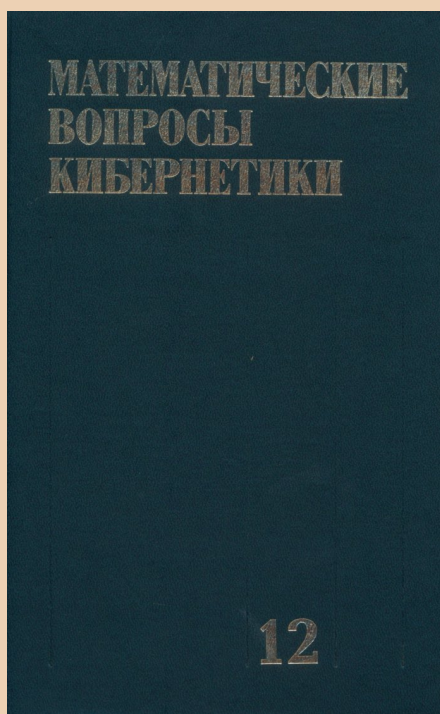




А. В. Чашкин

**Об одном методе
вычисления частичных
булевых функций**

Рекомендуемая форма библиографической ссылки:
Чашкин А. В. Об одном методе вычисления частичных
булевых функций // Математические вопросы кибернетики.
Вып. 12. — М.: ФИЗМАТЛИТ, 2003. — С. 231–246. URL:
<http://library.keldysh.ru/mvk.asp?id=2003-231>

ОБ ОДНОМ МЕТОДЕ ВЫЧИСЛЕНИЯ ЧАСТИЧНЫХ БУЛЕВЫХ ФУНКЦИЙ*)

А. В. ЧАШКИН

(МОСКВА)

§ 1. Введение

Весом частичной булевой функции называется число наборов в ее области определения, на которых значение функции равно единице. В настоящей работе изучается средняя сложность вычисления частичных булевых функций и частичных булевых функций данного веса неветвящимися программами с условной остановкой. Рассматриваемые программы обобщают понятие схемы из функциональных элементов и являются естественной моделью неветвящихся вычислений, т. е. вычислений, в которых нет условного перехода и косвенной адресации, но есть возможность досрочного прекращения работы при выполнении определенного условия. Такие вычисления можно представить следующим образом. Вычисления выполняет процессор, снабженный памятью, состоящей из отдельных ячеек. Эти ячейки будем обозначать символами y_i . В памяти выделяется особая ячейка, содержимое которой объявляется результатом работы программы. Эта ячейка обозначается символом z . Процессор работает под управлением программы, являющейся последовательностью вычислительных команд и команд остановки. Каждая вычислительная команда за единицу времени вычисляет значение некоторой двуместной булевой функции, аргументами которой являются величины, содержащиеся в определенных ячейках памяти. Вычисленный результат также помещается в одну из ячеек памяти. Команда остановки может прекратить выполнение программы. Каждая такая команда имеет единственный аргумент — содержимое некоторой ячейки памяти. Если значение аргумента равно единице, то процессор прекращает работу. Если значение аргумента равно нулю, то выполняется следующая команда программы. Различные вопросы, связанные со средним временем вычисления булевых функций неветвящимися программами с условной остановкой, изучались ранее в [5–8].

Сложность вычисления частичных булевых функций и булевых функций данного веса схемами из функциональных элементов изучалась в большом числе работ. Асимптотически точное поведение функции Шеннона для множества всех полностью определенных булевых функций данного веса найдено О. Б. Лупановым в [3]. Аналогичный результат для множества

*) Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (проект 02–01–00985), программы поддержки ведущих научных школ РФ (проект НШ–1807.2003.1) и программы "Университеты России" (проект УР.04.03.007).

частичных булевых функций, определенных на области данного размера, получен Л. А. Шоломовым в [10] и позднее А. Е. Андреевым в [1]. Методы, использованные в этих работах, существенным образом опираются на оценки Э. И. Нечипорука (см. [4]) мощности множества, содержащего доопределения всех частичных булевых функций определенного вида. Системы недоопределенных булевых функций изучались Л. А. Шоломовым в [9, 11]. Из опубликованных в этих работах результатов следует, в частности, асимптотически точная формула для функции Шеннона множества всех частичных булевых функций, вес которых незначительно отличается от размера области определения. Похожий результат независимо получен Н. Пиппенджером [14]. В последнее время в связи с изучением рандомизированных алгоритмов и их дерандомизации интерес к частичным булевым функциям заданного веса усилился. В 1999 г. П. Б. Милтерсеном в работе [13] было установлено*) асимптотически точное поведение функции Шеннона частичных функций, вес которых бесконечно мал относительно размера области определения. В результате общих усилий (работы [9, 13]) в настоящее время для функции Шеннона $L(n, m, w)$ множества всех частичных булевых функций, определенных на m -элементных областях и имеющих вес w , установлена асимптотически точная формула $L(n, m, w) \sim \log_2 \binom{m}{w} / \log_2 \log_2 \binom{m}{w} + O(n)$, справедливая для всех возможных значений m и всех значений веса w , не превосходящих $m/2$.

Средняя сложность частичных булевых функций заданного веса рассматривалась ранее в [8, 12], где было показано, что средняя сложность почти всех частичных булевых функций данного веса с точностью до постоянного множителя не зависит от размера области определения, а зависит только от веса. В [12], кроме того, обсуждалась связь частичных булевых функций и рандомизированных вычислений. В настоящей работе приводится новый метод вычисления частичных булевых функций, использование которого позволяет усилить результаты работ [8, 12].

§ 2. Основной результат

В этом параграфе дадим необходимые определения и сформулируем основную теорему о средней сложности частичных булевых функций.

Пусть $X = \{x_1, \dots, x_n\}$ — множество независимых булевых переменных. Введем множество переменных $Y = \{y_1, \dots, y_l\}$ и переменную z . Переменные из множества Y назовем *внутренними*, а переменную z — *выходной* переменной. Пусть, далее, $a \in Y \cup \{z\}$, $b, c \in X \cup Y \cup \{z\}$, f — булева функция, зависящая не более чем от двух переменных. *Вычислительной командой* p назовем выражение

$$p: \quad a = f(b, c),$$

переменную a назовем *выходом* этой команды, а переменные b, c — ее *входами*. Если переменная a является выходом команды p , то будем говорить, что команда p *изменяет значение этой переменной*, а если a не является выходом p , то будем говорить, что команда p *не изменяет ее значение*. Командой *остановки* p назовем выражение

$$p: \quad \text{Stop}(b),$$

а переменную b назовем *входом* этой команды.

*) В этой работе ошибочно утверждается, что полученный результат справедлив и в случае, когда вес функции равен по порядку размеру ее области определения.

Последовательность $P = p_1 \dots p_i \dots p_L$, состоящая из вычислительных команд и команд остановки, называется *неветвящейся программой с условной остановкой*, если при любом $j \in \{1, 2, \dots, L\}$ каждый вход команды p_j есть либо независимая переменная, либо выход некоторой вычислительной команды p_i , где $i < j$. Неветвящаяся программа работает в дискретные моменты времени $t = 0, 1, 2, \dots$, не изменяет значения независимых переменных и изменяет значения внутренних и выходных переменных. Значения $y_i(\mathbf{x}; t)$ внутренних переменных y_i и значение $z(\mathbf{x}; t)$ выходной переменной z программы P в произвольный момент времени t на наборе независимых переменных $\mathbf{x} = (x_1, \dots, x_n)$ определим индуктивно:

в начальный момент времени $t = 0$ значения всех внутренних и выходных переменных считаем неопределенными;

если команда p_t не изменяет значения внутренней переменной y_i (или выходной переменной z), то положим

$$y_i(\mathbf{x}; t) = y_i(\mathbf{x}; t - 1), \quad z(\mathbf{x}; t) = z(\mathbf{x}; t - 1);$$

если команда p_t изменяет значения внутренней переменной y_i (или выходной переменной z), и значения первого и второго входов команды p_t в момент времени $t - 1$ равны соответственно $b(\mathbf{x}; t - 1)$ и $c(\mathbf{x}; t - 1)$, то положим

$$\begin{aligned} y_i(\mathbf{x}; t) &= f_t(b(\mathbf{x}; t - 1), c(\mathbf{x}; t - 1)), \\ z(\mathbf{x}; t) &= f_t(b(\mathbf{x}; t - 1), c(\mathbf{x}; t - 1)). \end{aligned}$$

Значением команды p_t программы P на наборе независимых переменных $\mathbf{x} = (x_1, \dots, x_n)$ назовем значение ее выхода в момент времени t и обозначим через $p_t(\mathbf{x})$.

