ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Июль—сентябрь 1997. Серия 1. Том 4, № 3, 49–68

УДК 519.7

О ВЫЧИСЛЕНИИ БУЛЕВЫХ ФУНКЦИЙ ВЕРОЯТНОСТНЫМИ ПРОГРАММАМИ*)

А. В. Чашкин

Изучается среднее время вычисления значений булевых функций неветвящимися программами, содержащими датчики случайных чисел. Рассматриваются как надежные программы, всегда вычисляющие истинное значение реализуемой функции, так и программы, вычисляющие искомые значения лишь с некоторой вероятностью. Показано, что в обоих случаях использование датчиков случайных чисел не приводит к заметному уменьшению среднего времени вычисления на значительной доле аргументов. Точнее, для любой булевой функции от n аргументов, имеющей схемную сложность L, найдется область, на которой отношение L к среднему времени вычисления надежными программами не превосходит n; при вычислении программами с вероятностью, отличной от единицы, это отношение может лишь незначительно превосходить n.

Введение

Для многих практически важных задач неизвестны хорошие алгоритмы, решающие эти задачи за полиномиальное (относительно размера входа) время. В то же время эти задачи могут быть решены достаточно быстро «в среднем», т. е. существуют алгоритмы, быстро решающие задачи для почти всех входных данных. Однако, как правило, для каждого алгоритма, решающего быстро «в среднем» одну из таких задач, можно найти входные данные, на которых этот алгоритм работает долго. Ранее неоднократно высказывалось мнение [2, 3, 6], что вероятностные алгоритмы, т. е. алгоритмы, использующие в процессе работы датчики случайных чисел, лишены этого недостатка. Это мнение обосновывалось тем, что время работы алгоритма усредняется не только по входным данным, но и по величинам, полученным с помощью датчиков случайных чисел.

В настоящей работе предложена модель для изучения того, как сильно может увеличиться скорость решения сложных задач при использовании датчиков случайных чисел. Изучается реализация булевых функций

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

неветвящимися вероятностными программами, обладающими возможностью условной остановки. Исследуемые программы являются последовательностями операторов трех типов.

Каждый оператор нулевого типа с равными вероятностями порождает либо 0, либо 1. Действие каждого оператора первого типа заключается в вычислении значения некоторой двуместной булевой функции, аргументами которой могут быть либо величины, полученные в результате выполнения предыдущих операторов, либо значения независимых переменных. Операторы второго типа могут прекращать выполнение программы. Результат работы оператора второго типа определяется значениями, вычисленными программой на некоторых двух предыдущих шагах. Номера этих шагов фиксированы для каждого конкретного оператора и могут быть различными для различных операторов. Оператор второго типа останавливает программу, объявляя ее результатом значение, полученное на втором шаге, если значение, полученное на первом шаге, равно единице. Если это значение равно нулю, выполняется следующий оператор.

Последним оператором каждой программы является оператор первого типа, и если выполнение этой программы на предыдущих шагах прервано не было, то результатом работы программы считается величина, полученная на последнем шаге. Функции, реализуемые такими программами, случайны. Поэтому говорить о том, что вероятностная программа вычисляет конкретную булеву функцию, можно только с некоторой вероятностью, которая далее называется *надежностью*. Если эта вероятность равна единице, то программа называется *надежной*.

В п. 1 настоящей работы даны основные определения и доказана эквивалентность двух моделей вероятностных вычислений. Первая модель — это введенные выше вероятностные программы, вторая — детерминированные программы с вероятностными переменными. Различия между моделями чисто формальные. Достоинство первой модели заключается в том, что она является естественным описанием реальных вероятностных вычислений. Вторая модель более удобна с вычислительной точки зрения.

В п. 2 изучается вычисление булевых функций надежными вероятностными программами. Для этих программ установлено, что имеются области, на которых среднее время работы любой такой программы по порядку меньше обычной схемной сложности не более чем в n раз, где n — число аргументов вычисляемой функции.

В п. 3 и 4 изучается вычисление булевых функций произвольными вероятностными программами. Для программ, надежность которых не меньше $3/4$, установлены результаты, аналогичные соответствующим результатам для надежных вероятностных программ. Нетрудно показать, что все результаты остаются справедливым для любой надежности, строго большей $1/2$.

Таким образом, использование датчиков случайных чисел не позволяет избежать недостатков, присущих детерминированным программам.

1. Основные определения и понятия

Дадим формальные определения используемых ниже понятий. Многие из них являются аналогами соответствующих понятий для детерминированных программ, введенных в [8].

Пусть $B' = \{f : \{0,1\}^2 \to \{0,1\}\}$ — множество всех булевых функций, зависящих не более чем от двух переменных, $\pi : \{0,1\}^2 \to \{0,1\}^2$ — тождественный двуместный булев оператор, ξ — случайная функция, принимающая значения 0 и 1 с равными вероятностями, т. е. $P(\xi = 1) = P(\xi = 0) = 1/2$. Через $X_n = \{x_1, \ldots, x_n\}$ обозначим множество независимых булевых переменных. Положим $B = B' \cup \{\pi\} \cup \{\xi\}$. *Неветвящейся вероятностной программой* с условной остановкой назовем последовательность $P = p_1 p_2 \ldots p_s$, элементами которой являются операторы $p_i = f_i(p_{i,1}, p_{i,2})$, где $f_i \in B$, а $p_{i,1}, p_{i,2} \in \{p_1, \ldots, p_{i-1}\} \cup X_n$, причем если $p_{i,1} = p_k$, $p_{i,2} = p_l$, то f_k и f_l принадлежат множеству $B' \cup \{\xi\} \cup X_n$. Оператор p_i назовем *оператором нулевого типа*, или *случайным оператором*, если $f_i = \xi$. 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 $f_i = \pi$. Программы, состоящие только из операторов первого и второго типов, назовем детерминированными.

Положим $n(p_i) = i$, т. е. $n(p)$ — номер оператора p в программе P. Пусть $p_{i_1}, \ldots, p_{i_m}$ — все случайные операторы из P, $i_1 < \cdots < i_m$. Через r_t будем обозначать t-й случайный оператор программы P, т. е. $r_t = p_{i_t}$. Пусть $p_{j_1}, \ldots, p_{j_k}$ — все операторы второго типа из P, $j_1 < \cdots < j_k$. Через q_t будем обозначать t-й оператор второго типа программы P, а через $q_{t,1}$, $q_{t,2}$ — первый и второй аргументы этого оператора, т. е. операторы $p_{n(q_t),1}$ и $p_{n(q_t),2}$.

