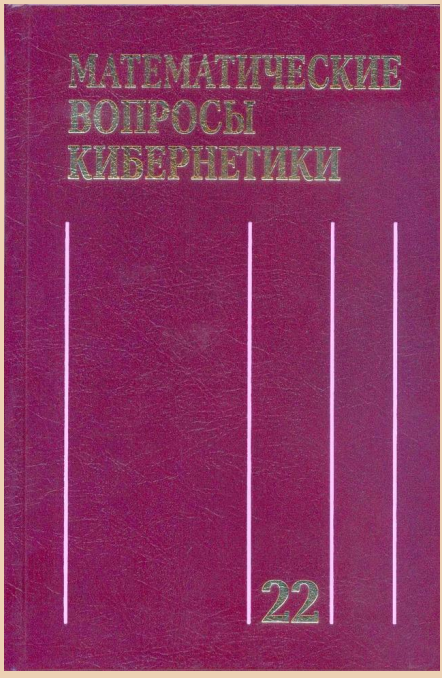
ИПМ им. М.В. Келдыша РАН • Электронная библиотека
Математические вопросы кибернетики • Выпуск 22



А. В. Чашкин

О вычислении частичных булевых функций

Рекомендуемая форма библиографической ссылки: Чашкин А. В. О вычислении частичных булевых функций // Математические вопросы кибернетики. Вып. 22. — М.: ФИЗМАТЛИТ, 2024. — С. 152–222. URL: https://library.keldysh.ru/mvk.asp?id=2024-152 DOI: 10.20948/mvk-2024-152

О ВЫЧИСЛЕНИИ ЧАСТИЧНЫХ БУЛЕВЫХ ФУНКЦИЙ*)

А. В. ЧАШКИН

(МОСКВА)

Оглавление

*) 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-2024-152

§ 1. Введение

В работе оценивается сложность вычисления частичных булевых функций данного веса схемами из функциональных элементов в произвольном полном конечном базисе $B=\{\varphi_i\}$, в котором каждой базисной функции φ_i приписан положительный вес ϱ_i, а сложностью схемы называется сумма весов ее элементов. Ниже будет показано, что для любой частичной n-местной булевой функции f, определенной на области из D элементов и равной единице на N наборах из этой области, при $n\to\infty$ справедливо неравенство

$$L_B(f)\lesssim \varrho\cdot\frac{\log_2\binom{D}{N}}{\log_2\log_2\binom{D}{N}}+\mathcal{O}(n), \tag{1.1}$$

где ϱ — это минимум приведенных весов $\frac{\varrho_i}{r_i-1}$ базиса B, взятый по всем более чем одноместным элементам базиса, $D\geqslant n$ и сложностью частичной функции называется сложность ее самого простого доопределения. Если $D<n$, то индукцией по числу наборов области нетрудно показать, что найдутся D компонент, в которых эти наборы различаются, и, следовательно, любую функцию, определенную на такой области, можно рассматривать как функцию от D переменных.

Из нижней мощностной оценки О. Б. Лупанова [4, 6] следует, что при

$$n\ll\frac{\log_2\binom{D}{N}}{\log_2\log_2\binom{D}{N}} \tag{1.2}$$

для сложности почти каждой из рассматриваемых функций справедливо неравенство

$$L_B(f)\gtrsim \varrho\cdot\frac{\log_2\binom{D}{N}}{\log_2\log_2\binom{D}{N}}. \tag{1.3}$$

Поэтому при выполнении условия (1.2) оценка (1.1) является асимптотически минимальной (в смысле Шеннона). Если (1.2) не выполняется, то (1.1) будет точной по порядку, так как среди рассматриваемых функций (при условии $D\geqslant n$) найдется функция существенно зависящая от всех переменных, сложность которой не меньше $n-1$. Таким образом, оценка (1.1) является асимптотически минимальной при всех значениях параметров D и N, при которых первое слагаемое в ее правой части растет быстрее, чем n, и точной по порядку в остальных случаях.

Доказательство неравенства (1.1) явилось итогом более чем сорокалетней работы многих математиков. Первые результаты, с которых началось доказательство (1.1), были получены О. Б. Лупановым в [4–6]. В этих работах Лупанов разработал метод локального кодирования и установил с его помощью справедливость неравенства (1.1) для полностью определенных булевых функций. Он показал, что

$$L_B(f)\lesssim \varrho\cdot\frac{\log_2\binom{2^n}{N}}{\log_2\log_2\binom{2^n}{N}} \tag{1.4}$$

при всех N, удовлетворяющих неравенству $\min(N,2^n-N)\gg\log_2 n$.

Следующий важный шаг в доказательстве (1.1) был сделан Э. И. Нечипоруком в [9–11], где рассматривалась, в частности, сложность реализации булевых матриц из различных классов вентильными схемами. В этих работах впервые появляется одна из основных идей, позволивших установить справедливость (1.1), — идея построения простого доопределения вычисляемой функции. Такое доопределение строится при помощи универсального множества, содержащего доопределения всех частичных булевых функций определенного вида. Из результатов Нечипорука легко следует частный случай (1.1) — неравенство

$$L_{B_1}(f) \lesssim \frac{D}{\log_2 D}, \quad \log_2 D \sim n \tag{1.5}$$

для схем в стандартном базисе $B_1 = \{\&, \vee, \neg\}$, где под сложностью схемы понимается число ее элементов.

Комбинируя методы Нечипорука и Лупанова, Л. А. Шоломов в [19] оценил сложность реализации систем частичных булевых функций. Следствием основного результата этой работы было впервые явно доказанное неравенство (1.1) для случая $\log_2 N \sim \log_2(D-N) \sim n$. К сожалению, основной результат работы [19] имеет сложную и не совсем «явную» формулировку, поэтому данная работа, как и ее продолжение [21], видимо, были не поняты и не оказали существенного влияния на последующие работы других авторов. Так, например, через десять лет после работы Шоломова Н. Пиппенджер опубликовал работу [28], одним из основных результатов которой было доказательство неравенства (1.1) для стандартного базиса при условии, что D и N по порядку величины равны 2^n. Этот результат, в отличие от более сильного результата Шоломова, был получен без использования метода локального кодирования, что в определенных ситуациях может иметь некоторые преимущества. Правда, следует заметить, что применение локального кодирования для стандартного базиса и условия $\log_2 N \sim \log_2(D-N) \sim n$ совсем не обязательно.

Следующий важный шаг на пути к полному доказательству неравенства (1.1) был сделан Шоломовым в [20], где он разработал технику использования инъективных и «почти инъективных» операторов для вложения области определения частичной функции в булев куб меньшей размерности с целью сведения задачи к рассмотренному ранее случаю $\log_2 N \sim \log_2(D-N) \sim n$. Эта техника позволила ему, не рассматривая зависимость сложности от параметра N, установить справедливость неравенства

$$L_B(f) \lesssim \varrho \cdot \frac{D}{\log_2 D}$$

в случае, когда $D \geqslant n \log_2^{1+\delta} n$, где δ — произвольная положительная постоянная. Л. А. Шоломов рассматривал булевы наборы в качестве двоичных чисел, а в качестве операторов использовал вычисление остатков от деления чисел на подходящие простые числа. Именно этим обстоятельством вызвано ограничение на размер области определения рассматриваемых им частичных функций. В [20] в подстрочном замечании указано, что создание более быстрого метода умножения целых чисел приведет к соответствующему уменьшению границы для размера области определения частичной функции. Следует заметить, что ко времени появления работы [20] в теории кодирования уже было известно, что инъективно отображать булевы области

можно при помощи линейных операторов, сложность реализации которых линейна при отображении областей полиномиального размера. Фактически здесь идет речь о неравенствах Варшамова—Гилберта для исправления ошибок произвольного вида [2]. К сожалению, эти результаты Шоломову были неизвестны и ему не удалось избавиться от ограничения на D. Примерно через 15 лет это смог сделать А. Е. Андреев, предложив использовать для реализации частичных функций линейные операторы. В работе [1] он показал, что

$$L_B(f) \lesssim \varrho \cdot \frac{D}{\log_2 D} + \mathcal{O}(n)$$

при любом D. Андреев существенным образом опирался на работы Нечипорука о вентильных и самокорректирующихся схемах, не применял метод локального кодирования, а его способ использования линейных операторов отличался от способа, которым Шоломов использовал свои операторы. Удивительно, что ни Шоломов, ни Андреев (в восьмидесятые годы) не использовали свои методы для доказательства (1.1) в общем случае. Хотя, как это будет показано ниже, сделать это нетрудно.

