ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Январь—март 1998. Серия 1. Том 5, № 1, 88–103

УДК 519.7

О СРЕДНЕМ ВРЕМЕНИ ВЫЧИСЛЕНИЯ БУЛЕВЫХ ОПЕРАТОРОВ*)

А. В. Чашкин

Изучается среднее время вычисления значений булевых операторов неветвящимися программами двух типов. Получены верхние и нижние оценки для соответствующих функций Шеннона. В случае, когда число компонент вычисляемых операторов растет вместе с числом аргументов, получены асимптотически точные формулы для функций Шеннона.

Введение

В [3] изучалось среднее время вычисления значений булевых функций неветвящимися программами с условной остановкой. В настоящей работе рассматриваются две разновидности аналогичных программ, позволяющие вычислять значения булевых операторов.

Неветвящейся программой первого типа с условной остановкой назовем последовательность операторов двух типов. Каждый оператор первого типа вычисляет значение некоторой булевой функции. Аргументами этой функции могут быть либо величины, вычисленные предыдущими операторами, либо значения входных переменных. Каждый оператор второго типа зависит от $m+1$ переменных, где m — число выходов программы, и может прекращать выполнение программы. Результат работы оператора второго типа определяется значениями, вычисленными программой на некоторых $m+1$ предыдущих шагах. Для каждого конкретного оператора номера́ этих шагов фиксированы и могут быть различными для различных операторов. Если на последний вход выполняемого оператора второго типа поступает единица, то выполнение программы прекращается и значения, поступившие на его другие входы, объявляются значениями программы на вычисляемом наборе переменных. Если на последний вход рассматриваемого оператора поступает ноль, то выполняется следующий оператор программы.

*) Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (код проекта 96–01–01068) и Федеральной программы «Интеграция» (код проекта 473).

Неветвящиеся программы второго типа с условной остановкой отличаются от обычных неветвящихся программ следующим: 1) некоторые операторы первого типа и, возможно, некоторые входы программы помечены целыми числами от 0 до m; 2) операторы, помеченные нулем, останавливают выполнение программы, если их значение равно единице; 3) i-м значением программы после ее остановки объявляется значение ее последнего выполненного оператора или входа, если такого оператора нет, помеченного числом i.

В работе найдены верхние и нижние оценки функций Шеннона для среднего времени вычисления булевых операторов программами первого и второго типа. В случае, когда число компонент вычисляемых операторов растет вместе с числом аргументов, получены асимптотически точные формулы.

1. Основные определения

Дадим формальные определения. Пусть $B \subseteq \{f : \{0,1\}^k \to \{0,1\}\}$ — базис в P_2, $\pi : \{0,1\}^{m+1} \to \{0,1\}^{m+1}$ — тождественный булев оператор, $X_n = \{x_1, \dots, x_n\}$ — множество независимых переменных.

Неветвящейся программой первого типа с условной остановкой назовем последовательность $P = p_1 \dots p_i \dots p_s$, элементами которой являются операторы $p_i = f_i(p_{i,1}, \dots, p_{i,l})$, где $p_{i,j} \in \{p_1, \dots, p_{i-1}\} \cup X_n$, $f_i \in B \cup \{\pi\}$, причем если $p_{i,j} = p_t \in \{p_1, \dots, p_{i-1}\}$, то $f_t \neq \pi$. Оператор p_i назовем *оператором первого типа*, или *функциональным оператором*, если $f_i \neq \pi$. Оператор p_i назовем *оператором второго типа*, или *оператором остановки*, если $f_i = \pi$. Будем говорить, что программа P имеет n входов, m выходов, и ее i-му входу приписана переменная x_i.

Положим $n(p_i) = i$, т. е. $n(p)$ — номер оператора p в программе P. Пусть $p_{i_1}, \dots, p_{i_r}$ — все операторы второго типа из P, $i_1 < \dots < i_r$. Через q_t будем обозначать t-й оператор второго типа программы P, а через $q_{t,j}$ — j-й аргумент этого оператора. Индуктивно определим значение оператора p программы P на произвольном двоичном наборе x. Для первого оператора положим $p_1(x) = f_1(x)$, а при $i > 1$ положим $p_i(x) = f_i(p_{i,1}(x), \dots, p_{i,l}(x))$. Результат действия программы P на наборе x обозначим через $P(x) = (P_1(x), \dots, P_m(x))$ и значение его j-й компоненты определим следующим образом:

$$\begin{aligned} P_j(x) = {} & q_{1,m+1}(x)q_{1,j}(x) \vee \overline{q}_{1,m+1}(x)(q_{2,m+1}(x)q_{2,j}(x) \vee \dots \\ & \vee \overline{q}_{r-2,m+1}(x)(q_{r-1,m+1}(x)q_{r-1,j}(x) \vee \overline{q}_{r-1,m+1}(x)q_{r,m+1}(x)q_{r,j}(x))\dots). \end{aligned}$$

Пусть $B \subseteq \{f : \{0,1\}^k \to \{0,1\}\}$ — базис в P_2, $X_n = \{x_1, \dots, x_n\}$ — множество независимых переменных, каждой из которых приписано некоторое число $a_i \in \{0, 1, \dots, m\}$.