Для случайных и функциональных операторов программы P определим их значения на произвольном двоичном наборе x. При любом x для каждого случайного оператора r_i положим $P(r_i(x) = 1) = P(r_i(x) = 0) = 1/2$, если программа не прекращает работу до выполнения $r_i(x)$. Для функциональных операторов значения на наборе x определим индуктивно. Для первого оператора положим $p_1(x) = f_1(x)$, а при $i > 1$ положим $p_i = f_i(p_{i,1}(x), p_{i,2}(x))$. Очевидно, что $p_i(x)$ — случайная величина. Пусть в программе P содержится ровно k операторов второго типа. Результат действия программы P на наборе переменных x обозначим через $P(x)$ и определим следующим образом:

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

где p_{end} — последний оператор программы P. Очевидно, что $P(x)$ — случайная величина.

Временем работы программы P на наборе x назовем минимальное $n(q_j)$ такое, что $q_{j,1}(x) = 1$, и обозначим через $t_P(x)$. Так как $q_{j,1}(x)$ — случайная величина, то $t_P(x)$ также является случайной величиной. Легко видеть, что $P(x)$ не зависит от операторов с номерами, большими $n(q_j)$. Поэтому можно говорить, что после выполнения $n(q_j)$ операторов программа P прекращает работу и $t_P(x)$ равно числу операторов, выполненных до остановки программы. *Средним временем работы программы P на наборе x* назовем величину

$$T_P(x) = M(t_P(x)),$$

где M — математическое ожидание. *Средним временем работы программы P на области D* назовем величину

$$T(P) = |D|^{-1} \sum_{x \in D} T_P(x).$$

Обозначение $T(P)$ подразумевает одно соглашение: предполагается, что фиксирована область D, ибо изменение области D может повлечь изменение $T(P)$.

Будем говорить, что вероятностная программа P вычисляет частичную булеву функцию $f : D \to \{0,1\}$ с надежностью $1-\varepsilon$, если для каждого $x \in D$ справедливо неравенство

$$P(P(x) \neq f(x)) \leqslant \varepsilon. \tag{1}$$

Сложностью $L(P)$ программы P назовем число операторов, входящих в P. Сложностью $L^{\varepsilon}(f)$ вычисления функции f назовем сложность самой простой программы, вычисляющей f с надежностью $1-\varepsilon$. Сложность $L^{\varepsilon}(f)$ определяет время работы в «худшем» случае. *Средним временем вычисления функции f с надежностью* $1-\varepsilon$ назовем величину $T^{\varepsilon}(f) = \min T(P)$, где минимум берется по всем программам, вычисляющим f с надежностью $1-\varepsilon$. Сложность самой простой схемы из функциональных элементов, реализующей функцию f в базисе из всех двуместных булевых функций, обозначим через $L(f)$. *Средним временем вычисления функции f* назовем величину $T(f) = \min T(P)$, где минимум берется по всем детерминированным программам, вычисляющим f.

Вероятностные программы, вычисляющие булевы функции с надежностью 1, будем называть *надежными*.

Пусть $P = p_1 \ldots p_i \ldots p_s$ — произвольная вероятностная программа. Представим P в виде

$$P = P_1 q_1 \ldots P_i q_i \ldots P_{t-1} q_{t-1} P_t, \tag{2}$$

где P_i — подпрограммы, состоящие только из операторов первого и нулевого типов, q_i — операторы второго типа. Представление (2) назовем *нормальным представлением программы* P.

Двоичный набор $y = (y_1, \ldots, y_k)$ назовем допустимым относительно вероятностной программы P и двоичного набора x, если в процессе вычисления $P(x)$ значение i-го оператора нулевого типа из программы P принимает значение y_i, $1 \leqslant i \leqslant k$, где k — число операторов нулевого типа, выполненных до остановки программы. Пусть D_x — множество всех наборов, допустимых относительно программы P и набора x. Очевидно, что D_x — префиксное множество, т. е. для любой упорядоченной пары $y, y' \in D_x$ набор y' не является началом набора y. Легко видеть, что элементы D_x можно рассматривать как значения случайной величины $\xi_{P(x)}$, порожденной программой P и набором x, причем

$$P(\xi_{P(x)} = y) = 2^{-l(y)}, \quad \sum_{y \in D_x} P(\xi_{P(x)} = y) = 1, \tag{3}$$

где $l(y)$ — длина набора y. Пусть программа P вычисляет булеву функцию $f : D \to \{0,1\}$ с надежностью $1 - \varepsilon$. Обозначим через $P(x,y)$ результат работы P на наборе x при условии, что $\xi_{P(x)} = y$. Так как при любых конкретных $x \in D$ и $y \in D_x$ величина $P(P(x) \neq f(x) \mid \xi_{P(x)} = y)$ равна либо нулю, либо единице, то

$$P(P(x) \neq f(x)) = \sum_{y \in D_x} P(P(x) \neq f(x) \mid \xi_{P(x)} = y) P(\xi_{P(x)} = y)$$

$$= \sum_{y \in D_x} (P(x,y) \oplus f(x)) 2^{-l(y)} \leqslant \varepsilon. \tag{4}$$

Обозначим через $T_P(x,y)$ время работы программы P на наборе x при условии, что $\xi_{P(x)} = y$. Тогда

$$T(P) = |D|^{-1} \sum_{x \in D, y \in D_x} T_P(x,y) P(\xi_{P(x)} = y) = |D|^{-1} \sum_{x \in D, y \in D_x} T_P(x,y) 2^{-l(y)}. \tag{5}$$

При различных $x \in D$ множества D_x состоят из наборов различной длины. Это создает определенные трудности при вычислении надежности и среднего времени работы вероятностных программ. Вводимые ниже понятия позволяют преодолеть эти трудности.

Пусть вероятностная программа P содержит ровно m случайных операторов. Введем множество новых независимых переменных $Y_m = \{y_1, \ldots, y_m\}$. Детерминированную программу P^* назовем *детерминированным вариантом* вероятностной программы P, если P^* получена из P заменой всех случайных операторов новыми переменными: i-й случайный оператор r_i программы P заменяется переменной y_i. Переменные из Y_m будем называть *вероятностными переменными*.

Пусть детерминированная программа P^* зависит от переменных $x_1, \ldots, x_n, y_1, \ldots, y_m$. Вероятностную программу P назовем *вероятностным вариантом* детерминированной программы P^*, если P получена из P^* заменой всех переменных $y_1, \ldots, y_m$ случайными операторами: i-я переменная y_i заменяется на случайный оператор r_i.

Пусть $D \subseteq \{0,1\}^n$ и P^* зависит от $n+m$ переменных. Будем говорить, что детерминированная программа P^* вычисляет булеву функцию $f : D \to \{0,1\}$ с надежностью $1-\varepsilon$, если справедливо неравенство

$$2^{-m} \sum_{y \in \{0,1\}^m} (P^*(x,y) \oplus f(x)) \leqslant \varepsilon,$$

где $x \in D$ и $y \in \{0,1\}^m$.