В девяностые годы, в связи с интенсивными исследованиями в области вероятностных вычислений, возрос интерес и к изучению частичных функций, которые естественным образом возникают в процессах дерандомизации. Так, в посвященной вопросам дерандомизации работе Андреева с соавторами [23] для базиса B_2, состоящего из всех не более чем двухместных булевых функций, было доказано неравенство

$$L_{B_2}(f) \lesssim \frac{\log_2 \binom{D}{N}}{\log_2 \log_2 \binom{D}{N}} + \mathcal{O}(n), \tag{1.6}$$

где $n^{1+\varepsilon} \leqslant N \leqslant n^{\mathcal{O}(1)}$, ε — положительная постоянная, $D = 2^{\Omega(n)}$. Также там была анонсирована справедливость (1.6) и при всех остальных значениях D и N. Однако в финальной версии [24] этой работы ограничения не только не были сняты, но и появились в формулировке соответствующей теоремы. Заметим, что основным препятствием для доказательства (1.6) при небольших ($N \ll n$) значениях N и больших ($D = 2^{\Omega(n)}$) значениях D является сложность применяемых линейных операторов.

Путь, позволяющий обойти это препятствие, был предложен в [26, 27] П. Б. Милтерсеном. Сначала, применив коды с минимальным расстоянием, пропорциональным длине и линейной относительно длины сложностью кодирования (существование таких кодов было установлено в [25]), Милтерсен в 1998 г. показал [26], что для произвольной области $\boldsymbol{D}$ из $\{0,1\}^n$ существует инъективный на этой области линейный оператор, сложность которого линейна, а ранг асимптотически не превосходит двух логарифмов мощности $\boldsymbol{D}$. Затем в [27] он использовал разработанную технику для вложения области определения вычисляемой функции в булев куб меньшей размерности и таким образом свел вычисление исходной частичной функции к вычислению полностью определенной функции меньшего числа аргументов, для оценки сложности которой уже можно воспользоваться неравенством (1.4). Такой подход расширил диапазон значений параметров N и D, при которых

выполняются (1.1) и (1.6), но его реализация в [27] не позволила избавиться от ограничений на N и D полностью*).

Тем не менее к началу 2000-х гг. общий запас идей и методов их реализации, накопленный в литературе, начиная с первых работ Лупанова и Нечипорука, оказался достаточным для полного доказательства (1.6). Такое доказательство было представлено в [14]. Оно следует логике доказательства из [20], использует результаты из [6, 25] и идею построения хороших линейных инъективных операторов из [26].

В первых пяти разделах настоящей работы дано полное и практически независимое от других источников доказательство неравенство (1.1). Отсутствующие здесь определения и факты можно найти в первой главе [7], девятой главе [15] или любом другом простом введении в область сложности булевых функций. В формулировках некоторых промежуточных утверждений присутствуют ограничения на вес**) N вычисляемых функций. Нетрудно видеть, что везде параметр N можно заменить на $\min(N, D-N)$, где D — размер области определения вычисляемой функции. Поэтому все утверждения с условием $N \leqslant D/2$ справедливы и без этого ограничения.

В последнем разделе работы развитая в первых разделах техника применяется для вычисления недетерминированных функций схемами в произвольном полном конечном базисе. Доказанные оценки обобщают полученные ранее А. Е. Андреевым в [22] аналогичные результаты для схем в базисе B_2.

Далее везде множества и их мощности обозначаются одинаковыми прописными буквами так, что для множеств используется жирный шрифт. Также одинаковыми, но уже строчными буквами, обозначаются функции и их векторы значений, векторы и их компоненты, — в этих случаях жирный шрифт используется для векторов. В частности, $\mathbf{0}$ и $\mathbf{1}$ — векторы, состоящие целиком из нулевых и, соответственно, единичных компонент.

§ 2. Сложность частичных функций

В этом разделе рассматривается сложность вычисления частичных булевых функций схемами в базисе B_2, состоящем из всех не более чем двухместных булевых функций. Сложностью $L(f)$ функции f в этом базисе будем называть сложность самой простой схемы вычисляющей f, где сложность схемы — это число составляющих эту схему функциональных элементов.

2.1. Теорема Шоломова. Доказываемая далее теорема о сложности частичных булевых функций является простым следствием доказанной Л. А. Шоломовым в 1967 году теоремы для схем в произвольном базисе [19]. Основное отличие настоящего доказательства от оригинального заключается в использовании линейных операторов вместо вычисления значений целых чисел по простому модулю. Такая замена позволяет снять присутствующее в [19] небольшое ограничение на D и методом из [19] получить

*) Доказательство основной теоремы в [27] содержит ошибки и не работает, например, при $\log_2 N \asymp \log_2 D$.

**) Число наборов, на которых функция равна единице.

окончательный результат, установленный в [1]. Второе существенное отличие — вычисление функций схемами не в произвольном, а вполне конкретном и просто устроенном базисе B_2, упрощает доказательство и позволяет обойтись без использованного в [19] метода локального кодирования Лупанова.

Т е о р е м а 2.1. *Пусть* $n \to \infty$, $\boldsymbol{D} \subseteq \{0,1\}^n$. *Тогда для каждой частичной булевой функции* f, *определенной на области* $\boldsymbol{D}$,

$$L(f) \lesssim \frac{D}{\log_2 D} + \mathcal{O}(n). \tag{2.1}$$

Теорема 2.1 является частным случаем нескольких доказываемых далее более общих теорем (например, теоремы 5.1 и 7.1) с существенно более сложными доказательствами. Однако структура всех этих доказательств аналогична приводимому далее доказательству теоремы 2.1, которое не содержит сложных технических фрагментов и может служить простым введением в круг рассматриваемых далее задач.

Доказательство теоремы 2.1 проведем в два этапа. На первом этапе установим справедливость неравенства (2.1) для больших областей, логарифм мощности которых асимптотически равен числу переменных. На втором этапе, используя линейные булевы операторы для вложения маленьких областей n-мерного пространства в пространство меньшей размерности m, сведем задачу вычисления произвольной частичной булевой функции к решенной на первом этапе задаче о вычислении частичной булевой функции, определенной на области большой (относительно нового числа переменных m) мощности.

2.2. Доопределения. 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 $\boldsymbol{B} \subseteq \{0,1\}^m$ назовем *доопределением множества* $\boldsymbol{A} \subseteq \{0,1,*\}^m$, если для каждого недоопределенного элемента $\boldsymbol{\alpha}$ из $\boldsymbol{A}$ в $\boldsymbol{B}$ найдется элемент $\boldsymbol{\beta}$, являющийся его доопределением. Следующее утверждение установлено Э. И. Нечипоруком в [10].

Л е м м а 2.1. *Пусть* $\boldsymbol{A}$ — *множество всех наборов из* $\{0,1,*\}^m$, *каждый из которых содержит ровно* k *булевых компонент. Тогда существует доопределение множества* $\boldsymbol{A}$, *состоящее не более чем из* $m2^k$ *наборов.*

Д о к а з а т е л ь с т в о. Составим таблицу T из 2^m строк и $\binom{m}{k}2^k$ столбцов. Каждой строке поставим в соответствие набор из $\{0,1\}^m$, а столбцу — недоопределенный набор из $\boldsymbol{A}$. В этой таблице на пересечении i-й строки, соответствующей набору $\boldsymbol{\beta}_i$ из $\{0,1\}^m$, и j-го столбца, соответствующего набору $\boldsymbol{\alpha}_j$ из $\boldsymbol{A}$, поставим единицу, если $\boldsymbol{\beta}_i$ будет доопределением $\boldsymbol{\alpha}_j$, и нуль в противном случае. Легко видеть, что в такой таблице в каждой строке стоит ровно $\binom{m}{k}$ единиц, а в каждом столбце — 2^{m-k} единиц.