Неветвящейся программой второго типа с условной остановкой назовем последовательность $P = p_1 \ldots p_i \ldots p_s$, элементами которой являются операторы $p_i = (f_i(p_{i,1}, \ldots, p_{i,l}), a_i)$, где $a_i \in \{0, 1, \ldots, m\}$, $f_i \in B$ и $p_{i,j} \in \{p_1, \ldots, p_{i-1}\} \cup X_n$. Оператор p_i назовем *оператором первого типа*, или *функциональным оператором*, если $a_i \neq 0$, и *оператором второго типа*, или *оператором остановки*, если $a_i = 0$. Будем говорить, что программа P имеет n входов, m выходов, и ее i-му входу приписана переменная x_i.

Значение оператора p программы второго типа P на произвольном двоичном наборе x определим так же, как и для операторов программ первого типа. Пусть, как и ранее, $n(p)$ — номер оператора p в программе P, q_t — t-й оператор второго типа программы P. Через $q_{t,j}$ обозначим либо оператор p_i такой, что $i = \max s$, где максимум берется по всем s таким, что $a_s = j$ и $s < n(q_t)$, либо, если такого оператора нет, переменную x_r с максимальным индексом r, которой приписано число j. Результат действия программы второго типа P на наборе x обозначим через $P(x) = (P_1(x), \ldots, P_m(x))$ и значение его j-й компоненты определим следующим образом:

$$\begin{aligned}P_j(x) = q_1(x)q_{1,j}(x) \vee \overline{q}_1(x)(q_2(x)q_{2,j}(x) \vee \ldots \\ \vee \overline{q}_{r-2}(x)(q_{r-1}(x)q_{r-1,j}(x) \vee \overline{q}_{r-1}(x)q_r(x)q_{r,j}(x))\ldots).\end{aligned}$$

Временем работы $T_P(x)$ программы первого типа P на наборе переменных x назовем минимальное $n(q_j)$ такое, что $q_{j,m+1}(x) = 1$, т. е. число операторов, выполненных до остановки программы. *Временем работы* $T_P(x)$ программы второго типа P на наборе переменных x назовем минимальное $n(q_j)$ такое, что $q_j(x) = 1$. Величину

$$T(P) = 2^{-n} \sum T_P(x),$$

где суммирование производится по всем двоичным наборам длины n, назовем *средним временем работы* программы P. Если для некоторого булева оператора f и любого двоичного набора x справедливо равенство $f(x) = P(x)$, то будем говорить, что программа P вычисляет оператор f. Величину

$$T_{B,i}(f) = \min T(P),$$

где минимум берется по всем программам i-го типа, вычисляющим f в базисе B, назовем *средним временем вычисления* оператора f. Программу P, вычисляющую оператор f со средним временем $T_{B,i}(f) = \min T(P)$, назовем *минимальной* программой. Число элементов минимальной схемы из функциональных элементов, реализующей оператор f в базисе B, назовем *сложностью* оператора f и обозначим через $L_B(f)$.

Введем функции Шеннона $T_{B,i}(n,m)$, определенные стандартным образом:

$$T_{B,i}(n,m) = \max T_{B,i}(f),$$

где максимум берется по всем булевым (n,m)-операторам f.

Далее будем рассматривать базис, состоящий из всех не более чем k-местных булевых функций, где k — постоянное число. Среднее время вычисления оператора f программами i-го типа в таком базисе будем обозначать через $T_{k,i}(f)$, а соответствующие функции Шеннона — через $T_{k,i}(n,m)$. Будем полагать, что n — число аргументов всех рассматриваемых ниже булевых операторов — достаточно велико, а для m — числа компонент этих операторов — справедливо соотношение $m = n^{O(1)}$. Через c и c_i, $i = 1,2,\ldots$, обозначаются подходящие константы, а log обозначает логарифм по основанию 2. Понятия, используемые без определений, можно найти в [2].

2. Основные результаты

Основные результаты работы — оценки функций Шеннона — приведены в теоремах 1 и 2. Случаи, когда для функций Шеннона удается получить асимптотически точные формулы, сформулированы в виде следствий из этих теорем. Верхние оценки доказываются традиционными методами [2], используемыми для построения схем из функциональных элементов. Нижние оценки доказываются мощностным методом — сравнением числа программ с числом булевых операторов.

Положим

$$\alpha(m,k) = \begin{cases} \frac{m}{m+k}, & \text{если } k < m+2, \\ \frac{m}{2k-2}, & \text{если } k \geqslant m+2, \end{cases} \qquad \beta(m,k) = \min\left(1, \frac{m}{2k-2}\right).$$

Теорема 1. *Пусть k — константа и $m = n^{O(1)}$. Тогда*

$$\alpha(m,k)\,\frac{2^n}{n}\,(1+o(1)) \leqslant T_{k,1}(n,m) \leqslant \beta(m,k)\,\frac{2^n}{n}\,(1+o(1)).$$

Нижняя оценка теоремы следует из доказанных ниже лемм 5 и 6. Верхняя оценка следует из лемм 8 и 9.

Теорема 2. *Пусть k — константа и $m = n^{O(1)}$. Тогда*

$$\frac{2^{n-1}m}{nk}(1+o(1)) \leqslant T_{k,2}(n,m) \leqslant \frac{2^{n-1}(m+1)}{nk}(1+o(1)).$$

Нижняя оценка теоремы следует из леммы 7. Верхняя оценка следует из леммы 10.

Из теорем 1 и 2 легко извлекаются следующие утверждения.

