:

1) $d \geqslant 2^{n-1}$;

2) $d < 2^{n-1}$.

Случай 1. Обозначим через D множество всех наборов $(x_1, \ldots, x_n)$ из $\{0, 1\}^n$, в которых $x_1 = 1$. Пусть $\tilde{f}(x_2, \ldots, x_n)$ такая полностью определенная функция, что

$$T(\tilde{f}) = T(n - 1).$$

В D рассмотрим функцию $f = \tilde{f}$. Для частичной функции f и любой программы P, вычисляющей эту функцию, справедливы неравенства

$$T(P) = 2^{-n}\Big(\sum_{x \in D} T_P(x) + \sum_{x \notin D} T_P(x)\Big) \geqslant \frac{1}{2}2^{-(n-1)}\sum_{x \in D} T_P(x)$$
$$\geqslant \frac{1}{2}T(\tilde{f}) = \frac{1}{2}T(n - 1).$$

Утверждение теоремы следует из теоремы 1.

Случай 2. Докажем теорему методом от противного. Пусть f — произвольная частичная булева функция от n переменных, определенная в области мощности d. Тогда должно выполняться неравенство

$$T(f) \leqslant \frac{c_{17}d}{\log d}, \tag{32}$$

где c_{17} — достаточно малая константа. Пусть P — программа, которая вычисляет функцию f и для которой справедлива оценка (32). Пусть P' — начальная подпрограмма программы P, достаточная для вычисления значений f на всех наборах с номерами, не превосходящими 2^{n-1}.

Из леммы 3 и (32) следует, что число таких подпрограмм P' не превосходит $2^{c_{17}c_{18}d}$. Теперь, используя P', оценим число булевых функций от n переменных, определенных в областях мощности d, для которых справедлива оценка (32). Нетрудно видеть, что число R таких функций удовлетворяет неравенству

$$R \leqslant 2^{c_{12}c_{17}d}\left(\sum_{i=0}^{d}\binom{2^{n-1}}{d-i}\binom{2^{n-1}}{i}2^i\right).$$

Так как

$$\frac{\binom{2^{n-1}}{i}2^i}{\binom{2^n}{i}} = \frac{2^{n-1}!(2^n-i)!2^i}{(2^{n-1}-i)!2^n!} = 2^i\prod_{j=0}^{i-1}\frac{2^{n-1}-j}{2^n-j} = \prod_{j=0}^{i-1}\frac{2^n-2j}{2^n-j} \leqslant 1,$$

то

$$\binom{2^{n-1}}{i}2^i \leqslant \binom{2^n}{i}.$$

Поэтому

$$\sum_{i=0}^{d}\binom{2^{n-1}}{d-i}\binom{2^{n-1}}{i}2^i \leqslant \sum_{i=0}^{d}\binom{2^{n-1}}{d-i}\binom{2^n}{i} = \binom{3\cdot 2^{n-1}}{d}.$$

Следовательно,

$$R \leqslant 2^{c_{12}c_{17}d}\binom{3\cdot 2^{n-1}}{d}. \tag{33}$$

Далее, число рассматриваемых частичных булевых функций равно $2^d\binom{2^n}{d}$. Положим

$$\varphi(n,d) = \binom{3\cdot 2^{n-1}}{d}\Big/\left(2^d\binom{2^n}{d}\right)$$

и убедимся в том, что при любом d, $1 \leqslant d \leqslant 2^{n-1}$, справедливо неравенство

$$\varphi(n,d) < \left(\frac{25}{27}\right)^d. \tag{34}$$

Действительно, пользуясь формулой Стирлинга, получаем

$$\varphi(n,d) = \frac{(3\cdot 2^{n-1})!(2^n-d)!}{(3\cdot 2^{n-1}-d)!2^n!2^d} < \frac{3^{3\cdot 2^{n-1}}2^{3(n-1)2^{n-1}}(2^n-d)^{2^n-d}}{(3\cdot 2^{n-1}-d)^{3\cdot 2^{n-1}-d}2^{n2^n}2^d}$$