Пусть $p_{t_1}, \dots, p_{t_r}$ — все команды остановки программы P , причем $t_1 < \dots < t_r$. Тогда j -ю команду остановки программы P будем обозначать символом s_j , т. е. $s_j \equiv p_{t_j}$. Вычислительную команду p_i (переменную x_i) назовем *нулевым аргументом* команды остановки s_j и обозначим через q_j , если:

(i) выход команды p_i (переменная x_i) является входом команды s_j ;

(ii) среди вычислительных команд p_t , находящихся в программе между командами p_i и s_j , нет команды, выход которой совпадает с выходом команды p_i .

Вычислительную команду p_i назовем *первым аргументом* команды остановки s_j если:

(i) выходом команды p_i является переменная z ;

(ii) среди вычислительных команд p_t , находящихся в программе между командами p_i и s_j , нет команды, выходом которой является переменная z .

Будем говорить, что k -я команда остановки s_k *прекращает вычисления программы P на наборе $\mathbf{x}$* , если

$$q_1(\mathbf{x}) = \dots = q_{k-1}(\mathbf{x}) = 0, \quad q_k(\mathbf{x}) = 1.$$

Результат действия программы P на наборе $\mathbf{x}$ обозначим через $P(\mathbf{x})$ и определим следующим образом:

$$P(\mathbf{x}) = \begin{cases} z(\mathbf{x}; t_k), & \text{если } q_1(\mathbf{x}) = \dots = q_{k-1}(\mathbf{x}) = 0, \quad q_k(\mathbf{x}) = 1, \\ z(\mathbf{x}; L), & \text{если } q_1(\mathbf{x}) = \dots = q_r(\mathbf{x}) = 0, \end{cases}$$

т. е. $P(\mathbf{x})$ равно значению выходной переменной z в момент остановки программы. Легко видеть, что

$$\begin{aligned} P(\mathbf{x}) &= q_1(\mathbf{x})z(\mathbf{x}; t_1) \vee \bar{q}_1(\mathbf{x})q_2(\mathbf{x})z(\mathbf{x}; t_2) \vee \dots \\ &\dots \vee \bar{q}_1(\mathbf{x})\bar{q}_2(\mathbf{x}) \dots \bar{q}_{k-1}(\mathbf{x})q_k(\mathbf{x})z(\mathbf{x}; t_k) \vee \dots \\ &\dots \vee \bar{q}_1(\mathbf{x})\bar{q}_2(\mathbf{x}) \dots \bar{q}_{r-1}(\mathbf{x})q_r(\mathbf{x})z(\mathbf{x}; t_r) \vee \bar{q}_1(\mathbf{x})\bar{q}_2(\mathbf{x}) \dots \bar{q}_r(\mathbf{x})z(\mathbf{x}; L). \end{aligned}$$

Пусть $D \subseteq \{0, 1\}^n$ и $\mathbf{x} = (x_1, \dots, x_n)$ — набор независимых булевых переменных из D . Время работы программы P на наборе переменных $\mathbf{x}$ (число выполненных команд) обозначим через $T_P(\mathbf{x})$. Величину

$$T(P) = \frac{1}{|D|} \sum T_P(\mathbf{x}),$$

где суммирование производится по всем двоичным наборам из D , назовем *средним временем работы* программы P на области D . Если для некоторой частичной n -местной булевой функции $f: D \rightarrow \{0, 1\}$ и любого двоичного набора $\mathbf{x}$ из D справедливо равенство $f(\mathbf{x}) = P(\mathbf{x})$, то будем говорить, что *программа P вычисляет функцию f* . Величину

$$T(f) = \min T(P),$$

где минимум берется по всем программам, вычисляющим f , назовем *средней сложностью* функции f . Программу P , вычисляющую функцию f , для которой справедливо равенство $T(P) = T(f)$, назовем *минимальной* программой. Нетрудно видеть [7], что в минимальной программе разные команды остановки имеют разные нулевые аргументы.

В качестве примера рассмотрим программы $P_\vee$ и $P_\&$, вычисляющие соответственно дизъюнкцию и конъюнкцию четырех переменных $x_1, \dots, x_4$:

$$\begin{array}{ll} z = x_1 \vee x_2 & y = \overline{x_1 \& x_2} \\ \text{Stop}(z) & z = 0 \\ z = x_3 \vee x_4 & \text{Stop}(y) \\ & z = x_3 \& x_4 \end{array}$$

Первая команда программы $P_\vee$ вычисляет дизъюнкцию переменных x_1 и x_2 и объявляет вычисленное значение результатом работы программы. Вторая команда останавливает вычисления, если дизъюнкция равна единице. Если $x_1 \vee x_2 = 0$, то выполняется третья команда, которая вычисляет дизъюнкцию переменных x_3 и x_4 и объявляет ее значение результатом работы программы. Легко видеть, что вторая команда программы $P_\vee$ останавливает вычисления на 12 наборах (у каждого из этих наборов хотя бы на одном из первых двух мест стоит единица), т. е. программа $P_\vee$ на 12 наборах выполняет два действия, а на остальных четырех наборах — три. Следовательно,

$$T(P_\vee) = \frac{1}{16} (2 \cdot 12 + 3 \cdot 4) = 2\frac{1}{4}.$$

Нетрудно видеть, что среднее время работы второй программы равно $3\frac{1}{4}$.

Отметим, что неветвящаяся программа, не содержащая команды остановки и вычисляющая функцию, отличную от независимой переменной, является обычной схемой из функциональных элементов, базис которой состоит из всех не более чем двухместных булевых функций. Поэтому средняя сложность $T(f)$ любой булевой функции $f(\mathbf{x})$, существенно зависящей не менее чем от двух переменных, не больше ее схемной сложности $L(f)$.

Пусть $\{A_n\}_{n=1}^\infty$ — последовательность конечных множеств возрастающей мощности. Будем говорить, что *почти каждый* элемент множества A_n обладает свойством $\mathcal{B}$, если при $n \rightarrow \infty$ отношение числа элементов множества A_n , обладающих свойством $\mathcal{B}$, к мощности A_n стремится к единице.

Для частичной булевой функции f , определенной на области $D \subseteq \{0, 1\}^n$, положим

$$N_0(f) = |\{\mathbf{x} \in D \mid f(\mathbf{x}) = 0\}|, \quad N_1(f) = |\{\mathbf{x} \in D \mid f(\mathbf{x}) = 1\}|.$$

Основным результатом работы является следующая теорема.

Теорема. Пусть $D \subseteq \{0, 1\}^n$, $n \log_2 n \ll N_1(f) \leq \frac{1}{2}|D|$.

Тогда существуют такие постоянные c_1 и c_2 , что:

(i) для почти каждой частичной булевой функции $f: D \rightarrow \{0, 1\}$

$$T_D(f) \gtrsim \frac{c_1 N_1(f)}{\log_2 N_1(f)};$$

(ii) для каждой частичной булевой функции $f: D \rightarrow \{0, 1\}$

$$T_D(f) \lesssim \frac{c_2 N_1(f)}{\log_2 N_1(f)}.$$

Верхняя оценка теоремы доказывается в двух следующих параграфах. В первом из них устанавливаются вспомогательные утверждения о сложности схем из функциональных элементов, реализующих частичные булевы функции, а во втором (в лемме 8) на основе этих схем строятся неветвящиеся программы с условной остановкой с требуемым средним временем работы. При построении схем из функциональных элементов применяется новый метод вычисления частичных булевых функций, существенно отличающийся от ранее известных. Нижняя оценка теоремы устанавливается в пятом параграфе в лемме 10.