Следствие 1. *Пусть k — константа и $k \geqslant m + 2$. Тогда*

$$T_{k,1}(n,m) = \frac{2^{n-1}m}{n(k-1)}(1 + o(1)).$$

Следствие 2. *Пусть k — константа, $m \to \infty$ и $m = n^{O(1)}$. Тогда*

$$T_{k,1}(n,m) = \frac{2^n}{n}(1 + o(1)).$$

Следствие 3. *Пусть k — константа, $m \to \infty$ и $m = n^{O(1)}$. Тогда*

$$T_{k,2}(n,m) = \frac{2^{n-1}m}{nk}(1 + o(1)).$$

3. Оценки числа программ

Программу первого типа $P = p_1 \ldots p_s$ назовем *тупиковой*, если для любого $i \in \{1, \ldots, s\}$ найдется набор x такой, что $P(x) \neq P'(x)$, где $P' = p_1 \ldots p_{i-1} p_{i+1} \ldots p_s$. Программу второго типа P назовем *приведенной*, если значения, вычисленные операторами остановки, не используются в качестве аргументов других операторов.

Очевидно, что любая программа первого типа может быть преобразована в такую тупиковую программу, что среднее время работы новой программы будет не больше среднего времени работы исходной программы. Аналогичное утверждение справедливо и для программ второго типа — любая программа второго типа может быть преобразована в такую приведенную программу, что среднее время работы приведенной программы будет не больше среднего времени работы исходной программы.

Действительно, предположим, что в некоторой программе второго типа есть оператор остановки, значение которого является аргументом другого оператора. В этом случае, если значение оператора остановки равно нулю, оно может быть заменено константой, если же его значение равно единице, оно также может быть заменено нулем, так как оператор останавливает работу программы, и это значение дальше нигде не используется.

Каждой программе первого типа P с m выходами, входам которой приписаны переменные $x_1, \ldots, x_n$, поставим в соответствие ориентированный граф GP. Сделаем это следующим образом:

(1) каждой переменной x_i и каждому оператору p_j программы P поставим в соответствие вершину графа GP;

(2) вершине, соответствующей переменной x_i, припишем символ x_i;

(3) вершине, соответствующей оператору p_j, припишем символ f_j;

(4) вершины u_i и u_j связаны дугой, направленной от u_i к u_j, если вершина u_j соответствует оператору p, s-м аргументом которого является оператор, которому соответствует вершина u_i, $1 \leqslant s \leqslant \max(m+1, k)$; каждой такой дуге припишем символ s;

(5) вершины u_i и u_j связаны дугой, направленной от u_i к u_j, если они соответствуют операторам, являющимся l-м и $(l+1)$-м операторами остановки программы P; каждой такой дуге припишем символ 0.

Каждой программе второго типа P с m выходами, входам которой приписаны переменные $x_1, \ldots, x_n$, поставим в соответствие ориентированный граф GP. Сделаем это следующим образом:

(1) каждой переменной x_i и каждому оператору p_j программы P поставим в соответствие вершину графа GP;

(2) вершине, соответствующей переменной x_i, припишем символ x_i;

(3) вершине, соответствующей оператору p_j, припишем символ f_j;

(4) вершины u_i и u_j связаны дугой, направленной от u_i к u_j, если вершина u_j соответствует оператору p, s-м аргументом которого является оператор, которому соответствует вершина u_i, $1 \leqslant s \leqslant k$; каждую такую дугу назовем функциональной и припишем ей символ s;

(5) вершины u_i и u_j связаны дугой, направленной от u_i к u_j, если вершина u_j соответствует оператору остановки q_t, вершина u_i — оператору $q_{t,s}$ и $q_{t,s} \neq q_{r,s}$ для всех $r < t$, $1 \leqslant s \leqslant m$; каждую такую дугу назовем особой и припишем ей символ s;

(6) вершины u_i и u_j связаны дугой, направленной от u_i к u_j, если они соответствуют операторам, являющимся l-м и $(l+1)$-м операторами остановки программы P; каждую такую дугу назовем дугой остановки и припишем ей символ 0.

Программы P_1 и P_2 назовем *изоморфными*, если изоморфны соответствующие им графы. Легко видеть, что с точностью до изоморфизма любая программа восстанавливается по соответствующему ей графу.

Введем следующие обозначения:

$N_1(k, n, m, L_1, L_2)$ — число неизоморфных программ первого типа в базисе из всех не более чем k-местных булевых функций, содержащих не более L_1 функциональных операторов и не более L_2 операторов остановки с n входами и m выходами;

$N_1(k, n, m, L)$ — число неизоморфных тупиковых программ первого типа в базисе из всех не более чем k-местных булевых функций, содержащих не более L операторов с n входами и m выходами;

$N_2(k, n, m, L_1, L_2)$ — число неизоморфных программ второго типа в базисе из всех не более чем k-местных булевых функций, содержащих не более L_1 функциональных операторов и не более L_2 операторов остановки с n входами и m выходами;

$N_2(k,n,m,L)$ — число неизоморфных приведенных программ второго типа в базисе из всех не более чем k-местных булевых функций, содержащих не более L операторов с n входами и m выходами.

Лемма 1. *Если k — константа, то*

$$N_1(k,n,m,L_1,L_2) \leqslant (c_1 m\,(L_1+L_2+n))^{(k-1)L_1+(m+1)L_2},$$
$$N_2(k,n,m,L_1,L_2) \leqslant (c_1 m\,(L_1+L_2+n))^{(k-1)(L_1+L_2)+(m+1)L_2}.$$

Доказательство. Поскольку оба неравенства леммы доказываются аналогично, докажем только первое. Для его доказательства достаточно оценить сверху число графов, соответствующих рассматриваемым программам. Каждый граф содержит не более L_1+L_2+n вершин и не более $kL_1+(m+2)L_2-1$ дуг. Число таких графов не превосходит (см., например, [1])

$$(c\,(L_1+L_2+n))^{kL_1+(m+2)L_2-L_1-L_2-n}.$$

Дуги графа могут быть помечены не более чем $k^{kL_1}(m+2)^{(m+2)L_2}$ способами, вершины — не более чем $(L_1+L_2+n)^n\,(\dot{c}(k))^{L_1+L_2}$ способами, где $c(k)$ — константа, зависящая от k. Следовательно, число различных помеченных графов не превосходит произведения трех приведенных величин, т. е.

$$N_1(k,n,m,L_1,L_2) \leqslant (c_1 m\,(L_1+L_2+n))^{(k-1)L_1+(m+1)L_2}.$$

Лемма 1 доказана.

