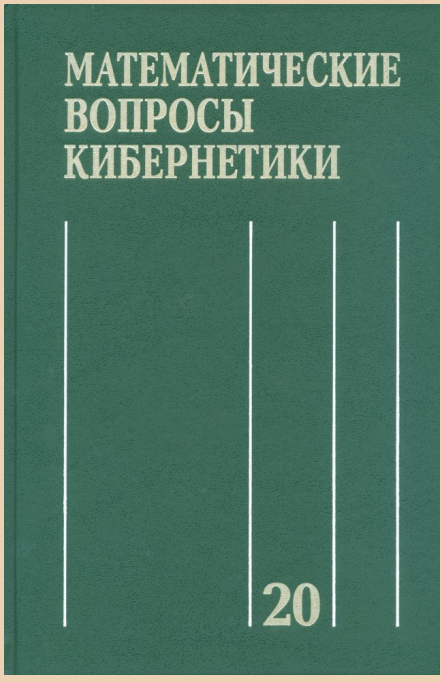
ИПМ им. М.В. Келдыша РАН • Электронная библиотека
Математические вопросы кибернетики • Выпуск 20



А. В. Чашкин

Асимптотические оценки средней сложности булевых функций

Рекомендуемая форма библиографической ссылки: Чашкин А. В. Асимптотические оценки средней сложности булевых функций // Математические вопросы кибернетики. Вып. 20. — М.: ФИЗМАТЛИТ, 2022. — С. 257–306. URL: http://library.keldysh.ru/mvk.asp?id=2022-257 DOI: 10.20948/mvk-2022-257

АСИМПТОТИЧЕСКИЕ ОЦЕНКИ СРЕДНЕЙ СЛОЖНОСТИ БУЛЕВЫХ ФУНКЦИЙ*)

А. В. ЧАШКИН

(МОСКВА)

Мы видим признаки ухудшающейся эпидситуации, и заключаются они в том, что в 35 регионах показатель превышает среднероссийский.

Из выступления главы Роспотребнадзора А. Поповой на президиуме Координационного совета при Правительстве РФ по борьбе с коронавирусом.

В работе рассматриваются некоторые из полученных в последние годы результатов, связанных со средней сложностью вычисления булевых функций неветвящимися программами с условной остановкой. Эти программы обобщают понятие схемы из функциональных элементов и являются естественной моделью неветвящихся вычислений — вычислений, в которых нет условного перехода и косвенной адресации, но есть возможность досрочного прекращения работы при выполнении определенного условия. Такие вычисления неформально можно представить следующим образом. Вычисления выполняет процессор, снабженный памятью, состоящей из отдельных ячеек. Процессор способен вычислять некоторое количество элементарных функций, составляющих базис вычисления. Каждая ячейка памяти в любой момент времени доступна процессору как для чтения, так и для записи информации. Процессор работает под управление программы, являющейся последовательностью элементарных команд двух видов. Каждая команда первого вида вычисляет значение некоторой базисной функции, аргументами которой является содержимое определенных ячеек памяти. Вычисленный результат также помещается в одну из ячеек памяти. Команда второго вида может прекратить выполнение программы. Каждая такая команда имеет единственный аргумент — содержимое некоторой ячейки памяти. Если значение аргумента равно определенному фиксированному числу, например

*) На заключительном этапе работа выполнялась при частичной финансовой поддержке Минобрнауки России в рамках реализации программы Московского центра фундаментальной и прикладной математики по соглашению № 075–15–2022–284.

DOI: 10.20948/mvk-2022-257

единице, то процессор прекращает работу. Если значение аргумента иное, то выполняется следующая команда программы. В памяти выделяется ряд специальных ячеек, содержимое которых после прекращения работы объявляется результатом работы программы. Естественной мерой сложности таких программ является среднее по всем возможным аргументам время работы.

Рассматриваемые далее результаты получены в работах с не всегда совпадающими формальными моделями, конкретный выбор которых часто определялся решаемой задачей. Поэтому возможны существенные различия между доказательствами и формулировками в данной работе и доказательствами и формулировками в работах по ссылкам.

Следует также отметить, что в работе рассматривается лишь небольшой круг вопросов, касающихся средней сложности булевых функций, относящихся в основном к классическим задачам сложности в «шенноновском» смысле. Не затронуты вопросы о средней сложности индивидуальных функций [15,18], о вычислениях в монотонном базисе [18], который в программах с условной остановкой является полным. Не рассмотрены вопросы надежности программ из ненадежных команд [1,2], ряд других вопросов [22,23].

§ 1. Программы и схемы

Пусть $X = \{x_1, \ldots, x_n\}$ — множество независимых булевых переменных, B — конечное множество булевых функций. Введем два множества булевых переменных: внутренние переменные $Y = \{\mathtt{y}_1, \ldots, \mathtt{y}_l\}$ и выходные $Z = \{\mathtt{z}_1, \ldots, \mathtt{z}_m\}$. Пусть, далее, $\mathtt{a} \in Y \cup Z$, $\mathtt{b} \in X \cup Y \cup Z$, f — k-местная функция из B. *Вычислительной командой* $\mathtt{p}$ назовем равенство

$$\mathtt{p}: \quad \mathtt{a} = f(\mathtt{b}_1, \ldots, \mathtt{b}_k).$$

Будем говорить, что команда $\mathtt{p}$ реализует функцию f, переменная $\mathtt{a}$ является *выходом*, а переменные $\mathtt{b}_1, \ldots, \mathtt{b}_k$ — *входами* этой команды. Вычислительная команда $\mathtt{p}$ изменяет значение своего выхода — переменной $\mathtt{a}$ и не изменяет значения других переменных. *Командой остановки* $\mathtt{p}$ назовем выражение

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

где переменная $\mathtt{b}$ — вход этой команды.

Последовательность

$$\mathsf{P} = \mathtt{p}_1 \ldots \mathtt{p}_i \ldots \mathtt{p}_L, \tag{1}$$

состоящая из вычислительных команд и команд остановки, называется *неветвящейся программой с условной остановкой* в базисе B и с множеством независимых переменных X, если при любом $j \in \{1, 2, \ldots, L\}$ каждый вход команды $\mathtt{p}_j$ есть либо независимая переменная из X, либо выход некоторой вычислительной команды $\mathtt{p}_i$, где $i < j$.

Каждая неветвящаяся программа работает в дискретные моменты времени $t = 0, 1, 2, \ldots$, не изменяет значения независимых переменных и изменяет значения внутренних и выходных переменных. Значения $\mathtt{y}_i(\boldsymbol{x}; t)$ внутренних переменных $\mathtt{y}_i$ и значения $\mathtt{z}_j(\boldsymbol{x}; t)$ выходных переменных $\mathtt{z}_j$ программы P в произвольный момент времени t на наборе независимых переменных $\boldsymbol{x} = (x_1, \ldots, x_n)$ 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_j, то

$$\mathsf{y}_i(\boldsymbol{x};t)=\mathsf{y}_i(\boldsymbol{x};t-1),\qquad \mathsf{z}_j(\boldsymbol{x};t)=\mathsf{z}_j(\boldsymbol{x};t-1);$$

— если команда p_t изменяет значения внутренней переменной y_i или выходной переменной z_j, и значение ее i-го входа в момент времени $t-1$ есть $\mathsf{b}_i(\boldsymbol{x};t-1)$, то

$$\mathsf{y}_i(\boldsymbol{x};t)=f_t(\mathsf{b}_1(\boldsymbol{x};t-1),\ldots,\mathsf{b}_k(\boldsymbol{x};t-1)),$$
$$\mathsf{z}_j(\boldsymbol{x};t)=f_t(\mathsf{b}_1(\boldsymbol{x};t-1),\ldots,\mathsf{b}_k(\boldsymbol{x};t-1)).$$

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

Пусть переменная b является входом команды p_i программы P, а переменная a — выходом вычислительной команды p_j этой программы, т.е. $\mathsf{p}_i:\mathsf{a}=f(\cdot,\mathsf{b},\cdot)$. Будем говорить, что на входе команды p_i вычисляется булева функция $g(\boldsymbol{x})$, если

$$\mathsf{b}(\boldsymbol{x};i-1)=g(\boldsymbol{x})$$

при всех значениях независимых переменных, при которых значение переменной b определено. Аналогичным образом скажем, что на выходе вычислительной команды p_i вычисляется булева функция $h(\boldsymbol{x})$, если

$$\mathsf{a}(\boldsymbol{x};i)=h(\boldsymbol{x})$$

при всех значениях независимых переменных, при которых значение переменной a определено.

Через $n(\mathsf{p})$ обозначим номер команды p в программе P, т.е. для команды p_i из (1) имеет место равенство $n(\mathsf{p}_i)=i$. Пусть $\mathsf{p}_{t_1},\ldots,\mathsf{p}_{t_r}$ — все команды остановки из P, причем $t_1<\ldots<t_r$. Тогда через s_k будем обозначать k-ю команду остановки программы P, т.е. $\mathsf{s}_k=\mathsf{p}_{t_k}$.

Теперь для $j\in\{0,1,\ldots,m\}$ определим j-е аргументы команды остановки s_k. Вычислительную команду p_i или переменную x_l назовем *нулевым аргументом* команды остановки s_k, $n(\mathsf{s}_k)=t_k$, и обозначим через q_k, если:

(i) выход команды p_i или переменная x_l является входом команды s_k;

(ii) среди команд p_t, $i<t<t_k$, нет команды, выход которой совпадает с выходом команды p_i.

Вычислительную команду p_i назовем *j-м аргументом* команды остановки s_k, $n(\mathsf{s}_k)=t_k$, если:

(i) переменная z_j является выходом команды p_i;

(ii) среди команд p_t, $i<t<t_k$, нет команды, выходом которой является переменная z_j.

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

$$\mathsf{q}_1(\boldsymbol{x})=\ldots=\mathsf{q}_{k-1}(\boldsymbol{x})=0,\quad \mathsf{q}_k(\boldsymbol{x})=1.$$

Результат действия программы P на наборе $\boldsymbol{x}$ обозначим через $\mathsf{P}(\boldsymbol{x})$ и его j-ю компоненту $\mathsf{P}_j(\boldsymbol{x})$ определим следующим образом:

$$\mathsf{P}_j(\boldsymbol{x}) = \begin{cases} \mathsf{z}_j(\boldsymbol{x}; t_k), & \text{если } \mathsf{q}_1(\boldsymbol{x}) = \ldots = \mathsf{q}_{k-1}(\boldsymbol{x}) = 0, \quad \mathsf{q}_k(\boldsymbol{x}) = 1, \\ \mathsf{z}_j(\boldsymbol{x}; L), & \text{если } \mathsf{q}_1(\boldsymbol{x}) = \ldots = \mathsf{q}_r(\boldsymbol{x}) = 0, \end{cases}$$

т. е. $\mathsf{P}_j(\boldsymbol{x})$ равно значению j-й выходной переменной z_j в момент остановки программы. Легко видеть, что

$$\begin{aligned} \mathsf{P}_j(\boldsymbol{x}) = {} & \mathsf{q}_1(\boldsymbol{x})\mathsf{z}_j(\boldsymbol{x}; t_1) \vee \overline{\mathsf{q}}_1(\boldsymbol{x})\mathsf{q}_2(\boldsymbol{x})\mathsf{z}_j(\boldsymbol{x}; t_2) \vee \ldots \\ & \ldots \vee \overline{\mathsf{q}}_1(\boldsymbol{x}) \cdots \overline{\mathsf{q}}_{k-1}(\boldsymbol{x})\mathsf{q}_k(\boldsymbol{x})\mathsf{z}_j(\boldsymbol{x}; t_k) \vee \ldots \\ & \ldots \vee \overline{\mathsf{q}}_1(\boldsymbol{x}) \cdots \overline{\mathsf{q}}_{r-1}(\boldsymbol{x})\mathsf{q}_r(\boldsymbol{x})\mathsf{z}_j(\boldsymbol{x}; t_r) \vee \overline{\mathsf{q}}_1(\boldsymbol{x}) \cdots \overline{\mathsf{q}}_r(\boldsymbol{x})\mathsf{z}_j(\boldsymbol{x}; L). \end{aligned} \tag{2}$$

Если в (2) последовательно выносить за скобки общие множители $\overline{\mathsf{q}}_{k-1}(\boldsymbol{x})$, то эту формулу можно представить в «рекуррентном» виде

$$\begin{aligned} \mathsf{P}_j(\boldsymbol{x}) = {} & \mathsf{q}_1(\boldsymbol{x})\mathsf{z}_j(\boldsymbol{x}; t_1) \vee \overline{\mathsf{q}}_1(\boldsymbol{x})\big(\mathsf{q}_2(\boldsymbol{x})\mathsf{z}_l(\boldsymbol{x}; t_2) \vee \overline{\mathsf{q}}_2(\boldsymbol{x})\big(\ldots \\ & \ldots \big(\mathsf{q}_{k-1}(\boldsymbol{x})\mathsf{z}_j(\boldsymbol{x}; t_{k-1}) \vee \overline{\mathsf{q}}_{k-1}(\boldsymbol{x})\big(\ldots \\ & \ldots \vee \overline{\mathsf{q}}_{r-1}\big(\mathsf{q}_r(\boldsymbol{x})\mathsf{z}_j(\boldsymbol{x}; t_r) \vee \overline{\mathsf{q}}_r(\boldsymbol{x})\mathsf{z}_j(\boldsymbol{x}; L)\big) \ldots\big)\big) \ldots\big)\big). \end{aligned} \tag{3}$$

Будем говорить, что программа P вычисляет n-местную булеву функцию f, если $\mathsf{P}(\boldsymbol{x}) = f(\boldsymbol{x})$ для любого $\boldsymbol{x}$ из области определения f.

Сложностью $C(\mathsf{P})$ программы P назовем число команд этой программы, а сумму числа ее внутренних и выходных переменных — объемом памяти этой программы. *Временем работы* $T_{\mathsf{P}}(\boldsymbol{x})$ программы P на наборе переменных $\boldsymbol{x}$ назовем минимальное $n(\mathsf{s}_k)$ такое, что $\mathsf{q}_k(\boldsymbol{x}) = 1$, т. е. это — число команд, выполненных до остановки программы на $\boldsymbol{x}$. Если все $\mathsf{q}_k(\boldsymbol{x}) = 0$, то выполняются все команды программы и в этом случае $T_{\mathsf{P}}(\boldsymbol{x}) = C(\mathsf{P})$. Пусть $D \subseteq \{0,1\}^n$, $f : D \to \{0,1\}^m$. Величину

$$T(\mathsf{P}) = |D|^{-1} \sum T_{\mathsf{P}}(\boldsymbol{x}),$$

где суммирование производится по всем двоичным наборам из D, назовем *средним временем работы* программы P. Величину

$$T_B(f) = \min T(\mathsf{P}),$$

где минимум берется по всем вычисляющим f программам в базисе B, назовем *средним временем вычисления или средней сложностью* функции f. Программу P, вычисляющую функцию f, для которой справедливо равенство $T(\mathsf{P}) = T_B(f)$, назовем *минимальной* программой. Величину

$$C_B(f) = \min C(\mathsf{P}),$$

где минимум берется по всем вычисляющим f программам в базисе B, назовем *программной сложностью* функции f. Величина $C_B(f)$ характеризует время необходимое для вычисления f в «худшем» случае, поэтому $C_B(f)$ также будем называть сложностью в худшем случае.

Далее будем рассматривать программы, в которых:

— вход каждой команды остановки программы не является тождественной постоянной;
— никакие две команды остановки программы не имеют общего нулевого аргумента.

Нетрудно показать, что любая программа без увеличения сложности и среднего времени работы может быть преобразована в программу, удовлетворяющую этим двум условиям.

Каждая неветвящаяся программа, которая не содержит команды остановки и вычисляет существенно зависящую хотя бы от одной переменной функцию $f: \{0,1\}^n \to \{0,1\}^m$, является обычной схемой из функциональных элементов. Поэтому для любой такой функции ее средняя сложность T_B, программная сложность C_B и сложность вычисления L_B схемами в базисе B связаны неравенствами

$$T_B(f(x_1,\ldots,x_n)) \leqslant C_B(f(x_1,\ldots,x_n)) \leqslant L_B(f(x_1,\ldots,x_n)).$$

С другой стороны, используя равенство (3), нетрудно показать, что при $m=1$ для функции $f: \{0,1\}^n \to \{0,1\}$ по вычисляющей эту функцию программе P можно построить схему, доставляющую неравенство

$$L_B(f) \leqslant C_B(\mathsf{P}) \cdot (2L_B(\&) + L_B(\vee) + L_B(\neg) - 1), \tag{4}$$

которое в случае базиса B_0, состоящего из всех не более чем двухместных булевых функций, превращается в неравенство

$$L(f) \leqslant 2 \cdot C(\mathsf{P}). \tag{5}$$

Однако при больших m возможна ситуация, когда значительная доля команд вычисляющей функцию f программы P является командами остановки и между большинством соседних команд остановки выходные переменные вообще не вычисляются, а происходит только определение новых условий остановки. В этом случае сложность построенной по программе P и формуле (3) схемы S по порядку может быть в m раз больше сложности исходной программы. В следующей теореме описывается способ преобразования произвольной программы в схему, при котором сложность схемы не более чем в четыре раза превосходит сложность программы. Эта теорема и все следующие утверждения доказываются для базиса B_0. Поэтому, как и в (5), символы базиса в функционалах сложности функций далее опускаются.

Теорема 1. *Пусть* $f: \{0,1\}^n \to \{0,1\}^m$. *Программа* P, *вычисляющая функцию* f, *может быть преобразована в вычисляющую эту функцию схему из функциональных элементов* S *так, что* $L(\mathsf{S}) \leqslant 4C(\mathsf{P})$.

Доказательство. Пусть $\mathsf{P} = \mathsf{p}_1 \ldots \mathsf{p}_L$ — произвольная программа, $\mathsf{s}_1, \ldots, \mathsf{s}_r$ — все ее команды остановки, $\mathsf{q}_1, \ldots, \mathsf{q}_r$ — нулевые аргументы команд остановки. Как и в (2) полагаем, что i-я команда остановки s_i программы P является ее t_i-й командой. Введем вспомогательные функции h_i и h'_i. Положим

$$h'_0(\boldsymbol{x}) \equiv 1, \qquad h'_k(\boldsymbol{x}) = \bigwedge_{i=1}^{k} \overline{\mathsf{q}}_i(\boldsymbol{x}) \qquad \text{при } k \in \{1,2,\ldots,r\},$$
$$h_{r+1}(\boldsymbol{x}) = h'_r(\boldsymbol{x}), \quad h_k(\boldsymbol{x}) = h'_{k-1}(\boldsymbol{x})\mathsf{q}_j(\boldsymbol{x}) \text{ при } k \in \{1,2,\ldots,r\}.$$

Используя введенные функции h_i, преобразуем (2):

$$\mathsf{P}_l(\boldsymbol{x}) = h_1(\boldsymbol{x})\mathbf{z}_l(\boldsymbol{x}; t_1) \vee \ldots \vee h_r(\boldsymbol{x})\mathbf{z}_l(\boldsymbol{x}; t_r) \vee h_{r+1}(\boldsymbol{x})\mathbf{z}_l(\boldsymbol{x}; L). \tag{6}$$

Теперь при всех i, j таких, что $1 \leqslant i < j \leqslant r+1$, определим функции

$$h_{i,j}(\boldsymbol{x}) = \bigvee_{k=i}^{j} h_k(\boldsymbol{x}).$$

Предположим, что l-я выходная переменная программы P вычисляется только перед первой командой остановки и после команд остановки, индексы которых принадлежат множеству $\{i_1, \ldots, i_k\}$, т.е. $\mathbf{z}_l(\boldsymbol{x}; t_i) = \mathbf{z}_l(\boldsymbol{x}; t_1)$ при всех $i \in \{1, \ldots, i_1\}$ и $\mathbf{z}_l(\boldsymbol{x}; t_i) = \mathbf{z}_l(\boldsymbol{x}; t_{i_{s+1}})$ при всех $i \in \{i_s + 1, \ldots, i_{s+1}\}$. В этом случае равенство (6) после несложных преобразований приводится к виду

$$\begin{aligned}\mathsf{P}_l(\boldsymbol{x}) = {} & h_{1,i_1}(\boldsymbol{x})\mathbf{z}_l(\boldsymbol{x}; t_1) \vee h_{i_1+1,i_2}(\boldsymbol{x})\mathbf{z}_l(\boldsymbol{x}; t_{i_1+1}) \vee \ldots \\ & \ldots \vee h_{i_{k-1}+1,i_k}(\boldsymbol{x})\mathbf{z}_l(\boldsymbol{x}; t_{i_{k-1}+1}) \vee h_{i_k+1,r+1}(\boldsymbol{x})\mathbf{z}_l(\boldsymbol{x}; t_{i_k+1}).\end{aligned} \tag{7}$$

Легко видеть, что функции h'_i и h_j определены так, что

$$h'_i(\boldsymbol{x})h_j(\boldsymbol{x}) = \begin{cases} 0, & \text{если } i \geqslant j, \\ h_j(\boldsymbol{x}), & \text{если } i < j. \end{cases}$$

Поэтому при $i < j$

$$h'_i(\boldsymbol{x})h_{1,j}(\boldsymbol{x}) = h_{i+1}(\boldsymbol{x}) \vee \ldots \vee h_j(\boldsymbol{x}) = h_{i+1,j}(\boldsymbol{x}),$$

т.е. при вычисленных функциях h'_i и $h_{1,i}$ для вычисления каждой функции $h_{i,j}$, встречающейся в (7), достаточно одной вычислительной команды.

Преобразуем программу P в программу P', которая состоит только из вычислительных команд и вычисляет тот же булев оператор, что и P. Число вычислительных команд программы P обозначим через L_1. Тогда $L = L_1 + r$. Преобразование программы P состоит в следующем:

- вычисляем все функции h'_i, h_i и $h_{1,i}$. Для этого потребуется $3r - 2$ команд;
- вычисляем все необходимые функции $h_{i,j}$. Для этого потребуется столько команд, сколько раз в программе P вычисляются выходные переменные. Так как каждый раз каждая выходная переменная вычисляется собственной вычислительной командой, то потребуется не более L_1 команд;
- в соответствии с равенством (7) вычисляем все компоненты P_l. Для этого потребуется не более $2L_1$ команд;
- удаляем все команды остановки.

Легко видеть, что общее число дополнительных команд не превосходит $3L$. Следовательно, сложность программы P' не превосходит $4L$. Так как эта программа не содержит команды остановки, то ее можно рассматривать как схему из функциональных элементов. Теорема доказана.

§ 2. Средняя сложность почти всех функций

Рассмотрим классическую задачу об определении средней сложности «почти всех» булевых функций n переменных. Покажем, что средняя сложность «почти каждой» n-местной булевой функции f с точностью до постоянного множителя совпадает с ее обычной сложностью, которая, как известно [8], при $n \to \infty$ удовлетворяет асимптотическому равенству

$$L(f) \sim \frac{2^n}{n}.$$

Нижняя оценка теоремы 2 не является наилучшей. Эту оценку можно усилить, если для оценки числа программ воспользоваться леммой 22.