По аналогии с вероятностными программами для каждой детерминированной программы P^*, зависящей от переменных $x_1, \ldots, x_n, y_1, \ldots, y_m$, введем функции $T'_{P^*}(x)$ и $T'(P^*)$. Положим

$$T'_{P^*}(x) = 2^{-m} \sum_{y \in \{0,1\}^m} T_{P^*}(x,y), \quad T'(P^*) = |D|^{-1} \sum_{x \in D} T_{P^*}(x).$$

В дальнейшем введенные функции будем обозначать так же, как среднее время работы детерминированной программы на наборе переменных и среднее время работы детерминированной программы на области, т. е. будем опускать штрихи. Подобное совпадение не приведет к неоднозначности, так как всегда будет ясно, какую именно функцию вычисляет рассматриваемая программа.

Пусть вероятностная программа P вычисляет функцию $f : D \to \{0,1\}$ с надежностью $1-\varepsilon$. Тогда ее детерминированный вариант P^* вычисляет некоторую булеву функцию $h(x,y) : D' \to \{0,1\}$, где $D' = \bigcup\limits_{x \in D} (x \times D_x)$. Доопределим функцию h до функции $f^* : D \times \{0,1\}^m \to \{0,1\}$ следующим образом: $f^*(x,y) = h(x,y')$, если $y' \in D_x$, $y' \in \{0,1\}^k$, $y_i = y'_i$ при $1 \leqslant i \leqslant k$, т. е. если набор y' совпадает с началом набора y. Легко видеть, что на множестве $D \times \{0,1\}^m$ программа P^* вычисляет функцию f^*, т. е. имеет место равенство $P^*(x,y) = f^*(x,y)$.

Справедливо следующее

Утверждение 1. *Пусть $D \subseteq \{0,1\}^n$, вероятностная программа P содержит ровно m случайных операторов и вычисляет булеву функцию $f : D \to \{0,1\}$ с надежностью $1-\varepsilon$. Тогда ее детерминированный вариант P^* также вычисляет функцию f с надежностью $1-\varepsilon$ и для каждого $x \in D$ справедливы соотношения*:

(a) $2^{-m} \sum\limits_{y \in \{0,1\}^m} (P^*(x,y) \oplus f(x)) = \sum\limits_{y \in D_x} ((P^*(x,y) \oplus f(x))\, 2^{-l(y)})$;

(b) $T_P(x) = T_{P^*}(x)$;

(c) $T(P) = T(P^*)$.

Доказательство. Из (4) следует, что при любом $x \in D$ справедливо неравенство

$$\sum_{y \in D_x} (P^*(x,y) \oplus f(x)) 2^{-l(y)} = \sum_{y \in D_x} (P(x,y) \oplus f(x))\ 2^{-l(y)} \leqslant \varepsilon.$$

Так как для любого $y \in D_x$ существует ровно $2^{m-l(y)}$ наборов из $\{0,1\}^m$, начала которых совпадают с y, то

$$2^{-m} \sum_{y \in \{0,1\}^m} (P^*(x,y) \oplus f(x)) = 2^{-m} \sum_{y \in D_x} (P^*(x,y) \oplus f(x))\ 2^{m-l(y)}$$
$$= \sum_{y \in D_x} (P^*(x,y) \oplus f(x))\ 2^{-l(y)} \leqslant \epsilon.$$

Пункты (a) и (b) доказаны. Далее имеем

$$T_{P^*}(x) = 2^{-m} \sum_{y \in \{0,1\}^m} T_{P^*}(x,y) = 2^{-m} \sum_{y \in D_x} T_{P^*}(x,y) 2^{m-l(y)}$$
$$= \sum_{y \in D_x} T_P(x,y) 2^{-l(y)} = T_P(x).$$

Так как $T_P(x) = T_{P^*}(x)$, то $T(P) = T(P^*)$. Утверждение 1 доказано.

Утверждение 1 позволяет рассматривать произвольную вероятностную программу P как детерминированную программу с дополнительными вероятностными переменными. При этом можно считать, что вероятностные переменные независимы, а их значения не зависят ни от P, ни от входных данных. Следующее утверждение доказывается аналогично. Поэтому приведем его без доказательства.

Утверждение 2. *Пусть $D \subseteq \{0,1\}^n$, детерминированная программа P^* зависит от переменных $x_1, \ldots, x_n, y_1, \ldots, y_m$ и вычисляет булеву функцию $f : D \to \{0,1\}$ с надежностью $1 - \varepsilon$. Тогда ее вероятностный вариант P также вычисляет функцию f с надежностью $1 - \varepsilon$ и для каждого $x \in D$ справедливы соотношения:*

(a) $T_P(x) = T_{P^*}(x)$;

(b) $T(P) = T(P^*)$.

Утверждение 2 является в некотором смысле обратным к утверждению 1 и позволяет переносить результаты, полученные для детерминированных программ, на вероятностные программы.

Пусть вероятностная программа P содержит ровно m случайных операторов. Паре булевых наборов (x,y), где $x \in D \subseteq \{0,1\}^n$ — набор длины n, а y — набор длины m, поставим в соответствие ее номер $N_P(x,y)$ такой, что $1 \leqslant N_P(x,y) \leqslant |D|2^m$; $N_P(x,y) < N_P(x',y')$, если $T_{P^*}(x,y) < T_{P^*}(x',y')$; $N_P(x,y) < N_P(x',y')$, если $T_{P^*}(x,y) = T_{P^*}(x',y')$

и $xy < x'y'$, где наборы сравниваются как целые числа, двоичными представлениями которых они являются. Так как детерминированные программы являются частным случаем вероятностных программ при $m = 0$, то функция $N_P(x)$ определена также и для детерминированных программ.

Пусть $D' \subseteq D \subseteq \{0,1\}^n$. *Сужением функции* $h : D \to \{0,1\}$ на область D' называется функция $g : D' \to \{0,1\}$ такая, что при всех $x \in D'$ справедливо равенство $g(x) = h(x)$. Сужение функции f на область D будем обозначать через f_D.

Определения понятий, используемых ниже, можно найти в [5, 7]. Через c и c_i, $i = 1, 2, \ldots$, обозначаются подходящие константы. Всюду в этой статье log обозначает логарифм по основанию 2.

2. Надежные программы

При исследовании надежных программ основным результатом является теорема 2. В ней для всех достаточно сложных булевых функций устанавливается существование таких областей в $\{0,1\}^n$, что при вычислении значений функций в этих областях использование датчиков случайных чисел малоэффективно.