Из леммы 1 легко следует лемма 2. Эту лемму приведем без доказательства.

Лемма 2. *Если $k \geqslant m+2$, то*

$$N_1(k,n,m,L) \leqslant (c_2 m\,(L+n))^{(k-1)L}.$$

Лемма 3. *Если $k \leqslant m+2$, то*

$$N_1(k,n,m,L) \leqslant (c_3 m\,(L+n))^{(L+n)(m+k)/2}.$$

Доказательство. Покажем, что если программа является тупиковой, то $q_{i,m+1} \neq q_{j,m+1}$ при $i \neq j$. Предположим, что $q_{i,m+1} = q_{j,m+1}$ и $i<j$. Тогда если $q_{i,m+1}=1$, то оператор q_i останавливает выполнение программы и оператор q_j не выполняется. Если $q_{i,m+1}=0$, то оператор q_j не останавливает выполнение программы. Следовательно, оператор q_j можно удалить из программы. Поэтому сделанное предположение противоречит тупиковости программы. Из неравенства $q_{i,m+1} \neq q_{j,m+1}$

следует, что $L_2 \leqslant L_1 + n$. Тогда $L_2 \leqslant (L+n)/2$, $L_1 = L - L_2$. Следовательно,

$$(k-1)L_1 + (m+1)L_2 \leqslant (k-1)(L-L_2) + (m+1)L_2 \leqslant (k-1)L$$
$$+(m+1-k+1)L_2 \leqslant (2k-2)\frac{L+n}{2} + (m-k+2)\frac{L+n}{2} \leqslant (m+k)\frac{L+n}{2}.$$

Подставив полученную оценку в первое неравенство леммы 1, получим требуемое неравенство. Лемма 3 доказана.

Лемма 4. *Если k — константа, то*

$$N_2(k,n,m,L) \leqslant (c_4 m\,(L+n))^{kL-n}.$$

Доказательство. Оценим сверху число графов, соответствующих рассматриваемым программам. Пусть L_1 — число функциональных операторов в программе, а L_2 — число операторов остановки. Очевидно, что $L = L_1 + L_2$ и каждый граф содержит не более $L + n$ вершин. Оценим число дуг. Из каждой вершины, соответствующей функциональному оператору, выходит не более одной особой дуги. Число особых дуг обозначим через N. Очевидно, что из вершин, соответствующих операторам остановки, особые и функциональные дуги не выходят. Поэтому $N \leqslant L_1$. Каждый граф содержит $L_2 - 1$ дугу остановки и не более kL функциональных дуг. Следовательно, общее число дуг не превосходит $kL + L_2 + N$. Легко видеть, что число графов тем больше, чем больше разность числа дуг и вершин (см. [1]). Преобразуем эту разность:

$$(k-1)L + L_2 + N - n \leqslant (k-1)L + L_2 + L_1 - n = kL - n.$$

Учитывая число способов, которыми можно пометить дуги и вершины графов, получаем

$$N_2(k,n,m,L) \leqslant (c_4 m\,(L+n))^{kL-n}.$$

Лемма 4 доказана.

4. Нижние оценки

Пусть f — булев оператор, P — программа, вычисляющая f. Каждому двоичному 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 $x < y$.

Лемма 5. *Пусть $k < m + 2$. Тогда для почти всех булевых (n,m)-операторов f справедливо неравенство*

$$T_{k,1}(f) \geqslant \frac{2^n m}{n(m+k)}(1 + o(1)).$$

Доказательство. Пусть f — булев оператор, P — минимальная программа, вычисляющая f. Пусть x_i таково, что $N_P(x_i) = \frac{i2^n}{q}$, где $q = 2^{q_0}$, q_0 — целое и $q \asymp \frac{n}{\log^2 n}$, $i = 2,3,\ldots,q$. Оценим сверху число булевых операторов, которые могут быть реализованы минимальными программами, содержащими x_i такое, что $T_P(x_i) \leqslant \frac{(i-1)2^n}{qn} \cdot \frac{2m}{m+k}$. Каждый такой оператор однозначно определяется первыми $T_P(x_i)$ операторами своей минимальной программы и набором не более чем $2^n - N_P(x_i)$ двоичных векторов длины m — значениями на тех аргументах, время работы на которых больше времени работы на x_i. В силу леммы 3 для числа N_i, равного числу различных программ, сложность которых не превосходит $T_P(x_i)$, справедливо неравенство

$$N_i \leqslant \left(c_3 m\left(\frac{(i-1)2^n}{qn} \cdot \frac{2m}{m+k} + n\right)\right)^{\left(\frac{(i-1)2^n}{qn} \cdot \frac{2m}{m+k} + n\right)\frac{m+k}{2}}.$$

Учитывая, что $m = n^{O(1)}$, после несложных преобразований получаем неравенство

$$N_i \leqslant 2^{\frac{(i-1)m2^n}{q}\left(1+O\left(\frac{\log n}{n}\right)\right)}.$$