Т е о р е м а 2. *Пусть $n \to \infty$. Тогда*:

(1) *для любой положительной постоянной ε доля n-местных булевых функций f, для которых выполняется неравенство*

$$T(f) \geqslant (1-\varepsilon)\frac{2^{n-2}}{n},$$

стремится к единице;

(2) *для каждой n-местной булевой функции f*

$$T(f) \lesssim \frac{2^{n-1}}{n}.$$

Первое утверждение теоремы следует из доказываемой далее леммы 2, второе утверждение — из леммы 3.

Докажем нижнюю мощностную оценку для средней сложности булевых функций. В доказательстве будем рассматривать только программы специального вида, в которых перезапись значений допускается только для выходной переменной. Но так как произвольная программа P может быть легко преобразована в специальную программу P' так, что $C(\mathsf{P}) = C(\mathsf{P}')$ и $T(\mathsf{P}) = T(\mathsf{P}')$, то, очевидно, что установленная далее в лемме 2 нижняя оценка справедлива в общем случае. Для доказательства этой леммы потребуется верхняя оценка функции $N(L, n)$, равной числу программ специального вида, каждая из которых вычисляет n-местную функцию и состоит из не более чем L команд

Л е м м а 1. *Справедливо неравенство*

$$N(L, n) \leqslant (9(L+n))^{2L}. \tag{8}$$

Д о к а з а т е л ь с т в о. Пусть P — программа специального вида из k команд. Эта программа однозначно определяется списком команд p_i, каждая из которых однозначно задается следующими данными:

— типом команды — будем рассматривать три варианта, в которых команда может быть: (1) командой остановки, (2) вычислительной командой, выходом которой будет очередная внутренняя переменная y_i, (3) вычислительной командой, выходом которой будет выходная переменная z;

— двуместной булевой функцией f_i, реализуемой вычислительной командой (для команды остановки эта информация опускается) — существует всего 16 различных двухместных булевых функций;

— номерами переменных, независимых или внутренних, являющихся входами команды — полагаем, что независимые переменные нумеруются числами от $k+1$ до $k+n$, таким образом общее число пар номеров не превосходит $(k+n)^2$.

Поэтому для числа $N(k,n)$, равного числу различных программ, состоящих из k команд, справедливо неравенство

$$N \leqslant \left(3 \cdot 16 \cdot (k+n)^2\right)^k \leqslant (8(k+n))^{2k}.$$

Суммируя правые части получившегося неравенства по всем k от единицы до L, получаем неравенство (8). Лемма доказана.

С каждой программой P, вычисляющей в общем случае частичную n-местную булеву функцию $f : D \to \{0,1\}^m$, свяжем линейный порядок на множестве наборов из ее области определения. Для этого каждому двоичному набору $\boldsymbol{x}$ из D поставим в соответствие его номер $N_{\mathsf{P}}(\boldsymbol{x})$ такой, что:

$$N_{\mathsf{P}}(\boldsymbol{x}) \in \{1,2,\ldots,|D|\};$$
$$N_{\mathsf{P}}(\boldsymbol{x}) < N_{\mathsf{P}}(\boldsymbol{y}), \text{ если } T_{\mathsf{P}}(\boldsymbol{x}) < T_{\mathsf{P}}(\boldsymbol{y});$$
$$N_{\mathsf{P}}(\boldsymbol{x}) < N_{\mathsf{P}}(\boldsymbol{y}), \text{ если } T_{\mathsf{P}}(\boldsymbol{x}) = T_{\mathsf{P}}(\boldsymbol{y}) \text{ и } |\boldsymbol{x}| < |\boldsymbol{y}|,$$

где $|\boldsymbol{x}| = \sum\limits_{i=1}^{n} x_i 2^{i-1}$. Далее эту функцию будем использовать в доказательстве всех нижних мощностных оценок.

Л е м м а 2. *Пусть $n \to \infty$. Тогда для любой постоянной $\varepsilon > 0$ доля n-местных булевых функций f, для которых*

$$T(f) \geqslant (1-\varepsilon)\frac{2^{n-2}}{n},$$

стремится к единице.

Д о к а з а т е л ь с т в о. Пусть f — n-местная булева функция, P — минимальная программа, вычисляющая f. Без ограничения общности будем полагать, что $2^n/n$ целое. Пусть набор $\boldsymbol{x}_i$ такой, что $N_{\mathsf{P}}(\boldsymbol{x}_i) = \dfrac{i2^n}{n}$, где $i = 1,2,\ldots,n-1$. Оценим число булевых функций, у минимальных программ которых найдется такой набор $\boldsymbol{x}_i$, что $T_{\mathsf{P}}(\boldsymbol{x}_i) \leqslant \dfrac{(1-\varepsilon)i2^{n-1}}{n^2}$. Каждая такая функция однозначно определяется первыми $T_{\mathsf{P}}(\boldsymbol{x}_i)$ командами своей минимальной программы и двоичным набором длины не более чем $2^n - N_{\mathsf{P}}(\boldsymbol{x}_i)$ — значениями на тех аргументах, время работы на которых больше времени работы на $\boldsymbol{x}_i$. В силу предыдущей леммы для числа N_i, равного числу различных программ, сложность которых не превосходит $T_{\mathsf{P}}(\boldsymbol{x}_i)$, справедливо неравенство

$$N_i \leqslant \left(9\left(T_{\mathsf{P}}(\boldsymbol{x}_i)+n\right)\right)^{2T_{\mathsf{P}}(\boldsymbol{x}_i)} \leqslant$$
$$\leqslant \left(9\left((1-\varepsilon)\frac{(i-1)2^{n-1}}{n^2}+n\right)\right)^{2(1-\varepsilon)\cdot\frac{i2^{n-1}}{n^2}} \leqslant 2^{(1-\varepsilon)\cdot i2^n/n}.$$

Следовательно, M — число рассматриваемых функций — не превосходит величины

$$\sum_{i=1}^{n-1} 2^{\frac{(1-\varepsilon)i2^n}{n}} \cdot 2^{2^n - \frac{i2^n}{n}} = \sum_{i=1}^{n-1} 2^{2^n - \frac{\varepsilon i2^n}{n}} = o\left(2^{2^n}\right).$$

Сравнивая полученную оценку величины M с числом всех n-местных булевых функций, видим, что для $i = 1, 2, \ldots, n-1$ все минимальные программы почти всех булевых функций удовлетворяют условию:

$$\text{если набор } \boldsymbol{x}_i \text{ такой, что } N_{\mathsf{P}}(x_i) = \frac{i2^n}{n}, \text{ то } T_{\mathsf{P}}(\boldsymbol{x}_i) > \frac{(1-\varepsilon)i2^{n-1}}{n^2}.$$

Положим $X_i = \{\boldsymbol{x} \mid N_{\mathsf{P}}(\boldsymbol{x}_i) < N_{\mathsf{P}}(\boldsymbol{x}) \leqslant N_{\mathsf{P}}(\boldsymbol{x}_{i+1})\}$. Тогда для среднего времени работы каждой такой программы имеем

$$T(\mathsf{P}) = \frac{1}{2^n}\sum_{\boldsymbol{x}} T_{\mathsf{P}}(\boldsymbol{x}) \geqslant \frac{1}{2^n}\sum_{i=1}^{n-1} T_{\mathsf{P}}(\boldsymbol{x}_i)|X_i| = \frac{1}{2^n}\sum_{i=1}^{n-1} T_P(x_i)\frac{2^n}{n} >$$
$$> \frac{1}{n}\sum_{i=1}^{n-1}\frac{(1-\varepsilon)i2^{n-1}}{n^2} = \frac{(1-\varepsilon)n(n-1)2^{n-1}}{2n^3} \sim (1-\varepsilon)\cdot\frac{2^{n-2}}{n}.$$

Таким образом, при $n \to \infty$ для любой положительной постоянной ε средняя сложность почти каждой булевой функции, зависящей от n переменных, не меньше, чем $(1-\varepsilon)\frac{2^{n-2}}{n}$. Лемма доказана.

Л е м м а 3. *Пусть $n \to \infty$. Тогда для каждой n-местной булевой функции f*

$$T(f) \lesssim \frac{2^{n-1}}{n}.$$

Д о к а з а т е л ь с т в о. Положим $s = \lfloor n - \log_2 n \rfloor$. Функцию f разложим по первым $n-s$ переменным:

$$f(x_1, \ldots, x_n) = \bigvee_{\sigma_1 \ldots \sigma_{n-s}} f(\sigma_1, \ldots, \sigma_{n-s}, x_{n-s+1}, \ldots, x_n)\cdot x_1^{\sigma_1}\cdots x_{n-s}^{\sigma_{n-s}}.$$

Программу, вычисляющую функцию f, представим в следующем виде:

$$\mathsf{P} = \mathsf{P}_0 \ldots \mathsf{P}_j \ldots \mathsf{P}_{2^{n-s}-1},$$

где $j = |(\sigma_1, \ldots, \sigma_{n-s}|$, P_j — программа, вычисляющая функцию

$$f_j(x_{n-s+1}, \ldots, x_n) = f(\sigma_1, \ldots, \sigma_{n-s}, x_{n-s+1}, \ldots, x_n)$$

и прекращающая работу программы P, если $x_1^{\sigma_1}\cdots x_{n-s}^{\sigma_{n-s}} = 1$. Так как сложность произвольной булевой функции, зависящей от s переменных, асимптотически не превосходит $\frac{2^s}{s}$, то $L(\mathsf{P}_j) \lesssim \frac{2^s}{s}$. Поэтому

$$T(\mathsf{P}) \sim \frac{1}{2^n}\sum_{j=0}^{2^{n-s}-1}\left(2^s\sum_{i=1}^{j} L(\mathsf{P}_i)\right) = \frac{2^s}{2^n}\sum_{j=0}^{2^{n-s}-1}\sum_{i=1}^{j} L(P_i) \lesssim$$
$$\lesssim \frac{2^s}{2^n}\cdot\frac{2^s}{s}\sum_{j=0}^{2^{n-s}-1} j \lesssim \frac{2^s}{2^n}\cdot\frac{2^s}{s}\cdot\frac{2^{2(n-s)}}{2} \sim \frac{2^{n-1}}{s} \sim \frac{2^{n-1}}{n}.$$

Лемма доказана.

Нижняя оценка в теореме 2 в два раза меньше верхней оценки, которая, видимо, является истинной. Связано это с грубой оценкой числа программ. Эта грубость связана с необходимостью учета линейного порядка команд

остановки и их аргументов в программе. Необходимость учитывать этот порядок в программе из двухвходовых команд превращает каждую команду остановки фактически в команду с тремя аргументами — к двум аргументам добавляется третий — предыдущая команда остановки. Более точная оценка числа программ в лемме 22 позволяет немного повысить нижнюю оценку, но верхняя оценка остается пока недостижимой. Тем не менее в ряде случаев влияние «лишнего» аргумента у команды остановки удается преодолеть. Например, для достижения асимптотического равенства верхней и нижней оценок достаточно потребовать, чтобы в программах число команд остановки было существенно меньше общего числа команд или чтобы базис программ содержал функцию с не менее чем тремя существенными аргументами. Два более интересных случая рассматриваются в следующем разделе.

§ 3. Программы с ограниченной памятью

Будем рассматривать вычисление булевых функций программами с двумя видами ограничений на использование памяти. В первом случае будет ограничен общий объем используемой памяти, во втором — каждое вычисленное значение можно использовать только один раз.

3.1. Ограничение общего объема памяти. Будем рассматривать программы, у которых общий объем памяти не превосходит некоторой величины D и которые вычисляют булевы функции, отображающие $\{0,1\}^n$ в $\{0,1\}^m$. Далее функционалы сложности, отвечающие рассматриваемым программам, будем отмечать верхним символом D, а рассматриваемые функции будем называть (n,m)-операторами. Схемы с ограниченной памятью ранее рассматривал В. К. Коробков. Из его неопубликованных результатов следует, что при $n \to \infty$ и $D - n = \Omega(n)$ для сложности самой сложной n-местной булевой функции f справедливо асимптотическое равенство

$$L^D(f) \sim \frac{2^n}{\log_2 D},$$

которое легко обобщается на случай вычисления (n,m)-операторов. Близкую задачу изучала и Н. А. Карпова, из результатов которой в [7] следует, что для любой постоянной $t \geqslant 3$ и любой n-местной булевой функции f

$$L^{n+t}(f) \lesssim \frac{2^n}{\log_2 n}.$$

Аналоги этих результатов для средней сложности получены в следующей теореме.

Т е о р е м а 3. *Пусть* $n, m \to \infty$, $D - n - m = \Omega(n)$ *и* $\log_2 m = o(\log_2 D)$. *Тогда*:

(1) *для любой положительной постоянной* ε *доля булевых* (n,m)*-операторов* f, *для которых выполняется неравенство*

$$T^D(f) \geqslant (1-\varepsilon)\frac{2^{n-2}m}{\log_2 D},$$

стремится к единице;

(2) *для каждого булева* (n, m)*-оператора* f

$$T^D(f) \lesssim \frac{2^{n-2}m}{\log_2 D}.$$

Утверждение теоремы следует из доказываемых далее лемм 5 и 6.

Две программы назовем эквивалентными, если одна может быть получена из другой переименованием внутренних переменных. Через $N(n, m, D, L)$ обозначим число неэквивалентных программ с n независимыми и m выходными переменными, объем памяти которых не превосходит D, а число команд не превосходит L.

Лемма 4. *Справедливо неравенство*

$$N(n, m, D, L) \leqslant (cm\,(D+n))^{2L},$$

где c *— константа.*

Доказательство. Любая программа P задается списком своих команд p_i, каждая из которых однозначно определяется следующими данными:

1) типом команды — возможны всего два варианта — команда может быть либо вычислительной, либо командой остановки;

2) двухместной булевой функцией h_i вычислительной команды (для команды остановки эта информация опускается); существует всего 16 различных двухместных булевых функций;

3) номерами независимых, внутренних или выходных переменных, являющихся входами команды; число всех этих переменных не превосходит $D+n$, поэтому общее число пар номеров не превосходит $(D+n)^2$;

4) номером выходной или внутренней переменной, являющейся выходом вычислительной команды (для команд остановки эта информация опускается), общее число этих переменных не превосходит D.

Таким образом, одна команда определяется выбором одного из не более чем $2 \cdot 16 \cdot (D+n)^2 \cdot D$ вариантов. Покажем, что последнее число можно уменьшить, если определенным образом зафиксировать порядок использования внутренних переменных так, чтобы номер внутренней переменной, являющейся выходом очередной вычислительной команды, однозначно определялся предшествующими командами. Сделаем это следующим образом. Приведенные выше п. 3 и п. 4 заменим новыми. В п. 3 добавим пару чисел (α_1, α_2) таких, что $\alpha_i = 1$, если значение i-го входа команды используется в программе далее и $\alpha_i = 0$ в противном случае. Нулевое значение α указывает, что соответствующая внутренняя переменная становится свободной и может быть использована для запоминания нового промежуточного значения. Если входом является независимая или выходная переменная, то соответствующее значения α всегда равно единице. Эти новые данные позволяют в п. 4 определить выход вычислительной команды целым числом от 0 до m. Нулевое значение указывает, что выходом команды является внутренняя переменная, а ее номер определяется как минимальный номер всех свободных в данный момент внутренних переменных. Положительное число указывает номер выходной переменной в том случае, когда такая переменная является выходом команды.

Нетрудно видеть, что теперь команда определяется выбором одного из не более чем $128(D+n)^2(m+1)$ вариантов. Поэтому для числа N, равного числу различных неэквивалентных программ, состоящих из не более

чем L команд, справедливо неравенство

$$N \leqslant \left(128(D+n)^2 \cdot (m+1)\right)^L \leqslant \left(cm(D+n)\right)^{2L}, \tag{9}$$

где c — константа. Лемма доказана.

Л е м м а 5. *Пусть* $n \to \infty$, $D - n - m = \Omega(n)$ *и* $\log_2 m = o(\log_2 D)$. *Тогда для любой положительной постоянной* ε *доля булевых* (n, m)*-операторов* f, *для которых выполняется неравенство*

$$T^D(f) \geqslant (1-\varepsilon)\frac{2^{n-2}m}{\log_2 D},$$

стремится к единице.

Д о к а з а т е л ь с т в о. Пусть f — булев оператор, P — минимальная программа, вычисляющая f. Пусть $q_0 = \left\lfloor \log_2 \sqrt{\log_2 D / \log_2 m} \right\rfloor$, $q = 2^{q_0}$, набор $\boldsymbol{x}_i$ такой, что $N_P(\boldsymbol{x}_i) = \dfrac{i2^n}{q}$, где $i = 2, 3, \ldots, q$. Оценим число булевых операторов, у минимальных программ которых найдется такой набор $\boldsymbol{x}_i$, что $T_{\mathsf{P}}(\boldsymbol{x}_i) \leqslant \dfrac{(i-1)2^n}{q \log_2 D} \cdot \dfrac{m}{2}$. Каждый такой оператор однозначно определяется первыми $T_P(\boldsymbol{x}_i)$ командами своей минимальной программы и набором не более чем из $2^n - N_{\mathsf{P}}(\boldsymbol{x}_i)$ двоичных векторов длины m — значениями на тех аргументах, время работы на которых больше времени работы на $\boldsymbol{x}_i$. В силу леммы 4 для числа N_i, равного числу различных программ, сложность которых не превосходит $T_{\mathsf{P}}(\boldsymbol{x}_i)$, справедливо неравенство

$$N_i \leqslant \left(cm\,(D+n)\right)^{2\left(\frac{(i-1)2^n}{q \log_2 D} \cdot \frac{m}{2}\right)} \leqslant 2^{\frac{(i-1)m2^n}{q} \cdot \left(1 + \mathcal{O}\left(q^{-2}\right)\right)}.$$

Следовательно, M — число рассматриваемых операторов — не превосходит величины

$$\sum_{i=2}^{q} 2^{\frac{(i-1)m2^n}{q} \cdot \left(1 + \mathcal{O}\left(q^{-2}\right)\right)} \cdot 2^{m2^n - \frac{mi2^n}{q}}.$$

Нетрудно видеть, что для показателя величины, стоящей под знаком суммы, справедливо равенство

$$m2^n - \frac{mi2^n}{q} + \frac{(i-1)m2^n}{q} \cdot \left(1 + \mathcal{O}\left(q^{-2}\right)\right) = m2^n - \frac{m2^n}{q} + \mathcal{O}\left(\frac{m2^n}{q^2}\right).$$

Так как $1 \ll q \ll n$, то, начиная с некоторого n,

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

Сравнивая полученную оценку величины M с числом всех булевых (n, m)-операторов, видим, что при $q_0 = \left\lfloor \log_2 \sqrt{\log_2 D / \log_2 m} \right\rfloor$ и $q = 2^{q_0}$ для $i = 2, 3, \ldots, q$ все минимальные программы почти всех булевых операторов удовлетворяют условию:

$$\text{если набор } \boldsymbol{x}_i \text{ такой, что } N_{\mathsf{P}}(x_i) = \frac{i2^n}{q}, \text{ то } T_{\mathsf{P}}(\boldsymbol{x}_i) > \frac{(i-1)2^n}{q \log_2 D} \cdot \frac{m}{2}.$$

Положим $X_i = \{\boldsymbol{x} \mid N_{\mathsf{P}}(\boldsymbol{x}_i) < N_{\mathsf{P}}(\boldsymbol{x}) \leqslant N_{\mathsf{P}}(\boldsymbol{x}_{i+1})\}$. Тогда для любой положительной постоянной ε при $n \to \infty$ для среднего времени работы каждой

такой программы имеем

$$T(\mathsf{P}) = \frac{1}{2^n}\sum_{\boldsymbol{x}} T_{\mathsf{P}}(\boldsymbol{x}) \geqslant \frac{1}{2^n}\sum_{i=2}^{q-1} T_{\mathsf{P}}(\boldsymbol{x}_i)|X_i| = \frac{1}{2^n}\sum_{i=2}^{q-1} T_P(x_i)\frac{2^n}{q} >$$
$$> \frac{1}{q}\sum_{i=2}^{q-1}\frac{(i-1)2^n}{q\log_2 D}\cdot\frac{m}{2} = \frac{(q-1)(q-2)2^n}{2q^2\log_2 D}\cdot\frac{m}{2} \geqslant (1-\varepsilon)\frac{2^{n-2}m}{\log_2 D}.$$

Лемма доказана.