Будем говорить, что i-я строка покрывает j-й столбец, если на их пересечении стоит единица. Для доказательства леммы достаточно показать, что в T найдется набор не более чем из $m2^k$ строк, покрывающих в совокупности все ее столбцы. Такой набор будем формировать последовательно,

произвольно выбрав строку на первом шаге и добавляя в него на каждом следующем шаге строку, покрывающую максимальное число еще не покрытых столбцов.

Положим $A_0 = \binom{m}{k} 2^k$, и пусть A_r — число столбцов, остающихся непокрытыми после r шагов алгоритма. Допустим, что для A_r имеет место неравенство

$$A_r \leqslant A_0(1 - 2^{-k})^r,$$

справедливость которого при $r = 0$ очевидна. На каждом шаге в каждом непокрытом столбце находится ровно 2^{m-k} единиц (все единицы непокрытого столбца находятся в еще невыбранных строках). Поэтому общее число единиц в непокрытых столбцах равно $A_r 2^{m-k}$, и следовательно, найдется строка, в которой число единиц не меньше их среднего числа. Такая строка покрывает не менее

$$\frac{A_r 2^{m-k}}{2^m - r} \geqslant \frac{A_r 2^{m-k}}{2^m} = A_r 2^{-k}$$

столбцов. Выбрав эту строку в качестве $(r+1)$-й строки формируемого набора, видим, что в этом случае

$$A_{r+1} \leqslant A_r - A_r 2^{-k} = A_r(1 - 2^{-k}) \leqslant A_0(1 - 2^{-k})^{r+1}.$$

Пусть $r = (m-1)2^k$. Тогда после r шагов алгоритма в таблице останется меньше, чем

$$\binom{m}{k} 2^k (1 - 2^{-k})^r = \binom{m}{k} 2^k (1 - 2^{-k})^{(m-1)2^k} \leqslant \binom{m}{k} 2^k 2^{-(m-1)} < 2^k$$

непокрытых столбцов, которые, очевидно, можно покрыть не более чем 2^k строками. Следовательно, число строк в покрытии не превосходит суммы $(m-1)2^k + 2^k$. Лемма доказана.

Лемма 2.2. *Пусть* $\boldsymbol{D} \subseteq \{0,1\}^n$. *Если* $\log_2 D \sim n$ *при* $n \to \infty$, *то для любой частичной булевой функции* $f : \boldsymbol{D} \to \{0,1\}$

$$L(f) \lesssim \frac{D}{n}.$$

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 j-му столбцу таблицы двоичный набор $(\sigma_1, \ldots, \sigma_k)$, являющийся двоичным представлением числа $j-1$, а i-й строке — набор $(\sigma_{k+1}, \ldots, \sigma_n)$, являющийся двоичным представлением числа $i-1$. В таблице на пересечении j-го столбца и i-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 $\boldsymbol{\alpha}$, каждый из которых, кроме, быть может, последнего, содержит R булевых компонент.

Множество всех элементарных наборов разобьем на классы, поместив в класс $\boldsymbol{P}_{ij}$ наборы, начинающиеся в i-й и заканчивающиеся в j-й позициях. Очевидно, что число различных классов не превосходит величины $\binom{2^k}{2} < 2^{2k-1}$.

Из леммы 2.1 следует, что для множества элементарных наборов $\boldsymbol{\alpha}$ из класса $\boldsymbol{P}_{i,j}$ существует множество $\boldsymbol{H}_{i,j} = \{\boldsymbol{\beta}\}$ их «доопределений» $\boldsymbol{\beta}$, которое состоит не более чем из $2^k 2^R$ наборов длины 2^k, в каждом из которых первые $i-1$ и последние $2^k - j$ компонент равны нулю. В общем случае для множества всех элементарных наборов существует множество их доопределений $\boldsymbol{H}$, которое состоит не более чем из $2^{3k}2^R$ наборов длины 2^k.

Преобразуем таблицу T_f. Для этого для каждого $j \in \{1, \ldots, 2^{n-k}\}$ заменим в T_f ее j-ю строку, состоящую из последовательных элементарных наборов $\boldsymbol{\alpha}_{j1}\boldsymbol{\alpha}_{j2}\ldots\boldsymbol{\alpha}_{jS_j}$, дизъюнкцией

$$\boldsymbol{\beta}_{j1} \vee \boldsymbol{\beta}_{j2} \vee \cdots \vee \boldsymbol{\beta}_{jS_j} \tag{2.2}$$

их доопределений из $\boldsymbol{H}$. Нетрудно видеть, что преобразованная таблица будет таблицей значений некоторой n-местной булевой функции h, являющейся доопределением функции f.

Пусть $|\boldsymbol{\sigma}| = \sum\limits_{i=1}^{k} \sigma_i 2^{i-1}$ и $\boldsymbol{\gamma} = (\gamma_1, \ldots, \gamma_{2^k}) \in \boldsymbol{H}$. Введем множество $\boldsymbol{G}$, состоящее из всех функций

$$g_{\boldsymbol{\gamma}}(x_1, \ldots, x_k) = \bigvee_{\boldsymbol{\sigma}=(\sigma_1,\ldots,\sigma_k)} x_1^{\sigma_1} \cdot \ldots \cdot x_k^{\sigma_k} \cdot \boldsymbol{\gamma}_{|\sigma|+1},$$

векторы значений которых, как нетрудно видеть, являются элементами множества $\boldsymbol{H}$. Поэтому $G = H \leqslant 2^{3k}2^R$ и функция h может быть выражена через функции системы $\boldsymbol{G}$ следующим образом:

$$\begin{aligned} h(x_1, \ldots, x_n) &= \bigvee_{\sigma_{k+1},\ldots,\sigma_n} h(x_1, \ldots, x_k, \sigma_{k+1}, \ldots, \sigma_n) \cdot x_{k+1}^{\sigma_{k+1}} \cdot \ldots \cdot x_n^{\sigma_n} = \\ &= \bigvee_{\boldsymbol{\sigma}=(\sigma_{k+1},\ldots,\sigma_n)} \Big(\bigvee_{g \in G} g(x_1, \ldots, x_k) \Big) x_{k+1}^{\sigma_{k+1}} \cdot \ldots \cdot x_n^{\sigma_n}, \end{aligned} \tag{2.3}$$

где внутренняя дизъюнкция выполняется по всем g, соответствующим наборам $\boldsymbol{\beta}$ из (2.2) при $j = |\boldsymbol{\sigma}| + 1$.

Оценим число функций g, входящих в правую часть формулы (2.3). Прежде всего заметим, что число функций, соответствующих наборам $\boldsymbol{\alpha}$, содержащим менее R булевых компонент, не превосходит числа строк таблицы, т. е. не больше чем 2^{n-k}. Число остальных функций, очевидно, не превосходит D/R. Поэтому общее число элементарных наборов в T_f, а следовательно, и функций g в (2.3) не превосходит

$$D \Big/ R + 2^{n-k}. \tag{2.4}$$

Теперь построим схему S, вычисляющую функцию h и удовлетворяющую требованиям леммы. Эта схема состоит из трех подсхем S_1–S_3, и ее конструкция основана на формуле (2.3). Подсхема S_1 вычисляет все элементарные конъюнкции первых k переменных и, используя эти конъюнкции, все функции из $\boldsymbol{G}$. Учитывая, что $G \leqslant 2^{3k}2^R$ и каждая функция из $\boldsymbol{G}$ является дизъюнкцией не более чем $m < 2^k$ элементарных конъюнкций, имеем неравенство

$$L(\mathsf{S}_1) \leqslant 2^{5k}2^R. \tag{2.5}$$

Подсхема S_2 вычисляет все элементарные конъюнкции последних $n-k$ переменных. Поэтому

$$L(\mathsf{S}_2) \lesssim 2^{n-k}. \tag{2.6}$$

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 (2.3). Из (2.4) следует, что

$$L(\mathsf{S}_3) \leqslant 2^{n-k+1} + D\Big/R. \tag{2.7}$$

Суммируя неравенства (2.5)–(2.7), видим, что

$$L(\mathsf{S}) \lesssim D\Big/R + 2^{5k}2^R + 2^{n-k+2}. \tag{2.8}$$

Положим

$$k = \lceil n - \log_2 D + 2\log_2 n \rceil, \qquad R = \lfloor \log_2 D - 5k - 2\log_2 n \rfloor. \tag{2.9}$$

Так как $\log_2 D \sim n$, то $k = o(n)$ и $R \sim n > 0$, т. е. параметры k и R выбраны корректно. Тогда, подставляя равенства (2.9) в (2.8) и учитывая условие $\log_2 D \sim n$, приходим к неравенству

$$L(\mathsf{S}) \lesssim \frac{D}{n}.$$

Лемма доказана.