§ 3. Схемы из функциональных элементов

Если частичная функция f определена на области A , частичная функция h определена на области B , $B \subseteq A$, и $f(\mathbf{x}) = h(\mathbf{x})$ для каждого $\mathbf{x}$ из B , то будем говорить, что функция h является сужением функции f на область B , и обозначать это так: $h(\mathbf{x}) = f_B(\mathbf{x})$.

Лемма 1. Пусть $n \rightarrow \infty$, $D \subseteq \{0, 1\}^n$, $|D| \geq n$. Тогда для каждой частичной булевой функции f , определенной на области D ,

$$L(f) \lesssim \frac{6|D|}{\log_2 |D|} + O(n).$$

Доказательство настоящей леммы опирается на доказываемые ниже леммы 2–6. В лемме 2 устанавливается существование линейных операторов, которые вкладывают область определения частичной функции в булев куб меньшей размерности так, что множество образов нулевых аргументов и множество образов единичных аргументов частичной функции имеют незначительное пересечение. В леммах 2 и 3 показано, как, используя подобные операторы, свести вычисление частичной функции $f: D \rightarrow \{0, 1\}$ к вычислению двух полностью определенных булевых функций, зависящих от $O(\log_2 |D|)$ переменных, и одной частичной булевой функции, определенной на области вдвое меньшего размера, чем функция f . Далее показано, что повторное применение леммы 3 сводит вычисление частичной функции f к вычислению последовательности полностью определенных булевых функций, зависящих от последовательно уменьшающегося числа переменных.

Лемма 2. Пусть A , B — непересекающиеся подмножества $\{0, 1\}^n$, k — натуральное, $m = \lceil \log_2 |B| \rceil + k$. Тогда существует линейный оператор $\mathcal{L}: \{0, 1\}^n \rightarrow \{0, 1\}^m$ такой, что

$$|\{(\mathbf{x}, \mathbf{y}) \mid \mathbf{x} \in A, \mathbf{y} \in B, \mathcal{L}(\mathbf{x}) = \mathcal{L}(\mathbf{y})\}| \leq \frac{1}{2^k} |A|.$$

Доказательство. Обозначим через $F(n, m)$ множество всех линейных операторов $\mathcal{L}: \{0, 1\}^n \rightarrow \{0, 1\}^m$. Очевидно, что $|F(n, m)| = 2^{nm}$. Так как для любых двух несовпадающих наборов $\mathbf{x}$ и $\mathbf{y}$ из $\{0, 1\}^n$ имеется ровно 2^{n-1} различных n -местных линейных функций f с нулевым свободным членом, значения которых на этих наборах совпадают, т. е. $f(\mathbf{x}) = f(\mathbf{y})$, то в $F(n, m)$ имеется 2^{nm-m} различных операторов $\mathcal{L}$ таких, что $\mathcal{L}(\mathbf{x}) = \mathcal{L}(\mathbf{y})$. Следовательно, величина

$$2^{-nm} \sum_{\mathbf{x} \in A, \mathbf{y} \in B} 2^{nm-m} = 2^{-m} |A||B|$$

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

$$2^{-m} |A||B| \leq \frac{|A||B|}{2^k |B|} = \frac{1}{2^k} |A|$$

парах $(\mathbf{x}, \mathbf{y})$, $\mathbf{x} \in A$, $\mathbf{y} \in B$. Лемма доказана.

Лемма 3. Пусть $D \subseteq \{0, 1\}^n$, $f: D \rightarrow \{0, 1\}$, $D_0 = \{\mathbf{x} \in D \mid f(\mathbf{x}) = 0\}$ и $D_1 = \{\mathbf{x} \in D \mid f(\mathbf{x}) = 1\}$. Тогда существуют булева функция g и область $D'_0 \subseteq D_0$ такие, что

$$\begin{aligned} |D'_0| &\leq \frac{1}{2} |D_0|, \quad f(\mathbf{x}) = g(\mathbf{x}) \cdot f_{D_1 \cup D'_0}(\mathbf{x}), \\ L(g) &\lesssim \frac{4|D_1|}{\log_2 4|D_1|} \left(1 + O\left(\frac{\log_2 \log_2 |D_1|}{\log_2 |D_1|}\right)\right) + O\left(n \left\lceil \frac{\log_2 |D_1|}{\log_2 n} \right\rceil\right). \end{aligned}$$

Доказательство. К областям D_0 и D_1 применим лемму 2, полагая, что $k = 1$, $m = \lceil \log_2 |D_1| \rceil + 1$, $A = D_0$ и $B = D_1$. В результате найдется такой линейный оператор $\mathcal{L}: \{0, 1\}^n \rightarrow \{0, 1\}^m$, что множество

$$D'_0 = \{(\mathbf{x}, \mathbf{y}) \mid \mathbf{x} \in D_0, \mathbf{y} \in D_1, \mathcal{L}(\mathbf{x}) = \mathcal{L}(\mathbf{y})\}$$

состоит не более чем из $\frac{1}{2} |D_0|$ наборов. Введем m -местную булеву функцию

$$g'(\mathbf{y}) = \begin{cases} 1, & \text{если } \exists \mathbf{x} \in D_1 \text{ такой, что } \mathbf{y} = \mathcal{L}(\mathbf{x}), \\ 0 & \text{в противном случае} \end{cases}$$

и определенную на области D частичную n -местную булеву функцию $g(\mathbf{x}) = g'(\mathcal{L}(\mathbf{x}))$. Для каждого $\mathbf{x} \in D$ из равенства $g(\mathbf{x}) = g'(\mathcal{L}(\mathbf{x})) = 0$ следует, что $\mathbf{x} \in D_0$, т. е. $f(\mathbf{x}) = 0$. Поэтому

$$f_D(\mathbf{x}) = \begin{cases} f_{D_1 \cup D'_0}(\mathbf{x}), & \text{если } g(\mathbf{x}) = 1, \\ g(\mathbf{x}), & \text{если } g(\mathbf{x}) = 0, \end{cases}$$

и, следовательно,

$$f_D(\mathbf{x}) = g(\mathbf{x}) \cdot f_{D_1 \cup D'_0}(\mathbf{x}).$$

Так как $g(\mathbf{x}) = g'(\mathcal{L}(\mathbf{x}))$, сложность g не превосходит суммы $L(g') + L(\mathcal{L})$. Оценим сложности функции g' и линейного оператора $\mathcal{L}$. Функция g' зависит от $m = \lceil \log_2 |D_1| \rceil + 1$ аргументов, поэтому (см. [2])

$$L(g') \lesssim \frac{4|D_1|}{\log_2 4|D_1|} \left(1 + O\left(\frac{\log_2 \log_2 |D_1|}{\log_2 |D_1|}\right)\right). \quad (1)$$

Оператор $\mathcal{L}$ имеет n аргументов и m компонент. Следовательно, его сложность удовлетворяет неравенству

$$L(\mathcal{L}) = O\left(n \left\lceil \frac{\log_2 |D_1|}{\log_2 n} \right\rceil\right). \quad (2)$$

Складывая неравенства (1) и (2), получаем требуемую оценку сложности функции g . Лемма доказана.