Пусть s, h — целые. Множество всех двоичных наборов длины s разобьем на $t = \lceil 2^s/h\rceil$ непересекающихся множеств Y_i так, что $(\sigma_1\ldots\sigma_s)\in Y_i$, если $(i-1)h \leqslant |(\sigma_1\ldots\sigma_s)| < ih$, где $|(\sigma_1\ldots\sigma_s)| = \sum\limits_{i=1}^{s}\sigma_{s-i}2^{i-1}$. Введем функции

$$I_j^1(x_1,\ldots,x_s) = \bigvee_{\sigma\in Y_j} x_1^{\sigma_1},\ldots,x_s^{\sigma_s}, \quad 1\leqslant j\leqslant t;$$
$$I_j^2(x_1,\ldots,x_s) = I_{2j-1}^1(x_1,\ldots,x_s)\vee I_{2j}^1(x_1,\ldots,x_s), \quad 1\leqslant j\leqslant \lceil t/2\rceil;$$
$$I_{j,l}(x_1,\ldots,x_n) = I_j^2(x_1,\ldots,x_s)\cdot x_{s+1}^{\sigma_{s+1}}\cdots x_n^{\sigma_n}, \quad 1\leqslant j\leqslant\lceil t/2\rceil,$$

где $l = |(\sigma_{s+1}\ldots\sigma_n)|$. Для произвольной булевой функции $f(x_1,\ldots,x_n)$ положим

$$f_l(x_1,\ldots,x_s) = f(x_1,\ldots,x_s,\sigma_{s+1},\ldots,\sigma_n),$$
$$f_{j,l}(x_1,\ldots,x_s) = f_l(x_1,\ldots,x_s)\cdot I_j^1(x_1,\ldots,x_s).$$

Легко видеть, что

$$f_{j,l}(x_1,\ldots,x_s)\cdot x_{s+1}^{\sigma_{s+1}}\cdots x_n^{\sigma_n} = f_{j,l}(x_1,\ldots,x_s)\cdot I_{\lceil j/2\rceil,l}(x_1,\ldots,x_n).$$

Поэтому справедливо разложение

$$f(x_1,\ldots,x_n) = \bigvee_{\sigma_{s+1}\ldots\sigma_n}\left(\bigvee_{j=1}^{t} f_{j,l}(x_1,\ldots,x_s)\right)\cdot x_{s+1}^{\sigma_{s+1}}\cdots x_n^{\sigma_n} =$$
$$= \bigvee_{\sigma_{s+1}\ldots\sigma_n}\bigvee_{k=1}^{\lceil t/2\rceil}\left(\bigvee_{r=1}^{2} f_{2(k-1)+r,l}(x_1,\ldots,x_s)\right)\cdot x_{s+1}^{\sigma_{s+1}}\cdots x_n^{\sigma_n} = \tag{10}$$
$$= \bigvee_{\sigma_{s+1}\ldots\sigma_n}\left(\bigvee_{k=1}^{\lceil t/2\rceil}\left(\bigvee_{r=1}^{2} f_{2(k-1)+r,l}(x_1,\ldots,x_s)\right)\cdot I_{k,l}(x_1,\ldots,x_n)\right).$$

Пусть R — множество, состоящее из всех встречающихся в (10) различных функций $f_{j,l}(x_1,\ldots,x_s)$ и всех функций $I_j^2(x_1,\ldots,x_s)$. Легко видеть, что число функций в R не превосходит $2^{h+s+1}/h$, а для сложности реализации этих функций схемами из функциональных элементов справедливо неравенство

$$L(R)\leqslant 2^{h+s+2}. \tag{11}$$

Лемма 6. *Пусть $n\to\infty$, $D - n - m = \Omega(n)$ и $m\leqslant D/2$. Тогда для произвольного булева (n,m)-оператора f справедливо неравенство*

$$T^D(f)\lesssim\frac{2^{n-2}(m+2)}{\log_2 D}.$$

Доказательство. Пусть

$$s = \lfloor 2\log_2\log_2 D\rfloor, h = \lfloor\log_2 D - 4\log_2\log_2 D\rfloor, t = \lceil 2^s/h\rceil.$$

Воспользуемся разложением (10) и каждую компоненту f_i оператора f представим в виде

$$f_i(x_1,\ldots,x_n) = \bigvee_{\sigma_{s+1}\ldots\sigma_n}\left(\bigvee_{k=1}^{\lceil t/2\rceil}\left(\bigvee_{r=1}^{2} f_{i,2(k-1)+r,l}(x_1,\ldots,x_s)\right)\cdot I_{k,l}(x_1,\ldots,x_n)\right). \qquad (12)$$

Программу P, вычисляющую оператор f, представим в виде последовательности программ

$$\mathsf{P}_0\mathsf{P}_1\ldots\mathsf{P}_l\ldots\mathsf{P}_{2^{n-s}}.$$

Программа P_0 вычисляет все функции $f_{i,j,l}(x_1,\ldots,x_s)$, встречающиеся в формуле (12), все функции $I_{k,l}(x_1,\ldots,x_s)$ и все элементарные конъюнкции $x_{s+1}^{\sigma_{s+1}}\cdots x_n^{\sigma_n}$. Очевидно, что в силу (11) при выбранных значениях параметров h и s

$$C(\mathsf{P}_0)\leqslant 2^{h+s+2}+2^{n-s+1}\leqslant\frac{8D}{\log_2^2 D}. \qquad (13)$$

При $l\geqslant 1$ программа P_l вычисляет функцию

$$\bigvee_{k=1}^{\lceil t/2\rceil}\left(\bigvee_{r=1}^{2} f_{i,2(k-1)+r,l}(x_1,\ldots,x_s)\right)\cdot I_{k,l}(x_1,\ldots,x_n)$$

и состоит из программ

$$\mathsf{P}_{1,l}P_{2,l}\ldots\mathsf{P}_{k,l}\ldots\mathsf{P}_{\lceil t/2\rceil,l}.$$

Каждая программа $\mathsf{P}_{k,l}$, используя результаты работы программы P_0, вычисляет значения m функций

$$z_{i,k,l}=\bigvee_{r=1}^{2} f_{i,(k-1)2+r,l}(x_1,\ldots,x_s)$$

и функции $I_{k,l}(x_1,\ldots,x_n)$, объявляет полученное значение $z_{i,k,l}$ значением i-й компоненты оператора f и останавливает работу программы P, если $I_{k,l}(x_1,\ldots,x_n)=1$. Каждая программа $P_{k,l}$ состоит из $m+2$ команд: m команд вычисляют функции $z_{i,k,l}$, следующая команда вычисляет функцию $I_{k,l}(x_1,\ldots,x_n)$, которая является входом последней команды — команды остановки. Каждая такая программа, кроме, быть может, программы $\mathsf{P}_{\lceil t/2\rceil,l}$, останавливает работу на $2h$ наборах.

Нетрудно видеть, что объем используемой программой P памяти не превосходит $8D/\log_2^2 D+m+\mathcal{O}(1)\leqslant D$, а для среднего времени работы этой программы справедлива следующая последовательность неравенств:

$$\begin{aligned}
T(\mathsf{P}) &= \frac{1}{2^n}\sum_{\sigma_{s+1}\ldots\sigma_n}\sum_{\sigma_1\ldots\sigma_s} T_{\mathsf{P}}(\sigma_1\ldots\sigma_n) = \\
&= \frac{1}{2^n}\sum_{\sigma_{s+1}\ldots\sigma_n}\sum_{k=1}^{\lceil t/2\rceil}\sum_{(\sigma_1\ldots\sigma_s)\in Y_{2k-1}\bigcup Y_{2k}} T_{\mathsf{P}}(\sigma_1\ldots\sigma_n)\leqslant \\
&= \frac{1}{2^n}\sum_{l=1}^{2^{n-s}}\sum_{k=1}^{\lceil t/2\rceil}\left(C(\mathsf{P}_0)+\left((l-1)\left\lceil\frac{t}{2}\right\rceil+k\right)(m+2)\right)2h\leqslant \\
&\leqslant \frac{1}{2^n}\left(C(\mathsf{P}_0)2^{n-s}\left\lceil\frac{t}{2}\right\rceil+\left(2^{2n-2s}\frac{1}{2}\left\lceil\frac{t}{2}\right\rceil^2+2^{n-s}\left\lceil\frac{t}{2}\right\rceil^2\frac{1}{2}\right)(m+2)\right)2h.
\end{aligned}$$

Так как $th \sim 2^s$, $2^s = \Theta(\log_2^2 D)$ и $h \sim \log_2 D$, то, учитывая (13), видим, что

$$T(\mathsf{P}) \lesssim \frac{1}{2^n}\left(C(\mathsf{P}_0)\cdot 2^n + \left(\frac{2^{2n}}{4h} + \frac{2^{n+s}}{4h}\right)(m+2)\right) =$$

$$= C(\mathsf{P}_0) + \left(\frac{2^n}{4h} + \frac{2^s}{4h}\right)(m+2) \lesssim \left(\frac{8D}{\log_2^2 D} + \frac{2^n(m+2)}{4\log_2 D}\right) \sim \frac{2^n(m+2)}{4\log_2 D}.$$

Лемма доказана.

3.2. Программы без памяти. Программы, в которых каждая внутренняя переменная используется в качестве аргумента какой-либо команды только один раз, будем называть программами без памяти. Программа без памяти и без команд остановки является формулой. Далее функционалы сложности, отвечающие вычислениям без памяти, будем отмечать верхним индексом 0. Сложность вычисления булевых функций формулами изучалась в ряде работ О. Б. Лупановым. Им, например в [8], показано, что при $n \to \infty$ сложность вычисления самой сложной n-местной булевой функции формулами в стандартном базисе асимптотически совпадает с $2^n/\log_2 n$. Средняя сложность вычисления булевых функций программами без памяти изучалась Р. Н. Забалуевым в [5], где были установлены неравенства следующей теоремы.

Т е о р е м а 4. *Пусть $n \to \infty$. Тогда:*

(1) *для любой положительной постоянной ε доля n-местных булевых функций f, для которых не выполняется неравенство*

$$T^0(f) \geqslant (1-\varepsilon)\frac{2^{n-1}}{\log_2 n},$$

стремится к единице;

(2) *для каждой n-местной булевой функции f*

$$T^0(f) \lesssim \frac{2^{n-1}}{\log_2 n}.$$

Утверждение теоремы следует из доказываемых далее лемм 9 и 10.

Пусть $N_0'(L,k,n)$ — число программ без памяти с n входами и L командами, k из которых — команды остановки.

Л е м м а 7. *Пусть c' — постоянная. Тогда*

$$N_0'(L,k,n) \leqslant (c'n)^{L+k+1}.$$

Д о к а з а т е л ь с т в о. Произвольной программе P поставим в соответствие плоский ориентированный граф G, в котором каждой команде p_i этой программы соответствует вершина v_i, помеченная символом операции, выполняемой командой p_i. Вершины v_s и v_t свяжем дугой, направленной от v_s к v_t и помеченной символом j, если переменная y_s является j-м аргументом команды p_t. Если аргументом команды p_l является переменная x_m, то в G добавим вершину, помеченную символом x_m, и свяжем эту вершину с вершиной v_l дугой, направленной к v_l и помеченной символом j, если переменная x_m является j-м аргументом команды p_l.

Граф G будет лесом, состоящим из $k+1$ бинарного ориентированного корневого дерева. Листья этих деревьев помечены символами независимых переменных, дуги ориентированы по направлению к их корням v_{i_j},

где каждый из первых k корней v_{i_j} соответствует j-й команде остановки, а последний корень $v_{i_{k+1}}$ — последней команде p_L. Нетрудно видеть, что G содержит L внутренних вершин и $L+k+1$ листьев. Упорядочим деревья, добавив в граф k дуг e_j так, что e_j выходит из v_{i_j} и входит в $v_{i_{j+1}}$.

Теперь G полностью определяет программу P и является деревом из L внутренних вершин, помеченных символами из множества $P_2(2) \cup \{\mathtt{Stop}\}$, $L+k+1$ листьев, помеченных символами переменных x_i, и $2L+k$ дуг, $2L$ из которых помечены единицами и двойками. Следовательно,

$$N_0(L,k,n) \leqslant 4^{2L+k} \cdot 17^L \cdot 2^{2L} \cdot n^{L+k+1} \leqslant (c'n)^{L+k+1},$$

где c' — постоянная. Лемма доказана.

При доказательстве следующей леммы воспользуемся очевидным свойством минимальных программ: *в любой минимальной программе нулевые аргументы разных команд остановки различны.*

Пусть $N_0(L,n)$ — число минимальных программ без памяти с n входами и не более чем L командами.

Лемма 8. *Пусть* $n \to \infty$, c — *постоянная*, $\log_2 L \gg \log_2 n$. *Тогда*

$$N_0(L,n) \leqslant (cn)^{L+o(L)}.$$

Доказательство. Допустим, что в минимальной программе P из L' команд содержится не менее $k = \dfrac{4L' \log_2(c'n)}{\log_2 L'}$ команд остановки. Без ограничения общности для упрощения записи формул будем считать значения всех встречающихся далее дробей целыми. Пусть L_i — количество команд, участвующих в вычислении нулевого аргумента i-й команды остановки. Без ограничения общности будем считать, что $L_i \leqslant L_{i+1}$ при $i = 1, \ldots, k-1$. Очевидно, что $\sum\limits_{i=1}^{k} L_i < L'$. Тогда $L_i \leqslant 2L'/k$ для каждого $i \leqslant k/2$, так как в противном случае $\sum\limits_{i=k/2}^{k} L_i > (k/2) \cdot (2L'/k) = L'$. Таким образом, в силу предыдущей леммы число различных функций среди нулевых аргументов первых $k/2$ команд остановки не превосходит

$$n + (c'n)^{2L'/k} \leqslant n + (c'n)^{2L' \Big/ \frac{4L' \log_2(c'n)}{\log_2 L'}} = n + \sqrt{L'}.$$

Так как при $L' \gg n$

$$k/2 = \frac{2L' \log_2(c'n)}{\log_2 L'} > n + \sqrt{L'},$$

то среди нулевых аргументов первых $k/2$ команд остановки найдутся одинаковые, что противоречит минимальности программы P. Поэтому при $\log_2 L \gg \log_2 n$ в любой минимальной программе из L' команд число команд остановки не превосходит $\dfrac{4L' \log_2(c'n)}{\log_2 L'} = o(L')$. Теперь для доказательства леммы достаточно воспользоваться предыдущей леммой и условием $\log_2 L \gg \log_2 n$:

$$\begin{aligned} N_0(L,n) &\leqslant \sum_{L'=0}^{L} \sum_{k} N_1(L',k,n) \leqslant \\ &\leqslant \sum_{L'=0}^{L/n} \sum_{k} N_1(L',k,n) + \sum_{L'=L/n+1}^{L} \sum_{k} N_1(L',k,n) \leqslant \\ &\leqslant \sum_{L'=0}^{L/n} L' \cdot (c'n)^{2L'} + \sum_{L'=L/n+1}^{L} L' \cdot (c'n)^{L'+o(L')} \leqslant (cn)^{L+o(L)}. \end{aligned}$$

Лемма доказана.

Л е м м а 9. *Пусть $n \to \infty$. Тогда для любой постоянной $\varepsilon > 0$ доля n-местных булевых функций f, для которых*

$$T^0(f) \geqslant (1-\varepsilon)\frac{2^{n-1}}{\log_2 n},$$

стремится к единице.

Д о к а з а т е л ь с т в о. Пусть f — n-местная булева функция, P — минимальная программа, вычисляющая f. Без ограничения общности будем полагать, что $2^n/n$ целое. Пусть набор $\boldsymbol{x}_i$ такой, что $N_{\mathsf{P}}(\boldsymbol{x}_i) = \frac{i2^n}{n}$, где $i = 1, 2, \ldots, n-1$. Оценим число булевых функций, у минимальных программ которых найдется такой набор $\boldsymbol{x}_i$, что $T_{\mathsf{P}}(\boldsymbol{x}_i) \leqslant \frac{(1-\varepsilon)i2^n}{n\log_2 n}$. Каждая такая функция однозначно определяется первыми $T_{\mathsf{P}}(\boldsymbol{x}_i)$ командами своей минимальной программы и двоичным набором длины не более чем $2^n - N_{\mathsf{P}}(\boldsymbol{x}_i)$ — значениями на тех аргументах, время работы на которых больше времени работы на $\boldsymbol{x}_i$. В силу предыдущей леммы для числа N_i, равного числу различных программ без памяти, сложность которых не превосходит $T_{\mathsf{P}}(\boldsymbol{x}_i)$, справедливо неравенство

$$N_i \leqslant (cn)^{T_{\mathsf{P}}(\boldsymbol{x}_i)+o(T_{\mathsf{P}}(\boldsymbol{x}_i))} \leqslant$$
$$\leqslant (cn)^{(1-\varepsilon)(1+o(1))\cdot i2^n/n\log_2 n} \leqslant 2^{(1-\varepsilon)(1+o(1))\cdot i2^n/n}.$$

Следовательно, M — число рассматриваемых функций — не превосходит величины

$$\sum_{i=1}^{n-1} 2^{(1-\varepsilon)(1+o(1))\cdot i2^n/n}\cdot 2^{2^n - i2^n/n} = \sum_{i=1}^{n-1} 2^{2^n-(\varepsilon-o(1))\cdot i2^n/n} = o\left(2^{2^n}\right).$$

Сравнивая полученную оценку величины M с числом всех n-местных булевых функций, видим, что для $i = 1, 2, \ldots, n-1$ все минимальные программы почти всех булевых функций удовлетворяют условию:

$$\text{если набор } \boldsymbol{x}_i \text{ такой, что } N_{\mathsf{P}}(x_i) = \frac{i2^n}{n}, \text{ то } T_{\mathsf{P}}(\boldsymbol{x}_i) > \frac{(1-\varepsilon)i2^n}{n\log_2 n}.$$

Положим $X_i = \{\boldsymbol{x} \mid N_{\mathsf{P}}(\boldsymbol{x}_i) < N_{\mathsf{P}}(\boldsymbol{x}) \leqslant N_{\mathsf{P}}(\boldsymbol{x}_{i+1})\}$. Тогда для среднего времени работы каждой такой программы имеем:

$$T(\mathsf{P}) = \frac{1}{2^n}\sum_{\boldsymbol{x}} T_{\mathsf{P}}(\boldsymbol{x}) \geqslant \frac{1}{2^n}\sum_{i=1}^{n-1} T_{\mathsf{P}}(\boldsymbol{x}_i)|X_i| = \frac{1}{2^n}\sum_{i=1}^{n-1} T_P(x_i)\frac{2^n}{n} >$$
$$> \frac{1}{n}\sum_{i=1}^{n-1}\frac{(1-\varepsilon)i2^n}{n\log_2 n} = \frac{(1-\varepsilon)n(n-1)2^n}{2n^2\log_2 n} \geqslant (1-2\varepsilon)\cdot\frac{2^{n-1}}{\log_2 n}.$$

Таким образом, при $n \to \infty$ для любой положительной постоянной ε средняя сложность почти каждой булевой функции, зависящей от n переменных, не меньше чем $(1-2\varepsilon)\frac{2^{n-1}}{n\log_2 n}$. Лемма доказана.

Л е м м а 10. *Пусть $n \to \infty$. Тогда для каждой n-местной булевой функции f*

$$T^0(f) \lesssim \frac{2^{n-1}}{\log_2 n}.$$

Доказательство. Положим $s=\lfloor n-\log_2 n\rfloor$. Функцию f разложим по первым $n-s$ переменным:

$$f(x_1,\ldots,x_n)=\bigvee_{\sigma_1\ldots\sigma_{n-s}} f(\sigma_1,\ldots,\sigma_{n-s},x_{n-s+1},\ldots,x_n)\cdot x_1^{\sigma_1}\ldots x_{n-s}^{\sigma_{n-s}}.$$

Программу, вычисляющую функцию f, представим в следующем виде:

$$\mathsf{P}=\mathsf{P}_0\ldots\mathsf{P}_j\ldots\mathsf{P}_{2^{n-s}-1},$$

где $j=|(\sigma_1\ldots\sigma_{n-s})|$, P_j — программа, вычисляющая функцию

$$f_j(x_{n-s+1},\ldots,x_n)=f(\sigma_1,\ldots,\sigma_{n-s},x_{n-s+1},\ldots,x_n)$$

и прекращающая работу программы P, если $x_1^{\sigma_1}\cdot\ldots\cdot x_{n-s}^{\sigma_{n-s}}=1$. Так как формульная сложность произвольной булевой функции, зависящей от s переменных, асимптотически не превосходит $\frac{2^s}{\log_2 s}$ (см. [8]), то $L^0(\mathsf{P}_j)\lesssim\frac{2^s}{\log_2 s}$. Поэтому

$$T(\mathsf{P})\sim\frac{1}{2^n}\sum_{j=0}^{2^{n-s}-1}\left(2^s\sum_{i=1}^{j}L(\mathsf{P}_i)\right)=\frac{1}{2^n}2^s\sum_{j=0}^{2^{n-s}-1}\sum_{i=1}^{j}L(\mathsf{P}_i)\lesssim$$

$$\lesssim\frac{1}{2^n}2^s\frac{2^s}{\log_2 s}\sum_{j=0}^{2^{n-s}-1}j\lesssim\frac{1}{2^n}\frac{2^{2s}}{\log_2 s}\frac{2^{2(n-s)}}{2}=\frac{2^{n-1}}{\log_2 s}\sim\frac{2^{n-1}}{\log_2 n}.$$

Лемма доказана.

§ 4. Функции из специальных классов

В этом разделе рассмотрим три естественных класса булевых функций: симметрические функции, функции с ограниченным числом единичных значений и монотонные функции. В каждом из этих классов средняя сложность почти всех функций по порядку величины меньше их сложности вычисления схемами из функциональных элементов.

4.1. Симметрические функции. С точностью до постоянного множителя сложность любой симметрической булевой функции пропорциональна числу ее существенных аргументов. В случае средней сложности ситуация иная — средняя сложность зависит не от числа аргументов функции, а с точностью до постоянного множителя совпадает с величиной $n-l(f)+2$, где через $l(f)$ обозначается максимальное число последовательных слоев, на которых функция f принимает одинаковые значения. Для линейной функции $x_1\oplus\ldots\oplus x_n$ значение параметра l равно единице, для функции голосования n переменных — $\lceil(n+1)/2\rceil$, а для n-местных дизъюнкции и конъюнкции — n.

Теорема 5. *При $n\to\infty$ для любой n-местной симметрической булевой функции f справедливо равенство*

$$T(f)=\Theta(n-l(f)+2).$$

Доказательство. *Нижняя оценка.* Пусть f — произвольная симметрическая функция, зависящая от n аргументов. Рассмотрим два случая: $l(f)>n-2$ и $l(f)\leqslant n-2$.

(1) В первом случае $1 \leqslant n - l(f) + 2 < 4$. Поэтому нижняя оценка теоремы следует из очевидного неравенства $T(f) \geqslant 1$ справедливого для любой булевой функции.

(2) Во втором случае $n - l(f) - 1 \geqslant \frac{1}{4}(n - l(f) + 2)$. Поэтому для доказательства нижней оценки теоремы достаточно показать, что $T(f) \geqslant n - l(f) - 1$.

Пусть P — минимальная программа, вычисляющая f, s_1 — первая команда остановки этой программы, $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ — набор, на котором команда s_1 останавливает вычисления. Если команда s_1 является k-й командой P и $k < n - l(f) - 1$, то система функций $\{\mathsf{q}_1(\boldsymbol{x}), \mathsf{z}(\boldsymbol{x}; k-1)\}$, вычисляемая первыми k командами P, существенно зависит не более чем от $m = n - l(f) - 1$ переменных. Так как f симметрическая функция, то без ограничения общности полагаем, что этими переменными являются $x_1, \ldots, x_m$. В этом случае из минимальности программы P легко следует существование таких постоянных $\alpha_1, \ldots, \alpha_m$, что команда s_1 останавливает работу P вне зависимости от значений переменных $x_{m+1}, \ldots, x_n$. Следовательно, для любых значений $\sigma_{m+1}, \ldots, \sigma_n$ этих переменных выполняется равенство

$$f(\alpha_1, \ldots \alpha_m, \sigma_{m+1}, \ldots, \sigma_n) = \sigma,$$

где σ — булева константа. В то же время найдется такой набор $\beta_{m+1}, \ldots, \beta_n$, что

$$\mathsf{P}(\alpha_1, \ldots \alpha_m, 0, \ldots, 0) \neq \mathsf{P}(\alpha_1, \ldots \alpha_m, \beta_{m+1}, \ldots, \beta_n).$$

Если такой набор не существует, то f принимает одинаковое значение σ на наборах из $n - m = l(f) + 1$ последовательных слоев, что противоречит определению величины $l(f)$. Пришли к противоречию. Следовательно, $T(f) \geqslant k \geqslant n - l(f) - 1$.

Верхняя оценка. Теперь покажем, что для любой симметрической булевой функции f, зависящей от n переменных, ее средняя сложность $T(f)$ есть $\mathcal{O}(n - l(f) + 2)$. Рассмотрим два случая: $l(f) \leqslant \frac{n}{2}$ и $l(f) > \frac{n}{2}$.

(1) В первом случае $n - l(f) \geqslant \frac{n}{2}$, и для вычисления f достаточно использовать обычную схему из функциональных элементов. Очевидно, что

$$T(f) \leqslant L(f) = \mathcal{O}(n) = \mathcal{O}(n - l(f) + 2).$$

(2) Рассмотрим второй случай. Допустим, что максимальная последовательность слоев, на которых достигается величина $l(f)$, начинается с h-го слоя, и значение f на наборах из этих слоев равно σ. Положим $m = n - l(f) + 1$. Тогда $f(\alpha_1, \ldots, \alpha_n) = \sigma$ на любом наборе $(\alpha_1, \ldots, \alpha_n)$, содержащем не менее h единиц и не менее $n - (h + l(f) - 1) = m - h$ нулей. Воспользуемся этим свойством функции f для ее вычисления. Опишем программу P, вычисляющую функцию f. Положим $n = (2m - 1)t + k$, где $0 \leqslant k < 2m - 1$. Программу P представим в виде $t + 1$ последовательных подпрограмм $\mathsf{P} = \mathsf{P}_1 \ldots \mathsf{P}_j \ldots \mathsf{P}_t \mathsf{P}_{t+1}$, работающих следующим образом.