Теорема 1. *Пусть* $D \subseteq \{0,1\}^n$. *Тогда для любой функции* $f : D \to \{0,1\}$ *справедливо равенство*

$$T^0(f) = T(f).$$

Доказательство. Пусть $\widetilde{P}$ — вычисляющая функцию f надежная вероятностная программа, среднее время работы которой минимально, т. е. $T(\widetilde{P}) = T^0(f)$, $\widetilde{P}^*$ — детерминированный вариант программы $\widetilde{P}$, y_0 — набор вероятностных переменных, на котором среднее время работы программы $\widetilde{P}^*$ минимально среди всех наборов вероятностных переменных, т. е.

$$\sum_{x \in D} T_{\widetilde{P}^*}(x, y_0) = \min_{y \in \{0,1\}^m} \sum_{x \in D} T_{\widetilde{P}^*}(x, y).$$

Тогда

$$T(\widetilde{P}^*) = \frac{1}{|D|2^m} \sum_{x,y} T_{\widetilde{P}^*}(x, y_0) \geqslant \frac{1}{|D|} \sum_{x} T_{\widetilde{P}}(x, y_0).$$

Пусть P — детерминированная программа, полученная из $\widetilde{P}^*$ подстановкой вместо всех вероятностных переменных соответствующих им компонент набора y_0. Очевидно, что P вычисляет f и

$$T(f) \leqslant T(P) \leqslant \frac{1}{|D|} \sum_{x} T_{\widetilde{P}^*}(x, y_0) \leqslant T(\widetilde{P}^*) = T(\widetilde{P}) = T^0(f).$$

Так как детерминированная программа может считаться частным случаем вероятностной программы с нулевым числом операторов нулевого типа, то для любой функции f справедливо неравенство

$$T(f) \geqslant T^0(f).$$

Теорема 1 доказана.

Теорема 2. *Пусть функция* $f : \{0,1\}^n \to \{0,1\}$ *такая,что* $L(f) \geqslant n^2$, *и пусть* $q = \log(2^{n+4}/L(f)\log L(f))$. *Тогда найдется такая область* $D \subseteq \{0,1\}^n$, *что*

$$T^0(f_D) \geqslant \frac{c}{q} L(f).$$

Доказательство теоремы основано на теореме 1 и двух леммах. Перед доказательством теоремы сформулируем и докажем эти леммы.

Характеристическую функцию области $D \subseteq \{0,1\}^n$ будем обозначать через χ_D.

Лемма 1. *Пусть* $D \subseteq \{0,1\}^n$. *Тогда для любой* $f : D \to \{0,1\}$ *и любой константы* $c_1 > 1$ *существуют область* $D' \subseteq D$ *и функция* h *такие, что*

(a) $f_{D\setminus D'} = h_{D\setminus D'}$;

(b) $L(h, \chi_{D\setminus D'}) \leqslant 5c_1 T(f)$;

(c) $|D'| \leqslant |D|/c_1 + 1$.

Доказательство. Пусть P — детерминированная программа, реализующая f, на которой достигается минимальное среднее время, и пусть набор x_0 такой, что $N_P(x_0) = |D| - \lfloor |D|/c_1 \rfloor$. Тогда

$$T(f) \geqslant \frac{1}{|D|}\Bigg(\sum_{x | N_P(x) \geqslant N_P(x_0)} T_P(x)\Bigg) \geqslant \frac{1}{|D|}\left(\lfloor |D|/c_1 \rfloor + 1\right) T_P(x_0) \geqslant T_P(x_0)/c_1.$$

Следовательно,

$$T_P(x_0) \leqslant c_1 T(f).$$

Пусть $q_1, \ldots, q_k$ — операторы второго типа программы P, последний из которых останавливает работу этой программы на наборе x_0. Положим $D' = \{x \mid T_P(x) > T_P(x_0)\}$. Тогда $|D'| \leqslant |D|/c_1$, $\chi_{D'} = \bigwedge\limits_{t=1}^{k} \overline{q}_{i,1}$ и значения функции

$$h = q_{1,1}q_{1,2} \vee \overline{q}_{1,1}(q_{2,1}q_{2,2} \vee \cdots \vee \overline{q}_{k-2,1}(q_{k-1,1}q_{k-1,2} \vee \overline{q}_{k-1,1}q_{k,1}q_{k,2})\ldots)$$

совпадают на $D \setminus D'$ с соответствующими значениями f и равны нулю вне этой области. Очевидно, что

$$L(h, \chi_{D'}) \leqslant k + 3k + T_P(x_0) \leqslant 5c_1 T(f).$$

Лемма 1 доказана.

Лемма 2. *Пусть $D \subseteq \{0,1\}^n$. Тогда для любой функции $f : D \to \{0,1\}$ такой, что $L(f) \geqslant n^2$, существует такая область $D' \subseteq D$, что*

$$T(f_{D'}) \geqslant \frac{c_2 L(f)}{\log \dfrac{16|D|}{L(f)\log L(f)}}.$$

Доказательство. Докажем лемму методом от противного. Пусть c_3 — произвольная постоянная. Положим $T = c_3 L(f)/\log \frac{16|D|}{L(f)\log L(f)}$, $D_0 = D$. Предположим, что для любой области $D' \subseteq D_0$ справедливо неравенство

$$T(f_{D'}) < T.$$

Воспользуемся леммой 1, положив $c_1 = 2$. В силу этой леммы имеются область $D_1 \subseteq D_0$ и функция h^1 такие, что

$$f_{D_0 \setminus D_1} = h^1_{D_0 \setminus D_1}, \quad L(h^1, \chi_{D_1}) \leqslant 10T, \quad |D_1| \leqslant |D_0|/2 + 1.$$

Снова используем лемму 1, применив ее к функции f_{D_1}. В силу этой леммы существуют область $D_2 \subseteq D_1$ и функция h^2 такие, что

$$f_{D_1 \setminus D_2} = h^2_{D_1 \setminus D_2}, \quad L(h^2, \chi_{D_2}) \leqslant 10T, \quad |D_2| \leqslant |D_1|/2 + 1.$$

Повторим подобную процедуру еще $k-2$ раза. В результате для каждого i, $0 \leqslant i \leqslant k-1$, получим области D_{i+1}, $D_{i+1} \subseteq D_i$ и функции h^{i+1} такие, что

$$f_{D_i \setminus D_{i+1}} = h^{i+1}_{D_i \setminus D_{i+1}}, \tag{6}$$

$$L(h^{i+1}, \chi_{D_{i+1}}) \leqslant 10T, \tag{7}$$

$$|D_{i+1}| \leqslant |D_i|/2 + 1. \tag{8}$$

Из (6) следует, что

$$f_{D_i} = h^{i+1}_{D_i} \overline{\chi}_{D_{i+1}} \vee f_{D_{i+1}} \chi_{D_{i+1}}.$$

Поэтому

$$f = h^1 \overline{\chi}_{D_1} \vee \chi_{D_1}(h^2 \overline{\chi}_{D_2} \vee \ldots (h^k \overline{\chi}_{D_k} \vee \chi_{D_k} f_{D_k}) \ldots).$$