Л е м м а 4. Пусть $D \subseteq \{0, 1\}^n$, $f: D \rightarrow \{0, 1\}$ и $\lceil 3 \log_2 |D| \rceil \geq n$. Тогда существуют булевы функции $p(\mathbf{x})$ и $q(\mathbf{x})$ и область $D' \subseteq D$ такие, что

$$f(\mathbf{x}) = p(\mathbf{x})(q(\mathbf{x}) \vee f_{D'}(\mathbf{x})), \quad |D'| \leq \frac{1}{2}|D|,$$

$$L(p, q) \lesssim \frac{3|D|}{\log_2 |D|} \left(1 + O\left(\frac{\log_2 \log_2 |D|}{\log_2 |D|}\right)\right).$$

Д о к а з а т е л ь с т в о. Положим $D_0 = \{\mathbf{x} \in D \mid f(\mathbf{x}) = 0\}$ и $D_1 = \{\mathbf{x} \in D \mid f(\mathbf{x}) = 1\}$. Без ограничения общности будем полагать, что $|D_1| \leq |D_0|$. К функции f применим лемму 3. В результате получим функцию p и область D'_0 , $D'_0 \subseteq D_0$, такие, что $|D'_0| \leq \frac{1}{2}|D_0|$ и

$$f(\mathbf{x}) = p(\mathbf{x}) \cdot f_{D_1 \cup D'_0}(\mathbf{x}), \quad (3)$$

а для сложности функции $p(\mathbf{x})$ справедливо неравенство

$$L(p) \lesssim \frac{4|D_1|}{\log_2 |D_1|} \left(1 + O\left(\frac{\log_2 \log_2 |D_1|}{\log_2 |D_1|}\right)\right) + O\left(n \left\lceil \frac{\log_2 |D_1|}{\log_2 n} \right\rceil\right). \quad (4)$$

Далее лемму 3 применим к определенной на области $D_1 \cup D'_0$ частичной функции $\overline{f_{D_1 \cup D'_0}}$, которая равна нулю на области D_1 и единице на области D'_0 . В результате получим функцию g и область D'_1 , $D'_1 \subseteq D_1$, такие, что $|D'_1| \leq \frac{1}{2}|D_1|$ и $\overline{f_{D_1 \cup D'_0}}(\mathbf{x}) = g(\mathbf{x}) \cdot \overline{f_{D'_1 \cup D'_0}}(\mathbf{x})$, или

$$f_{D_1 \cup D'_0}(\mathbf{x}) = \overline{g(\mathbf{x}) \cdot \overline{f_{D'_1 \cup D'_0}}(\mathbf{x})} = \overline{g(\mathbf{x})} \vee f_{D'_1 \cup D'_0}(\mathbf{x}), \quad (5)$$

а для сложности функции g справедливо неравенство

$$L(g) \lesssim \frac{4|D'_0|}{\log_2 |D'_0|} \left(1 + O\left(\frac{\log_2 \log_2 |D'_0|}{\log_2 |D'_0|}\right)\right) + O\left(n \left\lceil \frac{\log_2 |D'_0|}{\log_2 n} \right\rceil\right). \quad (6)$$

Положим $D' = D'_0 \cup D'_1$, $q(\mathbf{x}) = \overline{g(\mathbf{x})}$ и подставим равенство (3) в (5). В результате получим

$$f_D(\mathbf{x}) = p(\mathbf{x})(\overline{g(\mathbf{x})} \vee f_{D'_1 \cup D'_0}(\mathbf{x})) = p(\mathbf{x})(q(\mathbf{x}) \vee f_{D'}(\mathbf{x})).$$

Так как $|D| = |D_0| + |D_1|$, $|D'| = |D'_0| + |D'_1|$, $|D'_0| \leq \frac{1}{2}|D_0|$ и $|D'_1| \leq \frac{1}{2}|D_1|$, то очевидно, что $|D'| \leq \frac{1}{2}|D|$.

Оценим сложность системы функций $\{p, q\}$. По предположению $|D_1| \leq |D_0|$, потому $2|D_0| + 4|D_1| \leq 3|D|$. Теперь из очевидного равенства $L(p, q) = L(g, q)$, выпуклости функции $x/\log_2 x$, условия $\lceil 3 \log_2 |D| \rceil \geq n$ и неравенств (4) и (6), легко следует, что

$$L(p, q) \lesssim \frac{3|D|}{\log_2 |D|} \left(1 + O\left(\frac{\log_2 \log_2 |D|}{\log_2 |D|}\right)\right).$$

Лемма доказана.

Л е м м а 5. Пусть $D \subseteq \{0, 1\}^n$ и $\lceil 2 \log_2 |D| \rceil \geq n$. Тогда для сложности любой функции $f: D \rightarrow \{0, 1\}$ справедливо неравенство

$$L(f) \lesssim \frac{6|D|}{\log_2 |D|} \left(1 + O\left(\frac{\log_2 \log_2 |D|}{\log_2 |D|} \right) \right).$$

Д о к а з а т е л ь с т в о. Из леммы 4 следует существование области D_1 , $D_1 \subseteq D$, которая состоит не более чем из $\frac{1}{2}|D|$ наборов, и таких функций p_1 и q_1 , что

$$f_D(\mathbf{x}) = p_1(\mathbf{x})(q_1(\mathbf{x}) \vee f_{D_1}(\mathbf{x})), \quad (7)$$

причем сложность совместной реализации функций p_1 и q_1 удовлетворяет неравенству

$$L(p_1, q_1) \lesssim \frac{3|D|}{\log_2 |D|} \left(1 + O\left(\frac{\log_2 \log_2 |D|}{\log_2 |D|} \right) \right).$$

Далее рассмотрим функцию $f_{D_1}: D_1 \rightarrow \{0, 1\}$ и снова воспользуемся леммой 4. В результате получим новую область D_2 , $D_2 \subseteq D_1$, состоящую не более чем из $\frac{1}{2}|D_1| \leq \frac{1}{4}|D|$ наборов, и такие функции p_2 и q_2 , что

$$f_{D_1}(\mathbf{x}) = p_2(\mathbf{x})(q_2(\mathbf{x}) \vee f_{D_2}(\mathbf{x})),$$

причем сложность совместной реализации функций p_2 и q_2 удовлетворяет неравенству

$$\begin{aligned} L(p_2, q_2) &\lesssim \frac{3|D_1|}{\log_2 |D_1|} \left(1 + O\left(\frac{\log_2 \log_2 |D_1|}{\log_2 |D_1|} \right) \right) \lesssim \\ &\lesssim \frac{1}{2} \cdot \frac{3|D|}{\log_2 |D|} \left(1 + O\left(\frac{\log_2 \log_2 |D|}{\log_2 |D|} \right) \right). \end{aligned}$$

Будем повторять подобные рассуждения (применение леммы 4 к функциям f_{D_i}) до тех пор, пока размер очередной области D_s не станет меньше чем $\frac{|D|}{(\log_2 |D|)^3}$. Так как $\lceil 2 \log_2 |D| \rceil \geq n$, то $\left\lceil 3 \log_2 \frac{|D|}{(\log_2 |D|)^3} \right\rceil \geq n$, и, следовательно, лемма 4 может быть использована нужное число раз. В результате получим последовательность вложенных областей $D_s \subseteq \dots \subseteq D_i \subseteq \dots \subseteq D_1 \subseteq D$, в которой i -я область D_i состоит не более чем из $\frac{1}{2}|D_{i-1}| \leq \frac{1}{2^i}|D|$ наборов, и такие функции p_i и q_i ($i \in \{1, 2, \dots, s\}$), что

$$f_{D_{i-1}}(\mathbf{x}) = p_i(\mathbf{x})(q_i(\mathbf{x}) \vee f_{D_i}(\mathbf{x})), \quad (8)$$

причем сложность совместной реализации функций p_i и q_i удовлетворяет неравенству

$$\begin{aligned} L(p_i, q_i) &\lesssim \frac{3|D_{i-1}|}{\log_2 |D_{i-1}|} \left(1 + O\left(\frac{\log_2 \log_2 |D_{i-1}|}{\log_2 |D_{i-1}|} \right) \right) \lesssim \\ &\lesssim \frac{1}{2^{i-1}} \cdot \frac{3|D|}{\log_2 |D|} \left(1 + O\left(\frac{\log_2 \log_2 |D|}{\log_2 |D|} \right) \right). \quad (9) \end{aligned}$$

Из (7) и (8) легко получить, что

$$\begin{aligned} f(\mathbf{x}) &= p_1(\mathbf{x})(q_1(\mathbf{x}) \vee p_2(\mathbf{x})(q_2(\mathbf{x}) \vee \dots \\ &\dots p_i(\mathbf{x})(q_i(\mathbf{x}) \vee \dots p_s(\mathbf{x})(q_s(\mathbf{x}) \vee f_{D_s}(\mathbf{x})) \dots) \dots)), \end{aligned}$$

поэтому справедливо неравенство

$$L(f) \leq \sum_{i=1}^s L(p_i, q_i) + L(f_{D_s}) + 2s, \quad (10)$$

пользуясь которым, оценим сложность функции f .