— Подпрограмма P_1 присваивает выходной переменной значение σ, вычисляет сумму первых $(2m - 1)$ переменных и останавливает вычисления, если эта сумма не меньше h и не больше $2m - 1 - (m - h) = m + h - 1$.

— При каждом $j \in \{2, 3, \ldots, t\}$ подпрограмма P_j вычисляет сумму

$$S_j = \sum_{i=(2m-1)(j-1)+1}^{(2m-1)j} x_i$$

и останавливает вычисления, если $h \leqslant S_j \leqslant m + h - 1$.
— Последняя подпрограмма P_{t+1} вычисляет $f(x_1, \ldots, x_n)$ и присваивает это значение выходной переменной.

Легко видеть, что при каждом $j \in \{1, \ldots, t\}$ подпрограмма P_j состоит из $\mathcal{O}(m)$ команд, а подпрограмма P_{t+1} — из $\mathcal{O}(n) = \mathcal{O}(mt)$ команд. Таким образом,

$$\begin{aligned} C(\mathsf{P}_j) &= \mathcal{O}(m), \ \ j \in \{1, \ldots, t\}; \\ C(\mathsf{P}_{t+1}) &= \mathcal{O}(mt); \\ C(\mathsf{P}) &= \mathcal{O}(mt). \end{aligned} \tag{14}$$

Оценим среднее время работы программы P. Нетрудно убедиться в том, что подпрограмма P_1 останавливает вычисления на

$$A_1 = 2^{n-(2m-1)} \sum_{i=h}^{m+h-1} \binom{2m-1}{i} \geqslant 2^{n-1} \tag{15}$$

наборах, а каждая подпрограмма P_j при всех j больших единицы и не превосходящих t — на

$$A_j = \left(2^n - \sum_{i=1}^{j-1} A_i\right) 2^{-(2m-1)} \left(\sum_{i=h}^{m+h-1} \binom{2m-1}{i}\right) \geqslant \frac{1}{2} \left(2^n - \sum_{i=1}^{j-1} A_i\right) \tag{16}$$

наборах. Индукцией по j покажем, что

$$\sum_{i=1}^{j} A_i \geqslant 2^n - 2^{n-j} \tag{17}$$

для всякого $j \in \{1, 2, \ldots, t\}$. В основание индукции ($j = 1$) положим неравенство (15). Далее предположим, что $\sum\limits_{i=1}^{s} A_i \geqslant 2^n - 2^{n-s}$ для любого $s \in \{1, \ldots, j-1\}$. Тогда из (16) и предположения индукции имеем:

$$\begin{aligned} \sum_{i=1}^{j} A_j = \sum_{i=1}^{j-1} A_i + A_j &\geqslant \sum_{i=1}^{j-1} A_i + \frac{1}{2} \left(2^n - \sum_{i=1}^{j-1} A_i\right) = \\ &= \frac{1}{2} \left(2^n + \sum_{i=1}^{j-1} A_i\right) \geqslant \frac{1}{2} \left(2^n + 2^n - 2^{n-j+1}\right) = 2^n - 2^{n-j}. \end{aligned}$$

Так как $\sum\limits_{i=1}^{j} A_i \leqslant 2^n$, то из (17) имеем:

$$\sum_{i=s}^{j} A_i = \sum_{i=1}^{j} A_i - \sum_{i=1}^{s-1} A_i \leqslant 2^n - (2^n - 2^{n-s+1}) = 2^{n-s+1}. \tag{18}$$

Также из (17) легко следует, что все вместе подпрограммы $\mathsf{P}_1, \ldots, \mathsf{P}_t$ прекращают вычисления не менее чем на $2^n \left(1 - 2^{-t}\right)$ наборах, и поэтому под-

программа P_{t+1} работает не более чем на 2^{n-t} наборах. Следовательно, учитывая неравенство (18) и равенство (14),

$$T(\mathsf{P}) = \frac{1}{2^n}\left(\sum_{j=1}^{t} A_j \sum_{i=1}^{j} C(\mathsf{P}_i) + 2^{n-t}C(\mathsf{P})\right) =$$
$$= \frac{\mathcal{O}(m)}{2^n}\left(\sum_{j=1}^{t} A_j j + t\cdot 2^{n-t}\right) = \frac{\mathcal{O}(m)}{2^n}\left(\sum_{j=1}^{t}\sum_{i=j}^{t} A_i + 2^n\right) =$$
$$= \frac{\mathcal{O}(m)}{2^n}\left(\sum_{j=1}^{t} 2^{n-j+1} + 2^n\right) = \mathcal{O}(m)\left(\sum_{j=1}^{\infty} 2^{1-j} + 1\right) = \mathcal{O}(m).$$

Теорема доказана.

4.2. Функции с ограниченным числом единичных значений. Далее в теореме 6 оценивается средняя сложность вычисления частичных булевых функций с ограниченным числом единиц. Для сложности вычисления схемами из функциональных элементов произвольной частичной n-местной функции f, определенной на области из N элементов и равной единице на N_1 наборах из этой области, справедливо неравенство

$$L(f) \lesssim \frac{\log_2 \binom{N}{N_1}}{\log_2 \log_2 \binom{N}{N_1}} + \mathcal{O}(n). \tag{19}$$

Данная оценка является асимптотически минимальной (в смысле Шеннона) при всех значениях параметров N и N_1, при которых первое слагаемое в правой части (19) растет быстрее чем n. Доказательство неравенства (19) стало итогом более чем сорокалетней работы многих математиков. Среди работ, внесших основной вклад в доказательство этого неравенства, следует отметить работы Э. И. Нечипорука о сложности реализации матриц из различных классов вентильными схемами [10, 11], классическую работу О. Б. Лупанова [9], работы Л. А. Шоломова [25, 26], А. Е. Андреева [4] и А. Е. Андреева с соавторами [27]. Полное доказательство неравенства (19) можно найти в [19]. Элементы этого доказательства вместе с методами из [16] используются в доказательстве верхней оценки теоремы 6.

Т е о р е м а 6. *Пусть $n \to \infty$, $D \subseteq \{0,1\}^n$, D состоит из N наборов, $n\log_2 n \ll N_1 \ll N$. Тогда:*

(1) *для каждой частичной булевой функции f, определенной на области D и принимающей в этой области N_1 единичных значений, справедливо неравенство*

$$T(f) \lesssim 4.135 \cdot \frac{N_1}{\log_2 N_1};$$

(2) *для любой положительной постоянной ε доля частичных булевых функций f, определенных на области D, принимающих в этой области N_1 единичных значений, и для которых выполняется неравенство*

$$T(f) \geqslant (1-\varepsilon)\frac{27}{32} \cdot \frac{N_1}{\log_2 N_1},$$

стремится к единице.

Утверждение теоремы следует из доказываемых далее лемм 20 и 23.

Набор $\boldsymbol{\alpha} \in \{0,1\}^m$ назовем доопределением набора $\boldsymbol{\beta} \in \{0,1,*\}^m$, если $\alpha_i = \beta_i$ для всех тех i, для которых $\beta_i \in \{0,1\}$. Множество $B \subseteq \{0,1\}^m$ назовем доопределением множества $A \subseteq \{0,1,*\}^m$, если для каждого элемента $\boldsymbol{\alpha}$ из A в B найдется элемент $\boldsymbol{\beta}$, являющийся доопределением $\boldsymbol{\alpha}$.

Лемма 11. *Пусть A — множество наборов из $\{0,1,*\}^m$, каждый из которых содержит s булевых элементов, среди которых t единиц и $s-t$ нулей. Существует доопределение множества A, состоящее из не более чем $2m^2\binom{s}{t}$ наборов.*

Доказательство. Пусть $B(m,k)$ — множество всех двоичных наборов длины m с k единицами. Допустим, что любое N-элементное подмножество множества $B(m,k)$ не является доопределением множества A. Тогда для каждого такого подмножества можно указать хотя бы один набор из A, для которого в этом подмножестве нет доопределения. Поэтому число пар $(\boldsymbol{\alpha}, B)$, где $\boldsymbol{\alpha} \in A$, а B — N-элементное подмножество множества $B(m,k)$, таких, что в B нет доопределения α, не меньше чем $\left(\binom{m}{k}\right)$. Так как A состоит из $\binom{m}{s}\binom{s}{t}$ элементов, то в A найдется такой набор $\boldsymbol{\alpha}$, что, по крайней мере, $\left(\binom{m}{k}\right) \Big/ \binom{m}{s}\binom{s}{t}$ N-элементных подмножеств множества $B(m,k)$ не содержат доопределение $\boldsymbol{\alpha}$. С другой стороны, легко видеть, что для любого набора из A ровно $\left(\binom{m}{k} - \binom{m-s}{k-t}\right)$ N-элементных подмножеств множества $B(m,k)$ не содержат его доопределение. Поэтому должно выполняться неравенство

$$\left(\binom{m}{k}\right) \Big/ \binom{m}{s}\binom{s}{t} \leqslant \left(\binom{m}{k} - \binom{m-s}{k-t}\right). \tag{20}$$

Определим максимальное N, при котором это возможно. Для этого оценим снизу величину $\left(\binom{m}{k}\right) \Big/ \left(\binom{m}{k} - \binom{m-s}{k-t}\right)$. Так как $\dfrac{X-k}{X-Y-k} \geqslant \dfrac{X}{X-Y}$ при $X-Y-k>0$ и $\left(1+\dfrac{1}{x}\right)^x \geqslant 2$ при $x \geqslant 1$, то

$$\begin{aligned}\binom{X}{N} \Big/ \binom{X-Y}{N} &= \prod_{k=0}^{N-1} \frac{X-k}{X-Y-k} \geqslant \left(\frac{X}{X-Y}\right)^N \geqslant \\ &\geqslant \left(1+\frac{Y}{X-Y}\right)^N \geqslant \left(1+\frac{Y}{X}\right)^{X/Y(NY/X)} \geqslant 2^{NY/X}.\end{aligned}$$

Объединяя полученную оценку и неравенство (20), имеем

$$2^{N\binom{m-s}{k-t}/\binom{m}{k}} \leqslant \left(\binom{m}{k}\right) \Big/ \left(\binom{m}{k} - \binom{m-s}{k-t}\right) \leqslant \binom{m}{s}\binom{s}{t}.$$

Так как $\binom{m}{s}\binom{s}{t} < 3^m$, то, вычисляя двоичные логарифмы от левой и правой частей получившегося неравенства, видим, что

$$N < \log_2 3 \cdot m\binom{m}{k} \Big/ \binom{m-s}{k-t}. \tag{21}$$

Далее рассмотрим равенство $\binom{m}{k} = \sum_{i=0}^{k} \binom{s}{i}\binom{m-s}{k-i}$. Покажем, что при фиксированных m, k и s произведения под знаком суммы возрастают вместе с i до некоторого максимального значения, а затем начинают убывать. Для этого рассмотрим отношение двух соседних произведений и выясним, когда оно не превосходит единицы:

$$\binom{s}{i-1}\binom{m-s}{k-i+1}\Big/\binom{s}{i}\binom{m-s}{k-i} = \\ = \frac{s!(m-s)!i!(s-i)!(k-i)!(m-s-k+i)!}{(i-1)!(s-i+1)!(k-i+1)!(m-s-k+i-1)!s!(m-s)!} = \\ = \frac{i(m-s-k+i)}{(s-i+1)(k-i+1)} \leqslant 1.$$

Продолжая преобразования, видим, что

$$0 \geqslant i(m-s-k+i) - (s-i+1)(k-i+1) = \\ = i^2 + i(m-s-k) - i^2 + i(s+k+2) - (s+1)(k+1) = \\ = i(m+2) - (s+1)(k+1).$$

Таким образом, при $i \leqslant \frac{(s+1)(k+1)}{m+2}$ значения произведений возрастают, при $i > \frac{(s+1)(k+1)}{m+2}$ — убывают и, следовательно, своего максимального значения достигают при

$$i = \left\lfloor \frac{(s+1)(k+1)}{m+2} \right\rfloor. \tag{22}$$

Рассматривая правую часть в (22) как функцию от k, легко видеть, что при возрастании k от нуля до m ее значение также возрастает, пробегая все целые числа между нулем и s, принимая, в частности, значение t. Пусть далее k такое, при котором максимум произведений $\binom{s}{i}\binom{m-s}{k-i}$ достигается при $i = t$. Продолжая неравенство (21) при выбранном значении k, имеем

$$N < \log_2 3 \cdot m\left(\sum_{i=0}^{k}\binom{s}{i}\binom{m-s}{k-i}\right)\Big/\binom{m-s}{k-t} \leqslant 2m^2\binom{s}{t}.$$

Таким образом, из предположения, что любое N-элементное подмножество множества $B(m,k)$ не является доопределением множества A, следует неравенство $N < 2m^2\binom{s}{t}$. Поэтому при N больших или равных $2m^2\binom{s}{t}$ среди N-элементных подмножеств множества $B(m,k)$ найдется хотя бы одно доопределение множества A. Лемма доказана.

На множестве наборов с компонентами из $\{0,1,*\}$ определим функцию I. Если набор $\boldsymbol{\alpha}$ из $\{0,1,*\}^n$ содержит s булевых компонент, t из которых равны единице, то положим $I(\boldsymbol{\alpha}) = \log_2\binom{s}{t}$.

Лемма 12. *Пусть $A = \{\boldsymbol{\alpha}\}$ — множество наборов из $\{0,1,*\}^m$ таких, что $I(\boldsymbol{\alpha}') < R$, где набор α' получается из $\boldsymbol{\alpha}$ заменой последней булевой компоненты символом $*$. Тогда существует доопределение множества A, состоящее из не более чем $2m^5 2^R$ наборов.*

Доказательство. Множество A разобьем на непересекающиеся классы, поместив в класс $A(s,t)$, $t \leqslant s$, все наборы с s булевыми компонентами, t из которых равны единице. Из леммы 11 следует, что для множества $A(s,t)$ существует доопределение $B(s,t)$, состоящее из не более чем $2m^2\binom{s}{t}$ наборов. Пусть $\boldsymbol{\alpha} \in A(s,t)$. Тогда $I(\boldsymbol{\alpha}) = \log_2 \binom{s}{t}$. Так как $\binom{s}{t} \leqslant m\binom{s-1}{t}$ и $\binom{s}{t} \leqslant m\binom{s-1}{t-1}$ и по условию леммы $I(\boldsymbol{\alpha}') < R$, то $\binom{s}{t} < m \cdot 2^R$.

Очевидно, что общее число классов (число возможных значений параметров s и t) не превосходит m^2. Поэтому множество $\cup_{s,t} B(s,t)$ состоит из не более чем $2m^5 2^R$ наборов и по построению является доопределением множества A. Лемма доказана.

Лемма 13. *Пусть $D \subseteq \{0,1\}^n$ состоит из N наборов, частичная булева функции $f : D \to \{0,1\}$ равна единице на N_1 наборах из D. Если параметры n, N, N_1 такие, что $N_1 \leqslant \frac{1}{2}N$ и $\log_2 \log_2 \binom{N}{N_1} \sim n$ при $n \to \infty$, то*

$$L(f) \lesssim \frac{\log_2 \binom{N}{N_1}}{\log_2 \log_2 \binom{N}{N_1}}.$$

Доказательство. Введем параметры R и k, значения которых определим позднее. Значения частичной n-местной булевой функции f запишем в таблице T_f из 2^k столбцов и 2^{n-k} строк, поставив в соответствие i-му столбцу таблицы*) двоичный набор $(\sigma_1, \ldots, \sigma_k)$, являющийся двоичным представлением числа i, а j-й строке — набор $(\sigma_{k+1}, \ldots, \sigma_n)$, являющийся двоичным представлением числа j. В таблице на пересечении i-го столбца и j-й строки поставим значение $f(\sigma_1, \ldots, \sigma_k, \sigma_{k+1}, \ldots, \sigma_n)$. Каждую строку таблицы представим в виде следующих друг за другом элементарных наборов $\boldsymbol{\alpha}$, для каждого из которых, кроме, быть может, последнего, справедливы неравенства $I(\boldsymbol{\alpha}) \geqslant R$ и $I(\boldsymbol{\alpha}') < R$. Множество таких наборов разобьем на классы, поместив в класс P_{ij} наборы, начинающиеся в i-й и заканчивающиеся в j-й позициях. Нетрудно видеть, что число различных классов не превосходит величины 2^{2k-1}.

Из леммы 12 следует, что для множества элементарных наборов класса P_{ij} существует множество их доопределений, которое состоит из не более чем $2^{5k+1}2^R$ наборов длины 2^k, в каждом из которых первые $i-1$ и последние $2^k - j$ компонент равны нулю. Следовательно, для множества всех элементарных наборов существует множество их доопределений H, которое состоит из не более чем $2^{7k}2^R$ наборов длины 2^k.

Преобразуем таблицу T_f, заменив в ней каждый элементарный набор каким-либо его доопределением из H. Нетрудно видеть, что преобразованная таблица будет таблицей значений некоторой n-местной булевой функции h, являющейся доопределением функции f.

Пусть $\boldsymbol{\gamma} = (\gamma_1, \ldots, \gamma_{2^k}) \in H$. Введем множество G, состоящее из функций

$$g_{\boldsymbol{\gamma}}(x_1, \ldots, x_k) = \bigvee_{\boldsymbol{\sigma}=(\sigma_1,\ldots,\sigma_k)} x_1^{\sigma_1} \cdot \ldots \cdot x_k^{\sigma_k} \cdot \gamma_{|\sigma|},$$

*) Столбцы и строки таблицы нумеруем целыми числами, начиная с нуля.

векторы значений которых, как нетрудно видеть, являются элементами множества H. Очевидно, что $|G| \leqslant 2^{7k}2^R$ и функция h может быть выражена через функции системы G следующим образом:

$$h(x_1, \ldots, x_n) = \bigvee_{\boldsymbol{\sigma}=(\sigma_{k+1},\ldots,\sigma_n)} \Big(\bigvee_{g\in G} g(x_1, \ldots, x_k)\Big) x_{k+1}^{\sigma_{k+1}} \cdot \ldots \cdot x_n^{\sigma_n}. \qquad (23)$$

Оценим число функций g в (23). Прежде всего заметим, что число функций, соответствующих наборам $\boldsymbol{\alpha}$ с $I(\boldsymbol{\alpha}) < R$, не превосходит числа строк таблицы, т. е. не больше, чем 2^{n-k}. Число остальных функций обозначим через p. Соответствующие этим функциям элементарные наборы перенумеруем числами от 1 до p. Пусть s_i и t_i — число булевых и число единичных компонент в i-м элементарном наборе. Так как $\sum\limits_{i=1}^{p} s_i \leqslant N$, $\sum\limits_{i=1}^{p} t_i \leqslant N_1$ и по условию леммы $N_1 \leqslant \frac{1}{2}N$, то

$$\log_2 \binom{N}{N_1} \geqslant \log_2 \binom{\sum s_i}{\sum t_i} \geqslant \log_2 \prod_{i=1}^{p} \binom{s_i}{t_i} = \sum_{i=1}^{p} \log_2 \binom{s_i}{t_i} \geqslant p \cdot R.$$

Таким образом, общее число элементарных наборов в T_f, а следовательно, и функций g в (23) не превосходит

$$\log_2 \binom{N}{N_1} \Big/ R + 2^{n-k}. \qquad (24)$$

Опишем схему S, вычисляющую функцию f и удовлетворяющую требованиям леммы. Эта схема состоит из трех подсхем S_1–S_3, и ее конструкция основана на формуле (23). Подсхема S_1 вычисляет все элементарные конъюнкции первых k переменных и, используя эти конъюнкции, все функции из G. Учитывая, что $|G| \leqslant 2^{7k}2^R$ и каждая функция из G является дизъюнкцией не более чем 2^k элементарных конъюнкций, имеем

$$L(\mathsf{S}_1) \leqslant 2^{8k}2^R. \qquad (25)$$

Подсхема S_2 вычисляет все элементарные конъюнкции последних $n-k$ переменных. Очевидно, что

$$L(\mathsf{S}_2) \leqslant 2^{n-k+1}. \qquad (26)$$

Подсхема S_3 подключена к выходам подсхем S_1 и S_2 и вычисляет полностью определенную функцию $h(x_1, \ldots, x_n)$ в соответствии с равенством (23). Из (24) следует, что

$$L(S_3) \leqslant 2^{n-k+1} + \log_2 \binom{N}{N_1} \Big/ R. \qquad (27)$$

Суммируя неравенства (25)–(27), видим, что

$$L(\mathsf{S}) \leqslant \log_2 \binom{N}{N_1} \Big/ R + 2^{8k}2^R + 2^{n-k+2}. \qquad (28)$$

Положим

$$k = \lceil n - \log_2 \log_2 \binom{N}{N_1} + 2 \log_2 \log_2 \log_2 \binom{N}{N_1} \rceil,$$

$$R = \lfloor \log_2 \log_2 \binom{N}{N_1} - 8k - 2 \log_2 \log_2 \log_2 \binom{N}{N_1} \rfloor.$$

Тогда, учитывая условие $\log_2 \log_2 \binom{N}{N_1} \sim n$, имеем:

$$\begin{gathered} R \sim \log_2 \log_2 \binom{N}{N_1}, \quad k = o\Big(\log_2 \log_2 \binom{N}{N_1}\Big), \\ R + 8k \leqslant \log_2 \log_2 \binom{N}{N_1} - 2 \log_2 \log_2 \log_2 \binom{N}{N_1}, \\ n - k \leqslant \log_2 \log_2 \binom{N}{N_1} - 2 \log_2 \log_2 \log_2 \binom{N}{N_1}. \end{gathered} \tag{29}$$

Подставляя оценки из (29) в (28), после несложных преобразований получаем требуемую оценку сложности схемы S:

$$L(\mathsf{S}) \leqslant \frac{\log_2 \binom{N}{N_1}}{\log_2 \log_2 \binom{N}{N_1}} \Big(1 + \mathcal{O}\Big(\frac{k}{R}\Big)\Big) \sim \frac{\log_2 \binom{N}{N_1}}{\log_2 \log_2 \binom{N}{N_1}}.$$

Лемма доказана.

Комбинируя доказательства лемм 13 и 3, нетрудно установить справедливость следующего утверждения, доказательство которого опустим.

Л е м м а 14. *Пусть $D \subseteq \{0,1\}^n$ состоит из N наборов, $\log_2 N \sim n$ при $n \to \infty$. Тогда для любой частичной булевой функции $f\colon D \to \{0,1\}$*

$$T(f) \lesssim \frac{N}{2 \log_2 n}.$$

В следующих леммах распространим утверждение леммы 13 на функции, определенные на областях небольшого размера.