Следовательно, в силу (7) и последней формулы имеет место неравенство

$$L(f) \leqslant 13kT + L(f_{D_k}). \tag{9}$$

Оценим сверху мощность множества D_k. В силу неравенства (8) имеем

$$|D_k| \leqslant \frac{1}{2}|D_{k-1}| + 1 \leqslant \frac{1}{2}\left(\frac{1}{2}|D_{k-2}| + 1\right) + 1 \leqslant \ldots$$

$$\leqslant \frac{1}{2}\left(\frac{1}{2}\left(\ldots\left(\frac{1}{2}|D_0| + 1\right)\ldots\right)\right) + 1 \leqslant \frac{1}{2^k}|D_0| + 2.$$

Положим $k = \left\lceil \log \frac{4|D|}{L(f)\log L(f)} \right\rceil + 1$. Тогда

$$|D_k| \leqslant \frac{|D|}{2^k} + 2 \leqslant \frac{1}{8}L(f)\log L(f) + 2 < \frac{1}{4}L(f)\log L(f). \qquad (10)$$

Из [1, 9] для произвольной функции $f : D \to \{0,1\}$, где $|D| \geqslant n^{c_4}$ и $c_4 > 1$, легко извлекается неравенство

$$L(f) \leqslant \frac{2|D|}{\log |D|}.$$

Подставляя (10) в это неравенство, получаем

$$L(f_{D_k}) < \frac{1}{2}L(f).$$

Далее, подставляя полученную оценку в (9) и выражая T через $L(f)$ и $|D|$, получаем

$$L(f) < 13kT + \frac{1}{2}L(f) \leqslant \frac{13c_3L(f)}{\log \dfrac{16|D|}{L(f)\log L(f)}} \left(\log \frac{4|D|}{L(f)\log L(f)} + 2\right) + \frac{1}{2}L(f) \leqslant \left(13c_3 + \frac{1}{2}\right) L(f).$$

При $c_3 < 1/26$ приходим к противоречию. Таким образом, сделанное предположение неверно. Лемма 2 доказана.

Доказательство теоремы 2. Из леммы 2 следует, что для любой функции f найдется такая область D, что

$$T(f_D) \geqslant \frac{c_2}{q}L(f).$$

В силу теоремы 1 справедливо равенство

$$T^0(f_D) = T(f_D).$$

Используя последние два соотношения, получаем

$$T^0(f_D) \geqslant \frac{c_2}{q}L(f).$$

Теорема 2 доказана.

3. Вероятностные программы

Доказываемые ниже теоремы являются аналогами теорем 1 и 2 для программ, вычисляющих булевы функции с надежностью, меньшей единицы. Основным результатом этого пункта является теорема 4.

Теорема 3. *Для любой функции* $f : \{0,1\}^n \to \{0,1\}$ *такой, что* $T(f) \geqslant n^2$, *и любого* $\varepsilon \leqslant 1/4$ *справедливо неравенство*

$$T^{\varepsilon}(f) \geqslant \frac{T(f)}{(n - \log(T(f)/n))^2}.$$

Перед доказательством теоремы 3 докажем две необходимые леммы.

Лемма 3. *Пусть программа* P *вычисляет функцию* f *с надежностью* $1 - \varepsilon \geqslant 3/4$. *Тогда для любого натурального* $l \geqslant 3$ *существует такая программа* $\widetilde{P}$, *вычисляющая* f *с надежностью* $1 - (4\varepsilon(1-\varepsilon))^{l/2}$, *что*

$$T(\widetilde{P}) \leqslant c_5 l^2 T(P).$$

Доказательство. Пусть $P^* = P_1 q_1 P_2 q_2 \dots P_i q_i \dots P_s$ — нормальное представление программы P^*, являющейся детерминированным вариантом программы P. Напомним, что через $q_{i,1}$ обозначается первый аргумент оператора q_i, а через $q_{i,2}$ — второй аргумент этого оператора. Возьмем l экземпляров программы P^*. Через $P^j = P_1^j q_1^j \dots P_i^j q_i^j \dots P_s^j$ обозначим j-й экземпляр этой программы. Определим новую программу $\widetilde{P}$, состоящую из l «параллельно» работающих экземпляров программы P^*. Положим

$$\widetilde{P} = \widetilde{P}_1 \widetilde{P}'_1 \dots \widetilde{P}_i \widetilde{P}'_i \dots \widetilde{P}_s \widetilde{P}'_s,$$

где $\widetilde{P}_i = P_i^1 \dots P_i^l$, $\widetilde{P}'_i$ — подпрограмма, которая при всех j, $1 \leqslant j \leqslant l$,

(a) вычисляет функции

$$z_{i,1}^j = \bigvee_{k=1}^{i} q_{k,1}^j, \quad z_{i,2}^j = z_{i-1,2}^j \vee \overline{z}_{i-1,1}^j q_{i,1}^j q_{i,2}^j, \quad z_{1,2}^j = q_{1,1}^j q_{1,2}^j;$$

(b) останавливает вычисления, если $\bigwedge_{j=1}^{l} \left(\bigvee_{t=1}^{i} z_{t,1}^j \right) = 1$;

(c) объявляет результатом работы программы значение $M(z_{i,2}^1, \dots, z_{i,2}^l)$, где M — функция голосования.

При любых i и j функция $z_{i,1}^j$ равна единице только в том случае, когда ко времени вычисления этой функции j-й экземпляр программы P^* закончил вычисления. При этом значение функции $z_{i,2}^j$ равно значению, вычисленному этим экземпляром программы P^*. Равенство $\bigwedge_{j=1}^{l} \left(\bigvee_{t=1}^{i} z_{t,1}^j \right) = 1$ имеет место только в том случае, если все экземпляры программы P^* закончили вычисления. Легко видеть, что $L(\widetilde{P}'_i) = O(l)$. Следовательно,

$$L(\widetilde{P}) \leqslant c_5 L(P). \tag{11}$$

Оценим среднее время работы построенной программы на произвольном наборе x. Наборы вероятностных переменных y перенумеруем так, что $1 \leqslant N(y) \leqslant 2^m$; $N(y) < N(y')$, если $T_{P^*}(x,y) < T_{P^*}(x,y')$; $N(y) < N(y')$, если $T_{P^*}(x,y) = T_{P^*}(x,y')$ и $y < y'$, где наборы сравниваются как целые числа. Пусть T_k — время работы программы P^* на x и k-м вероятностном наборе, т. е. $T_k = T_{P^*}(x,y)$, где $N(y) = k$. Тогда

$$T_{P^*}(x) = \frac{1}{2^m}\sum_{k=1}^{2^m} T_k.$$

Пусть, далее, $y_1, \ldots, y_l$ — вероятностные наборы, являющиеся аргументами программы $\widetilde{P}$, причем набор $y_i \in \{0,1\}^m$ является аргументом i-го экземпляра программы P^*. Очевидно, что время работы программы $\widetilde{P}$ на наборах $y_1, \ldots, y_l$ определяется временем работы программы P^* на максимальном наборе y_i, т. е. таком, что $N(y_i) > N(y_j)$ при всех $j \neq i$. Нетрудно показать, что