2.3. Линейные операторы. Будем говорить, что линейный булев оператор $\mathscr{L}\colon \{0,1\}^n \to \{0,1\}^m$ разделяет непересекающиеся множества $\boldsymbol{A}$ и $\boldsymbol{B}$ из $\{0,1\}^n$, если не пересекаются их образы $\mathscr{L}(\boldsymbol{A})$ и $\mathscr{L}(\boldsymbol{B})$ в $\{0,1\}^m$. Также скажем, что оператор $\mathscr{L}$ «почти разделяет» $\boldsymbol{A}$ и $\boldsymbol{B}$ при $A, B \to \infty$, если

$$\big|\mathscr{L}^{-1}(\mathscr{L}(\boldsymbol{A}) \cap \mathscr{L}(\boldsymbol{B}))\big| \ll |\boldsymbol{A} \cup \boldsymbol{B}|.$$

Докажем несколько утверждений о разделяющих и почти разделяющих произвольные непересекающиеся множества линейных булевых операторах, в которых оценивается качество «разделимости» множеств в зависимости от ранга оператора.

Лемма 2.3. *Для любых неравных наборов $\boldsymbol{x}$ и $\boldsymbol{y}$ из $\{0,1\}^n$ существует ровно 2^{nm-m} линейных операторов $\mathscr{L}\colon \{0,1\}^n \to \{0,1\}^m$, значения которых на $\boldsymbol{x}$ и $\boldsymbol{y}$ совпадают.*

Доказательство. Если $\mathscr{L}(\boldsymbol{x}) = \mathscr{L}(\boldsymbol{y})$, то $\mathscr{L}(\boldsymbol{x} \oplus \boldsymbol{y}) = 0$. Поэтому для доказательства леммы достаточно показать, что ненулевой набор $\boldsymbol{z} = \boldsymbol{x} \oplus \boldsymbol{y}$ лежит в ядре ровно 2^{nm-m} линейных операторов действующих из $\{0,1\}^n$ в $\{0,1\}^m$. Сделаем это для матриц рассматриваемых операторов.

Пусть $\boldsymbol{M}(n,m)$ — множество всех булевых матриц из m строк и n столбцов, $\boldsymbol{z} = (z_1, \ldots, z_n)$ — ненулевой вектор длины n. Без ограничения общности будем полагать, что $z_n = 1$. Нетрудно видеть, что $\boldsymbol{z}$ принадлежит нулевому пространству матрицы $\boldsymbol{M} = (m_{i,j})$ из $\boldsymbol{M}(n,m)$ тогда и только тогда, когда

$$m_{i,1}z_1 \oplus m_{i,2}z_2 \oplus \cdots \oplus m_{i,n-1}z_{n-1} = m_{i,n} \tag{2.10}$$

для каждого $i \in \{1, \ldots, m\}$. В равенстве (2.10) коэффициент $m_{i,n}$ однознач-

но определяется первыми $n-1$ коэффициентами $m_{i,j}$, которые можно выбрать 2^{n-1} различными способами.Поэтому ненулевой вектор $\boldsymbol{z}$ принадлежит нулевым пространствам ровно 2^{nm-m} различных матриц из $\boldsymbol{M}(n,m)$. Лемма доказана.

Л е м м а 2.4. *Пусть* $\boldsymbol{A},\boldsymbol{B}\subseteq\{0,1\}^n$, $\boldsymbol{A}\cap\boldsymbol{B}=\varnothing$, m — *целое. Тогда существует линейный оператор* $\mathscr{L}\colon\{0,1\}^n\to\{0,1\}^m$ *такой, что*

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

Д о к а з а т е л ь с т в о. Обозначим через $\boldsymbol{F}(n,m)$ множество всех линейных операторов $\mathscr{L}\colon\{0,1\}^n\to\{0,1\}^m$. Очевидно, что $F(n,m)=2^{nm}$. В силу предыдущей леммы для любых двух различных наборов $\boldsymbol{x}$ и $\boldsymbol{y}$ из $\{0,1\}^n$ имеется 2^{nm-m} различных операторов $\mathscr{L}$ таких, что $\mathscr{L}(\boldsymbol{x})=\mathscr{L}(\boldsymbol{y})$. Следовательно, величина

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

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

Л е м м а 2.5. *Пусть* $\boldsymbol{A},\boldsymbol{B}\subseteq\{0,1\}^n$, $\boldsymbol{A}\cap\boldsymbol{B}=\varnothing$, $m=\lceil\log_2 B+k\rceil$, *где* $k\geqslant 0$. *Тогда существует линейный оператор* $\mathscr{L}\colon\{0,1\}^n\to\{0,1\}^m$ *такой, что*

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

Д о к а з а т е л ь с т в о. Из леммы 2.4 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 $2^{-m}AB$ парах $(\boldsymbol{x},\boldsymbol{y})$, где $\boldsymbol{x}\in\boldsymbol{A}$, $\boldsymbol{y}\in\boldsymbol{B}$. Так как $2^m\geqslant 2^kB$, то $2^{-m}AB\leqslant 2^{-k}A$. Лемма доказана.

Л е м м а 2.6. *Пусть* $\boldsymbol{A}\subseteq\{0,1\}^n$, $m=\lfloor 2\log_2 A\rfloor$. *Тогда существует линейный оператор* $\mathscr{L}\colon\{0,1\}^n\to\{0,1\}^m$ *такой, что* $\mathscr{L}(\boldsymbol{x})\neq\mathscr{L}(\boldsymbol{y})$ *для любых* $\boldsymbol{x}\neq\boldsymbol{y}\in\boldsymbol{A}$.

Д о к а з а т е л ь с т в о. Из леммы 2.3 следует, что для любых двух различных наборов $\boldsymbol{x}$ и $\boldsymbol{y}$ из $\boldsymbol{A}$ в $\boldsymbol{F}(n,m)$ есть ровно 2^{nm-m} различных операторов $\mathscr{L}$ таких, что $\mathscr{L}(\boldsymbol{x})=\mathscr{L}(\boldsymbol{y})$. Следовательно, величина

$$2^{-nm}\sum_{\boldsymbol{x},\boldsymbol{y}\in\boldsymbol{A},\boldsymbol{x}\neq\boldsymbol{y}}2^{nm-m}=2^{-m-1}A(A-1)$$

является средним значением для числа таких пар $(\boldsymbol{x},\boldsymbol{y})$, на которых значения оператора из $\boldsymbol{F}(n,m)$ одинаковы. Поэтому в $\boldsymbol{F}(n,m)$ найдется оператор $\mathscr{L}$, для которого равенство $\mathscr{L}(\boldsymbol{x})=\mathscr{L}(\boldsymbol{y})$ выполняется менее чем на $2^{-m-1}A^2$ парах наборов. Так как

$$m+1=\lfloor 2\log_2 A\rfloor+1>2\log_2 A,$$

то целое число пар таких наборов строго меньше единицы. Лемма доказана.

Следующее утверждение о сложности линейных булевых операторов является простым следствием результатов О. Б. Лупанова [3] и Э. И. Нечипорука [9] о сложности реализации булевых матриц вентильными схемами. Приведем его без доказательства.

Лемма 2.7. *Пусть $n \to \infty$ и $m < n$. Тогда для любого линейного булева оператора $\mathscr{L}\colon \{0,1\}^n \to \{0,1\}^m$*

$$L(\mathscr{L}) = \mathcal{O}\left(n + \frac{nm}{\log_2 n}\right). \tag{2.11}$$

При $m \geqslant \log_2 n$ из (2.11) легко следует неравенство

$$L(\mathscr{L}) = \mathcal{O}\left(\frac{nm}{\log_2 n}\right). \tag{2.12}$$

Далее в оценках сложности линейных операторов, следующих из неравенств (2.11) и (2.12), как правило, не будем указывать ссылки на эти неравенства.