Л е м м а 15. *Пусть $A, B \subseteq \{0,1\}^n$, $A \cap B = \varnothing$, m — целое. Тогда существует линейный оператор $\mathscr{L}\colon \{0,1\}^n \to \{0,1\}^m$ такой, что*

$$|\{(\boldsymbol{x}, \boldsymbol{y}) \mid \boldsymbol{x} \in A, \boldsymbol{y} \in B, \mathscr{L}(\boldsymbol{x}) = \mathscr{L}(\boldsymbol{y})\}| \leqslant 2^{-m}|A||B|.$$

Д о к а з а т е л ь с т в о. Обозначим через $F(n,m)$ множество всех линейных операторов $\mathscr{L}\colon \{0,1\}^n \to \{0,1\}^m$. Очевидно, что $|F(n,m)| = 2^{nm}$. Так как для любых двух различных наборов $\boldsymbol{x}$ и $\boldsymbol{y}$ из $\{0,1\}^n$ имеется ровно 2^{n-1} n-местных линейных функций f с нулевым свободным членом, значения которых на этих наборах совпадают, т. е. $f(\boldsymbol{x}) = f(\boldsymbol{y})$, то поэтому в $F(n,m)$ имеется 2^{nm-m} различных операторов $\mathscr{L}$ таких, что $\mathscr{L}(\boldsymbol{x}) = \mathscr{L}(\boldsymbol{y})$. Следовательно, величина

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

является средним значением для числа таких пар $(\boldsymbol{x}, \boldsymbol{y})$, на которых значения оператора из $F(n,m)$ одинаковы. Поэтому в $F(n,m)$ найдется оператор $\mathscr{L}$, для которого равенство $\mathscr{L}(\boldsymbol{x}) = \mathscr{L}(\boldsymbol{y})$ выполняется не более чем на $2^{-m}|A||B|$ парах $(\boldsymbol{x}, \boldsymbol{y})$, $\boldsymbol{x} \in A$, $\boldsymbol{y} \in B$. Лемма доказана.

Л е м м а 16. *Пусть $A, B \subseteq \{0,1\}^n$, $A \cap B = \varnothing$, $m = \lceil \log_2 |B| + k \rceil$, где $k \geqslant 0$. Тогда существует линейный оператор $\mathscr{L}\colon \{0,1\}^n \to \{0,1\}^m$ такой, что*

$$|\{(\boldsymbol{x}, \boldsymbol{y}) \mid \boldsymbol{x} \in A, y \in B, \mathscr{L}(\boldsymbol{x}) = \mathscr{L}(\boldsymbol{y})\}| \leqslant \tfrac{1}{2^k}|A|.$$

Доказательство. Из леммы 15 следует, что найдется такой линейный (n,m)-оператор $\mathscr{L}$, для которого равенство $\mathscr{L}(\boldsymbol{x})=\mathscr{L}(\boldsymbol{y})$ выполняется не более чем на $2^{-m}|A||B|$ парах $(\boldsymbol{x},\boldsymbol{y})$, где $\boldsymbol{x}\in A$, $\boldsymbol{y}\in B$. Так как $2^m\geqslant 2^k|B|$, то $2^{-m}|A||B|\leqslant\frac{1}{2^k}|A|$. Лемма доказана.

Лемма 17. *Пусть $D\subseteq\{0,1\}^n$ состоит из N наборов, $\log_2 N\geqslant\frac{1}{3}n$, функция f определена на D и равна единице ровно на N_1 наборах из D, где $N_1\leqslant\frac{1}{2}N$ и $\log_2 N_1\sim\log_2 N$ при $n\to\infty$. Тогда*

$$L(f)\lesssim\frac{\log_2\binom{N}{N_1}}{\log_2\log_2\binom{N}{N_1}}.$$

Доказательство. Положим

$$D_0=\{\boldsymbol{x}\in D\mid f(\boldsymbol{x})=0\},\ D_1=\{\boldsymbol{x}\in D\mid f(\boldsymbol{x})=1\},\ k=3\log_2 n.$$

К областям D_0 и D_1 применим лемму 16, полагая, что $A=D_1$ и $B=D_0$. В результате найдется такой линейный оператор $\mathscr{L}\colon\{0,1\}^n\to\{0,1\}^m$, что $m=\lceil\log_2|D_0|+3\log_2 n\rceil$ и множество

$$D'=\{(\boldsymbol{x},\boldsymbol{y})\mid\boldsymbol{x}\in D_0,\boldsymbol{y}\in D_1,\mathscr{L}(\boldsymbol{x})=\mathscr{L}(\boldsymbol{y})\}$$

состоит из не более чем N_1/n^3 наборов. Далее введем определенную на области $\mathscr{L}(D)$ частичную m-местную булеву функцию

$$g(\boldsymbol{y})=\begin{cases}0, & \text{если }\exists\,\boldsymbol{x}\in D_0\text{ такой, что }\boldsymbol{y}=\mathscr{L}(\boldsymbol{x}),\\ 1 & \text{в противном случае}\end{cases}$$

и определенную на области D частичную функцию $h(\boldsymbol{x})=f(\boldsymbol{x})\oplus g(\mathscr{L}(\boldsymbol{x}))$. Нетрудно видеть, что $g(\boldsymbol{y})$ равна единице на не более чем N_1 наборах из $\mathscr{L}(D)$, а $h(\boldsymbol{x})$ равна единице на не более чем N_1/n^3 наборах из D. Так как $f(\boldsymbol{x})=h(\boldsymbol{x})\oplus g(\mathscr{L}(\boldsymbol{x}))$, то

$$L(f)L(g)+L(h)+L(\mathscr{L})+1.$$

Нетрудно видеть, что $\log_2\log_2\binom{N}{N_1}\sim m$, и поэтому для оценки сложности функции g можно воспользоваться леммой 13. Из этой леммы следует, что

$$L(g)\lesssim\frac{\log_2\binom{N}{N_1}}{\log_2\log_2\binom{N}{N_1}}.$$

Для вычисления функции h воспользуемся ее совершенной дизъюнктивной формой, полагая, что вне области D эта функция равна нулю. Так как $N_1\leqslant\log_2\binom{N}{N_1}$, то

$$L(h)\leqslant\frac{N_1 n}{\log_2^3 N_1}=\mathcal{O}\left(\frac{N_1}{\log_2^2 N_1}\right)=o\left(\frac{\log_2\binom{N}{N_1}}{\log_2\log_2\binom{N}{N_1}}\right).$$

Сложность оператора $\mathscr{L}$ по порядку не превосходит $\frac{n^2}{\log_2 n}$. Поэтому из условий леммы следует, что $L(\mathscr{L}) = o(g)$. Лемма доказана.

Л е м м а 18. *Пусть $D \subseteq \{0,1\}^n$ состоит из N наборов, функция f определена на D и равна единице ровно на N_1 наборах из D, где $N_1 \leqslant \frac{1}{2}N$ и $\log_2 N_1 \sim \log_2 N$ при $n \to \infty$. Тогда*

$$L(f) \lesssim \frac{\log_2 \binom{N}{N_1}}{\log_2 \log_2 \binom{N}{N_1}} + \mathcal{O}\left(\frac{n \log_2 N}{\log_2 n}\right).$$

Д о к а з а т е л ь с т в о. Если $\log_2 N \geqslant \frac{1}{3}n$, то утверждение настоящей леммы следует из леммы 17. Поэтому далее полагаем, что $\log_2 N \leqslant \frac{1}{3}n$.

Положим $D_0 = \{\boldsymbol{x} \in D \mid f(\boldsymbol{x}) = 0\}$, $D_1 = \{\boldsymbol{x} \in D \mid f(\boldsymbol{x}) = 1\}$, $k = \log_2 |D_1| + 1$. К областям D_0 и D_1 применим лемму 16, полагая, что $A = D_1$ и $B = D_0$. В результате найдется такой линейный оператор $\mathscr{L} \colon \{0,1\}^n \to \{0,1\}^m$, что $m = \lceil \log_2 |D_0| + \log_2 |D_1| + 1 \rceil$ и при этом нет таких элементов $\boldsymbol{x} \in D_0$ и $\boldsymbol{y} \in D_1$, что $\mathscr{L}(\boldsymbol{x}) = \mathscr{L}(\boldsymbol{y})$. Далее введем определенную на области $\mathscr{L}(D)$ частичную m-местную булеву функцию

$$g(\boldsymbol{y}) = \begin{cases} 0, & \text{если } \exists\ \boldsymbol{x} \in D_0 \text{ такой, что } \boldsymbol{y} = \mathscr{L}(\boldsymbol{x}), \\ 1, & \text{если } \exists\ \boldsymbol{x} \in D_1 \text{ такой, что } \boldsymbol{y} = \mathscr{L}(\boldsymbol{x}). \end{cases}$$

Нетрудно видеть, что функция g равна единице на не более чем N_1 наборах из $\mathscr{L}(D)$ и $f(\boldsymbol{x}) = g(\mathscr{L}(\boldsymbol{y}))$. Так как $m \leqslant \lceil 2 \log_2 N \rceil$, то можно воспользоваться леммой 17. В силу этой леммы

$$L(g) \lesssim \frac{\log_2 \binom{N}{N_1}}{\log_2 \log_2 \binom{N}{N_1}}.$$

Наконец заметим, что

$$L(\mathscr{L}) = \mathcal{O}\left(\frac{n \log_2 N}{\log_2 n}\right).$$

Лемма доказана.

Л е м м а 19. *Пусть $D \subseteq \{0,1\}^n$ состоит из N наборов, функция f определена на D и равна единице ровно на N_1 наборах из D, где $N_1 \leqslant \frac{1}{2}N$. Пусть $R > 0$, $D_0 = \{\boldsymbol{x} \in D \mid f(\boldsymbol{x}) = 0\}$ и $D_1 = \{\boldsymbol{x} \in D \mid f(\boldsymbol{x}) = 1\}$. Тогда существуют булева функция g и область $D_0' \subseteq D_0$ такие, что*

$$f(\boldsymbol{x}) = g(\boldsymbol{x}) \cdot f_{D_1 \cup D_0'}(\boldsymbol{x}), \quad |D_0'| \leqslant |D_0| \cdot 2^{-R},$$

$$L(g) \lesssim \frac{\log_2 \binom{2^{\lceil \log_2 N_1 + R \rceil}}{N_1}}{\log_2 \log_2 \binom{2^{\lceil \log_2 N_1 + R \rceil}}{N_1}} + \mathcal{O}\left(n \left\lceil \frac{\log_2 N_1}{\log_2 n} \right\rceil\right),$$

где $f_{D_1 \cup D_0'}$ *— сужение функции* f *на область* $D_1 \cup D_0'$.

Доказательство. К областям D_0 и D_1 применим лемму 16, полагая, что $k = R$, $m = \lceil \log_2 N_1 + R \rceil$, $A = D_0$ и $B = D_1$. В результате найдется такой линейный оператор $\mathscr{L}\colon \{0,1\}^n \to \{0,1\}^m$, что множество

$$D_0' = \{(\boldsymbol{x}, \boldsymbol{y}) \mid \boldsymbol{x} \in D_0, \boldsymbol{y} \in D_1, \mathscr{L}(\boldsymbol{x}) = \mathscr{L}(\boldsymbol{y})\}$$

состоит из не более чем $|D_0| \cdot 2^{-R}$ наборов. Далее введем m-местную булеву функцию

$$g'(\boldsymbol{y}) = \begin{cases} 1, & \text{если } \exists\, \boldsymbol{x} \in D_1 \text{ такой, что } \boldsymbol{y} = \mathscr{L}_1(\boldsymbol{x}), \\ 0 & \text{в противном случае} \end{cases}$$

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

$$f(\boldsymbol{x}) = \begin{cases} f_{D_1 \cup D_0'}(\boldsymbol{x}), & \text{если } g(\boldsymbol{x}) = 1, \\ g(\boldsymbol{x}), & \text{если } g(\boldsymbol{x}) = 0, \end{cases}$$

и, следовательно,

$$f(\boldsymbol{x}) = g(\boldsymbol{x}) \cdot f_{D_1 \cup D_0'}(\boldsymbol{x}).$$

Так как $g(\boldsymbol{x}) = g'(\mathscr{L}(\boldsymbol{x}))$, то сложность g не превосходит суммы $L(g') + L(\mathscr{L})$. Оценим сложности функции g' и линейного оператора $\mathscr{L}$. Функция g' зависит от $m = \lceil \log_2 N_1 + R \rceil$ аргументов и принимает не более N_1 единичных значений, поэтому, в силу леммы 13,

$$L(g') \lesssim \frac{\log_2 \binom{2^{\lceil \log_2 N_1 + R \rceil}}{N_1}}{\log_2 \log_2 \binom{2^{\lceil \log_2 N_1 + R \rceil}}{N_1}}. \tag{30}$$

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

$$L(\mathscr{L}) = \mathcal{O}\left(n \left\lceil \frac{\log_2 N_1}{\log_2 n} \right\rceil\right). \tag{31}$$

Складывая неравенства (30) и (31), получаем требуемую оценку сложности функции g. Лемма доказана.

Лемма 20. *Пусть* $n \to \infty$, *область* $D \subseteq \{0,1\}^n$ *состоит из* N *наборов, функция* f *определена на* D *и равна единице ровно на* N_1 *наборах из* D, *где* $n \log_2 n \ll N_1 \ll N$. *Тогда*

$$T(f) \lesssim 4.135 \cdot \frac{N_1}{\log_2 N_1}.$$

Доказательство. Положим $D_0 = \{\boldsymbol{x} \in D \mid f(\boldsymbol{x}) = 0\}$, $|D_0| = N_0$ и $D_1 = \{\boldsymbol{x} \in D \mid f(\boldsymbol{x}) = 1\}$. Введем положительную постоянную R так, чтобы

параметр $m = \log_2 N_1 + R$ был целым. К функции f применим лемму 19. В результате получим такие функцию g_1 и область $D_{01} \subseteq D_0$, что $|D_{01}| \leqslant 2^{-R} N_0$,

$$f(\boldsymbol{x}) = g_1(\boldsymbol{x}) \cdot f_{D_1 \cup D_{01}}(\boldsymbol{x}), \tag{32}$$

а для сложности функции g_1 в силу условия $N_1 \gg n \log_2 n$ и того, что m целое, справедливо асимптотическое неравенство

$$L(g_1) \lesssim \frac{\log_2 \binom{N_1 2^R}{N_1}}{\log_2 \log_2 \binom{N_1 2^R}{N_1}}$$

Далее лемму 19 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 19, и т. д. После i-го применения леммы 19 получим функцию g_i и область $D_{0i} \subseteq D_{0(i-1)}$ такие, что $|D_{0i}| \leqslant 2^{-iR} N_0$ и

$$f_{D_1 \cup D_{0(i-1)}}(\boldsymbol{x}) = g_i(\boldsymbol{x}) \cdot f_{D_1 \cup D_{0i}}(\boldsymbol{x}), \tag{33}$$

а для сложности функции g_i справедливо асимптотическое неравенство

$$L(g_i) \lesssim \frac{\log_2 \binom{N_1 2^R}{N_1}}{\log_2 \log_2 \binom{N_1 2^R}{N_1}}.$$

Будем порождать функции g_i и области D_{0i} до тех пор, пока размер очередной области не станет меньше N_1. Так как на каждом шаге размер порождаемой области уменьшается не меньше, чем в 2^R раз, то общее число шагов не превысит величины $s = \lceil \log_{2^R} N_0/N_1 \rceil$, и так как $|D_1 \cup D_{0s}| \leqslant 2N_1$, то сложность функции $f_{D_1 \cup D_{0s}}(\boldsymbol{x})$ асимптотически не будет превосходить правой части (33).

Из (32) и (33) легко следует, что

$$\begin{aligned} f(\boldsymbol{x}) = g_1(\boldsymbol{x}) \cdot f_{D_1 \cup D_{01}}(\boldsymbol{x}) &= g_1(\boldsymbol{x}) \cdot g_2(\boldsymbol{x}) \cdot f_{D_1 \cup D_{02}}(\boldsymbol{x}) = \ldots \\ &= g_1(\boldsymbol{x}) \cdot g_2(\boldsymbol{x}) \cdot \ldots \cdot g_s(\boldsymbol{x}) \cdot f_{D_1 \cup D_{0s}}(\boldsymbol{x}). \end{aligned} \tag{34}$$

Воспользуемся формулой (34) для построения программы P, вычисляющей функцию f. Эта программа строится на основе схем из функциональных элементов, вычисляющих функции g_i, и на произвольном наборе $\boldsymbol{x}$ работает следующим образом. Сначала вычисляется значение $g_1(\boldsymbol{x})$. Если $g_1(\boldsymbol{x}) = 0$, то программа останавливается и полагается, что $f(\boldsymbol{x}) = 0$. Если $g_1(\boldsymbol{x}) = 1$, то вычисляется значение $h_2(\boldsymbol{x})$. Если $g_2(\boldsymbol{x}) = 0$, то программа останавливается и полагается, что $f(\boldsymbol{x}) = 0$. Если $g_2(\boldsymbol{x}) = 1$, то вычисляется значение $g_3(\boldsymbol{x})$ и т. д. Если $g_s(\boldsymbol{x}) = 1$, то значение $f(\boldsymbol{x})$ 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 (34),

справедливы неравенства

$$T(\mathsf{P}) \lesssim \frac{1}{N}\left(\sum_{i=1}^{s} L(g_i)|D_1 \cup D_{0(i-1)}| + L(f_{D_1 \cup D_{0s}})|D_1 \cup D_{0s}|\right) \lesssim$$

$$\lesssim \frac{1}{N} \cdot \frac{\log_2 \binom{N_1 2^R}{N_1}}{\log_2 \log_2 \binom{N_1 2^R}{N_1}} \left((s+1)N_1 + \sum_{i=1}^{s+1} |D_{0(i-1)}|\right).$$

Так как $|D_{0i}| \leqslant 2^{-iR} N_0$ и $N_1 = |D_1| < |D_{0(s-1)}| \leqslant 2^{-(s-1)R} N_0$, то $s-1 \leqslant \log_{2^R} N_0/N_1$, и так как $(N_1/N_0)/\log_2(N_0/N_1) \ll 1$, то для суммы, стоящей в скобках в правой части последнего неравенства, справедливы следующие оценки:

$$(s+1)N_1 + \sum_{i=1}^{s+1} 2^{-(i-1)R} N_0 \leqslant \frac{N_1}{R} \log_2 \frac{2^{2R} N_0}{N_1} + N_0 \frac{1}{1-2^{-R}} \sim N_0 \frac{1}{1-2^{-R}}.$$

Нетрудно показать, что

$$\log_2 \binom{N_1 2^R}{N_1} \sim N_1 2^R H(2^{-R}),$$

где H — функция энтропии. Поэтому

$$T(\mathsf{P}) \lesssim \frac{N_1 2^R H(2^{-R})}{\log_2 N_1} \cdot \frac{1}{1-2^{-R}}. \tag{35}$$

Значение функции $2^R H(2^{-R})/(1-2^{-R})$ на отрезке от 0.59 до 1.59 не превосходит 4.135. Следовательно, найдется такое R, при котором из (35) получается неравенство

$$T(\mathsf{P}) \lesssim \frac{4.135 \cdot N_1}{\log_2 N_1}.$$

Лемма доказана.

Далее покажем, что использованная в доказательстве предыдущей леммы техника позволяет получать асимптотически точные формулы для сложности вычисления частичных функций ограниченного веса схемами из функциональных элементов.

Лемма 21. *Пусть $n \to \infty$, область $D \subseteq \{0,1\}^n$ состоит из N наборов, функция f определена на D и равна единице ровно на N_1 наборах из D, где $n \log_2 n \ll N_1 \ll N$. Тогда*

$$L(f) \lesssim \frac{N_1}{\log_2 N_1} \cdot \log_2 \frac{N}{N_1}.$$

Доказательство. Как и ранее, введем множества

$$D_0 = \{\boldsymbol{x} \in D \mid f(\boldsymbol{x}) = 0\}, D_1 = \{\boldsymbol{x} \in D \mid f(\boldsymbol{x}) = 1\}.$$

Для построения схемы S, вычисляющей f, воспользуемся равенством

$$f(\boldsymbol{x}) = g_1(\boldsymbol{x}) \cdot g_2(\boldsymbol{x}) \cdot \ldots \cdot g_s(\boldsymbol{x}) \cdot f_{D_1 \cup D_{0s}}(\boldsymbol{x}), \tag{36}$$

которое получается так же, как и при доказательстве леммы 20, но с новым значением параметра $R = \log_2 N/N_1$ и таким s, что $|D_{0s}| \leqslant N_1 \log_2 N/N_1 - N_1$.

Нетрудно видеть, что в этом равенстве функция g_1 определена на области $D = D_1 \cup D_0$, при $i = 2, \ldots, s$ функции g_i определены на областях $D_1 \cup D_{0(i-1)}$, при $i = 1, \ldots, s$ размер области D_{0i} не превосходит $N_0(\log_2 N/N_1)^{-i}$ и для функций g_i, в силу леммы 18, справедливо неравенство

$$L(g_i) \lesssim \frac{\log_2 \binom{2N_1 \log_2 N/N_1}{N_1}}{\log_2 \log_2 \binom{2N_1 \log_2 N/N_1}{N_1}} + \mathcal{O}\left(n \left\lceil \frac{\log_2 N_1}{\log_2 n} \right\rceil\right).$$

Так как

$$\log_2 \binom{2N_1 \log_2 N/N_1}{N_1} \leqslant \log_2 \left(\frac{6N_1 \log_2 N/N_1}{N_1}\right)^{N_1} \sim$$
$$\sim \log_2 \left(\log_2 N/N_1\right)^{N_1} = N_1 \log_2 \log_2 N/N_1$$

и $N_1 \gg n \log_2 n$, то

$$L(g_i) \lesssim \frac{N_1 \log_2 \log_2 N/N_1}{\log_2 N_1}. \tag{37}$$

Очевидно, что и сложность функции $f_{D_1 \cup D_{0s}}(\boldsymbol{x})$ асимптотически не превосходит правой части (37). Также легко видеть, что

$$s \leqslant \lceil \log_2 \frac{|D_0|}{|D_1|} \Big/ \log_2 \log_2 N/N_1 \rceil \sim \log_2 \frac{N}{N_1} \Big/ \log_2 \log_2 N/N_1,$$

Поэтому $L(f) \leqslant \sum\limits_{i=1}^{s} L(g_i) + L(f_{D_1 \cup D_{0s}}) + s$ и для сложности функции f имеем следующие неравенства:

$$L(f) \lesssim \frac{N_1 \log_2 \log_2 N/N_1}{\log_2 N_1} \cdot (s+1) \sim$$
$$\sim \frac{N_1 \log_2 \log_2 N/N_1}{\log_2 N_1} \cdot \log_2 \frac{N}{N_1} \Big/ \log_2 \log_2 N/N_1 = \frac{N_1}{\log_2 N_1} \cdot \log_2 \frac{N}{N_1}.$$

Лемма доказана.

Так как $\binom{N}{N_1} \geqslant (N/N_1)^{N_1}$, то найдется такая функция f, определенная на области размера N и принимающая на этой области N_1 единичных значений, что

$$L(f) \gtrsim \frac{\log_2 \binom{N}{N_1}}{\log_2 \log_2 \binom{N}{N_1}} \geqslant \frac{N_1}{\log_2 N_1} \cdot \log_2 \frac{N}{N_1}. \tag{38}$$

Таким образом, оценка леммы 21 является асимптотически точной. Более того, лемма 21 вместе с леммой 18 позволяют строить асимптотически минимальные схемы для почти всех функций, число единичных значений которых растет быстрее, чем $n \log_2 n$.