$$T_{\widetilde{P}}(x, y_1, \ldots, y_l) \leqslant c_5 T_k,$$

где $k = \max_{1 \leqslant j \leqslant l} N(y_j)$. Так как набор с номером k будет максимальным ровно для $k^l - (k-1)^l$ наборов вероятностных переменных $y_1, \ldots, y_l$ и $(1-1/k)^l \geqslant 1 - l/k$ при $k \geqslant 1$, то

$$\begin{aligned} T_{\widetilde{P}}(x) &= \frac{c_5 l}{2^{ml}}\sum_{k=1}^{2^m} T_k(k^l - (k-1)^l) = \frac{c_5 l}{2^{ml}}\sum_{k=1}^{2^m} T_k k^l\left(1 - \left(1 - \frac{1}{k}\right)^l\right) \\ &\leqslant \frac{c_5 l}{2^{ml}}\sum_{k=1}^{2^m} T_k k^l\left(1 - \left(1 - \frac{l}{k}\right)\right) \leqslant \frac{c_5 l^2}{2^{ml}}\sum_{k=1}^{2^m} T_k k^{l-1} \\ &= \frac{c_5 l^2}{2^m}\sum_{k=1}^{2^m} T_k\left(\frac{k}{2^m}\right)^{l-1} \leqslant \frac{c_5 l^2}{2^m}\sum_{k=1}^{2^m} T_k = c_5 l^2 T_{P^*}(x). \end{aligned}$$

Следовательно, в силу последних неравенств и доказанного в п. 1 утверждения 1 получаем

$$T(\widetilde{P}) \leqslant c_5 l^2 T(P^*) = c_5 l^2 T(P).$$

Оценим надежность, с которой программа $\widetilde{P}$ вычисляет функцию f. Пусть $l = 2l' + 1$. Поскольку значение $\widetilde{P}(x)$ вычисляется голосованием среди значений l экземпляров программы P^*, при $\varepsilon \leqslant 1/4$ имеем

$$\begin{aligned} P(\widetilde{P}(x) \neq f(x)) &= \sum_{i=l'+1}^{l}\binom{l}{i}\varepsilon^i(1-\varepsilon)^{l-i} = (1-\varepsilon)^l\sum_{i=l'+1}^{l}\binom{l}{i}\varepsilon^i(1-\varepsilon)^{-i} \\ &\leqslant (1-\varepsilon)^l 2^{l-1}\sum_{i=l'+1}^{l}\varepsilon^i(1-\varepsilon)^{-i} \leqslant (1-\varepsilon)^l 2^{l-1}\frac{\varepsilon^{l'+1}(1-\varepsilon)^{-l'-1}}{1-2\varepsilon} \\ &\leqslant 2^l(\varepsilon(1-\varepsilon))^{l'+1} \leqslant (4\varepsilon(1-\varepsilon))^{l/2}. \end{aligned}$$

Лемма 3 доказана.

Лемма 4. *Пусть $D \subseteq \{0,1\}^n$, $f : D \to \{0,1\}$, вероятностная программа $\widetilde{P}$ вычисляет функцию f с надежностью $1-\varepsilon$ и средним временем T_ε. Тогда для любого a, $\varepsilon < a \leqslant 1/2$, найдутся функция $h : D \to \{0,1\}$ и вычисляющая эту функцию детерминированная программа P такие, что*

(a) $w(f \oplus h) \leqslant a|D|$;

(b) $T(P) \leqslant T_\varepsilon \dfrac{1}{1-\varepsilon/a}$.

Доказательство. Для детерминированного варианта $\widetilde{P}^*$ программы $\widetilde{P}$ и любого $x \in D$ справедливо неравенство

$$\sum_{y \in \{0,1\}^m} (\widetilde{P}^*(x,y) \oplus f(x)) \leqslant \varepsilon 2^m.$$

Следовательно,

$$\sum_{x \in D} \sum_{y \in \{0,1\}^m} (\widetilde{P}^*(x,y) \oplus f(x)) \leqslant \varepsilon 2^m |D|.$$

Для произвольного положительного a оценим число N, равное мощности множества $\widetilde{N}$, состоящего из всех таких наборов вероятностных переменных y, что имеет место неравенство

$$\sum_{x \in D} (\widetilde{P}^*(x,y) \oplus f(x)) > a|D|.$$

Легко видеть, что

$$aN|D| < \varepsilon |D| 2^m.$$

Поэтому

$$N < \varepsilon 2^m / a. \qquad (12)$$

Так как

$$T_\varepsilon = T(\widetilde{P}^*) = \frac{1}{|D|2^m} \sum_{x,y} T_{\widetilde{P}^*}(x,y) \geqslant \frac{1}{|D|2^m} \sum_{x,y \notin \widetilde{N}} T_{\widetilde{P}^*}(x,y),$$

то в силу (12) среди наборов вероятностных переменных, не принадлежащих множеству $\widetilde{N}$, найдется набор y_0 такой, что

$$\frac{1}{|D|} \sum_x T_{\widetilde{P}^*}(x,y_0) \leqslant \frac{1}{|D|(2^m - N)} \sum_{x,y \notin \widetilde{N}} T_{\widetilde{P}^*}(x,y)$$

$$\leqslant \frac{2^m}{|D|(2^m - N)2^m} \sum_{x,y} T_{\widetilde{P}^*}(x,y) \leqslant \frac{2^m}{(2^m - N)} T_\varepsilon \leqslant \frac{1}{1-\varepsilon/a} T_\varepsilon.$$

Пусть P — программа, полученная из $\widetilde{P}^*$ подстановкой компонент набора y_0 вместо всех соответствующих вероятностных переменных. Очевидно, что вычисляемая программой P функция h отличается от функции f не более чем на $a|D|$ наборах, а для среднего времени $T(P)$ работы программы P справедливо неравенство

$$T(P) \leqslant \frac{1}{1-\varepsilon/a} T_\varepsilon.$$

Лемма 4 доказана.