2.4. Доказательство теоремы 2.1. Воспользуемся доказанными выше леммами о линейных операторах, разделяющих множества нулей и единиц вычисляемой частичной булевой функции f, для вложения ее небольшой области определения $\boldsymbol{D}$ в пространство, размерность которого будет асимптотически равна логарифму мощности области. Затем на образе $\boldsymbol{D}$ определим удовлетворяющую условиям леммы 2.2 частичную функцию g и покажем, как использовать эту функцию для вычисления f.

Лемма 2.8. *Пусть $n \to \infty$, $\boldsymbol{D} \subseteq \{0,1\}^n$, $\frac{1}{3}n \leqslant \log_2 D \leqslant n - 4\log_2 n$, функция f определена на $\boldsymbol{D}$. Тогда*

$$L(f) \lesssim \frac{D}{\log_2 D}.$$

Доказательство. Положим $k = 3\log_2 n$, $\boldsymbol{D}_0 = \{\boldsymbol{x} \in \boldsymbol{D} \mid f(\boldsymbol{x}) = 0\}$, $\boldsymbol{D}_1 = \{\boldsymbol{x} \in \boldsymbol{D} \mid f(\boldsymbol{x}) = 1\}$. Без ограничения общности будем полагать, что $D_0 \geqslant D_1$. К областям $\boldsymbol{D}_0$ и $\boldsymbol{D}_1$ применим лемму 2.5, полагая, что $\boldsymbol{A} = \boldsymbol{D}_1$ и $\boldsymbol{B} = \boldsymbol{D}_0$. В результате для $m = \lceil \log_2 D_0 + 3\log_2 n \rceil$ найдется такой линейный оператор $\mathscr{L}\colon \{0,1\}^n \to \{0,1\}^m$, что множество

$$\boldsymbol{C} = \{(\boldsymbol{x}, \boldsymbol{y}) \mid \boldsymbol{x} \in \boldsymbol{D}_0, \boldsymbol{y} \in \boldsymbol{D}_1, \mathscr{L}(\boldsymbol{x}) = \mathscr{L}(\boldsymbol{y})\}$$

состоит не более чем из D/n^3 пар наборов. Пусть $\boldsymbol{C}_0$ и $\boldsymbol{C}_1$ — множества наборов, входящих в эти пары и принадлежащих, соответственно, $\boldsymbol{D}_0$ и $\boldsymbol{D}_1$. Очевидно, что каждое из этих множеств состоит не более чем из D/n^3 наборов.

Далее введем определенную на области $\mathscr{L}(\boldsymbol{D})$ частичную m-местную булеву функцию

$$g(\boldsymbol{y}) = \begin{cases} 0, & \text{если } \exists\, \boldsymbol{x} \in \boldsymbol{D}_0 \text{ такой, что } \boldsymbol{y} = \mathscr{L}(\boldsymbol{x}), \\ 1 & \text{в противном случае} \end{cases}$$

и определенную на области $\boldsymbol{D}$ частичную n-местную булеву функцию $h(\boldsymbol{x}) = f(\boldsymbol{x}) \oplus g(\mathscr{L}(\boldsymbol{x}))$. Функция $h(\boldsymbol{x})$ равна единице только на наборах

из $\boldsymbol{C}_1$, и таких наборов не больше чем D/n^3. Так как $f(\boldsymbol{x}) = h(\boldsymbol{x}) \oplus g(\mathscr{L}(\boldsymbol{x}))$, то

$$L(f) \leqslant L(g) + L(h) + L(\mathscr{L}) + 1. \tag{2.13}$$

Без ограничения общности можно считать, что*) $\log_2 D \sim m$, и поэтому для оценки сложности функции g можно воспользоваться леммой 2.2. Из этой леммы следует, что

$$L(g) \lesssim \frac{D}{\log_2 D}.$$

Для вычисления функции h воспользуемся ее совершенной дизъюнктивной нормальной формой, полагая, что вне области $\boldsymbol{D}$ эта функция равна нулю. Так как h равна единице на не более чем D/n^3 наборах, то

$$L(h) \leqslant \frac{Dn}{n^3} = o\left(\frac{D}{\log_2 D}\right).$$

Очевидно, что сложность оператора $\mathscr{L}$ не превосходит n^2. Поэтому из условий леммы следует, что $L(\mathscr{L}) = o\left(\dfrac{D}{\log_2 D}\right)$. Подставляя полученные оценки $L(g), L(h)$ и $L(\mathscr{L})$ в (2.13), получаем требуемую оценку сложности f. Лемма доказана.

Л е м м а 2.9. *Пусть* $n \to \infty$, $\boldsymbol{D} \subseteq \{0,1\}^n$, $\log_2 D \leqslant \frac{1}{3}n$, *функция* f *определена на* $\boldsymbol{D}$. *Тогда*

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

Д о к а з а т е л ь с т в о. Положим $m = \lfloor 2\log_2 D \rfloor$. К области $\boldsymbol{D}$ применим лемму 2.6. В результате найдется инъективный на $\boldsymbol{D}$ линейный оператор $\mathscr{L}\colon \{0,1\}^n \to \{0,1\}^m$. Далее определим на области $\mathscr{L}(\boldsymbol{D})$ частичную m-местную булеву функцию

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

Нетрудно видеть, что $f(\boldsymbol{x}) = g(\mathscr{L}(\boldsymbol{x}))$, поэтому $L(f) \leqslant L(g) + L(\mathscr{L})$. Так как

$$\log_2 D \geqslant \tfrac{1}{3}\lfloor 2\log_2 D \rfloor = \tfrac{1}{3}m,$$

то для вычисления функции g можно воспользоваться леммой 2.8. В силу этой леммы

$$L(g) \lesssim \frac{D}{\log_2 D}.$$

Наконец, заметим, что для сложности линейного оператора $\mathscr{L}$ справедливо неравенство

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

*) Если образ $\mathscr{L}(\boldsymbol{D})$ не удовлетворяет этому равенству, то его можно расширить произвольным образом до нужного размера.

Следовательно,

$$L(f) \lesssim \frac{D}{\log_2 D} + \mathcal{O}\left(\frac{n \log_2 D}{\log_2 n}\right). \tag{2.14}$$

Если $D > n^3$, то при $n \to \infty$

$$\frac{D}{\log_2 D} \gg \frac{n \log_2 D}{\log_2 n},$$

а если $D \leqslant n^3$, то

$$\frac{n \log_2 D}{\log_2 n} = \mathcal{O}(n).$$

Таким образом, при $n \to \infty$ для любого D сумма в правой части (2.14) асимптотически не превосходит $\frac{D}{\log_2 D} + \mathcal{O}(n)$. Лемма доказана.

Доказательство теоремы 2.1 легко получается из лемм 2.5, 2.8 и 2.9. Если $\log_2 D \geqslant n - 5\log_2 n$, то $\log_2 D \sim n$ и утверждение теоремы следует из леммы 2.5. Если $\frac{1}{3} \leqslant \log_2 D \leqslant n - 4\log_2 n$, то утверждение теоремы следует из леммы 2.8. Если $\log_2 D \leqslant \frac{1}{3}n$, то утверждение теоремы следует из леммы 2.9. Теорема доказана.

§ 3. Функции ограниченного веса

В этом разделе рассматривается сложность вычисления полностью определенных булевых функций ограниченного веса схемами в базисе B_2. Полученные здесь результаты являются частными случаями классической теоремы О. Б. Лупанова о сложности булевых функций с данным числом единиц [4, 6], носят предварительный характер и будут усилены в следующих разделах.

3.1. Простой вариант теоремы Лупанова. Как было сказано во введении, для схем в произвольном полном конечном базисе задача о сложности вычисления полностью определенных булевых функций ограниченного веса была решена О. Б. Лупановым в [4, 6] при помощи метода локального кодирования. Ниже частный случай этого результата доказывается при сильном ограничении на вес вычисляемых функций, — логарифм веса должен расти быстрее логарифма числа переменных. Тем не менее приводимое далее доказательство интересно тем, что позволяет познакомиться с некоторыми деталями доказательства неравенства (1.1), не отягощенными тяжелыми техническими элементами. Оно достаточно близко к доказательству теоремы 2.1, обходится простыми «элементарными» средствами, не используя метод локального кодирования, и развитая в нем техника позволяет получать значительные результаты в других вычислительных моделях [12, 17, 18].