Из (9) следует, что для суммы сложностей функций p_i и q_i справедливы следующие неравенства:

$$\begin{aligned} \sum_{i=1}^s L(p_i, q_i) &\lesssim \sum_{i=1}^s \frac{1}{2^{i-1}} \cdot \frac{3|D|}{\log_2 |D|} \left(1 + O\left(\frac{\log_2 \log_2 |D|}{\log_2 |D|}\right)\right) \lesssim \\ &\lesssim \frac{6|D|}{\log_2 |D|} \left(1 + O\left(\frac{\log_2 \log_2 |D|}{\log_2 |D|}\right)\right). \end{aligned} \quad (11)$$

Для вычисления функции f_{D_s} можно воспользоваться ее совершенной дизъюнктивной нормальной формой. Так как функция f_{D_s} равна единице не более чем на $|D_s|$ наборах (полагаем, что вне области D_s она принимает только нулевые значения), то ее СДНФ содержит не более $|D_s|$ элементарных конъюнкций, каждая из которых состоит из $O(\log_2 |D|)$ сомножителей. Поэтому легко видеть, что

$$L(f_{D_s}) = O(|D_s| \log_2 |D|).$$

Область D_s состоит не более чем из $|D|/(\log_2 |D|)^3$ наборов, поэтому $L(f_{D_s}) = O(|D|/(\log_2 |D|)^2)$. Подставляя полученную оценку вместе с (11) в (10), получаем требуемое неравенство для $L(f)$. Лемма доказана.

Лемма 6. Пусть $D \subseteq \{0, 1\}^n$, $f: D \rightarrow \{0, 1\}$ и $l = \lceil 2 \log_2 |D| \rceil$. Если $l < n$, то существуют целое m , $m \leq l$, линейный оператор $\mathcal{L}: \{0, 1\}^n \rightarrow \{0, 1\}^m$ и частичная m -местная функция $h: \mathcal{L}(D) \rightarrow \{0, 1\}$ такие, что $f(\mathbf{x}) = h(\mathcal{L}(\mathbf{x}))$

для каждого $\mathbf{x}$ из D .

Доказательство. Положим $D_0 = \{\mathbf{x} \in D \mid f(\mathbf{x}) = 0\}$, $D_1 = \{\mathbf{x} \in D \mid f(\mathbf{x}) = 1\}$ и $m = \lceil \log_2 |D_0| \rceil + \lceil \log_2 |D_1| \rceil + 1$. Легко видеть, что $m \leq l$. К областям D_0 и D_1 применим лемму 2 с $k = \lceil \log_2 |D_0| \rceil + 1$, $A = D_0$ и $B = D_1$. Из этой леммы следует существование такого линейного оператора $\mathcal{L}: \{0, 1\}^n \rightarrow \{0, 1\}^m$, что

$$|\{(\mathbf{x}, \mathbf{y}) \mid \mathbf{x} \in D_0, \mathbf{y} \in D_1, \mathcal{L}(\mathbf{x}) = \mathcal{L}(\mathbf{y})\}| \leq \frac{1}{2^k} |D_0| < 1.$$

Следовательно, $\mathcal{L}(\mathbf{x}) \neq \mathcal{L}(\mathbf{y})$, если $f(\mathbf{x}) \neq f(\mathbf{y})$ для всех $\mathbf{x}$ и $\mathbf{y}$ из D . Воспользуемся этим свойством оператора $\mathcal{L}$ и определим требуемую m -местную булеву функцию h равенством

$$h(\mathbf{y}) = \begin{cases} f(\mathbf{x}), & \text{если } \exists \mathbf{x} \in D \text{ такой, что } \mathbf{y} = \mathcal{L}(\mathbf{x}), \\ 0, & \text{если } \mathbf{y} \neq \mathcal{L}(\mathbf{x}) \text{ для любого } \mathbf{x} \in D. \end{cases}$$

Легко видеть, что равенство $f(\mathbf{x}) = h(\mathcal{L}(\mathbf{x}))$ выполняется для каждого $\mathbf{x} \in D$. Лемма доказана.

Доказательство леммы 1. Если $\lceil 2 \log_2 |D| \rceil \geq n$, то требуемая оценка следует из леммы 5.

Если $\lceil 2 \log_2 |D| \rceil < n$, то положим $m = \lceil 2 \log_2 |D| \rceil$ и воспользуемся леммой 6. Из этой леммы следует существование линейного оператора $\mathcal{L}: \{0, 1\}^n \rightarrow \{0, 1\}^m$ и частичной m -местной функции h таких, что $f(\mathbf{x}) = h(\mathcal{L}(\mathbf{x}))$ для каждого $\mathbf{x} \in D$. Поэтому

$$L(f) \leq L(h) + L(\mathcal{L}).$$

Сложность оператора $\mathcal{L}$ равна $O\left(\frac{n \log_2 |D|}{\log_2 n}\right)$, а из леммы 5 следует, что $L(h)$ — сложность функции h — асимптотически не превосходит $\frac{6|D|}{\log_2 |D|}$, поэтому

$$L(f) \lesssim \frac{6|D|}{\log_2 |D|} + O\left(\frac{n \log_2 |D|}{\log_2 n}\right).$$

Наконец, заметим, что если $|D| = O(n \log_2 n)$ и $|D| \geq n$, то $\frac{n \log_2 |D|}{\log_2 n} = O(n)$, а если $n \log_2 n = o(|D|)$, то $\frac{n \log_2 |D|}{\log_2 n} = o\left(\frac{|D|}{\log_2 |D|}\right)$. Поэтому

$$L(f) \lesssim \frac{6|D|}{\log_2 |D|} + O(n).$$

Лемма доказана.

Напомним, что число наборов, на которых частичная булева функция $f: D \rightarrow \{0, 1\}$ равна нулю, обозначается через $N_0(f)$, а число наборов, на которых она равна единице, — через $N_1(f)$.

Л е м м а 7. Пусть $n \rightarrow \infty$, $D \subseteq \{0, 1\}^n$. Тогда для каждой частичной булевой функции f , определенной на области D и такой, что $n \log_2 n \ll \ll N_1(f) \leq \frac{1}{2}|D|$, справедливо неравенство

$$L(f) \lesssim \frac{4N_1(f) \log_2 \frac{16|D|}{N_1(f)}}{\log_2 N_1(f)}.$$

Доказательство. Положим $D_0 = \{\mathbf{x} \in D \mid f(\mathbf{x}) = 0\}$ и $D_1 = \{\mathbf{x} \in D \mid f(\mathbf{x}) = 1\}$. К функции f применим лемму 3. В результате получим функцию g_1 и область $D_{01} \subseteq D_0$ такие, что

$$\begin{aligned} |D_{01}| &\leq \frac{1}{2}|D_0|, \\ f(\mathbf{x}) &= g_1(\mathbf{x}) \cdot f_{D_1 \cup D_{01}}(\mathbf{x}), \end{aligned} \quad (12)$$

а для сложности функции g_1 справедливо неравенство

$$L(g_1) \lesssim \frac{4|D_1|}{\log_2 |D_1|} \left(1 + O\left(\frac{\log_2 \log_2 |D_1|}{\log_2 |D_1|}\right)\right) + O\left(n \left\lceil \frac{\log_2 |D_1|}{\log_2 n} \right\rceil\right).$$

Далее лемму 3 применим к функции $f_{D_1 \cup D_{01}}$. В результате получим новую область $D_{02} \subseteq D_{01}$ и новую функцию g_2 . К функции g_2 снова применим лемму 3 и т. д. После i -го применения леммы 3 получим функцию g_i и область $D_{0i} \subseteq D_{0(i-1)}$ такие, что

$$\begin{aligned} |D_{0i}| &\leq \frac{1}{2}|D_{0(i-1)}|, \\ f_{D_1 \cup D_{0(i-1)}}(\mathbf{x}) &= g_i(\mathbf{x}) \cdot f_{D_1 \cup D_{0i}}(\mathbf{x}), \end{aligned} \quad (13)$$

а для сложности функции g_i справедливо неравенство

$$L(g_i) \lesssim \frac{4|D_1|}{\log_2 |D_1|} \left(1 + O\left(\frac{\log_2 \log_2 |D_1|}{\log_2 |D_1|}\right)\right) + O\left(n \left\lceil \frac{\log_2 |D_1|}{\log_2 n} \right\rceil\right),$$

из которого с учетом условия $N_1(f) \gg n \log_2 n$ легко следует оценка

$$L(g_i) \lesssim \frac{4|D_1|}{\log_2 |D_1|}. \quad (14)$$

Будем порождать функции g_i и области D_{0i} до тех пор, пока размер очередной области не станет меньше $|D_1|$. Так как на каждом шаге размер порождаемой области уменьшается не меньше чем в два раза, то общее число шагов не превысит величины $s = \lceil \log_2 \frac{|D_0|}{|D_1|} \rceil \leq \lceil \log_2 \frac{|D|}{N_1(f)} \rceil$.