Доказательство теоремы 3. Пусть P — программа, вычисляющая f с надежностью $1-\varepsilon \geqslant 3/4$, на которой для данной надежности достигается минимальное среднее время работы, т. е. $T(P) = T^\varepsilon(f)$. Положим $l = \lfloor 6(n - \log(T(f)/n)) \rfloor$. Тогда имеем

$$\varepsilon_0 = (4\varepsilon(1-\varepsilon))^{l/2} \leqslant \left(\frac{3}{4}\right)^{l/2} \leqslant \left(\frac{1}{2}\right)^{l/6} \leqslant \frac{1}{n2^{n-1}} T(f).$$

Из леммы 3 следует существование такой программы P', которая вычисляет f с надежностью $1-\varepsilon_0 \geqslant 1 - T(f)/n2^{n-1}$ и

$$T(P') \leqslant c_6(n - \log(T(f)/n))^2 T(P).$$

В силу леммы 4 для функции f, программы P' и произвольной константы a существуют функция h и вычисляющая эту функцию детерминированная программа P'' такие, что

$$w(f \oplus h) \leqslant a2^n, \quad T(P'') \leqslant T(P') \frac{1}{1-\varepsilon_0/a}.$$

Положим $a = 2\varepsilon_0$. Тогда имеем

$$w(f \oplus h) \leqslant 4T(f)/n, \quad T(P'') \leqslant 2T(P'). \tag{13}$$

Из результата О. Б. Лупанова о сложности реализации булевых функций малого веса схемами из функциональных элементов [4] следует, что

$$L(f \oplus h) \leqslant T(f)/2. \tag{14}$$

Пусть $\widetilde{P} = P_1 P_2$ — программа, состоящая из программ P_1 и P_2, где P_1 моделирует минимальную схему, реализующую функцию $f \oplus h$, а P_2 вычисляет функцию h и складывает ее с величиной, вычисленной программой P_1. Программа P_2 может быть легко получена из программы P'' так, что $T(P_2) \leqslant 2T(P'')$. Для этого в каждую подпрограмму P_i из нормального представления P'' достаточно добавить по одному функциональному оператору, вычисляющему функцию $P_1(x) \oplus q_{i,2}(x)$, и объявить

этот оператор вторым аргументом оператора q_i. Так как $\widetilde{P}$ вычисляет f, то из (13), (14) и равенства $T(P) = T^{\varepsilon}(f)$ следует, что

$$\begin{aligned} T(f) &\leqslant L(P_1) + T(P_2) \leqslant T(f)/2 + 2T(P'') \\ &\leqslant T(f)/2 + 4T(P') \leqslant T(f)/2 + 4c_6(n - \log(T(f)/n))^2 T(P) \\ &\leqslant T(f)/2 + c_7(n - \log(T(f)/n))^2 T^{\varepsilon}(f). \end{aligned}$$

Поэтому справедливо неравенство

$$T(f) \leqslant 2c_7(n - \log(T(f)/n))^2 T^{\varepsilon}(f).$$

Теорема 3 доказана.

Положим $\log^{(k)} n = \underbrace{\log\log\ldots\log}_{k \text{ раз}} n$ и $\log^* n = k$, если $0 < \log^{(k)} n \leqslant 1$.

Теорема 4. *Для любой функции $f : \{0,1\}^n \to \{0,1\}$ такой, что $L(f) \geqslant n^4$, и любого $\varepsilon \leqslant 1/4$ найдется такая область $D \subseteq \{0,1\}^n$, что*

$$T^{\varepsilon}(f_D) \geqslant L(f)/\left(q \cdot a^{\log^* q}\right),$$

где $q = \log(2^{n+4}/L(f)\log L(f))$, a — константа.

Для доказательства теоремы потребуются две следующие леммы.

Лемма 5. *Пусть $D \subseteq \{0,1\}^n$, функция $f : D \to \{0,1\}$ такая, что $n^{c_8} \leqslant w(f) \leqslant |D|/a^3$, $c_8 > 3$ и $2^6 \leqslant a \leqslant \log|D|$. Тогда*

$$L(f) \leqslant \frac{|D|}{4a\log|D|}.$$

Доказательство. К функции, удовлетворяющей условиям настоящей леммы, можно применить лемму 6 из [8] и получить следующее неравенство:

$$L(f) \leqslant \frac{12\log\binom{|D|}{w(f)}}{\log\log\binom{|D|}{w(f)}}.$$

Так как

$$\binom{|D|}{|D|/a^3} \leqslant \frac{|D|^{|D|/a^3}}{(|D|/a^3)!} \leqslant \left(\frac{3|D|}{|D|/a^3}\right)^{|D|/a^3} = (3a^3)^{|D|/a^3},$$

то

$$L(f) \leqslant \frac{12(|D|/a^3)\log(3a^3)}{\log((|D|/a^3)\log(3a^3))} \leqslant \frac{|D|}{4a\log|D|}.$$

Лемма 5 доказана.

Лемма 6. *Пусть* $D \subseteq \{0,1\}^n$ *и функция* $f : D \to \{0,1\}$ *такова, что* $L(f) \geqslant n^4$, $L(f)\log L(f) \geqslant c_9|D|$, c_9 — *произвольная константа. Пусть программа* P *вычисляет функцию* f *с надежностью* $1-\varepsilon$, $\varepsilon \leqslant 1/2(c_{10})^3$, *где* c_{10} — *некоторая константа. Тогда существует такая константа* c_{11}, *зависящая от* c_9 *и* c_{10}, *что*

$$T(P) \geqslant c_{11}L(f).$$

Доказательство. В силу леммы 4 для функции f и произвольной константы a существуют функция h и вычисляющая эту функцию детерминированная программа P' такие, что

$$W(f \oplus h) \leqslant a|D|, \quad T(P') \leqslant T(P)\frac{1}{1-\varepsilon/a}.$$

Положим $a = 2\epsilon$. Тогда имеем

$$T(P') \leqslant 2T(P). \tag{15}$$

Из условий настоящей леммы и леммы 5 следует, что

$$L(f \oplus h) \leqslant \frac{|D|}{4c_{10}\log|D|} \leqslant \frac{1}{4c_{10}c_9}L(f). \tag{16}$$

В силу леммы 2 для функции f найдется такая область $D' \subseteq D$, что

$$T(f_{D'}) \geqslant \frac{c_2L(f)}{\log\dfrac{16|D|}{L(f)\log L(f)}} \geqslant \frac{c_2L(f)}{\log(16/c_9)} \geqslant c_{12}L(f).$$

Так как $L(f)\log L(f) \geqslant c_9|D|$ и для некоторой константы c_{13} из [1, 10] следует, что $L(f_{D'}) \leqslant c_{13}|D'|/\log|D'|$, то

$$\frac{c_{13}|D'|}{\log|D'|} \geqslant L(f_{D'}) \geqslant T(f_{D'}) \geqslant c_{12}L(f) \geqslant \frac{c_{12}c_9|D|}{\log|D|}.$$

Поэтому $|D'|/|D| \geqslant c_9c_{12}/2c_{13}$ и

$$T(f) \geqslant T(f_{D'})\frac{|D'|}{|D|} \geqslant c_{12}L(f)\frac{c_9c_{12}}{2c_{13}} = c_{14}L(f).$$

Заметим, что c_{14} не зависит от c_{10}. Пусть $\widetilde{P} = P''P'$ — программа, состоящая из программ P'' и P', где P'' вычисляет функцию $f \oplus h$ и на этой программе достигается оценка (16), а P' — программа, доставляемая леммой 4, для которой справедлива оценка (15). Так как $\widetilde{P}$ вычисляет f, то

$$T(f) \leqslant \frac{1}{4c_{10}c_9}L(f) + 2T(P).$$

Следовательно,

$$T(P) \geqslant \frac{1}{2}\left(T(f) - \frac{1}{4c_{10}c_9}L(f)\right) \geqslant \frac{1}{2}L(f)\left(c_{14} - \frac{1}{4c_{10}c_9}\right).$$

Пусть константа c_{10} такая, что разность $c_{14} - 1/4c_{10}$ положительна. Положим $c_{11} = (c_{14} - 1/4c_{10}c_9)/2$. Лемма 6 доказана.