Теорема 3.1. *Пусть $n \to \infty$. Если n-местная булева функция f равна единице на N наборах, $N \leqslant 2^{n-1}$ и $\log_2 N \gg \log_2 n$, то*

$$L(f) \lesssim \frac{\log_2 \binom{2^n}{N}}{\log_2 \log_2 \binom{2^n}{N}}.$$

Справедливость теоремы 3.1 легко следует из доказываемых далее лемм 3.1 и 3.3. Доказательство леммы 3.1 практически полностью повторяет доказательство леммы 2.2 из доказательства теоремы 2.1. Доказательство леммы 3.3 достаточно близко к доказательству лемм 2.8 и 2.9 и также использует линейные операторы, позволяющие свести вычисление исходной функции к вычислению функций с меньшим числом аргументов, для вычисления которых можно воспользоваться доказанной ранее леммой 3.1 и ее простым следствием — леммой 3.2.

3.2. Почти равновесные функции. Полностью определенную булеву функцию $f:\{0,1\}^n\to\{0,1\}$ назовем почти равновесной булевой функцией, если она равна единице на N наборах из $\{0,1\}^n$ и $\log_2 N\sim n$.

Лемма 3.1. *Пусть $n\to\infty$. Если n-местная булева функция f равна единице на N наборах, $N\leqslant 2^{n-1}$ и $\log_2 N\sim n$, то*

$$L(f)\lesssim\frac{\log_2\binom{2^n}{N}}{\log_2\log_2\binom{2^n}{N}}.$$

Доказательство. Введем параметры k и R, значения которых определим позднее. Значения n-местной булевой функции f запишем в таблице T_f из 2^k столбцов и 2^{n-k} строк, поставив в соответствие j-му столбцу таблицы двоичный набор $(\sigma_1,\ldots,\sigma_k)$, являющийся двоичным представлением числа $j-1$, а i-й строке — набор $(\sigma_{k+1},\ldots,\sigma_n)$, являющийся двоичным представлением числа $i-1$. В таблице на пересечении j-го столбца и i-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 $\boldsymbol{\alpha}_i$ длины s_i с t_i единицами, для каждого из которых, кроме, быть может, последнего,

$$\log_2\binom{s_i}{t_i}\geqslant R,\qquad \log_2\binom{s_i-1}{t_i}<R,\qquad \log_2\binom{s_i-1}{t_i-1}<R. \tag{3.1}$$

Так как $t\leqslant s\leqslant 2^k$ и

$$\binom{s}{t}=\binom{s-1}{t}\cdot\frac{s}{s-t}\leqslant 2^R2^k,\qquad \binom{s}{t}=\binom{s-1}{t-1}\cdot\frac{s}{t}\leqslant 2^R2^k,$$

то для числа элементарных наборов, удовлетворяющих неравенствам (3.1), справедлива оценка

$$\sum_{s,t}\binom{s}{t}\leqslant 2^k\binom{s}{t}\leqslant 2^R2^{2k}.$$

Набор $\boldsymbol{\alpha}$, расположенный в строке таблицы между ее i-й и j-й позициями, превратим в набор $\boldsymbol{\gamma}$ длины 2^k, дополнив его $i-1$ нулем слева и 2^k-j нулями справа. Пусть $\boldsymbol{H}=\{\boldsymbol{\gamma}\}$ — множество всех таких наборов. Место набора $\boldsymbol{\alpha}$ в строке можно выбрать не более чем 2^k способами, поэтому нетрудно видеть, что

$$H\leqslant 2^R2^{2k}2^k=2^R2^{3k}.$$

Наконец, заметим, что если i-я строка таблицы T_f состоит из последовательных наборов $\boldsymbol{\alpha}_{i,1},\ldots,\boldsymbol{\alpha}_{i,r_i}$, то эта же строка является покомпонентной дизъюнкцией $\boldsymbol{\gamma}_{i,1}\vee\ldots\vee\boldsymbol{\gamma}_{i,r_i}$ соответствующих наборов $\boldsymbol{\gamma}$ из множества $\boldsymbol{H}$.

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

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

векторы значений которых, как нетрудно видеть, являются элементами множества $\boldsymbol{H}$. Очевидно, что функция f может быть выражена через функции системы $\boldsymbol{G}$ следующим образом:

$$f(x_1,\ldots,x_n)=\bigvee_{\boldsymbol{\sigma}=(\sigma_{k+1},\ldots,\sigma_n)}\left(\bigvee_{j=1}^{r_{|\boldsymbol{\sigma}|}} g_{|\boldsymbol{\sigma}|,j}(x_1,\ldots,x_k)\right)\cdot x_{k+1}^{\sigma_{k+1}}\cdot\ldots\cdot x_n^{\sigma_n}. \tag{3.2}$$

Оценим число функций $g_{|\boldsymbol{\sigma}|,j}$ в (3.2). Прежде всего заметим, что число функций, соответствующих наборам длины s с t единицами, у которых $\log_2\binom{s}{t}<R$, 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 — длина и число единичных компонент в i-м элементарном наборе. Так как $\sum\limits_{i=1}^{p} s_i\leqslant 2^n$, $\sum\limits_{i=1}^{p} t_i\leqslant N$ и по условию леммы $N\leqslant 2^{n-1}$, то

$$\log_2\binom{2^n}{N}\geqslant\log_2\binom{\sum s_i}{\sum t_i}\geqslant\log_2\prod_{i=1}^{p}\binom{s_i}{t_i}=\sum_{i=1}^{p}\log_2\binom{s_i}{t_i}\geqslant p\cdot R.$$

Таким образом, общее число элементарных наборов в T_f, а следовательно, и функций g в (3.2) не превосходит

$$\log_2\binom{2^n}{N}\Big/R+2^{n-k}. \tag{3.3}$$

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 (3.2).

1. Подсхема S_1 вычисляет все элементарные конъюнкции первых k переменных и, используя эти конъюнкции, все функции из $\boldsymbol{G}$. Учитывая, что $G\leqslant 2^{3k}2^R$ и каждая функция из $\boldsymbol{G}$ является дизъюнкцией не более чем 2^k элементарных конъюнкций, имеем

$$L(\mathsf{S}_1)\leqslant 2^{4k}2^R. \tag{3.4}$$

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

$$L(\mathsf{S}_2)\leqslant 2^{n-k+1}. \tag{3.5}$$

3. Подсхема S_3 подключена к выходам подсхем S_1 и S_2 и вычисляет функцию $f(x_1,\ldots,x_n)$ в соответствии с равенством (3.2). Из (3.3) следует, что

$$L(S_3)\leqslant 2^{n-k+1}+\log_2\binom{2^n}{N}\Big/R. \tag{3.6}$$

Суммируя неравенства (3.4)–(3.6), видим, что

$$L(\mathsf{S})\leqslant\log_2\binom{2^n}{N}\Big/R+2^{4k}2^R+2^{n-k+2}. \tag{3.7}$$

Определим значения параметров k и R. Сделаем это так, чтобы первое слагаемое в (3.7) асимптотически совпадало с нижней мощностной оценкой

$$L(f) \gtrsim \frac{\log_2 \binom{2^n}{N}}{\log_2 \log_2 \binom{2^n}{N}},$$

а второе и третье росли медленнее правой части этой оценки. Для этого положим

$$k = \left\lceil n - \log_2 \log_2 \binom{2^n}{N} + 2 \log_2 \log_2 \log_2 \binom{2^n}{N} \right\rceil,$$
$$R = \left\lfloor \log_2 \log_2 \binom{2^n}{N} - 4k - 2 \log_2 \log_2 \log_2 \binom{2^n}{N} \right\rfloor.$$