Из (12) и (13) легко следует, что

$$\begin{aligned} f(\mathbf{x}) &= g_1(\mathbf{x}) \cdot f_{D_1 \cup D_{01}}(\mathbf{x}) = g_1(\mathbf{x}) \cdot g_2(\mathbf{x}) \cdot f_{D_1 \cup D_{02}}(\mathbf{x}) = \dots \\ &= g_1(\mathbf{x}) \cdot g_2(\mathbf{x}) \cdot \dots \cdot g_s(\mathbf{x}) \cdot f_{D_1 \cup D_{0s}}(\mathbf{x}). \end{aligned}$$

Поэтому $L(f) \leq \sum_{i=1}^s L(g_i) + L(f_{D_1 \cup D_{0s}}) + s$. В силу леммы 1 сложность функции $f_{D_1 \cup D_{0s}}$ асимптотически не превосходит величины $\frac{12|D_1|}{\log_2 |D_1|}$. Таким образом, учитывая (14), для сложности функции f имеем следующие неравенства:

$$L(f) \lesssim \frac{4|D_1| \cdot s}{\log_2 |D_1|} + \frac{12|D_1|}{\log_2 |D_1|} \lesssim \frac{4|D_1|(s+3)}{\log_2 |D_1|} \lesssim \frac{4N_1(f) \log_2 \frac{16|D|}{N_1(f)}}{\log_2 N_1(f)}.$$

Лемма доказана.

§ 4. Верхняя оценка средней сложности

Лемма 8. Пусть $D \subseteq \{0, 1\}^n$, $n \log_2 n \ll N_1(f) \leq \frac{1}{2}|D|$. Тогда для каждой частичной булевой функции $f: D \rightarrow \{0, 1\}$ справедливо неравенство

$$T_D(f) \lesssim \frac{16N_1(f)}{\log_2 N_1(f)}.$$

Доказательство. Как и ранее, положим $D_0 = \{\mathbf{x} \in D \mid f(\mathbf{x}) = 0\}$ и $D_1 = \{\mathbf{x} \in D \mid f(\mathbf{x}) = 1\}$. Для построения программы P , вычисляющей f , воспользуемся полученным в предыдущей лемме представлением

$$f(\mathbf{x}) = g_1(\mathbf{x}) \cdot g_2(\mathbf{x}) \cdot \dots \cdot g_s(\mathbf{x}) \cdot f_{D_1 \cup D_{0s}}(\mathbf{x})$$

функции f , в котором функция g_1 определена на области $D = D_1 \cup D_0$, при $i = 2, \dots, s$ функции g_i определены на областях $D_1 \cup D_{0(i-1)}$, при $i = 1, \dots, s$ размер области D_{0i} не превосходит $2^{-i}|D_0|$, и для функций g_i и функции $f_{D_1 \cup D_{0s}}$ справедливы неравенства

$$L(g_i) \lesssim \frac{4|D_1|}{\log_2 |D_1|}, \quad L(f_{D_1 \cup D_{0s}}) \lesssim \frac{12|D_1|}{\log_2 |D_1|}. \quad (15)$$

Опишем работу программы P на произвольном наборе $\mathbf{y}$. Эта программа строится на основе схем из функциональных элементов, вычисляющих функции g_i , и работает следующим образом. Сначала вычисляется значение $g_1(\mathbf{y})$. Если $g_1(\mathbf{y}) = 0$, то программа останавливается, и полагается, что $f(\mathbf{y}) = 0$. Если $g_1(\mathbf{y}) = 1$, то вычисляется значение $g_2(\mathbf{y})$. Если $g_2(\mathbf{y}) = 0$, то программа останавливается, и полагается, что $f(\mathbf{y}) = 0$. Если $g_2(\mathbf{y}) = 1$, то вычисляется значение $g_3(\mathbf{y})$ и т. д. Если $g_s(\mathbf{y}) = 1$, то значение $f(\mathbf{y})$ получается в результате работы программы, вычисляющей частичную функцию $f_{D_1 \cup D_{0s}}$.

Оценим сверху среднее время работы программы P . Положим $D_{00} = D_0$. Легко видеть, что первые $L(g_1) + 1$ команд программы P выполняются на всех наборах области D , следующие $L(g_2) + 1$ команд программы P выполняются на наборах из области $D_1 \cup D_{01}$, следующие $L(g_3) + 1$ команд — на наборах из $D_1 \cup D_{02}$ и т. д. Наконец, последние $L(f_{D_1 \cup D_{0s}})$ команд программы P выполняются на наборах из $D_1 \cup D_{0s}$. Поэтому, в силу оценок (15), справедливы неравенства

$$\begin{aligned} T_D(P) &\lesssim \frac{1}{|D|} \left(\sum_{i=1}^s L(g_i) |D_1 \cup D_{0(i-1)}| + L(f_{D_1 \cup D_{0s}}) |D| \right) \lesssim \\ &\lesssim \frac{4N_1(f)}{|D| \log_2 N_1(f)} \left(s |D_1| + \sum_{i=1}^s |D_{0(i-1)}| + 3 \cdot 2 |D_1| \right). \end{aligned}$$

Так как $|D_{0i}| \leq 2^{-i} |D_0|$ и $|D_1| < |D_{s-1}| \leq 2^{s-1} |D_0|$, то, продолжая предыдущее неравенство, имеем

$$\begin{aligned} T_D(P) &\lesssim \frac{4N_1(f)}{|D| \log_2 N_1(f)} \left(4 |D_1| + (s+1) |D_1| + |D_1| + \sum_{i=1}^s 2^{-(i-1)} |D_0| \right) \leq \\ &\leq \frac{4N_1(f)}{|D| \log_2 N_1(f)} \left(4 |D_1| + \frac{s+1}{2^{s-1}} |D_0| + \frac{1}{2^{s-1}} |D_0| + \left(2 - \frac{1}{2^{s-1}} \right) |D_0| \right) \leq \\ &\leq \frac{4N_1(f)}{|D| \log_2 N_1(f)} (4 |D_1| + 4 |D_0|) = \frac{16N_1(f)}{\log_2 N_1(f)}. \end{aligned}$$

Лемма доказана.

§ 5. Нижняя оценка средней сложности

Оценим число различных программ, состоящих из данного числа команд. Для этого каждой программе P , входам которой приписаны переменные $x_1, \dots, x_n$, поставим в соответствие ориентированный граф G_P без кратных ребер. Каждый такой граф зададим списком из девяти условий, которые будут определять его вершины, ребра и метки вершин и ребер. Первые пять условий определяют вершины и метки вершин графа G_P .

(1) Каждой переменной x_i и каждой команде p_j программы P поставим в соответствие вершину графа G_P .

(2) Вершине, соответствующей переменной x_i , припишем символ x_i .

(3) Вершине, соответствующей вычислительной команде $p_j: a = f_j(b, c)$, припишем символ f_j .

(4) Вершине, соответствующей команде остановки, припишем слово Stop.

(5) Вершине, соответствующей последней команде с выходом z , припишем символ z .

Следующие два условия определяют ребра и метки ребер графа. Ребра в свою очередь определяют порядок выполнения команд, находящихся между двумя последовательными командами остановки.