Вернемся к доказательству теоремы 6 и докажем нижнюю оценку. Оценим число различных программ, состоящих из данного числа команд. Для этого каждой программе P, входам которой приписаны независимые переменные $x_1, \ldots, x_n$, поставим в соответствие помеченный ориентированный граф G_{P} без кратных ребер. Каждый такой граф зададим списком из девяти условий, которые будут определять его вершины, дуги и метки вершин и дуг. Первые пять условий определяют вершины и метки вершин графа G_{P}.

(1) Каждой независимой 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 $\mathsf{a} = f_j(\mathsf{b}_1, \mathsf{b}_2)$, 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 дуги и метки дуг графа. Дуги, в свою очередь, определяют порядок выполнения команд, находящихся между двумя последовательными командами остановки.

(6) Вершины u_i и u_j связаны дугой, направленной 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_l); (ii) команда p' (переменная x_l) является s-м аргументом команды p, $1 \leqslant s \leqslant 2$; каждую такую дугу назовем функциональной и припишем ей символ s.

(7) Вершины u_i и u_j связаны дугой, направленной от u_i к u_j, если: (i) вершина u_j соответствует команде остановки s_t, вершина u_i соответствует вычислительной команде p' (независимой переменной x_l); (ii) команда p' (переменная x_l) является нулевым аргументом команды s_t; каждую такую дугу назовем функциональной и припишем ей 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 дугой, направленной от u_i к u_j, если они соответствуют l-й и $(l+1)$-й командам остановки программы P; каждую такую дугу назовем дугой остановки.

(9) Вершины u_i и u_j связаны дугой, направленной от u_i к u_j, если: (i) вершина u_j соответствует команде остановки s_t, вершина u_i соответствует вычислительной команде p с выходом z; (ii) вершина u_i не является нулевым аргументом команды остановки s_t; (iii) переменная z не является выходом никакой другой вычислительной команды p' при $n(\mathsf{p}) < n(\mathsf{p}') < n(\mathsf{s}_t)$; каждую такую дугу назовем особой и припишем ей символ $*$.

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 программ в базисе из всех не более чем двухместных булевых функций, содержащих не более L команд и имеющих n входов и один выходов.

Лемма 22. *При $L \geqslant n$ справедливо неравенство*

$$N(n, L) \leqslant (c\,(L+n))^{\frac{4}{3}L},$$

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 дуг.

Число особых дуг обозначим через N. Из каждой вершины, соответствующей вычислительной команде, выходит не более одной особой дуги. Очевидно, что из вершин, соответствующих независимым переменным, командам остановки и их аргументам, особые дуги не выходят. Поэтому $N \leqslant L_1 - L_2$. С другой стороны, в каждую вершину, соответствующую команде остановки, входит не более одной особой дуги. Поэтому также справедливо неравенство $N \leqslant L_2$. Объединяя два последних неравенства, при любом γ из $[0, 1]$ имеем

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

Каждый граф содержит $L_2 - 1$ дуг остановки и не более $2L_1 + L_2$ функциональных дуг. Следовательно, общее число дуг не больше, чем $2L_1 + 2L_2 + N$. Известно (см. [9]), что число различных связанных графов с p вершинами и q дугами 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 дуг и вершин. Преобразуем эту разность:

$$\begin{aligned} R &\leqslant 2L_1 + 2L_2 + N - L - n \leqslant \\ &\leqslant L_1 + L_2 - n + (1-\gamma)(L_1 - L_2) + \gamma L_2 \leqslant \\ &\leqslant (2-\gamma)L_1 + \gamma 2L_2 - \gamma n. \end{aligned}$$

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

$$N(n, L) \leqslant \left(c\,(L+n)\right)^{\frac{4}{3}L},$$

где c — постоянная. Лемма доказана.

Лемма 23. *Пусть $D \subseteq \{0,1\}^n$, $|D| = N$, $n \log_2 n \ll N_1 \leqslant \frac{1}{2}N$ и $n \to \infty$. Тогда для любой положительной постоянной ε доля частичных булевых функций f, определенных на области D, принимающих в этой области N_1 единичных значений, и для которых выполняется неравенство*

$$T(f) \geqslant (1-\varepsilon)\frac{27}{32} \cdot \frac{N_1}{\log_2 N_1},$$

стремится к единице.

Доказательство. Положим $T_i = (1 - 3\varepsilon)\frac{3i \cdot N_1}{4 \log_2 N_1}$, где ε — положительная постоянная. Для программы P и целых $i = 1, \ldots, s = \lfloor \log_2 N - \log_2 N_1 - 1 \rfloor$ введем наборы $\boldsymbol{x}_i \in D$ такие, что $N_{\mathsf{P}}(\boldsymbol{x}_i) = N - N2^{-i}$. Оценим мощность множества R, состоящего из всех рассматриваемых булевых функций, у минимальных программ которых найдется такой набор $\boldsymbol{x}_i$, что $T_{\mathsf{P}}(\boldsymbol{x}_i) \leqslant T_i$. Каждая такая функция однозначно определяется первыми T_i командами своей минимальной программы P и двоичным набором длины не более чем $N - N_{\mathsf{P}}(\boldsymbol{x}_i) = N2^{-i}$ — значениями на тех аргументах, время работы программы P на которых больше времени работы на $\boldsymbol{x}_i$. Поэтому число функций в R не превосходит суммы

$$\sum_{i=1}^{s} \left(N(T_i, n) \sum_{k=0}^{N_1} \binom{N2^{-i}}{k} \right). \tag{39}$$

Оценим логарифм суммы (39). В силу предыдущей леммы

$$\log_2 N(T_i,n)\leqslant \frac{4}{3}\cdot(1-3\varepsilon)\frac{3i\cdot N_1}{4\log_2 N_1}\log_2\left(c\left((1-3\varepsilon)\frac{3i\cdot N_1}{4\log_2 N_1}+n\right)\right)\leqslant$$
$$\leqslant(1-2\varepsilon)iN_1.$$

Кроме того, так как

$$\binom{2^{-i}N}{N_1}\Big/\binom{N}{N_1}\leqslant\frac{2^{-i}N\left(2^{-i}N-1\right)\cdots\left(2^{-i}N-N_1+1\right)}{N(N-1)\cdots(N-N_1+1)}\leqslant$$
$$\leqslant\left(\frac{2^{-i}N}{N}\right)^{N_1}\leqslant 2^{-iN_i}$$

и $2^{-i}N\geqslant 2N_1$, то справедливо неравенство

$$\sum_{k=0}^{N_1}\binom{2^{-i}N}{k}\leqslant(N_1+1)\binom{2^{-i}N}{N_1}=2^{\log_2(N_1+1)-iN_1}\binom{N}{N_1}. \tag{40}$$

Следовательно, логарифм i-го слагаемого в сумме (39) удовлетворяет неравенству

$$\log_2\left(N(T_i,n)\sum_{k=0}^{N_1}\binom{N2^{-i}}{k}\right)\leqslant(1-2\varepsilon)iN_1+\log_2(N_1+1)-iN_1+\log_2\binom{N}{N_1}=$$
$$=\log_2(N_1+1)-2i\varepsilon N_1+\log_2\binom{N}{N_1}.$$

Поэтому при достаточно больших n

$$\log_2|R|\leqslant\log_2(N_1+1)-2\varepsilon N_1+\log_2\binom{N}{N_1}+\log_2 s\leqslant-\varepsilon N_1+\log_2\binom{N}{N_1}.$$

Следовательно,

$$|R|<2^{-\varepsilon N_1}\binom{N}{N_1}=o\left(\binom{N}{N_1}\right).$$

Таким образом, все минимальные программы почти всех рассматриваемых функций удовлетворяют условию:

если $\boldsymbol{x}_i$ такое, что $N_{\mathsf{P}}(\boldsymbol{x}_i)=N-N2^{-i}$,
то $T_{\mathsf{P}}(\boldsymbol{x}_i)>(1-3\varepsilon)\cdot\frac{3}{4}\cdot\frac{i\cdot N_1}{\log_2 N_1}$.

Определим $s-1$ множество $X_i=\{\boldsymbol{x}\mid N_{\mathsf{P}}(\boldsymbol{x}_i)\leqslant N_{\mathsf{P}}(\boldsymbol{x})<N_{\mathsf{P}}(\boldsymbol{x}_{i+1})\}$ для $i=1,\ldots,s-1$, множество $X_s=\{\boldsymbol{x}\mid N_{\mathsf{P}}(\boldsymbol{x}_s)\leqslant N_{\mathsf{P}}(\boldsymbol{x})\leqslant N\}$ и множество $X=\bigcup\limits_{i=1}^{s}X_i$. Нетрудно видеть, что

$$|X_i|=N2^{-i-1}\text{ при }i=1,\ldots,s-1,\qquad |X_s|=N2^{-s}+1.$$

В этом случае при $n\to\infty$ для среднего времени работы каждой такой программы справедливы неравенства

$$T(\mathsf{P})=\frac{1}{N}\sum_{x\in D}T_{\mathsf{P}}(\boldsymbol{x})\geqslant\frac{1}{N}\sum_{x\in X}T_{\mathsf{P}}(\boldsymbol{x})\geqslant\frac{1}{N}\sum_{i=1}^{s}T_{\mathsf{P}}(\boldsymbol{x}_i)|X_i|\geqslant$$
$$\geqslant\frac{1}{N}\sum_{i=1}^{s}\frac{(1-3\varepsilon)3i\cdot N_1}{4\log_2 N_1}N2^{-i-1}=\frac{(1-3\varepsilon)3\cdot N_1}{4\log_2 N_1}\sum_{i=1}^{s}i2^{-i-1}\geqslant(1-4\varepsilon)\frac{3}{4}\cdot\frac{N_1}{\log_2 N_1}.$$

Полученную оценку перепишем в виде

$$T_X(\mathsf{P}) \geqslant (1-4\varepsilon)\frac{3}{4}\cdot\frac{N_1}{\log_2 N_1}, \tag{41}$$

где нижний индекс явно указывает на множество наборов, учитываемых при подсчете средней сложности. В данном случае X состоит из тех наборов, номера которых не превосходят $N/2$. Оценим вклад в среднюю сложность наборов не попавших в X.

Положим $T_i^{\boldsymbol{y}} = (1-3\varepsilon)\frac{3i\cdot N_1}{8\log_2 N_1\cdot\log_2(N/N_1)}$. Для программы P и целых $i=1,\ldots,t=\lfloor\log_2(N/N_1)\rfloor$ введем наборы $\boldsymbol{y}_i\in D$ такие, что $N_{\mathsf{P}}(\boldsymbol{y}_i)=\frac{iN}{2\log_2(N/N_1)}$. Оценим мощность множества R_y, состоящего из всех рассматриваемых булевых функций, у минимальных программ которых найдется такой набор $\boldsymbol{y}_i$, что $T_{\mathsf{P}}(\boldsymbol{y}_i)\leqslant T_i^{\boldsymbol{y}}$. Каждая такая функция однозначно определяется первыми $T_i^{\boldsymbol{y}}$ командами своей минимальной программы P и двоичным набором длины не более чем

$$N-N_{\mathsf{P}}(\boldsymbol{y}_i)=N-\frac{iN}{2\log_2(N/N_1)}=N\left(1-\frac{i}{2\log_2(N/N_1)}\right),$$

— значениями на тех аргументах, время работы программы P на которых больше времени работы на $\boldsymbol{y}_i$. Поэтому число функций в $R_{\boldsymbol{y}}$ не превосходит суммы

$$\sum_{i=1}^{t}\left(N(T_i^{\boldsymbol{y}},n)\sum_{k=0}^{N_1}\binom{N\left(1-\frac{i}{2\log_2(N/N_1)}\right)}{k}\right). \tag{42}$$

Оценим логарифм суммы (42). В силу предыдущей леммы

$$\log_2 N(T_i^{\boldsymbol{y}},n)\leqslant\frac{4}{3}\cdot\frac{(1-3\varepsilon)3i\cdot N_1}{8\log_2 N_1\cdot\log_2\frac{N}{N_1}}\log_2\left(c\left(\frac{(1-3\varepsilon)3i\cdot N_1}{8\log_2 N_1\cdot\log_2\frac{N}{N_1}}+n\right)\right)\leqslant$$
$$\leqslant(1-2\varepsilon)\frac{i\cdot N_1}{2\log_2\frac{N}{N_1}}.$$

Кроме того, так как

$$\binom{N\left(1-\frac{i}{2\log_2(N/N_1)}\right)}{N_1}\Bigg/\binom{N}{N_1}\leqslant\left(\frac{N\left(1-\frac{i}{2\log_2(N/N_1)}\right)}{N}\right)^{N_1}=$$
$$=\left(1-\frac{i}{2\log_2(N/N_1)}\right)^{\frac{2\log_2(N/N_1)}{i}\cdot\frac{iN_1}{2\log_2(N/N_1)}}\leqslant 2^{-\frac{iN_1}{2\log_2(N/N_1)}}$$

и $N/2\geqslant 2N_1$, то справедливо неравенство

$$\sum_{k=0}^{N_1}\binom{N\left(1-\frac{i}{2\log_2(N/N_1)}\right)}{k}\leqslant 2^{\log_2(N_1+1)-\frac{iN_1}{2\log_2(N/N_1)}}\binom{N}{N_1}. \tag{43}$$

Следовательно, логарифм i-го слагаемого в сумме (42) удовлетворяет неравенствам

$$\log_2\left(N(T_i^{\boldsymbol{y}},n)\sum_{k=0}^{N_1}\binom{N\left(1-\frac{i}{2\log_2(N/N_1)}\right)}{N_1}\right)\leqslant$$
$$\leqslant(1-2\varepsilon)\tfrac{iN_1}{2\log_2(N/N_1)}+\log_2(N_1+1)-\tfrac{iN_1}{2\log_2(N/N_1)}+\log_2\binom{N}{N_1}=$$
$$=\log_2(N_1+1)-\tfrac{i\varepsilon N_1}{\log_2(N/N_1)}+\log_2\binom{N}{N_1}.$$

Поэтому при достаточно больших n

$$\log_2|R_{\boldsymbol{y}}|\leqslant\log_2(N_1+1)-\tfrac{\varepsilon N_1}{2\log_2(N/N_1)}+\log_2\binom{N}{N_1}+\log_2 t\leqslant$$
$$\leqslant-\varepsilon\tfrac{N_1}{2\log_2(N/N_1)}+\log_2\binom{N}{N_1}.$$

Следовательно,

$$|R_{\boldsymbol{y}}|<2^{-\varepsilon\frac{N_1}{2\log_2(N/N_1)}}\binom{N}{N_1}=o\left(\binom{N}{N_1}\right).$$

Таким образом, все минимальные программы почти всех рассматриваемых функций удовлетворяют условию:

$$\text{если } \boldsymbol{y}_i \text{ такое, что } N_{\mathsf{P}}(\boldsymbol{y}_i)=\frac{iN}{2\log_2(N/N_1)},$$
$$\text{то } T_{\mathsf{P}}^{\boldsymbol{y}}(\boldsymbol{y}_i)>(1-3\varepsilon)\cdot\frac{3i\cdot N_1}{8\log_2 N_1\cdot\log_2(N/N_1)}.$$

Определим $t-1$ множество $Y_i=\{\boldsymbol{x}\mid N_{\mathsf{P}}(\boldsymbol{y}_i)\leqslant N_{\mathsf{P}}(\boldsymbol{x})<N_{\mathsf{P}}(\boldsymbol{y}_{i+1})\}$ для $i=1,\ldots,t-1$, множество $Y_t=\{\boldsymbol{x}\mid N_{\mathsf{P}}(\boldsymbol{y}_t)\leqslant N_{\mathsf{P}}(\boldsymbol{x})\leqslant N/2\}$ и $Y=\bigcup_{i=1}^{t}$. Нетрудно видеть, что каждое Y_i состоит из не менее чем $\frac{N}{2\log_2(N/N_1)}$ наборов. Поэтому при $n\to\infty$ для среднего времени работы каждой такой программы, вычисленного с учетом времени работы на наборах только из Y, справедливы неравенства

$$T_Y(\mathsf{P})=\frac{1}{N}\sum_{x\in Y}T_{\mathsf{P}}(\boldsymbol{x})\geqslant\frac{1}{N}\sum_{i=1}^{t}T_{\mathsf{P}}(\boldsymbol{y}_i)|Y_i|\geqslant$$
$$\geqslant\frac{1}{N}\sum_{i=1}^{t}\frac{(1-3\varepsilon)3i\cdot N_1}{8\log_2 N_1\cdot\log_2(N/N_1)}\cdot\frac{N}{2\log_2(N/N_1)}=$$
$$=\frac{(1-3\varepsilon)3\cdot N_1}{16\log_2 N_1\cdot\log_2^2(N/N_1)}\sum_{i=1}^{t}i\geqslant(1-4\varepsilon)\frac{3}{32}\frac{N_1}{\log_2 N_1}.$$

Таким образом, так как множества X и Y не пересекаются, то из (41) и предыдущего неравенства видим, что

$$T(\mathsf{P})=T_X(\mathsf{P})+T_Y(\mathsf{P})\geqslant(1-4\varepsilon)\frac{27}{32}\cdot\frac{N_1}{\log_2 N_1}.$$

Лемма доказана.

4.3. Монотонные функции. Сложность вычисления монотонных булевых функций изучается в математике с середины 50-х годов прошлого века. Мощностным методом нетрудно показать, что при $n \to \infty$ для сложности $L(f)$ вычисления почти каждой n-местной монотонной булевой функции f схемами в базисе из всех не более чем двухместных булевых функций справедливо асимптотическое неравенство

$$L(f) \gtrsim \frac{2^n}{n\sqrt{\pi n/2}}. \tag{44}$$

Из результата А. Б. Угольникова 1976 года [12] следует, что для каждой n-местной монотонной булевой функции f сложность ее вычисления схемами в базисе из всех не более чем двухместных булевых функций удовлетворяет асимптотическому неравенству

$$L(f) \lesssim \frac{2^n}{n\sqrt{\pi n/2}}. \tag{45}$$

Среднюю сложность монотонных булевых функций изучал Р. Н. Забалуев. В его опубликованной в 2006 году работе [6] доказаны аналоги неравенств (44) и (45) для средней сложности. Из этих оценок для самой сложной «в среднем» n-местной монотонной булевой функции f следует, что

$$T(f) = \Theta\left(\frac{2^n}{n^2}\right).$$

Константы из последнего неравенства были улучшены в [20]. Результаты из [20] уточняются в следующей теореме.

Т е о р е м а 7. *Пусть $n \to \infty$. Тогда*:

(1) *для любой n-местной монотонной булевой функции f*

$$T(f) \lesssim 6.36 \cdot \frac{2^n}{\pi n^2};$$

(2) *для любой постоянной $\varepsilon > 0$ доля n-местных монотонных булевых функций f, для которых справедливо неравенство*

$$T(f) \geqslant (1-\varepsilon)\frac{3}{4} \cdot \frac{2^n}{\pi n^2},$$

стремится к единице.

Утверждение теоремы следует из доказываемых далее лемм 28 и 29. При доказательстве верхней оценки удобно говорить об области определения n-местной монотонной булевой функции как об n-мерном булевом кубе с естественным частичным порядком $\preceq$, вершины которого поделены на $n+1$ слой так, что i-й слой состоит из вершин с i единичными компонентами.

Пусть $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \{0,1\}^n$, $\boldsymbol{\alpha} \preceq \boldsymbol{\beta}$, $d(\boldsymbol{\alpha}, \boldsymbol{\beta}) = k$ и $\boldsymbol{i} = (i_1, i_2, \ldots, i_k)$, где $\alpha_{i_j} \neq \beta_{i_j}$. Множество $I(\boldsymbol{\alpha}, \boldsymbol{\beta}) = \{\boldsymbol{\gamma} \mid \boldsymbol{\alpha} \preceq \boldsymbol{\gamma} \preceq \boldsymbol{\beta}\}$ вершин n-мерного булева куба называется интервалом размерности k, проходящим в направлении $\boldsymbol{i}$. Интервал $I(\boldsymbol{\alpha}, \boldsymbol{\beta})$ назовем непостоянным интервалом монотонной функции f, если $f(\boldsymbol{\alpha}) = 0$ и $f(\boldsymbol{\beta}) = 1$.

Л е м м а 24. *Для любой n-местной монотонной булевой функции число непостоянных интервалов размерности k не превосходит*

$$k\binom{n}{k}\binom{n-k}{\lfloor (n-k)/2 \rfloor}.$$

Доказательство. Пусть N — множество всех непостоянных интервалов $I(\boldsymbol{\alpha}, \boldsymbol{\beta})$ размерности k, а N_s — его подмножество, состоящее из всех тех интервалов $I(\boldsymbol{\alpha}, \boldsymbol{\beta})$, в которых вершина $\boldsymbol{\alpha}$ лежит в s-м слое. Если $I(\boldsymbol{\alpha}, \boldsymbol{\beta}) \in N_s$, то через этот интервал проходит ровно $s!k!(n-k-s)!$ максимальных цепей. Так как в n-мерном булевом кубе существует ровно $n!$ различных максимальных цепей и каждая максимальная цепь проходит не более чем через k непостоянных интервалов размерности k, то

$$k \cdot n! \geqslant \sum_{s=0}^{n-k} s!k!(n-k-s)!|N_s| = \sum_{s=0}^{n-k} \frac{s!k!(n-k-s)!n!(n-k)!|N_s|}{n!(n-k)!} =$$

$$= n!\Big(\sum_{s=0}^{n-k} |N_s| \Big/ \binom{n}{k}\binom{n-k}{s}\Big) \geqslant n!|N| \Big/ \binom{n}{k}\binom{n-k}{\lfloor (n-k)/2 \rfloor}.$$

Следовательно, $|N| \leqslant k\binom{n}{k}\binom{n-k}{\lfloor (n-k)/2 \rfloor}$. Лемма доказана.

Из леммы 24 легко следует

Лемма 25. *Для любой n-местной монотонной булевой функции найдется направление $\boldsymbol{i}$, в котором проходит не более*

$$k\binom{n-k}{\lfloor (n-k)/2 \rfloor}$$

непостоянных интервалов размерности k.

Пусть $\boldsymbol{i} = (i_1, i_2, \ldots, i_k)$ и $\boldsymbol{\alpha} = (\alpha_1\alpha_2 \ldots \alpha_k)$. Символом $f_{\boldsymbol{i}}^{\boldsymbol{\alpha}}(\boldsymbol{x})$ обозначим n-местную функцию с k фиктивными переменными, получающуюся из n-местной булевой функции f подстановкой констант α_j вместо ее i_j-х аргументов, а символом $\boldsymbol{x}_{\boldsymbol{i}}^{\boldsymbol{\alpha}}$ обозначим булев набор длины n, у которого i_j-е разряды равны величинам α_j.