$$= \frac{3^{3\cdot 2^{n-1}}2^{3(n-1)2^{n-1}}2^{n(2^n-d)}}{3^{3\cdot 2^{n-1}-d}2^{(n-1)(3\cdot 2^{n-1}-d)}2^{n2^n}2^d}\cdot\frac{\left(1-\frac{d}{2^n}\right)^{2^n-d}}{\left(1-\frac{d}{3\cdot 2^{n-1}}\right)^{3\cdot 2^{n-1}-d}}$$

$$= \left(\frac{3}{4}\right)^d\left(1-\frac{d}{2^n}\right)^{2^n-d}\Big/\left(1-\frac{d}{3\cdot 2^{n-1}}\right)^{3\cdot 2^{n-1}-d}$$

$$= \left(\left(3-\frac{d}{2^{n-1}}\right)\Big/\left(4-\frac{4d}{2^n}\right)\right)^d\left(\left(1-\frac{d}{2^n}\right)^2\Big/\left(1-\frac{d}{3\cdot 2^{n-1}}\right)^3\right)^{2^{n-1}}.$$

Ясно, что в интервале $[1, 2^{n-1}]$ выражение $\left(3 - \frac{d}{2^{n-1}}\right) / \left(4 - \frac{4d}{2^n}\right)$, как функция от d, возрастает и не превосходит 1, а выражение $\left(1 - \frac{d}{2^n}\right)^2 / \left(1 - \frac{d}{3 \cdot 2^{n-1}}\right)^3$ убывает. Поэтому справедливы следующие неравенства:

(a) если $d \in [1, 3 \cdot 2^{n-2}]$, то

$$\varphi(n,d) < \left(\left(3 - \frac{d}{2^{n-1}}\right) \Big/ \left(4 - \frac{4d}{2^n}\right)\right)^d < \left(\left(3 - \frac{3 \cdot 2^{n-3}}{2^{n-1}}\right) \Big/ \left(4 - \frac{4 \cdot 3 \cdot 2^{n-3}}{2^n}\right)\right)^d < \left(\frac{9}{10}\right)^d;$$

(b) если $d \in [3 \cdot 2^{n-3}, 2^{n-1}]$, то

$$\varphi(n,d) < \left(\left(1 - \frac{d}{2^n}\right) \Big/ \left(1 - \frac{d}{3 \cdot 2^{n-1}}\right)^3\right)^d < \left(\left(1 - \frac{3 \cdot 2^{n-3}}{2^n}\right) \Big/ \left(1 - \frac{3 \cdot 2^{n-3}}{3 \cdot 2^{n-1}}\right)^3\right)^d \leqslant \left(\frac{25}{27}\right)^d.$$

Таким образом, при любом d, $1 \leqslant d \leqslant 2^{n-1}$, справедливо неравенство (33).

Из (33) и (34) следует, что

$$\frac{R}{2^d \binom{2^n}{d}} < 2^{c_{12} c_{17} d} \left(\frac{25}{27}\right)^d.$$

Поэтому при достаточно малом c_{12} справедливо неравенство

$$R \Big/ \left(2^d \binom{2^n}{d}\right) < 1,$$

т. е. величина R меньше числа всех частичных булевых функций от n переменных, определенных в областях мощности d. Это означает, что сделанное предположение неверно. Теорема 5 доказана.

Автор выражает искреннюю благодарность О. Б. Лупанову и Ю. В. Таранникову, прочитавшим первоначальный вариант статьи и сделавшим ряд полезных замечаний.

ЛИТЕРАТУРА

1. **Андреев А. Е.** О сложности реализации частичных булевых функций схемами из функциональных элементов // Дискрет. математика. 1989. Т. 1, № 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. **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

Статья поступила
25 января 1997 г.