(6) Вершины u_i и u_j связаны ребром, направленным от u_i к u_j , если:

(i) вершина u_j соответствует вычислительной команде p , вершина u_i соответствует вычислительной команде p' (независимой переменной x_i);

(ii) команда p' (переменная x_i) является s -м аргументом команды p , $1 \leq s \leq 2$; каждое такое ребро назовем *функциональным* и припишем ему символ s .

(7) Вершины u_i и u_j связаны ребром, направленным от u_i к u_j , если:

(i) вершина u_j соответствует команде остановки s_i , вершина u_i соответствует вычислительной команде p' (независимой переменной x_i);

(ii) команда p' (переменная x_i) является нулевым аргументом команды s_i ;

каждое такое ребро назовем *функциональным* и припишем ему символ 0.

Последние два условия определяют порядок выполнения команд остановки и устанавливают связь между командами остановки и командами, вычисляющими значения выходной переменной z .

(8) Вершины u_i и u_j связаны ребром, направленным от u_i к u_j , если они соответствуют командам, являющимся l -й и $(l+1)$ -й командами остановки программы P ; каждое такое ребро назовем *ребром остановки*.

(9) Вершины u_i и u_j связаны ребром, направленным от u_i к u_j , если:

(i) вершина u_j соответствует команде остановки s_i , вершина u_i соответствует вычислительной команде p ;

(ii) команда p является первым аргументом команды s_i , не является нулевым аргументом этой команды и не является первым аргументом другой команды $s_{i'}$ при $t' < t$;

каждое такое ребро назовем *особым* и припишем ему символ 1.

Заметим, что особые ребра не могут выходить из вершин, соответствующих нулевым аргументам команд остановки.

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

Через $N(n, L)$ обозначим число неизоморфных приведенных программ в базисе из всех не более чем двухместных булевых функций, содержащих не более L команд и имеющих n входов.

Л е м м а 9. *Справедливо неравенство*

$$N(n, L) \leq (c(L+n))^{(4/3)L+n},$$

где c — некоторая постоянная.

Доказательство. Оценим число графов, соответствующих рассматриваемым программам. Пусть L_1 — число вычислительных команд в программе, а L_2 — число команд остановки. Очевидно, что $L = L_1 + L_2$, и каждый граф содержит не более $L+n$ вершин. Оценим число ребер.

Число особых ребер обозначим через N . Из каждой вершины, соответствующей вычислительной команде, выходит не более одного особого ребра. Очевидно, что из вершин, соответствующих командам остановки и их нулевым аргументам, особые ребра не выходят. Поэтому $N \leq L_1 - L_2 + n$. С другой стороны, в каждую вершину, соответствующую команде остановки, входит не более одного особого ребра. Поэтому также справедливо неравенство $N \leq L_2$. Объединяя два последних неравенства, при любом γ из $[0, 1]$ имеем

$$N \leq (1-\gamma)(L_1 - L_2 + n) + \gamma L_2.$$

Каждый граф содержит $L_2 - 1$ ребро остановки и не более $2L_1 + L_2$ функциональных ребер. Следовательно, общее число ребер не больше, чем $2L_1 + 2L_2 + N$. Известно (см. [3]), что число различных связанных графов с p вершинами и q ребрами не превосходит величины $a^p q^{q-p}$, где a — некоторая константа. Поэтому легко видеть, что число рассматриваемых графов тем больше, чем больше R — разность числа ребер и вершин. Преобразуем эту разность:

$$R = 2L_1 + 2L_2 + N - L - n \leq$$

$$\leq L_1 + L_2 + (1-\gamma)(L_1 - L_2 + n) + \gamma L_2 - n \leq (2-\gamma)L_1 + \gamma 2L_2 - \gamma n.$$

Положим $\gamma = \frac{2}{3}$. Тогда $R \leq \frac{1}{3}(4L - 2n)$. Теперь, учитывая число способов, которыми можно пометить ребра и вершины графов, получаем, что

$$N(n, L) \leq (c(L + n))^{(4/3)L + n},$$

где c — постоянная. Лемма доказана.

Пусть f — частичная n -местная булева функция, определенная на области D , P — программа, вычисляющая f . Каждому двоичному набору $\mathbf{x}$ из D , рассматриваемому как двоичная запись натурального числа, поставим в соответствие его номер $N_P(\mathbf{x})$ такой, что $1 \leq N_P(\mathbf{x}) \leq |D|$; $N_P(\mathbf{x}) < N_P(\mathbf{y})$, если $T_P(\mathbf{x}) < T_P(\mathbf{y})$; $N_P(\mathbf{x}) < N_P(\mathbf{y})$, если $T_P(\mathbf{x}) = T_P(\mathbf{y})$ и $\mathbf{x} < \mathbf{y}$.

Лемма 10. Пусть $D \subseteq \{0, 1\}^n$, $n \log_2 n \ll w \leq \frac{1}{2}|D|$ и $n \rightarrow \infty$. Тогда для почти каждой частичной булевой функции f , определенной на области D и такой, что $N_1(f) = w$, справедливо неравенство

$$T(f) \gtrsim \frac{1}{4} \cdot \frac{w}{\log_2 w}.$$

Доказательство. Рассмотрим множество R , состоящее из всех частичных функций, определенных на D и принимающих значение 1 ровно на w наборах, для которых справедливо неравенство

$$T_D(f) < (1 - 3\varepsilon) \frac{w}{4 \log_2 w}, \quad (16)$$

где ε — произвольное положительное число не превосходящее $1/3$. Оценим $|R|$. Пусть f — функция из R , P — программа, которая вычисляет функцию f и для которой справедлива оценка (16). Пусть, далее, $\mathbf{x}_0$ — некоторый набор из D и P' — начальная часть программы P достаточная для вычисления значений функции f на всех наборах с номерами, не превосходящими номер набора $\mathbf{x}_0$. Тогда из определения среднего времени работы программы следует, что

$$T(P) = \frac{1}{|D|} \sum_{\mathbf{y} \in D} T_P(\mathbf{y}) > \frac{1}{|D|} \sum_{\mathbf{y} | N_P(\mathbf{y}) > N_P(\mathbf{x}_0)} T_P(\mathbf{y}) \geq \frac{|D| - N_P(\mathbf{x}_0)}{|D|} T_P(\mathbf{x}_0).$$

Положим $T = (1 - 3\varepsilon) \frac{w}{4 \log_2 w}$. Так как $T(P) = T_D(f) < T$, то из предыдущего неравенства легко видеть, что

$$T_P(\mathbf{x}_0) < \frac{T \cdot |D|}{|D| - N_P(\mathbf{x}_0)}. \quad (17)$$

Каждая функция однозначно определяется первыми $T_P(\mathbf{x}_0)$ командами своей минимальной программы P и двоичным вектором длины не более чем $|D| - N_P(\mathbf{x}_0)$, состоящим из значений функции f на тех аргументах, время работы программы P на которых больше времени ее работы на $\mathbf{x}_0$. Поэтому число функций в R не превосходит произведения $N(T_P(\mathbf{x}_0), n) \sum_{i=0}^w \binom{|D| - N_P(\mathbf{x}_0)}{i}$. Из леммы 9 и неравенства (17) следует, что

$$\log_2 |R| \leq \left(\frac{4}{3} \cdot \frac{T|D|}{|D| - N_P(\mathbf{x}_0)} + n \right) \log_2 \left(c \left(\frac{T|D|}{|D| - N_P(\mathbf{x}_0)} + n \right) \right) + \log_2 \sum_{i=0}^w \binom{|D| - N_P(\mathbf{x}_0)}{i}. \quad (18)$$

Далее рассмотрим два случая: $\frac{1}{3}|D| \leq w \leq \frac{1}{2}|D|$; $w < \frac{1}{3}|D|$.