Лемма 26. *Для любой n-местной монотонной булевой функции f найдется такой набор $\boldsymbol{i}$ длины k, что соотношение $f_{\boldsymbol{i}}^{\boldsymbol{0}}(\boldsymbol{x}) \neq f_{\boldsymbol{i}}^{\boldsymbol{1}}(\boldsymbol{x})$ имеет место не более чем для $k2^k\binom{n-k}{\lfloor (n-k)/2 \rfloor}$ различных наборов $\boldsymbol{x}$ длины n.*

Доказательство. Если $f_{\boldsymbol{i}}^{\boldsymbol{0}}(\boldsymbol{\gamma}) \neq f_{\boldsymbol{i}}^{\boldsymbol{1}}(\boldsymbol{\gamma})$ для некоторого $\boldsymbol{\gamma}$, то аналогичное неравенство $f_{\boldsymbol{i}}^{\boldsymbol{0}}(\boldsymbol{x}) \neq f_{\boldsymbol{i}}^{\boldsymbol{1}}(\boldsymbol{x})$ справедливо для всех 2^k наборов $\boldsymbol{x}$ длины n из интервала $I(\boldsymbol{x}_{\boldsymbol{i}}^{\boldsymbol{0}}, \boldsymbol{x}_{\boldsymbol{i}}^{\boldsymbol{1}})$. Следовательно, для направления $\boldsymbol{i}$, в котором у функции f проходит не более $k\binom{n-k}{\lfloor (n-k)/2 \rfloor}$ непостоянных интервалов размерности k, найдется не более чем $k2^k\binom{n-k}{\lfloor (n-k)/2 \rfloor}$ различных наборов $\boldsymbol{x}$ длины n, для которых $f_{\boldsymbol{i}}^{\boldsymbol{0}}(\boldsymbol{x}) \neq f_{\boldsymbol{i}}^{\boldsymbol{1}}(\boldsymbol{x})$. Лемма доказана.

Из леммы 26 и формулы Стирлинга легко следует

Лемма 27. *При $n \to \infty$ и $k = o(n)$ для любой n-местной монотонной булевой функции f найдется такой набор $\boldsymbol{i}$ длины k, что $f_{\boldsymbol{i}}^{\boldsymbol{0}}(\boldsymbol{x}) \neq f_{\boldsymbol{i}}^{\boldsymbol{1}}(\boldsymbol{x})$ для не более чем*

$$\frac{k \cdot 2^n}{\sqrt{\pi n/2}}(1 + o(1))$$

различных наборов $\boldsymbol{x}$ длины n.

Лемма 28. *При $n\to\infty$ для любой n-местной монотонной булевой функции f*

$$T(f)\lesssim 6.36\cdot\frac{2^n}{\pi n^2}.$$

Доказательство. Положим $s=\lceil\log_2\log_2 n\rceil$. В силу леммы 27 для любого $k\in\{1,\dots,s\}$ найдется такой набор $\boldsymbol{i}_k$ длины 2^k, что $f^{\mathbf{0}}_{\boldsymbol{i}_k}(\boldsymbol{x})\neq f^{\mathbf{1}}_{\boldsymbol{i}_k}(\boldsymbol{x})$ для не более чем

$$\frac{2^k\cdot 2^n}{\sqrt{\pi n/2}}(1+o(1)) \tag{46}$$

различных наборов $\boldsymbol{x}$ длины n. Пусть A_k — множество всех таких наборов, $A_{s+1}=\{0,1\}^n$. Нетрудно видеть, что функции $f^{\mathbf{0}}_{\boldsymbol{i}_k}(\boldsymbol{x})$ и $f^{\mathbf{1}}_{\boldsymbol{i}_k}(\boldsymbol{x})$, зависящие от $n-2^k$ переменных, можно вычислить схемами, сложность которых асимптотически не превосходит величин

$$\frac{2^{n-2^k}}{(n-2^k)\sqrt{\pi(n-2^k)/2}}\sim\frac{2^{n-2^k}}{n\sqrt{\pi n/2}}. \tag{47}$$

При $0\leqslant k\leqslant s$ в каждом множестве A_{k+1} выделим два подмножества: A^1_{k+1}, состоящее из таких $\boldsymbol{x}\in A_{k+1}$, что $f^{\mathbf{0}}_{\boldsymbol{i}_k}(\boldsymbol{x})=1$, и A^0_{k+1}, состоящее из таких $\boldsymbol{x}\in A_{k+1}$, что $f^{\mathbf{1}}_{\boldsymbol{i}_k}(\boldsymbol{x})=0$. Далее без ограничения общности будем полагать, что $|A^1_{k+1}|\geqslant|A^0_{k+1}|$ и что $\boldsymbol{i}_1=(n-1,n)$, т. е. при $k=1$ функции $f^{\mathbf{0}}_{\boldsymbol{i}_1}(\boldsymbol{x})$ и $f^{\mathbf{1}}_{\boldsymbol{i}_1}(\boldsymbol{x})$ не зависят от x_{n-1} и x_n.

Опишем алгоритм, на основе которого далее будет построена программа с требуемой средней сложностью. Алгоритм делится на $s+1$ раундов. Действия, выполняемые в первых s раундах, одинаковы.

В первом раунде используются функции $f^{\mathbf{0}}_{\boldsymbol{i}_s}(\boldsymbol{x})$ и $f^{\mathbf{1}}_{\boldsymbol{i}_s}(\boldsymbol{x})$, которые разбивают n-мерный булев куб на три множества: A^{11}_s, A^{00}_s и A^{01}_s. На элементах первого множества $f^{\mathbf{0}}_{\boldsymbol{i}_s}(\boldsymbol{x})=f^{\mathbf{1}}_{\boldsymbol{i}_s}(\boldsymbol{x})=1$, на элементах второго $f^{\mathbf{0}}_{\boldsymbol{i}_s}(\boldsymbol{x})=f^{\mathbf{1}}_{\boldsymbol{i}_s}(\boldsymbol{x})=0$ и на элементах третьего $f^{\mathbf{0}}_{\boldsymbol{i}_s}(\boldsymbol{x})=0$ и $f^{\mathbf{1}}_{\boldsymbol{i}_s}(\boldsymbol{x})=1$. Функции f присваиваем единичное значение и вычисляем $f^{\mathbf{0}}_{\boldsymbol{i}_s}(\boldsymbol{x})$. Если $f^{\mathbf{0}}_{\boldsymbol{i}_s}(\boldsymbol{x})=1$, то $\boldsymbol{x}\in A^{11}_s$ и $f(\boldsymbol{x})\geqslant f^{\mathbf{0}}_{\boldsymbol{i}_s}(\boldsymbol{x})=1$. Вычисления прекращаем. Если $f^{\mathbf{0}}_{\boldsymbol{i}_s}(\boldsymbol{x})=0$, то функции f присваиваем нулевое значение и вычисляем $f^{\mathbf{1}}_{\boldsymbol{i}_s}(\boldsymbol{x})$. Если $f^{\mathbf{1}}_{\boldsymbol{i}_s}(\boldsymbol{x})=0$, то $\boldsymbol{x}\in A^{00}_s$ и $f(\boldsymbol{x})\leqslant f^{\mathbf{1}}_{\boldsymbol{i}_s}(\boldsymbol{x})=0$. Вычисления прекращаем. Если $f^{\mathbf{1}}_{\boldsymbol{i}_s}(\boldsymbol{x})=1$, то $\boldsymbol{x}$ лежит в множестве $A^{01}_s=A_s$, состоящем, в силу (46), асимптотически из не более чем $\dfrac{2^n\cdot 2^s}{\sqrt{\pi n/2}}$ элементов. Переходим к следующему раунду.

Во втором раунде перечисленные выше действия выполняются на множестве A_s, элементы которого, в зависимости от значений функций $f^{\mathbf{0}}_{\boldsymbol{i}_{s-1}}(\boldsymbol{x})$ и $f^{\mathbf{1}}_{\boldsymbol{i}_{s-1}}(\boldsymbol{x})$, распределяются по трем подмножествам A^{11}_{s-1}, A^{00}_{s-1} и A^{01}_{s-1}, где, очевидно, $A^{01}_{s-1}\subseteq A_{s-1}$ и $|A_{s-1}|\lesssim\dfrac{2^n\cdot 2^{s-1}}{\sqrt{\pi n/2}}$. После выполнения s раундов значения функции f не будут вычислены только на некотором подмножестве множества A_1, состоящем асимптотически из не более чем $\dfrac{2^n}{2\sqrt{\pi n/2}}$ 4-элементных подмножеств, в каждом из которых наборы отличаются только в последних двух компонентах. Поэтому если в наборе $\boldsymbol{x}$ две его компоненты равны единице, то $f(\boldsymbol{x})=f^{\mathbf{1}}_{\boldsymbol{i}_1}(\boldsymbol{x})=1$; если эти компоненты равны

нулю, то $f(\boldsymbol{x}) = f^{\mathbf{0}}_{i_1}(\boldsymbol{x}) = 0$. Это свойство позволяет в последнем раунде вычислить $f(\boldsymbol{x})$, если $x_{n-1} = x_n$. Если это не так, то значение $f(\boldsymbol{x})$ вычисляется как значение частичной функции, определенной на не более чем $\frac{2^n}{\sqrt{\pi n/2}}$ наборах.

Основанную на приведенном выше алгоритме и вычисляющую функцию $f(\boldsymbol{x})$ программу P представим в виде последовательности подпрограмм

$$\mathsf{P} = \mathsf{P}_s\mathsf{P}_{s-1}\ldots\mathsf{P}_k\ldots\mathsf{P}_1\mathsf{P}_0.$$

Здесь для $k = s, \ldots, 1$ каждая подпрограмма P_k состоит из двух подпрограмм P^1_k и P^0_k. При $k>0$ подпрограмма P^1_k выполняет следующие действия:

— объявляет 1 значением функции $f(\boldsymbol{x})$;
— вычисляет значения функции $f^{\mathbf{0}}_{i_k}(\boldsymbol{x})$;
— останавливает вычисления, если $f^{\mathbf{0}}_{i_k}(\boldsymbol{x}) = 1$.

Затем подпрограмма P^0_k:

— объявляет 0 значением функции $f(\boldsymbol{x})$;
— вычисляет значения функции $f^{\mathbf{1}}_{i_k}(\boldsymbol{x})$;
— останавливает вычисления, если $f^{\mathbf{1}}_{i_k}(\boldsymbol{x}) = 0$.

При $k = 0$ подпрограмма P^1_0:

— объявляет 1 значением функции $f(\boldsymbol{x})$;
— останавливает вычисления, если $x_{n-1}\&x_n = 1$;
— объявляет 0 значением функции $f(\boldsymbol{x})$;
— останавливает вычисления, если $x_{n-1} \vee x_n = 0$.

Подпрограмма P^0_0 является минимальной программой частичной функции f_D, которая определена на множестве $D = \{\boldsymbol{x} \in A_1 \mid x_{n-1} \neq x_n\}$ и совпадает на этом множестве с f.

Пусть B^i_k — множество наборов, на котором в программе P работает подпрограмма P^i_k. Тогда

$$T(\mathsf{P}) \leqslant \frac{1}{2^n}\left(\sum_{k=s}^{1}\left(|B^1_k|C(\mathsf{P}^1_k) + |B^0_k|C(\mathsf{P}^0_k)\right) + |B^1_0|C(\mathsf{P}^1_0) + |B^0_0|T_1(f_D)\right). \quad (48)$$

Из конструкции P следует, что

$$B^1_k \subseteq A_{k+1}, \quad B^0_0 = D, \quad B^0_k \subseteq A_{k+1} \setminus A^1_{k+1} \quad \text{при } k \neq 0.$$

Тогда

$$|B^i_s| \leqslant 2^n, \quad |B^0_0| \lesssim \frac{2^n}{\sqrt{\pi n/2}}, \quad |B^1_k| \lesssim \frac{2^{k+1}2^n}{\sqrt{\pi n/2}} \quad \text{при } k \neq s. \quad (49)$$

Так как $A_{k+1} = A^1_{k+1} \sqcup A^0_{k+1} \sqcup (A_k \cap A_{k+1})$ и $|A^1_{k+1}| \geqslant |A^0_{k+1}|$, то

$$|B^0_k| \leqslant |A_{k+1} \setminus A^1_{k+1}| \leqslant \frac{1}{2}|A_{k+1}| + \frac{1}{2}|A_k| \lesssim \frac{3}{4}\cdot\frac{2^{k+1}2^n}{\sqrt{\pi n/2}} \quad \text{при } k \neq 0, s. \quad (50)$$

Легко видеть, что $C(\mathsf{P}^1_0) = 6$ и, что в силу (47),

$$C(\mathsf{P}^i_k) \lesssim \frac{2^{n-2^k}}{n\sqrt{\pi n/2}} \quad \text{при } k \neq 0 \text{ и } i = 0, 1. \quad (51)$$

Для функции f_D из (49) и леммы 14 следует существование такой вычисляющей эту функцию программы P_D, что

$$T(\mathsf{P}_D)|D| \lesssim \frac{2^{n-1}}{n\sqrt{\pi n/2}} \cdot \frac{2^n}{\sqrt{\pi n/2}} = \frac{2^{2n}}{\pi n^2}. \tag{52}$$

Таким образом, при $n \to \infty$ для слагаемых в (48) справедливы следующие неравенства: при $k = s$ из (49) и (51) следует, что

$$|B_s^1|C(\mathsf{P}_s^1) + |B_s^0|C(\mathsf{P}_s^0) \lesssim 2^n \cdot \frac{2^{n-2^s+1}}{n\sqrt{\pi n/2}} \leqslant \frac{2^{2n+1}}{n^2\sqrt{\pi n/2}};$$

при $k = 1, \ldots, s-1$ из (49)–(51) и неравенства $k - 2^k \leqslant -k$ следует, что

$$|B_k^1|C(\mathsf{P}_k^1) + |B_k^0|C(\mathsf{P}_k^0) \lesssim \frac{7}{4} \cdot \frac{2^{k+1}2^n}{\sqrt{\pi n/2}} \cdot \frac{2^{n-2^k}}{n\sqrt{\pi n/2}} \leqslant \frac{7}{4} \cdot \frac{2^{2n-k+2}}{\pi n^2}; \tag{53}$$

для двух последних слагаемых из (49) и (52) следует, что

$$|B_0^1|C(\mathsf{P}_0^1) + |B_0^0|T(f_D) \sim |B_0^0|T(f_D) \lesssim \frac{2^{2n}}{\pi n^2}.$$

Следовательно,

$$T(\mathsf{P}) \lesssim \frac{2^{n+1}}{n^2\sqrt{\pi n/2}} + \sum_{k=s-1}^{1} \frac{7 \cdot 2^{n-k}}{\pi n^2} + \frac{2^n}{\pi n^2} \sim \frac{8 \cdot 2^n}{\pi n^2}. \tag{54}$$

Теперь заметим, что если вместо степеней двойки длины первых семи наборов $\boldsymbol{i}_k$ взять равными $2, 4, 7, 10, 14, 18, 24$, то константа в числителе (53) уменьшится с 7 до 5.36, а в числителе (54) — с 8 до 6.36. Лемма доказана.

Установим нижние оценки среднего времени вычисления монотонных функций.

Лемма 29. *При $n \to \infty$ для любой постоянной $\varepsilon > 0$ доля n-местных монотонных булевых функций f, для которых справедливо неравенство*

$$T(f) \geqslant (1-\varepsilon)\frac{3}{4} \cdot \frac{2^n}{\pi n^2},$$

стремится к единице.

Доказательство. Пусть f — n-местная монотонная булева функция, P — минимальная программа, вычисляющая f, ε — сколь угодно малая положительная постоянная, $\alpha = 1 + \varepsilon$. Рассмотрим наборы $\boldsymbol{x}_i$ такие, что $N_{\mathsf{P}}(\boldsymbol{x}_i) = 2^n - \alpha^{-i}\binom{n}{\lfloor n/2 \rfloor}$, где $i = 1, 2, \ldots, k = \lceil \log_\alpha n \rceil$ [*]). Оценим число n-местных монотонных булевых функций, у минимальных программ которых найдется $\boldsymbol{x}_i$ такое, что

$$T_{\mathsf{P}}(\boldsymbol{x}_i) \leqslant \frac{3}{4} \cdot \frac{(1-\alpha^{-i})(1-\varepsilon) \cdot \binom{n}{\lfloor n/2 \rfloor}}{n}.$$

Каждая такая функция однозначно определяется первыми $T_{\mathsf{P}}(\boldsymbol{x}_i)$ командами своей минимальной программы и двоичным вектором длины не более

[*]) Без ограничения общности можно полагать, что $\alpha^{-i}\binom{n}{\lfloor n/2 \rfloor}$ является целым.

чем $2^n - N_{\mathsf{P}}(\boldsymbol{x}_i) = \alpha^{-i}\binom{n}{\lfloor n/2\rfloor}$ — значениями на тех аргументах, время работы на которых больше времени работы на $\boldsymbol{x}_i$. В силу леммы 22 для числа N_i, равного числу различных программ, сложность которых не превосходит $T_{\mathsf{P}}(\boldsymbol{x}_i)$, справедливо неравенство

$$N_i \leqslant \left(c_1\left(T_{\mathsf{P}}(\boldsymbol{x}_i)+n\right)\right)^{4/3\cdot\left(T_{\mathsf{P}}(\boldsymbol{x}_i)\right)}.$$

После несложных преобразований получаем неравенство

$$N_i \leqslant \left(c_1\left(\frac{3}{4}\cdot\frac{(1-\alpha^{-i})(1-\varepsilon)}{n}\binom{n}{\lfloor n/2\rfloor}+n\right)\right)^{\frac{(1-\alpha^{-i})(1-\varepsilon)}{n}\binom{n}{\lfloor n/2\rfloor}} \leqslant 2^{\left(1-\alpha^{-i}\right)(1-\varepsilon)\binom{n}{\lfloor n/2\rfloor}}.$$

Поэтому для R — числа рассматриваемых функций — справедливо неравенство

$$R \leqslant \sum_{i=1}^{k} 2^{\left(1-\alpha^{-i}\right)(1-\varepsilon)\binom{n}{\lfloor n/2\rfloor}}\cdot 2^{\alpha^{-i}\binom{n}{\lfloor n/2\rfloor}} = \sum_{i=1}^{k} 2^{\binom{n}{\lfloor n/2\rfloor}(1-(1-\alpha^{-i})\varepsilon)} \leqslant$$
$$\leqslant \log_\alpha n\cdot 2^{\binom{n}{\lfloor n/2\rfloor}(1-(1-\alpha^{-1})\varepsilon)} = \log_\alpha n\cdot 2^{\binom{n}{\lfloor n/2\rfloor}(1-\varepsilon^2/(1+\varepsilon))} = o\left(2^{\binom{n}{\lfloor n/2\rfloor}}\right).$$

Сравнивая полученную оценку величины R с числом всех n-местных монотонных булевых функций, видим, что все минимальные программы почти всех этих функций удовлетворяют условию:

если $\boldsymbol{x}_i$ такое, что $N_{\mathsf{P}}(\boldsymbol{x}_i) = 2^n - \alpha^{-i}\binom{n}{\lfloor n/2\rfloor}$,

то $T_{\mathsf{P}}(\boldsymbol{x}_i) > \frac{3}{4}\cdot\frac{(1-\alpha^{-i})(1-\varepsilon)}{n}\binom{n}{\lfloor n/2\rfloor}$.

Положим $X_i = \{\boldsymbol{x} \mid N_{\mathsf{P}}(\boldsymbol{x}_i) \leqslant N_{\mathsf{P}}(\boldsymbol{x}) < N_{\mathsf{P}}(\boldsymbol{x}_{i+1})\}$ для $i = 1,\ldots,k-1$ и $X_k = \{\boldsymbol{x} \mid N_{\mathsf{P}}(\boldsymbol{x}_k) \leqslant N_{\mathsf{P}}(\boldsymbol{x}) \leqslant 2^n\}$. Нетрудно видеть, что

$$|X_i| = \binom{n}{\lfloor n/2\rfloor}\left(\alpha^{-i}-\alpha^{-i-1}\right) \text{ при } i = 1,\ldots,k-1,$$
$$|X_k| = \binom{n}{\lfloor n/2\rfloor}\alpha^{-k}+1.$$

Тогда для среднего времени работы каждой такой программы имеем:

$$T(\mathsf{P}) = \frac{1}{2^n}\sum_{\boldsymbol{x}\in\{0,1\}^n} T_{\mathsf{P}}(\boldsymbol{x}) \geqslant \frac{1}{2^n}\sum_{i=1}^{k} T_{\mathsf{P}}(x_i)|X_i| \geqslant$$
$$\geqslant \frac{3(1-\varepsilon)}{2^n\cdot 4n}\binom{n}{\lfloor n/2\rfloor}^2\left(\sum_{i=1}^{k-1}\left(1-\frac{1}{\alpha^i}\right)\left(\frac{1}{\alpha^i}-\frac{1}{\alpha^{i+1}}\right)+\left(1-\frac{1}{\alpha^k}\right)\frac{1}{\alpha^k}\right) \geqslant$$
$$\geqslant \frac{3(1-2\varepsilon)\cdot 2^n}{2\pi n^2}\left(\sum_{i=1}^{k-1}\left(\frac{1}{\alpha^i}-\frac{1}{\alpha^{i+1}}-\frac{1}{\alpha^{2i}}+\frac{1}{\alpha^{2i+1}}\right)+\frac{1}{\alpha^k}-\frac{1}{\alpha^{2k}}\right) =$$
$$= \frac{3(1-2\varepsilon)\cdot 2^n}{2\pi n^2}\left(\frac{1}{\alpha}-\frac{1}{\alpha^2}\sum_{i=0}^{2k-2}\left(-\frac{1}{\alpha}\right)^i\right) \geqslant$$
$$\geqslant \frac{3(1-2\varepsilon)\cdot 2^n}{2\pi n^2}\left(\frac{1}{\alpha}-\frac{1}{\alpha(1+\alpha)}\right) = \frac{3(1-2\varepsilon)\cdot 2^n}{2\pi n^2}\cdot\frac{1}{1+\alpha}.$$

Так как $\alpha = 1+\varepsilon$, то

$$T(\mathsf{P}) \geqslant \frac{3\cdot 2^n}{2\pi n^2}\cdot\frac{1-2\varepsilon}{2+\varepsilon} \geqslant \frac{3}{4}\cdot\frac{2^n}{\pi n^2}\cdot(1-3\varepsilon),$$

где ε — сколь угодно малая положительная постоянная. Лемма доказана.

Методы, использованные при доказательстве теоремы 7, хорошо переносятся на случай вычисления монотонных булевых функций программами без памяти. В [24] при помощи этих методов показано, что при $n \to \infty$ для любой n-местной монотонной булевой функции f

$$T^0(f) \lesssim 6.36 \cdot \frac{2^n}{\pi n \log_2 n}$$

и для любой постоянной $\varepsilon > 0$ доля n-местных монотонных булевых функций f, для которых справедливо неравенство

$$T^0(f) \gtrsim \frac{2^n}{\pi n \log_2 n},$$

стремится к единице. Ранее для сложности вычисления формулами самой сложной n-местной монотонной булевой функции А. Е. Андреевым в [3] была получена асимптотически точная формула

$$L^0(f) \sim \frac{2^n}{\sqrt{\pi n/2}\log_2 n}.$$

§ 5. Соотношения между сложностью и средней сложностью

Определим насколько сильно могут различаться среднее время вычисления конкретной булевой функции и сложность ее вычисления схемами из функциональных элементов. Положим

$$\mu(f) = \frac{L(f)}{T(f)}, \quad \mu(n, L) = \max \mu(f), \quad \mu(n) = \max \mu(f),$$

где первый максимум берется по всем n-местным булевым функциям, сложность которых равна L, а второй максимум — по всем n-местным булевым функциям. Из теоремы 2 следует, что средняя сложность и сложность вычисления для почти всех булевых функций схемами из функциональных элементов различаются не более чем в постоянное число раз, т. е. $\mu(f) = \text{const}$ для почти каждой булевой функции. В то же время результаты предыдущего раздела показывают, что отношение сложности минимальной схемы к средней сложности может расти вместе с ростом числа аргументов у функций. Покажем, что для некоторых функций это отношение может быть экспоненциально большим.