Следовательно, обозначив через M число рассматриваемых булевых операторов, имеем

$$M \leqslant \sum_{i=2}^{q} 2^{\frac{(i-1)m2^n}{q}\left(1+O\left(\frac{\log n}{n}\right)\right)}\, 2^{m2^n - \frac{mi2^n}{q}}.$$

Преобразуем показатель величины, стоящей под знаком суммы. Учитывая, что $i \leqslant q \asymp \frac{n}{\log^2 n}$, имеем

$$m2^n - \frac{mi2^n}{q} + \frac{(i-1)m2^n}{q}\left(1+O\left(\frac{\log n}{n}\right)\right)$$
$$= m2^n - \frac{m2^n}{q}\left(i-(i-1)\left(1+O\left(\frac{\log n}{n}\right)\right)\right) = m2^n - \frac{m2^n}{q}\left(1+O\left(\frac{1}{\log n}\right)\right).$$

Поэтому

$$M \leqslant q \cdot 2^{m2^n - \frac{m2^n}{q}\left(1+O\left(\frac{1}{\log n}\right)\right)} = 2^{m2^n - \frac{m2^n}{q}\left(1+O\left(\frac{1}{\log n}\right)\right)}.$$

Сравнивая полученную оценку для M с числом всех булевых (n,m)-операторов, видим, что все минимальные программы почти всех булевых операторов удовлетворяют следующему условию:

$$\text{если } x_i \text{ таково, что } N_P(x_i) = \frac{i2^n}{q}, \text{ где } q = 2^{q_0},\ q_0 \text{ — целое и}$$
$$q \asymp \frac{n}{\log^2 n},\ i = 2,3,\ldots,q, \quad \text{то } T_P(x_i) > \frac{(i-1)2^n}{qn} \cdot \frac{2m}{m+k}. \qquad (1)$$

Положим $X_i = \{x \mid N_P(x_i) < N_P(x) \leqslant N_P(x_{i+1})\}$. Тогда для среднего времени работы $T(P)$ каждой такой программы P имеем

$$T(P) = 2^{-n}\sum_{x} T_P(x) \geqslant 2^{-n}\sum_{i=2}^{q-1} T_P(x_i)|X_i|$$
$$= 2^{-n}\sum_{i=2}^{q-1} T_P(x_i)\frac{2^n}{q} > \frac{1}{q}\sum_{i=2}^{q-1}\frac{(i-1)2^n}{qn}\cdot\frac{2m}{m+k} = \frac{(q-1)(q-2)2^n}{q^2 n}\cdot\frac{m}{m+k}$$
$$= \frac{2^n m}{n(m+k)}\left(1+O\left(\frac{\log^2 n}{n}\right)\right).$$

Лемма 5 доказана.

Лемма 6. *Пусть $k \geqslant m+2$. Тогда для почти всех булевых (n,m)-операторов f справедливо неравенство*

$$T_{k,1}(f) \geqslant \frac{2^{n-1}m}{n(k-1)}\,(1+o(1)).$$

ДОКАЗАТЕЛЬСТВО. Как и при доказательстве предыдущей леммы, нетрудно показать, что все минимальные программы P, реализующие почти все булевы операторы, удовлетворяют следующему условию:

$$\begin{gathered}\text{если } x_i \text{ таково, что } N_P(x_i) = \frac{i2^n}{q}, \text{ где } q = 2^{q_0},\ q_0 \text{— целое и}\\ q \asymp \frac{n}{\log^2 n},\ i = 2,3,\ldots,q, \ \text{ то } T_P(x_i) > \frac{(i-1)2^n}{qn}\cdot\frac{m}{k-1}.\end{gathered} \tag{2}$$

Доказательство условия (2) аналогично доказательству условия (1); только вместо леммы 3 необходимо воспользоваться леммой 2. Снова положим $X_i = \{x \mid N_P(x_i) < N_P(x) \leqslant N_P(x_{i+1})\}$. Тогда для среднего времени $T(P)$ работы каждой программы P, удовлетворяющей (2), имеем

$$T(P) = 2^{-n}\sum_{x} T_P(x) \geqslant 2^{-n}\sum_{i=2}^{q-1} T_P(x_i)|X_i|$$
$$= 2^{-n}\sum_{i=2}^{q-1} T_P(x_i)\frac{2^n}{q} > \frac{1}{q}\sum_{i=2}^{q-1}\frac{(i-1)2^n}{qn}\cdot\frac{m}{k-1} = \frac{(q-1)(q-2)2^n}{2q^2 n}\cdot\frac{m}{k-1}$$
$$= \frac{2^{n-1} m}{n(k-1)}\left(1+O\left(\frac{\log^2 n}{n}\right)\right).$$

Лемма 6 доказана.

Следующую лемму приведем без доказательства. Оно почти дословно совпадает с доказательством леммы 5. Единственное отличие состоит в использовании леммы 4 вместо леммы 3 и условия

если x_i таково, что $N_P(x_i) = \dfrac{i2^n}{q}$, где $q = 2^{q_0}$, q_0 — целое и
$q \asymp \dfrac{n}{\log^2 n}$, $i = 2, 3, \dots, q$, то $T_P(x_i) > \dfrac{(i-1)2^n}{qn} \cdot \dfrac{m}{k}$,

вместо условия (1).