Доказательство теоремы 4. В [9, теорема 5] показано существование таких констант c_{15}, c_{16}, что для любой функции $h : \{0,1\}^n \to \{0,1\}$ найдется такая область $D \subseteq \{0,1\}^n$, что

$$L(h_D)\log L(h_D) \geqslant c_{15}|D|, \quad L(h_D) \geqslant L(h)/\left(qc_{16}^{\log^* q}\right). \tag{17}$$

Пусть D — такая область для функции f, а P — программа, вычисляющая f_D с надежностью $1 - \varepsilon \geqslant 3/4$ и работающая минимальное среднее время. Положим $l = \lfloor 20 \log c_{10} \rfloor$. Тогда получаем

$$(4\varepsilon(1-\varepsilon))^{l/2} \leqslant \frac{1}{2(c_{10})^3}.$$

Из леммы 3 следует, что существует такая программа P', вычисляющая f_D с надежностью $1 - \varepsilon' \geqslant 1 - 1/2(c_{10})^3$, что

$$T(P') \leqslant c_5 l^2 T(P).$$

В силу (17) и леммы 6 имеем

$$T(P') \geqslant c_{11}L(f_D).$$

Следовательно,

$$c_{11}L(f_D) \leqslant T(P') \leqslant c_5 l^2 T(P)$$

или

$$T(P) \geqslant c_{17}L(f_D).$$

Так как $L(f_D) \geqslant L(f)/\left(qc_{16}^{\log^* q}\right)$, то $T(P) \geqslant c_{17}L(f)/\left(qc_{16}^{\log^* q}\right)$. Положим $a = c_{16}/c_{17}$. Очевидно, что при таком a

$$T(P) \geqslant L(f)/\left(qa^{\log^* q}\right).$$

Теорема 4 доказана.

4. Вероятностные программы. Общий случай

Определяя в п. 1 функцию $T(P)$ — среднее время работы вероятностной программы P, мы полагали, что появление всех аргументов равновероятно. Теперь для вероятностной программы P определим среднее

время работы $\widehat{T}(P)$, не зависящее от распределения вероятностей на множестве аргументов этой программы, а для полностью определенной булевой функции рассмотрим ее среднее время работы $\widehat{T}^{\varepsilon}(f)$, не зависящее от распределения вероятностей на множестве аргументов этой функции.

Пусть F — распределение вероятностей на $\{0,1\}^n$, $P_F(x)$ — вероятность появления набора x. Напомним, что символ $\xi_{P(x)}$ обозначает набор значений случайных операторов программы P при работе этой программы на x, а $T_P(x,y)$ обозначает время работы P на наборе x при условии, что $\xi_{P(x)} = y$. Положим

$$T_F(P) = \sum_{x\in\{0,1\}^n} (P_F(x) \sum_{y\in D_x} T_P(x,y)P(\xi_{P(x)} = y)), \quad \widehat{T}(P) = \max T_F(P),$$

где максимум берется по всем возможным распределениям F. Для булевой функции $f : \{0,1\}^n \to \{0,1\}$ положим

$$\widehat{T}^{\varepsilon}(f) = \min P(\widehat{T}(P)),$$

где минимум берется по всем возможным программам P, вычисляющим f с надежностью, не меньшей $1-\varepsilon$. Доказанные выше теоремы 2 и 4 переформулируем, используя функцию $\widehat{T}^{\varepsilon}(f)$. Легко видеть, что справедлива следующая

Теорема 5. *Для любой функции* $f : \{0,1\}^n \to \{0,1\}$ *такой, что* $L(f) \geqslant n^4$, *и любого* $\varepsilon \leqslant 1/4$ *справедливы неравенства*

(a) $\widehat{T}^{\varepsilon}(f) \geqslant L(f)/\left(q\, a^{\log^* q}\right)$;

(b) $\widehat{T}^{0}(f) \geqslant \frac{c}{q} L(f)$, *где* $q = \log(2^{n+4}/L(f)\log L(f))$, a — *константа.*

Для доказательства теоремы достаточно рассмотреть области D_2 и D_4, доставляемые теоремами 2 и 4, и распределения F_2 и F_4, при которых $P_{F_i}(x) = P_{F_i}(x') > 0$ для любых x, $x' \in D_i$ и $P_{F_i}(x) = 0$, если $x \notin D_i$.

В заключение для неветвящихся программ рассмотрим еще одну меру сложности. Эта мера сложности часто используется при изучении времени работы вероятностных алгоритмов [7].

Будем говорить, что вероятностная программа P вычисляет булеву функцию $f : \{0,1\}^n \to \{0,1\}$ с надежностью $1-\varepsilon$ за время t, если для каждого $x \in \{0,1\}^n$ справедливо неравенство

$$P(P(x) = f(x),\ \ t_P(x) \leqslant t) \geqslant 1-\varepsilon.$$

Легко видеть, что если программа P вычисляет булеву функцию f с надежностью $1-\varepsilon$ за время t и $\varepsilon \leqslant 1/4$, то справедливо неравенство $T^{\varepsilon} \leqslant t$.

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

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. **Карп Р.** Комбинаторика, сложность и случайность // Лекции лауреатов премии Тьюринга. М.: Мир, 1993. С. 498–521.
3. **Кук С.** Обзор вычислительной сложности // Лекции лауреатов премии Тьюринга. М.: Мир, 1993. С. 475–497.
4. **Лупанов О. Б.** Об одном подходе к синтезу управляющих систем — принципе локального кодирования // Проблемы кибернетики. М.: Наука, 1965. Вып. 14. С. 31–110.
5. **Лупанов О. Б.** Асимптотические оценки сложности управляющих систем. М.: Изд-во МГУ, 1984.
6. **Тарьян Р.** Сложность комбинаторных алгоритмов // Кибернетический сб. М.: Мир, 1980. Вып. 17. С. 61–113.
7. **Фрейвалд Р. В.** Ускорение распознавания некоторых множеств применением датчика случайных чисел // Проблемы кибернетики. М.: Наука, 1979. Вып. 36. С. 209–224.
8. **Чашкин А. В.** О среднем времени вычисления значений булевых функций // Дискрет. анализ и исслед. операций. Сер. 1. 1997. Т. 4, № 1. С. 60–78.
9. **Чашкин А. В.** Нижние оценки сложности сужений булевых функций // Дискрет. анализ и исслед. операций. Сер. 1. 1997. Т. 4, № 2. С. 75–111.
10. **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
7 апреля 1997 г.