Т е о р е м а 8. *Пусть* $n \to \infty$, $L \geqslant n$. *Тогда*

$$\mu(n, L) = \begin{cases} \Theta(L), & \text{если } L \leqslant \sqrt{\dfrac{2^n}{n}}, \\ \Theta\left(\dfrac{2^n}{L \log_2 L}\right), & \text{если } L > \sqrt{\dfrac{2^n}{n}}. \end{cases} \tag{55}$$

Д о к а з а т е л ь с т в о. Положим $k = \lceil \log_2 L + \log_2 \log_2 L \rceil$. Тогда $L \log_2 L \leqslant 2^k \leqslant 2L \log_2 L$. Пусть g — любая из «почти всех» самых сложных булевых функций от k переменных. Тогда

$$L \leqslant \frac{2^k}{k} \leqslant L(g) \lesssim \frac{2^k}{k} \leqslant 2L.$$

Рассмотрим функцию

$$f(x_1, \ldots, x_n) = \overline{x}_{k+1} \& \cdots \& \overline{x}_n \& g(x_1, \ldots, x_k)$$

и схему S, вычисляющую функцию g с минимальной сложностью. Нетрудно видеть, что следующая программа P

$$\begin{array}{ll} \mathsf{p}_1: & \mathtt{z} = 0 \\ \mathsf{p}_2: & \mathtt{Stop}(x_{k+1}) \\ \mathsf{p}_3: & \mathtt{Stop}(x_{k+2}) \\ \ldots\ldots & \ldots\ldots\ldots\ldots \\ \mathsf{p}_{n-k+1}: & \mathtt{Stop}(x_n) \\ \mathsf{S} & \end{array}$$

вычисляет f. Учитывая, что $L(\mathsf{S})$ асимптотически не превосходит $2L$, после несложных вычислений для средней сложности программы P находим, что при $k \geqslant \log_2 n + \log_2 \log_2 n$

$$T(\mathsf{P}) \leqslant \frac{1}{2^n}\left(\sum_{j=1}^{n-k}(j+1)2^{n-j} + (n-k+1+L(g))2^k\right) \lesssim$$

$$\lesssim \frac{1}{2^n}\left(3\cdot 2^n + 2L\cdot 2^k\right) \leqslant \frac{1}{2^n}\left(3\cdot 2^n + 4L^2\log_2 L\right) = 3 + \frac{L^2\log_2 L}{2^{n-2}}.$$

Следовательно, $T(\mathsf{P}) \leqslant 7$ при $L \leqslant \sqrt{2^n/n}$ и $T(\mathsf{P}) = \mathcal{O}\left(L^2\log_2 L \Big/ 2^n\right)$ при $L > \sqrt{\frac{2^n}{n}}$. Воспользуемся этими неравенствами и оценим $\mu(f)$ снизу. Так как

$$\mu(f) = \frac{L(f)}{T(f)} \geqslant \frac{L(f)}{T(\mathsf{P})} \geqslant \frac{L(g)}{T(\mathsf{P})} \geqslant \frac{L}{T(\mathsf{P})},$$

то нетрудно видеть, что для отношения сложности функции f к ее средней сложности справедливы неравенства:

$$\mu(f) = \Omega(L), \qquad \text{если } L \leqslant \sqrt{\frac{2^n}{n}},$$

$$\mu(f) = \Omega\left(\frac{2^n}{L\log_2 L}\right), \qquad \text{если } L > \sqrt{\frac{2^n}{n}}.$$

Таким образом, нижние оценки равенства (55) установлены.

Прежде чем доказывать верхние оценки равенства (55), установим вспомогательное утверждение.

Лемма 30. *Для любой n-местной булевой функции f такой, что $L(f) \gg n\log_2 n$, справедливо неравенство*

$$2^{n+6}T(f) \geqslant L(f)^2\log_2 L(f).$$

Доказательство. Пусть f — произвольная n-местная булева функция, P — программа, которая вычисляет f, и среднее время работы которой минимально. Рассмотрим такой набор $\boldsymbol{x}_0$, что выполнено $N_{\mathsf{P}}(\boldsymbol{x}_0) = 2^n - \frac{1}{8}L(f)\log_2 L(f)$. Так как

$$T(\mathsf{P}) = \frac{1}{2^n}\sum_{\boldsymbol{x}} T_{\mathsf{P}}(\boldsymbol{x}) > \frac{1}{2^n}\sum_{\boldsymbol{x}\ \mid\ N(\boldsymbol{x}) > N(\boldsymbol{x}_0)} T_{\mathsf{P}}(\boldsymbol{x}) \geqslant \frac{1}{2^{n+3}}T_{\mathsf{P}}(\boldsymbol{x}_0)L(f)\log_2 L(f),$$

то легко видеть, что

$$2^{n+3}T(f) > T_{\mathsf{P}}(\boldsymbol{x}_0)L(f)\log_2 L(f). \tag{56}$$

Далее, пусть $\widetilde{f}$ — частичная булева функция, определенная на всех таких наборах $\boldsymbol{x}$, что $T_{\mathsf{P}}(\boldsymbol{x}) > T_{\mathsf{P}}(\boldsymbol{x}_0)$, и совпадающая на этих наборах с f. Очевидно, что область определения $\widetilde{f}$ не превосходит $\frac{1}{8}L(f)\log_2 L(f)$. Поэтому из неравенства $L(f) \gg n\log_2 n$ следует существование вычисляющей частичную функцию $\widetilde{f}$ схемы S такой, что

$$L(\mathsf{S}) \leqslant \tfrac{1}{4}L(f). \tag{57}$$

Теперь покажем, что $T_{\mathsf{P}}(\boldsymbol{x}_0) \geqslant \frac{1}{8}L(f)$. Предположим, что это не так. Рассмотрим программу P', которая вычисляет функцию f и устроена следующим образом. Начало программы P' (первые $T_{\mathsf{P}}(\boldsymbol{x}_0)$ команд) совпадает с началом программы P и вычисляет значения функции f на всех наборах $\boldsymbol{x}$ таких, что $T_{\mathsf{P}}(\boldsymbol{x}) \leqslant T_{\mathsf{P}}(\boldsymbol{x}_0)$. Оставшиеся команды образуют схему S и вычисляют значения функции f на всех таких наборах $\boldsymbol{x}$, что $T_{\mathsf{P}}(\boldsymbol{x}) > T_{\mathsf{P}}(\boldsymbol{x}_0)$. В этом случае в силу неравенства (5)

$$L(f) \leqslant 2C(\mathsf{P}') = 2(T_{\mathsf{P}}(\boldsymbol{x}_0) + L(\mathsf{S})) < 2\left(\tfrac{1}{8}L(f) + \tfrac{1}{4}L(f)\right) = \tfrac{3}{4}L(f) < L(f).$$

Пришли к противоречивому неравенству $L(f) < L(f)$. Следовательно, сделанное предположение ложно и поэтому $T_{\mathsf{P}}(\boldsymbol{x}_0) \geqslant \frac{1}{8}L(f)$. Подставляя полученное неравенство в (56), видим, что

$$2^{n+6}T(f) \geqslant L(f)^2\log_2 L(f).$$

Лемма доказана.

Завершим доказательство теоремы. Если $L \leqslant \sqrt{\frac{2^n}{n}}$, то неравенство $\mu(n, L) \leqslant L$ очевидно, так как $T(f) \geqslant 1$ для каждой булевой функции f. Если $L > \sqrt{\frac{2^n}{n}}$, неравенство $\mu(n, L) \leqslant \frac{2^{n+6}}{L\log_2 L}$ вытекает из неравенства леммы 30. Теорема доказана.

Следующая теорема является простым следствием теоремы 8.

Т е о р е м а 9.

$$\mu(n) = \Theta\left(\sqrt{\frac{2^n}{n}}\right).$$

Хотя средняя сложность рассмотренной в теореме 8 функции f значительно меньше ее обычной сложности, в области определения f есть достаточно большая подобласть (состоящая из наборов, удовлетворяющих равенству $\overline{x}_{k+1}\& \cdots \& \overline{x}_n = 1$), в которой f является типичным представителем «почти всех» функций. Поэтому в силу теоремы 2 для почти каждой функции f, определенной описанным выше способом, ее средняя по этой подобласти сложность будет отличаться от $L(f)$ только постоянным множителем. Покажем, что этот эффект связан не со способом определения f,

а является отражением общей ситуации: для любой булевой функции, зависящей от n переменных, существует подобласть, в которой ее средняя сложность отличается от ее схемной сложности по порядку величины не более чем в $n/\log_2 n$ раз.

Далее нижний индекс D у функции T_D определяет область D, на которой вычисляется средняя сложность, а такой же индекс у функции f_D, как и ранее, обозначает сужение функции f на область D.

Теорема 10. *Пусть* $D\subseteq\{0,1\}^n$, $|D|=N$, $n\to\infty$. *Тогда*:

(1) *для любой функции* $f: D\to\{0,1\}$, *сложность которой удовлетворяет неравенству* $L(f)\gg n\log_2 N$, *найдется такая область* $D'\subseteq D$, *что*

$$T_{D'}(f)=\Omega\left(L(f)\Big/\log_2\frac{16N}{L(f)\log_2 L(f)}\right);$$

(2) *для любого целого* L, *удовлетворяющего неравенствам* $n\log_2 n\ll L\leqslant N/\log_2 N$, *найдется такая частичная функция* $f: D\to\{0,1\}$, *что* $L(f)=L$ *и для любой области* $D'\subseteq D$

$$T_{D'}(f)=\mathcal{O}\left(L(f)\Big/\log_2\frac{16N}{L(f)\log_2 L(f)}\right).$$

Перед доказательством теоремы докажем необходимую лемму. Характеристическую функцию области $D\subseteq\{0,1\}^n$ будем обозначать символом χ_D.

Лемма 31. *Пусть* $D\subseteq\{0,1\}^n$, $|D|=N$. *Для любой* $f: D\to\{0,1\}$ *существуют область* $D'\subseteq D$ *и функция* h *такие, что*:

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

(2) $L(h,\chi_{D\setminus D'})\leqslant 8T_D(f)$;

(3) $|D'|\leqslant N/2+1$.

Доказательство. Пусть P — вычисляющая функцию f программа, на которой достигается минимальное среднее время, и пусть набор $\boldsymbol{x}_0$ такой, что $N_{\mathsf{P}}(\boldsymbol{x}_0)=N-\lfloor N/2\rfloor$. Тогда

$$T_D(f)\geqslant\frac{1}{N}\left(\sum_{\boldsymbol{x}\,|\,N_{\mathsf{P}}(\boldsymbol{x})\geqslant N_{\mathsf{P}}(\boldsymbol{x}_0)}T_{\mathsf{P}}(\boldsymbol{x})\right)\geqslant\frac{1}{N}\left(\left\lfloor\frac{N|}{2}\right\rfloor+1\right)T_{\mathsf{P}}(\boldsymbol{x}_0)\geqslant\frac{T_{\mathsf{P}}(\boldsymbol{x}_0)}{2}.$$

Следовательно,

$$T_{\mathsf{P}}(\boldsymbol{x}_0)\leqslant 2T_D(f).$$

Пусть $\mathsf{q}_1,\ldots,\mathsf{q}_k$ — команды, являющиеся нулевыми аргументами команд остановки программы P, последняя из которых останавливает работу этой программы на наборе $\boldsymbol{x}_0$. Положим $D'=\{\boldsymbol{x}\mid T_{\mathsf{P}}(\boldsymbol{x})>T_{\mathsf{P}}(\boldsymbol{x}_0)\}$. Тогда $|D'|\leqslant N/2$, $\chi_{D'}=\bigwedge\limits_{i=1}^{k}\overline{\mathsf{q}}_i$ и значения функции

$$h(\boldsymbol{x})=\mathsf{q}_1(\boldsymbol{x})\mathsf{z}(\boldsymbol{x};t_1)\vee\overline{\mathsf{q}}_1(\boldsymbol{x})(\mathsf{q}_2(\boldsymbol{x})\mathsf{z}(\boldsymbol{x};t_2)\vee\ldots$$
$$\vee\overline{\mathsf{q}}_{k-2}(\boldsymbol{x})(\mathsf{q}_{k-1}(\boldsymbol{x})\mathsf{z}(\boldsymbol{x};t_{k-1})\vee\overline{\mathsf{q}}_{k-1}(\boldsymbol{x})\mathsf{q}_k(\boldsymbol{x})\mathsf{z}(\boldsymbol{x};t_k))\ldots),$$

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

$$L(h,\chi_{D'})\leqslant k+3k-k+T_{\mathsf{P}}(x_0)\leqslant 8T_D(f).$$

Лемма доказана.

Доказательство теоремы 10. (1) Докажем теорему методом от противного. Пусть c — произвольная постоянная. Положим

$$T = cL(f)\Big/\log_2 \frac{16N}{L(f)\log_2 L(f)}, \qquad D_0 = D.$$

Предположим, что для любой области $D' \subseteq D_0$ справедливо неравенство

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

Воспользуемся леммой 31. В силу этой леммы существуют область $D_1 \subseteq D_0$ и функция h^1 такие, что

$$f_{D_0 \setminus D_1} = h^1_{D_0 \setminus D_1}, \quad L(h^1, \chi_{D_1}) \leqslant 8T, \quad |D_1| \leqslant |D_0|/2 + 1.$$

Снова используем лемму 31, применив ее к функции f_{D_1}. В силу этой леммы существуют область $D_2 \subseteq D_1$ и функция h^2 такие, что

$$f_{D_1 \setminus D_2} = h^2_{D_1 \setminus D_2}, \quad L(h^2, \chi_{D_2}) \leqslant 8T, \quad |D_2| \leqslant |D_1|/2 + 1.$$

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

$$f_{D_i \setminus D_{i+1}} = h^{i+1}_{D_i \setminus D_{i+1}}, \tag{58}$$

$$L(h^{i+1}, \chi_{D_{i+1}}) \leqslant 8T, \tag{59}$$

$$|D_{i+1}| \leqslant |D_i|/2 + 1. \tag{60}$$

Из (58) 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 (59) и последней формулы, имеет место неравенство

$$L(f) \leqslant 11kT + L(f_{D_k}). \tag{61}$$

Оценим мощность множества D_k. В силу неравенства (60) имеем

$$\begin{aligned} |D_k| &\leqslant \tfrac{1}{2}|D_{k-1}| + 1 \leqslant \tfrac{1}{2}\left(\tfrac{1}{2}|D_{k-2}| + 1\right) + 1 \leqslant \ldots \\ &\leqslant \tfrac{1}{2}\left(\tfrac{1}{2}\left(\ldots\left(\tfrac{1}{2}|D_0| + 1\right)\ldots\right)\right) + 1 \leqslant \tfrac{1}{2^k}|D_0| + 2 = \tfrac{1}{2^k}N + 2. \end{aligned}$$

Положим $k = \left\lceil \log \frac{8N}{L(f)\log_2 L(f)} \right\rceil$. Тогда

$$|D_k| \leqslant \frac{N}{2^k} + 2 \leqslant \tfrac{1}{8}L(f)\log_2 L(f) + 2 < \tfrac{1}{4}L(f)\log_2 L(f). \tag{62}$$

Для сложности произвольной частичной функции $f : D_k \to \{0,1\}$, где $|D_k| \gg n\log_2 n$, из полученных выше результатов легко извлекается неравенство

$$L(f_{D_k}) \leqslant \frac{2|D_k|}{\log_2 |D_k|},$$

которое вместе с (62) показывает, что

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

Подставляя полученную оценку $L(f_{D_k})$ в (61) и выражая T через $L(f)$ и N, видим, что

$$L(f) < 11kT + \frac{1}{2}L(f) \leqslant$$
$$\leqslant \frac{11cL(f)}{\log_2 \frac{16N}{L(f)\log_2 L(f)}} \left(\log_2 \frac{16N}{L(f)\log_2 L(f)}\right) + \frac{1}{2}L(f) \leqslant \left(11c + \frac{1}{2}\right) L(f).$$

При $c < 1/22$ приходим к противоречию. Таким образом, сделанное предположение неверно.

(2) Пусть $n \log_2 n \ll N_1 \leqslant N/2$. Рассмотрим множество M, состоящее из частичных функций, определенных на области D и принимающих в D значение единица ровно на N_1 наборах. Пусть $f : D \to \{0, 1\}$ — самая сложная функция в M. Тогда в силу лемм 18 и 21, неравенства (38) и теоремы 6 справедливы неравенства

$$L(f) = \Theta\left(\frac{N_1}{\log_2 N_1} \cdot \log_2 \frac{N}{N_1}\right), \quad T_{D'}(f) = \mathcal{O}\left(\frac{N_1}{\log_2 N_1}\right),$$

где D' — произвольное подмножество D. Легко видеть, что

$$L(f) \,/ T_{D'}(f) = \Omega\left(\log_2 \frac{N}{N_1}\right).$$

С другой стороны, так как $L(f)\log_2 L(f) = \Theta\left(N_1 \log_2 \frac{N}{N_1}\right)$, то

$$\log_2 \frac{16N}{L(f)\log_2 L(f)} = \Theta\left(\log_2 \frac{16N}{N_1} - \log_2 \log_2 \frac{N}{N_1}\right) = \Theta\left(\log_2 \frac{N}{N_1}\right).$$

Следовательно,

$$T_{D'}(f) = \mathcal{O}\left(L(f) \Big/ \log_2 \frac{16N}{L(f)\log_2 L(f)}\right).$$

Теорема доказана.

СПИСОК ЛИТЕРАТУРЫ

1. Алехина М. А., Грабовская С. М. О надежности неветвящихся программ в произвольном полном конечном базисе // Изв. вузов. Матем. — 2012 . — № 2. — С. 13–22.
2. Алехина М. А., Грабовская С. М. О сколь угодно надежной реализации булевых функций неветвящимися программами с оператором условной остановки в базисах с обобщенной конъюнкцией // ПДМ. — 2019. — № 43. — С. 70–77.
3. Андреев А. Е. О сложности монотонных функций // Вестник МГУ. Серия 1. Математика. Механика. — 1985. — № 4. — С. 83–87.
4. Андреев А. Е. О сложности реализации частичных булевых функций схемами из функциональных элементов // Дискретная математика. — 1989. — Т. 1, № 4. — С. 36–45.
5. Забалуев Р. Н. О реализации булевых функций программами одного типа // Вестник МГУ. Серия 1. Математика. Механика. — 2005. — № 5. — С. 9–13.

6. Забалуев Р. Н. О средней сложности монотонных функций // Дискретная математика. — 2006. — Т. 18, № 2. — С. 71–83.
7. Карпова Н. А. О вычислениях с ограниченной памятью // Математические вопросы кибернетики. Вып. 2. — М.: Наука, 1989. — С. 131–144.
8. Лупанов О. Б. О синтезе некоторых классов управляющих систем // Проблемы кибернетики. Вып. 10. — М.: Наука, 1963. — С. 63–97.
9. Лупанов О. Б. Об одном подходе к синтезу управляющих систем — принципе локального кодирования // Проблемы кибернетики. Вып. 14. — М.: Физматгиз, 1965. — С. 31–110.
10. Нечипорук Э. И. О топологических принципах самокорректирования // Проблемы кибернетики. Вып. 21. — М.: Наука, 1969. — С. 5–102.
11. Нечипорук Э. И. О сложности вентильных схем, реализующих булевские матрицы с неопределенными элементами // ДАН СССР — 1965. — Т. 163, № 1. — С. 40–42.
12. Угольников А. Б. О реализации монотонных функций схемами из функциональных элементов // Проблемы кибернетики. Вып. 31. — М.: Наука, 1976. — С. 167–185.
13. Чашкин А. В. О среднем времени вычисления значений булевых функций // Дискретный анализ и исследование операций. — 1997. — Т. 4, № 1. — С. 60–78.
14. Чашкин А. В. О среднем времени вычисления булевых операторов // Дискретный анализ и исследование операций. — 1998. — Т. 5, № 1. — С. 88–103.
15. Чашкин А. В. Среднее время вычисления значений элементарных булевых функций // Дискретная математика. — 2000. — Т. 12, № 4. — С. 109–120.
16. Чашкин А. В. Об одном методе вычисления частичных булевых функций // Математические вопросы кибернетики. Вып. 12. — М.: ФИЗМАТЛИТ, 2003. — С. 231–246.
17. Чашкин А. В. Средняя сложность симметрических булевых функций // Вестник МГУ. Серия 1. Математика. Механика. — 2003. — № 1. — С. 16–19.
18. Чашкин А. В. О средней монотонной сложности булевых функций // Дискретный анализ и исследование операций. — 2004. — Т. 11, № 4. — С. 68–80.
19. Чашкин А. В. О реализации частичных булевых функций // Труды VII Международной конференции «Дискретные модели в теории управляющих систем» (Покровское, 4–6 марта 2006 г.). — М.: МАКС Пресс, 2006. — С. 390–404.
20. Чашкин А. В. Оценки средней сложности монотонных булевых функций // Дискретная математика. — 2016. — Т. 28, № 2. — С. 146–153.
21. Чашкин А. В. Среднее время вычисления булевых операторов программами с ограниченной памятью // Вестник МГУ. Серия 1. Математика. Механика. — 2017. — № 3. — С. 16–21.
22. Чашкин А. В. О средней сложности недоопределенных функций // Дискретная математика. — 2017. — Т. 29, № 2. — С. 133–159.
23. Чашкин А. В. О средней сложности булевых функций с биномиальным распределением на области определения // Дискретная математика. — 2020. — Т. 32, № 3. — С. 130–134.
24. Чашкин А. В. О реализации монотонных булевых функций программами без памяти // Вестник МГУ. Серия 1. Математика. Механика. — 2022. — № 3. — С. 25–32.
25. Шоломов Л. А. О функционалах, характеризующих сложность систем недоопределенных булевых функций // Проблемы кибернетики. Вып. 19. — М.: Наука, 1967. — С. 123–140.
26. Шоломов Л. А. О реализации недоопределенных булевых функций схемами из функциональных элементов // Проблемы кибернетики. Вып. 21. — М.: Наука, 1969. — С. 215–226.
27. Andreev A. E., Clementi A. E. F., Rolim J. D. P. Worst-case hardness suffices for derandomization: A new method for hardness-randomness trade-offs // International Colloquium on Automata, Languages and Programming. — Springer, Berlin, Heidelberg, 1997. — P. 177–187.

Поступило в редакцию 6 VII 2022.