Лемма 7. *Для почти всех булевых (n, m)-операторов f справедливо неравенство*

$$T_{k,2}(f) \geqslant \frac{2^{n-1}m}{nk}\,(1 + o(1)).$$

5. Верхние оценки

Пусть $\sigma = (\sigma_1, \dots, \sigma_s)$ — двоичный набор. На множестве таких наборов введем функцию $N(\sigma) = \sum\limits_{i=1}^{s} \sigma_i 2^{i-1}$.

Лемма 8. *Для произвольного булева (n, m)-оператора f справедливо неравенство*

$$T_{k,1}(f) \leqslant \frac{2^{n-1}m}{n(k-1)}\,(1 + o(1)).$$

Доказательство. Пусть $f = (f_1, \dots, f_m)$, где f_i — i-я компонента оператора f. Положим $s = \lfloor \log n \rfloor$. Разложим f_i по первым s переменным. Тогда имеем

$$\begin{aligned} f_i(x_1, \dots, x_n) &= \bigvee_{(\sigma_1, \dots, \sigma_s)} f_i(\sigma_1, \dots, \sigma_s, x_{s+1}, \dots, x_n) x_1^{\sigma_1} \dots x_s^{\sigma_s} \\ &= \bigvee_{(\sigma_1, \dots, \sigma_s)} f_{i,j}(x_{s+1}, \dots, x_n) x_1^{\sigma_1} \dots x_s^{\sigma_s}, \end{aligned}$$

где $j = N(\sigma_1, \dots, \sigma_s)$. Программу P, вычисляющую f, представим в следующем виде:

$$P = P_1 q_1 \dots P_{2^s} q_{2^s},$$

где программа P_j вычисляет функции $f_{1,j}, \dots, f_{m,j}$, $x_1^{\sigma_1}, \dots, x_s^{\sigma_s}$ и состоит только из функциональных операторов; оператор q_j останавливает работу программы P, если конъюнкция $x_1^{\sigma_1} \dots x_s^{\sigma_s} = 1$, где $j = N(\sigma_1, \dots, \sigma_s)$, и объявляет i-м значением программы величину $f_{i,j}(x_{s+1}, \dots, x_n)$. Из [2] следует, что

$$L(P_i) \leqslant \frac{2^{n-s}m}{(k-1)(n-s)}\,(1 + o(1)).$$

Поэтому

$$T(P) = 2^{-n} \sum_{(\sigma_{s+1},\ldots,\sigma_n)} \sum_{(\sigma_1,\ldots,\sigma_s)} T_P(\sigma_1,\ldots,\sigma_n)$$

$$\leqslant 2^{-n} \sum_{i=1}^{2^s} \frac{m2^{n-s}}{(k-1)(n-s)} 2^{n-s} i\ (1+o(1))$$

$$\leqslant 2^{-n} \frac{m2^{2n-2s}}{(k-1)(n-s)} 2^{2s-1}(1+o(1)) \leqslant \frac{m2^{n-1}}{(k-1)n}\ (1+o(1)).$$

Лемма 8 доказана.

Пусть s, h — целые. Множество всех двоичных наборов длины s разобьем на непересекающиеся множества Y_i такие, что $\sigma \in Y_i$, если $(i-1)h \leqslant N(\sigma) < ih$. Введем функции

$$g_j(x_1,\ldots,x_s) = \bigvee_{\sigma \in Y_j} x_1^{\sigma_1}\ldots x_s^{\sigma_s},$$

$$g_{j,l}(x_1,\ldots,x_n) = g_j(x_1,\ldots,x_s)\ x_{s+1}^{\sigma_{s+1}}\ldots x_n^{\sigma_n},$$

где $N(\sigma_{s+1},\ldots,\sigma_n) = l$. Пусть $z(x_1,\ldots,x_n)$ — произвольная булева функция. Положим $z_l(x_1,\ldots,x_s) = z(x_1,\ldots,x_s,\sigma_{s+1},\ldots,\sigma_n)$, где $N(\sigma_{s+1},\ldots,\sigma_n) = l$, и $z_{j,l}(x_1,\ldots,x_s) = z_j(x_1,\ldots,x_s)\ g_l\ (x_1,\ldots,x_s)$. Пусть $t = \lceil 2^s/h \rceil$. Тогда справедливо разложение [2]

$$z(x_1,\ldots,x_n) = \bigvee_{(\sigma_{s+1},\ldots,\sigma_n)} \left(\bigvee_{j=1}^{t} z_{j,l}(x_1,\ldots,x_s) \right) x_{s+1}^{\sigma_{s+1}}\ldots x_n^{\sigma_n},$$

где $N(\sigma_{s+1},\ldots,\sigma_n) = l$. Легко видеть, что

$$z_{j,l}(x_1,\ldots,x_s) x_{s+1}^{\sigma_{s+1}}\ldots x_n^{\sigma_n} = z_{j,l}(x_1,\ldots,x_s) g_{j,l}(x_1,\ldots,x_n).$$

Следовательно, справедливо разложение

$$z(x_1,\ldots,x_n) = \bigvee_{(\sigma_{s+1},\ldots,\sigma_n)} \left(\bigvee_{j=1}^{t} z_{j,l}(x_1,\ldots,x_s) g_{j,l}(x_1,\ldots,x_n) \right). \tag{3}$$