При таких k и R условия для второго и третьего слагаемых в (3.7), очевидно, выполняются, так как

$$\begin{aligned} R + 4k &\leqslant \log_2 \log_2 \binom{2^n}{N} - 2 \log_2 \log_2 \log_2 \binom{2^n}{N}, \\ n - k &\leqslant \log_2 \log_2 \binom{2^n}{N} - 2 \log_2 \log_2 \log_2 \binom{2^n}{N}. \end{aligned} \tag{3.8}$$

Далее из оценок

$$\left(\frac{2^n}{N}\right)^N \leqslant \binom{2^n}{N} \leqslant \left(\frac{3 \cdot 2^n}{N}\right)^N$$

биномиального коэффициента получаем оценки его повторного логарифма

$$\log_2 N + \log_2 \log_2 \frac{2^n}{N} \leqslant \log_2 \log_2 \binom{2^n}{N} \leqslant \log_2 N + \log_2 \log_2 \frac{3 \cdot 2^n}{N},$$

где верхняя и нижняя оценки отличаются не более чем постоянным слагаемым

$$\log_2 \log_2 \frac{3 \cdot 2^n}{N} - \log_2 \log_2 \frac{2^n}{N} = \log_2 \left(1 + \frac{\log_2 3}{\log_2 \frac{2^n}{N}}\right) < 2.$$

Поэтому

$$\log_2 \log_2 \binom{2^n}{N} \sim \log_2 N \sim n$$

и, следовательно,

$$k \ll \log_2 \log_2 \binom{2^n}{N}, \qquad R \sim \log_2 \log_2 \binom{2^n}{N}. \tag{3.9}$$

Подставляя оценки из (3.8) и (3.9) в (3.7), после несложных преобразований получаем требуемую верхнюю асимптотическую оценку сложности схемы S:

$$L(\mathsf{S}) \lesssim \frac{\log_2 \binom{2^n}{N}}{\log_2 \log_2 \binom{2^n}{N}}.$$

Лемма доказана.

Из доказательства леммы 3.1 легко следует ее простое обобщение, которое приведем без доказательства.

Л е м м а 3.2. *Пусть $n\to\infty$. Если n-местная булева функция f равна единице не более чем на N наборах, $N\leqslant 2^{n-1}$ и $\log_2 N\sim n$, то*

$$L(f)\lesssim \frac{\log_2\binom{2^n}{N}}{\log_2\log_2\binom{2^n}{N}}.$$

3.3. Функции с небольшим весом. В следующей лемме ослабим условие $\log_2 N\sim n$ на число единичных значений.

Л е м м а 3.3. *Пусть $n\to\infty$. Если n-местная булева функция f равна единице на N наборах и $n\log_2 n\leqslant N\ll 2^n$, то*

$$L(f)\lesssim \frac{N}{\log_2 N}\cdot\log_2\frac{2^n}{N}.$$

Д о к а з а т е л ь с т в о. Пусть $\boldsymbol{A}=\{\boldsymbol{x}\mid f(\boldsymbol{x})=0\}$, $\boldsymbol{B}=\{\boldsymbol{x}\mid f(\boldsymbol{x})=1\}$, $k=\log_2\log_2\frac{2^n}{N}$. К областям $\boldsymbol{A}$ и $\boldsymbol{B}$ применим лемму 2.5. В силу этой леммы для $m=\lceil\log_2 N+\log_2\log_2\log_2\frac{2^n}{N}\rceil$ найдется такой линейный оператор $\mathscr{L}_1\colon\{0,1\}^n\to\{0,1\}^m$, что

$$L(\mathscr{L}_1)=\mathcal{O}\left(\frac{n\log_2 N}{\log_2 n}\right),$$

и при этом множество

$$\boldsymbol{C}_1=\{(\boldsymbol{x},\boldsymbol{y})\mid\boldsymbol{x}\in\boldsymbol{A},\boldsymbol{y}\in\boldsymbol{B},\mathscr{L}_1(\boldsymbol{x})=\mathscr{L}_1(\boldsymbol{y})\}$$

состоит не более чем из $A\Big/\log_2\log_2\frac{2^n}{N}$ пар наборов. Множество $\boldsymbol{A}$ разобьем на подмножества $\boldsymbol{A}_0$ и $\boldsymbol{A}_1$ так, что $\boldsymbol{A}_0$ состоит из всех тех наборов $\boldsymbol{x}$, которые не образуют пары из $\boldsymbol{C}_1$, $\boldsymbol{A}_1$ содержит все остальные наборы. Очевидно, что $A_1\leqslant A\Big/\log_2\log_2\frac{2^n}{N}$. На множестве $\boldsymbol{B}\cup\boldsymbol{A}_1$ определим функцию f_1, а на множестве $\{0,1\}^m$ функцию h_1 так, что

$$f_1(\boldsymbol{x})=\begin{cases}0, & \text{если } \boldsymbol{x}\in\boldsymbol{A}_1;\\ 1, & \text{если } \boldsymbol{x}\in\boldsymbol{B};\end{cases}\qquad h_1(\boldsymbol{y})=\begin{cases}0, & \text{если } \boldsymbol{y}\notin\mathscr{L}_1(\boldsymbol{B});\\ 1, & \text{если } \boldsymbol{y}\in\mathscr{L}_1(\boldsymbol{B}).\end{cases}$$

Определенные так функции f_1 и h_1 связаны с f равенством

$$f(\boldsymbol{x})=f_1(\boldsymbol{x})\cdot h_1(\mathscr{L}_1(\boldsymbol{x})),$$

причем m-местная функция h_1 равна единице не более чем на N наборах. Так как при $m=\left\lceil\log_2 N+\log_2\log_2\log_2\frac{2^n}{N}\right\rceil$

$$\log_2\log_2\log_2\frac{2^n}{N}\leqslant\log_2\log_2 n\ll\log_2 N\sim m,$$

то можно воспользоваться леммой 3.2. В этом случае из неравенств

$$\log_2 \binom{2^m}{N} \leqslant \log_2 \left(\frac{3 \cdot 2N \log_2 \log_2 \frac{2^n}{N}}{N} \right)^N \lesssim N \log_2 \log_2 \log_2 \frac{2^n}{N}$$

и утверждения леммы 3.2 легко следует, что

$$L(h_1) \lesssim \frac{\log_2 \binom{2^m}{N}}{\log_2 \log_2 \binom{2^m}{N}} \lesssim$$

$$\lesssim \frac{N \log_2 \log_2 \log_2 \frac{2^n}{N}}{\log_2 N + \log_2 \log_2 \log_2 \log_2 \frac{2^n}{N}} \sim \frac{N \log_2 \log_2 \log_2 \frac{2^n}{N}}{\log_2 N}.$$

Повторим все выполненные ранее действия с функцией f_1 и множествами $\boldsymbol{A}_1$ и $\boldsymbol{B}$. В результате получим новое множество $\boldsymbol{A}_2 \subseteq \boldsymbol{A}_1$, $A_2 \leqslant A_1 \Big/ \log_2 \log_2 \frac{2^n}{N}$, линейный оператор $\mathscr{L}_2 \colon \{0,1\}^n \to \{0,1\}^m$ и функции

$$f_2(\boldsymbol{x}) = \begin{cases} 0, & \text{если } \boldsymbol{x} \in \boldsymbol{A}_2; \\ 1, & \text{если } \boldsymbol{x} \in \boldsymbol{B}; \end{cases} \qquad h_2(\boldsymbol{y}) = \begin{cases} 0, & \text{если } \boldsymbol{y} \notin \mathscr{L}_2(\boldsymbol{B}); \\ 1, & \text{если } \boldsymbol{y} \in \mathscr{L}_2(\boldsymbol{B}), \end{cases}$$

для которых справедливы равенства

$$f_1(\boldsymbol{x}) = f_2(\boldsymbol{x}) \cdot h_2(\mathscr{L}_2(\boldsymbol{x})), \quad f(\boldsymbol{x}) = f_2(\boldsymbol{x}) \cdot h_2(\mathscr{L}_2(\boldsymbol{x})) \cdot h_1(\mathscr{L}_1(\boldsymbol{x}))$$

и оценки

$$L(\mathscr{L}_2) = \mathscr{O}\left(\frac{n \log_2 N}{\log_2 n} \right), \quad L(h_2) \lesssim \frac{N \log_2 \log_2 \log_2 \frac{2^n}{N}}{\log_2 N}.$$