Пусть $\frac{1}{3}|D| \leq w \leq \frac{1}{2}|D|$. В этом случае в качестве $\mathbf{x}_0$ возьмем набор с номером $N_P(\mathbf{x}_0) = |D| - w$. Тогда, учитывая справедливое при достаточно больших n неравенство $\varepsilon w \geq 4n \log_2 n$, имеем

$$\frac{4}{3} \left(\frac{T \cdot |D|}{|D| - N_P(\mathbf{x}_0)} \right) + n = \frac{4T \cdot |D|}{3w} + n \leq \frac{4T \cdot 3w}{3w} + n \leq \frac{(1-2\varepsilon)w}{\log_2 w},$$

$$\sum_{i=0}^w \binom{|D| - N_P(\mathbf{x}_0)}{i} = \sum_{i=0}^w \binom{w}{i} = 2^w.$$

Поэтому из неравенства (18) следует, что

$$\log_2 |R| \leq \frac{(1-2\varepsilon)w}{\log_2 w} \log_2 \left(c \left(\frac{(1-2\varepsilon)w}{\log_2 w} + n \right) \right) + \log_2 2^w \leq 2w - 2w\varepsilon. \quad (19)$$

С другой стороны, для любой положительной постоянной ε при $n \rightarrow \infty$ справедливо неравенство

$$\binom{|D|}{w} \geq \binom{2w}{w} \geq 2^{(2-\varepsilon)w}. \quad (20)$$

Таким образом, сравнивая (19) и (20), видим, что имеет место неравенство

$$|R| < 2^{-\varepsilon w} \binom{|D|}{w} = o\left(\binom{|D|}{w}\right),$$

т. е. при $\frac{1}{3}|D| \leq w \leq \frac{1}{2}|D|$ утверждение леммы справедливо.

Рассмотрим второй случай когда $w < \frac{1}{3}|D|$. Пусть набор $\mathbf{x}_0 \in D$ такой, что $N_P(\mathbf{x}_0) = \lfloor \frac{1}{3}|D| \rfloor$. Тогда, как и в предыдущем случае, имеем

$$\frac{4}{3} \left(\frac{T \cdot |D|}{|D| - N_P(\mathbf{x}_0)} \right) + n \leq \frac{3 \cdot 4T \cdot |D|}{3 \cdot 2|D|} + n \leq \frac{(1-2\varepsilon)w}{2 \log_2 w}. \quad (21)$$

Кроме того, так как

$$\left(\left\lceil \frac{2}{3}|D| \right\rceil \right) / \binom{|D|}{w} \leq \frac{\left(\frac{2}{3}|D| + 1 \right) \frac{2}{3}|D| \cdots \left(\frac{2}{3}|D| - w + 2 \right)}{|D|(|D| - 1) \cdots (|D| - w + 1)} \leq$$

$$\leq \left(\frac{\frac{2}{3}|D| + 1}{|D|} \right)^w \leq \left(\frac{2}{3} \right)^w \left(1 + \frac{3}{2|D|} \right)^{(1/3)|D|} \leq 2^{-(1/2)w},$$

то для любой положительной постоянной ε при $n \rightarrow \infty$ справедливо неравенство

$$\sum_{i=0}^w \binom{|D| - N_P(\mathbf{x}_0)}{i} \leq \sum_{i=0}^w \binom{\left\lceil \frac{2}{3}|D| \right\rceil}{i} \leq w \binom{\left\lceil \frac{2}{3}|D| \right\rceil}{w} = 2^{-(1/2)(1-\varepsilon)w} \binom{|D|}{w}. \quad (22)$$

Подставляя оценки (21) и (22) в (18), имеем

$$\log_2 |R| \leq \frac{(1-2\varepsilon)w}{2 \log_2 w} \log_2 \left(c \left(\frac{(1-2\varepsilon)w}{2 \log_2 w} + n \right) \right) - \frac{1}{2}(1-\varepsilon)w + \log_2 \binom{|D|}{w} \leq$$

$$\leq \frac{1}{2}(1-2\varepsilon)w - \frac{1}{2}(1-\varepsilon)w + \log_2 \binom{|D|}{w} \leq -\frac{1}{2}\varepsilon w + \log_2 \binom{|D|}{w}.$$

Следовательно,

$$|R| < 2^{-\frac{1}{2}\varepsilon w} \binom{|D|}{w} = o\left(\binom{|D|}{w}\right),$$

т. е. и при $w \leq \frac{1}{3}|D|$ утверждение леммы также справедливо. Лемма доказана полностью.

§ 6. Заключение

Сделаем несколько замечаний о результатах настоящей работы. Прежде всего отметим, что конструкции схем из лемм 1 и 7 (являющихся в настоящей работе вспомогательными утверждениями) хотя и не являются асимптотически минимальными, тем не менее представляют и самостоятельный интерес. Это связано прежде всего с достаточно простой структурой этих схем, а также с тем, что их глубины легко могут быть сделаны минимальными по порядку, а при более чем полиномиальных размерах областей определения и асимптотически минимальными.

Также заметим, что приведенные в леммах 8 и 10 верхняя и нижняя оценки средней сложности не являются наилучшими. В частности, верхнюю оценку средней сложности частичных функций можно понизить не менее чем в четыре раза. К сожалению, доказательство этой уточненной оценки достаточно громоздко. Нижнюю оценку из леммы 10 также можно улучшить. Например, для функций, вес которых есть о-малое от размера области определения, ее можно повысить не менее чем в четыре раза. Однако, как и для верхней оценки, доказательство более точной нижней оценки в общем случае становится слишком длинным.

Наконец, заметим, что, несколько удлинив доказательства лемм 7 и 10, нетрудно показать, что утверждение теоремы остается справедливым если в ее формулировке неравенство $N_1(f) \gg n \log_2 n$ заменить более слабым неравенством $N_1(f) \geq n \log_2 n$.

СПИСОК ЛИТЕРАТУРЫ

1. Андреев А. Е. О сложности реализации частичных булевых функций схемами из функциональных элементов // Дискретная математика. — 1989. — Т. 1, вып. 4. — С. 36–45.
2. Лупанов О. Б. О синтезе некоторых классов управляющих систем // Проблемы кибернетики. Вып. 10. — М.: Физматгиз, 1963. — С. 63–97.
3. Лупанов О. Б. Об одном подходе к синтезу управляющих систем — принципе локального кодирования // Проблемы кибернетики. Вып. 14. — М.: Наука, 1965. — С. 31–110.
4. Нечипорук Э. И. О сложности вентильных схем, реализующих булевские матрицы с неопределенными элементами // ДАН. — 1965. — Т. 163, № 1. — С. 40–42.
5. Чашкин А. В. О среднем времени вычисления значений булевых функций // Дискретный анализ и исследование операций. — 1997. — Т. 4, № 1. — С. 60–78.
6. Чашкин А. В. О среднем времени вычисления булевых операторов // Дискретный анализ и исследование операций. — 1998. — Т. 5, № 1. — С. 88–103.
7. Чашкин А. В. Среднее время вычисления значений элементарных булевых функций // Дискретная математика. — 2000. — Т. 12, вып. 4. — С. 109–120.
8. Чашкин А. В. Средняя сложность булевых функций // Дискретная математика и ее приложения: сборник лекций. — М.: Изд-во Центра прикладных исследований при механико-математическом факультете МГУ. — 2001. — С. 145–170.
9. Шоломов Л. А. О функционалах, характеризующих сложность систем недоопределенных булевых функций // Проблемы кибернетики. Вып. 19. — М.: Наука, 1967. — С. 123–140.
10. Шоломов Л. А. О реализации недоопределенных булевых функций схемами из функциональных элементов // Проблемы кибернетики. Вып. 21. — М.: Наука, 1969. — С. 215–226.
11. Шоломов Л. А. Информационные свойства функционалов сложности для систем недоопределенных булевых функций // Проблемы кибернетики. Вып. 34. — М.: Наука, 1978. — С. 133–150.
12. Chashkin A. V. Average-case complexity of partial boolean functions // Proceedings of SAGA 2003. — Hatfield, UK, Springer, LNCS 2827, 2003. — P. 146–156.
13. Miltersen P. B. On the Shannon function for partially defined Boolean functions. Работа доступна по адресу: <http://www.brics.dk/~bromille/Papers/index.html>.
14. Pipenger N. Information theory and the complexity of Boolean function // Math. Syst. Theory. — 1976/77. — V. 10, № 2. — P. 129–167.