Пусть R — число различных функций $z_{j,l}(x_1,\ldots,x_s)$, L_z — сложность реализации этих функций схемами из функциональных элементов. Легко видеть, что $R \leqslant 2^{h+s}/h$ и

$$L_z \leqslant 2^{h+s+1}. \tag{4}$$

Лемма 9. *Для произвольного булева (n, m)-оператора f справедливо неравенство*

$$T_{k,1}(f) \leqslant \frac{2^n}{n}\ (1+o(1)).$$

Доказательство. Лемму докажем для случая $m = 1$. Доказательство в общем случае отличается от приводимого ниже только дополнительными индексами в формулах. Пусть $z(x_1, \ldots, x_n)$ — произвольная булева функция. Положим $s = \lfloor 2\log n \rfloor$, $h = \lfloor n - 4\log n \rfloor$ и воспользуемся разложением (3). Программу, вычисляющую функцию z, представим в следующем виде:

$$P = P_1 p_{1,1} q_{1,1} \ldots p_{j,l} q_{j,l} \ldots p_{t,d} q_{t,d},$$

где $t = \lceil 2^s/h \rceil$, $d = 2^{n-s}$, P_1 — программа, вычисляющая все возможные функции $z_{j,l}(x_1, \ldots, x_s)$, все функции $g_j(x_1, \ldots, x_s)$ и все произведения $x_{s+1}^{\sigma_{s+1}} \ldots x_n^{\sigma_n}$, оператор $p_{j,l}$ вычисляет функцию $g_{j,l}(x_1, \ldots, x_n)$, оператор $q_{j,l}$ останавливает программу, если $p_{j,l} = 1$, и объявляет результатом ее работы значение функции $z_{j,l}(x_1, \ldots, x_s)$, вычисленное программой P_1. Легко видеть, что если $(\sigma_1, \ldots, \sigma_s)$ и $(\sigma'_1, \ldots, \sigma'_s)$ принадлежат одному и тому же множеству Y_j, то $T_P(\sigma_1, \ldots, \sigma_s, x_{s+1}, \ldots, x_n) = T_P(\sigma'_1, \ldots, \sigma'_s, x_{s+1}, \ldots, x_n)$ при всех $x_{s+1}, \ldots, x_n$. Так как $2^{h+s}h^{-1} \leqslant 2^n n^{-2}$, то из (3) и (4) следует, что

$$\begin{aligned}
T(P) &= 2^{-n} \sum_{(\sigma_{s+1},\ldots,\sigma_n)} \sum_{(\sigma_1,\ldots,\sigma_s)} T_P(\sigma_1, \ldots, \sigma_n) \\
&= 2^{-n} \sum_{(\sigma_{s+1},\ldots,\sigma_n)} \sum_{j=1}^{t} \sum_{(\sigma_1,\ldots,\sigma_s)\in Y_j} T_P(\sigma_1, \ldots, \sigma_n) \\
&\leqslant 2^{-n} \sum_{(\sigma_{s+1},\ldots,\sigma_n)} \sum_{j=1}^{t} h\,(L_z + 2(N(\sigma_{s+1}, \ldots, \sigma_n)\, t + j)) \\
&\leqslant 2^{-n} \left(L_z h\, td + \sum_{l=1}^{d} \sum_{j=1}^{t} (2h((l-1)t + j) \right) \\
&\leqslant 2^{-n} \left(2^{n+1} 2^n n^{-2} + 2h \sum_{i=1}^{dt} i \right) \leqslant 2^{-n} \left(2^{2n+1} n^{-2} + h(td)^2 \right) \\
&\leqslant 2^{-n} \left(2^{2n+1} n^{-2} + h 2^{2n} h^{-2} (1 + o(1)) \right) \leqslant 2^n n^{-1} (1 + o(1)).
\end{aligned}$$

Наконец, заметим, что любой булев оператор может быть вычислен программой, которая отличается от описанной выше только числом аргументов у операторов остановки. Поэтому среднее время работы построенной подобным образом программы первого типа не зависит от числа ее аргументов. Лемма 5 доказана.

Лемма 10. *Для произвольного булева (n, m)-оператора f справедливо неравенство*

$$T_{k,2}(f) \leqslant \frac{2^{n-1}(m+1)}{nk} (1 + o(1)).$$

ДОКАЗАТЕЛЬСТВО. Положим $s = \lfloor 2\log n \rfloor$, $h = \lfloor n - 4\log n \rfloor$, $t = \lceil 2^s/h \rceil$. Воспользуемся разложением (3). Каждую компоненту f_i оператора f представим в виде

$$f_i(x_1, \ldots, x_n) = \bigvee_{(\sigma_{s+1}, \ldots, \sigma_n)} \left(\bigvee_{j=1}^{t} f_{i,j,l}(x_1, \ldots, x_s)\, g_{j,l}\, (x_1, \ldots, x_n) \right).$$

Множество всех двоичных наборов длины s разобьем на непересекающиеся подмножества $Y_{j'}$ такие, что $\sigma \in Y_{j'}$, если $(j'-1)kh \leqslant N(\sigma) < j'hk$. Функции $f_{i,j,l}$ объединим в группы $\widehat{Y}_{j',l}$ так, что каждая группа, за исключением, быть может, последней, состоит из k функций, причем $f_{i,j,l} \in \widehat{Y}_{j',l}$, если $(j'-1)k \leqslant l < j'k$. Пусть $w = \lceil t/k \rceil$. Положим

$$\hat{g}_{j',l}(x_1, \ldots, x_n) = \bigvee_{r=1}^{k} g_{(j'-1)k+r,l}(x_1, \ldots, x_n).$$

Так как $f_{i,j,l}\, g_{q,l} = 0$ при $j \neq q$, то

$$f_i(x_1, \ldots, x_n) = \bigvee_{(\sigma_{s+1}, \ldots, \sigma_n)} \left(\bigvee_{j'=1}^{w} \left(\bigvee_{r=1}^{k} f_{i,(j'-1)k+r,l}(x_1, \ldots, x_s) \right) \hat{g}_{j',l}(x_1, \ldots, x_n) \right).$$

Программу, вычисляющую оператор f, представим в следующем виде:

$$P = P_0 P_1 \ldots P_l \ldots P_{2^{n-s}},$$

где P_0 — программа, вычисляющая все функции $f_{i,j,l}(x_1, \ldots, x_s)$ и все функции $g_{j,l}(x_1, \ldots, x_n)$, P_l — программа, вычисляющая функции $\bigvee_{j=1}^{t} f_{i,j,l}(x_1, \ldots, x_s)$ и имеющая вид

$$P_j = P_{j,1} \ldots P_{j',l} \ldots P_{w,l},$$

где $P_{j',l}$ — программа, вычисляющая $\hat{g}_{j',l}(x_1, \ldots, x_n)$, все функции $\hat{f}_{i,j',l} = \bigvee_{r=1}^{k} f_{i,(j'-1)k+r,l}(x_1, \ldots, x_s)$, останавливающая работу программы, если $\hat{g}_{j',l}(x_1, \ldots, x_n) = 1$, и объявляющая значение $\hat{f}_{i,j',l}$ значением i-й компоненты оператора f. Легко видеть, что каждая программа $P_{j',l}$ состоит не более чем из $m+1$ операторов: k-входовый оператор остановки вычисляет функцию $\hat{g}_{j',l}(x_1, \ldots, x_n)$, m операторов, каждый из которых имеет k входов, вычисляют функции $\hat{f}_{i,j',l}$. Очевидно, что для L_z — сложности схемной реализации всех возможных функций $f_{i,j,l}$ и функций $g_{j,l}(x_1, \ldots, x_n)$, справедливо неравенство (4). Так же легко видеть, что если наборы $(\sigma_1, \ldots, \sigma_s)$ и $(\sigma'_1, \ldots, \sigma'_s)$ принадлежат одному и тому же множеству $Y_{l'}$, то $T_P(\sigma_1, \ldots, \sigma_s, x_{s+1}, \ldots, x_n) = T_P(\sigma'_1, \ldots, \sigma'_s, x_{s+1}, \ldots, x_n)$ при всех $(x_{s+1}, \ldots, x_n)$. Положим $d = 2^{n-s}$. Тогда

$$\begin{aligned}
T(P) &= 2^{-n} \sum_{(\sigma_{s+1},\ldots,\sigma_n)} \sum_{(\sigma_1,\ldots,\sigma_s)} T_P(\sigma_1, \ldots, \sigma_n) \\
&= 2^{-n} \sum_{(\sigma_{s+1},\ldots,\sigma_n)} \sum_{j'=1}^{w} \sum_{(\sigma_1,\ldots,\sigma_s)\in Y_{j'}} T_P(\sigma_1, \ldots, \sigma_n) \\
&\leqslant 2^{-n} \sum_{j=1}^{d} \sum_{l'=1}^{w} (L_z + ((l-1)w + j')(m+1))hk \\
&\leqslant 2^{-n} \left(L_z dw + \sum_{j=1}^{d} \sum_{l'=1}^{w} ((l-1)w + j')(m+1)hk \right) \\
&\leqslant \left(L_z dw + \frac{(m+1)hk(dw)^2}{2} \right) \\
&\leqslant \left(\frac{2^{2n+1}}{n^2} + \frac{(m+1)hk2^{2n}(hk)^{-2}}{2} \right) (1 + o(1)) \\
&\leqslant \frac{2^{n-1}(m+1)}{nk} (1 + o(1)).
\end{aligned}$$

Лемма 10 доказана.

6. Программы с ограниченным числом операторов остановки

Приведем без доказательства результаты, касающиеся среднего времени работы программ с ограничениями на число условных остановок. Будем рассматривать программы первого типа, в которых число операторов остановки есть $o(\frac{2^n}{mn})$, и программы второго типа, в которых число операторов остановки есть $o(\frac{2^n}{n})$. Соответствующие функции Шеннона обозначим через $T'_{k,1}$ и $T'_{k,2}$. Справедлива следующая

Теорема 3. *Пусть k — константа. Тогда*

$$T'_{k,1}(n, m) = \frac{m2^{n-1}}{(k-1)n} (1 + o(1)),$$
$$T'_{k,2}(n, m) = \frac{m2^{n-1}}{(k-1)n} (1 + o(1)).$$

Доказательства верхних оценок теоремы легко получить, используя лемму 8, а нижние оценки доказываются так же, как и лемма 5, при этом число программ оценивается при помощи леммы 1.

Автор благодарен профессору О. Б. Лупанову за внимание к работе и Р. М. Колпакову, указавшему на некоторые неточности, содержавшиеся в первоначальном варианте статьи.

ЛИТЕРАТУРА

1. **Лупанов О. Б.** Об асимптотических оценках числа графов и сетей с n ребрами // Проблемы кибернетики. М.: Физматгиз, 1960. Вып. 4. С. 61–80.
2. **Лупанов О. Б.** О синтезе некоторых классов управляющих систем // Проблемы кибернетики. М.: Физматгиз, 1963. Вып. 9. С. 63–97.
3. **Чашкин А. В.** О среднем времени вычисления значений булевых функций // Дискрет. анализ и исслед. операций. Серия 1. 1997. Т. 4, № 1. С. 60–78.

Адрес автора:

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

Статья поступила
8 сентября 1997 г.