Выполним указанные действия в общей сложности t раз. В результате получим последовательность из t вложенных множеств

$$\boldsymbol{A}_t \subseteq \boldsymbol{A}_{t-1} \subseteq \ldots \subseteq \boldsymbol{A}_1, \quad \text{где} \quad A_i \leqslant 2^n \Big/ \Big(\log_2 \log_2 \frac{2^n}{N} \Big)^i,$$

последовательность из t линейных операторов $\mathscr{L}_i \colon \{0,1\}^n \to \{0,1\}^m$, последовательность из t частичных функций $f_i \colon \boldsymbol{B} \cup \boldsymbol{A}_i \to \{0,1\}$ и последовательность из t функций $h_i \colon \{0,1\}^m \to \{0,1\}$, удовлетворяющих неравенствам

$$L(\mathscr{L}_i) = \mathscr{O}\left(\frac{n \log_2 N}{\log_2 n} \right), \quad L(h_i) \lesssim \frac{N \log_2 \log_2 \log_2 \frac{2^n}{N}}{\log_2 N}.$$

При этом f выражается через $\mathscr{L}_i$, h_i и f_t следующим образом:

$$f(\boldsymbol{x}) = f_t(\boldsymbol{x}) \cdot h_t(\mathscr{L}_t(\boldsymbol{x})) \cdot h_{t-1}(\mathscr{L}_{t-1}(\boldsymbol{x})) \cdot \ldots \cdot h_1(\mathscr{L}_1(\boldsymbol{x})).$$

Пусть t — минимальное целое, для которого $\big(\log_2 \log_2 \frac{2^n}{N} \big)^t \geqslant \frac{2^n}{N}$. Тогда

$$t \sim \frac{\log_2 \frac{2^n}{N}}{\log_2 \log_2 \log_2 \frac{2^n}{N}}.$$

При таком t справедливы неравенства

$$A_t \leqslant N, \quad |\boldsymbol{B} \cup \boldsymbol{A}_t| \leqslant 2N, \quad L(f_t) \lesssim \frac{2N}{\log_2 N} \ll L(f_{t-1}),$$

последнее из которых следует из двух первых и теоремы 2.1. Так как $n \log_2 n \leqslant N \ll 2^n$, то, как и в (2.14), нетрудно видеть, что*) $L(\mathscr{L}_i) \ll L(h_i)$ для каждого i. Поэтому

$$L(f) \lesssim \frac{N \log_2 \log_2 \log_2 \frac{2^n}{N}}{\log_2 N} \cdot \frac{\log_2 \frac{2^n}{N}}{\log_2 \log_2 \log_2 \frac{D}{N}} \sim \frac{N}{\log_2 N} \cdot \log_2 \frac{2^n}{N}.$$

Лемма доказана.

3.4. Доказательство теоремы 3.1. При $2^n/n \leqslant N \leqslant 2^{n-1}$ утверждение теоремы следует из леммы 3.1. Пусть $N < 2^n/n$ и $\log_2 N \gg \log_2 n$. Так как

$$N \log_2 \frac{2^n}{N} \leqslant \log_2 \binom{2^n}{N} \leqslant N \log_2 \frac{3 \cdot 2^n}{N}, \tag{3.10}$$

то при $N \ll 2^n$ для разности верхней и нижней оценок $\log_2 \binom{2^n}{N}$ справедливо неравенство

$$N \log_2 \frac{3 \cdot 2^n}{N} - N \log_2 \frac{2^n}{N} = N \log_2 3 \ll N \log_2 \frac{2^n}{N} \leqslant \log_2 \binom{2^n}{N},$$

из которого легко следует асимптотическое равенство верхней и нижней оценок в (3.10), что, в свою очередь, приводит к асимптотике

$$\frac{\log_2 \binom{2^n}{N}}{\log_2 \log_2 \binom{2^n}{N}} \sim \frac{N \log_2 \frac{2^n}{N}}{\log_2 N + \log_2 \log_2 \frac{2^n}{N}}.$$

Наконец, заметим, что в рассматриваемом случае $\log_2 n \ll \log_2 N$. Поэтому $\log_2 \log_2 \frac{2^n}{N} \leqslant \log_2 n \ll \log_2 N$ и, следовательно, имеет место асимптотическое равенство

$$\frac{\log_2 \binom{2^n}{N}}{\log_2 \log_2 \binom{2^n}{N}} \sim \frac{N \log_2 \frac{2^n}{N}}{\log_2 N},$$

правая часть которого совпадает с оценкой из утверждения леммы 3.3. Теорема доказана.

§ 4. Локальное кодирование

Для вычисления булевых функций из множеств, в которых все функции обладают какими-либо определенными одинаковыми свойствами (например, имеют одинаковый вес), О. Б. Лупанов предложил в [4, 6] (и развил далее в [8]) общий и достаточно универсальный подход, названный

*) Формально следует написать, что $L(\mathscr{L}_i)$ растет медленнее оценки $L(h_i)$.

им принципом локального кодирования. Идея этого принципа заключается в использовании при построении схем промежуточного объекта — кода функции, компактно и экономно представляющего вычисляемую функцию. Технически принцип локального кодирования в [6] — это система теорем, позволяющая «автоматизировать» доказательство верхних оценок сложности для функций из различных множеств.

4.1. Нетехническое введение. Опишем упрощенный вариант реализации этого принципа, в котором доля автоматизации минимальна, а доказываемые далее теоремы 4.1 и 4.2 позволяют проводить необходимые действия с кодом функции в «ручном» режиме, не используя общие теоремы из [6].

Пусть функции с заданными свойствами формируют некоторое множество $\boldsymbol{F}$. Каждой n-местной булевой функции f из этого множества ставится в соответствие ее код — двоичный набор $\boldsymbol{\lambda}$ длины M, по которому f определяется однозначно и который рассматривается далее как вектор значений $\lceil \log_2 M \rceil$-местной булевой функции λ. Этот код должен обладать свойством локальности кодирования a) и свойствами простоты декодирования b) и c):

a) для вычисления значения функции f на конкретном наборе $\boldsymbol{\sigma}$ достаточно знать только соответствующий этому набору кусок кода $\boldsymbol{\pi}$, длина которого не очень велика относительно M;

b) достаточно просто по набору $\boldsymbol{\sigma}$ должно вычисляться положение этого куска внутри кода, определяемое позицией $\boldsymbol{\alpha}$, с которой он начинается в $\boldsymbol{\lambda}$, и его длиной r;

c) также достаточно просто по набору $\boldsymbol{\sigma}$ и соответствующему куску кода $\boldsymbol{\pi}$ должно вычисляться значение $f(\boldsymbol{\sigma})$.

При выполнении указанных свойств вычисление $f(\boldsymbol{\sigma})$ проводится следующим образом.

1) Сначала по $\boldsymbol{\sigma}$ вычисляются $\boldsymbol{\alpha}$ и r.

2) Затем, начиная со значения $\lambda(\boldsymbol{\alpha})$, вычисляются r последовательных значений функции λ. Эти значения образуют кусок $\boldsymbol{\pi}$.

3) Наконец, по $\boldsymbol{\sigma}$ и $\boldsymbol{\pi}$ вычисляется $f(\boldsymbol{\sigma})$.

Слова «достаточно» в b) и c) означают, что вычисления в 1) и 3) можно сделать существенно проще вычислений в 2). Также заметим, что функция λ и вычисления в 1) и 3) зависят от $\boldsymbol{F}$, а вот вычисления в 2) универсальны.

Далее оценим сложность таких универсальных вычислений. Сделаем это в двух вариантах. В первом — простом (теорема 4.1), сделаем это без сложных технических элементов для схем в базисе B_2. Во втором варианте (теорема 4.2) сделаем это для схем в произвольном полном конечном базисе.

4.2. Последовательные наборы. Для каждого $\boldsymbol{\sigma} \in \{0,1\}^n$ определим его номер $|\boldsymbol{\sigma}| = \sum\limits_{i=1}^{n} \sigma_i 2^{i-1}$. В $\{0,1\}^n$ рассмотрим подмножество $\boldsymbol{S}$, состоящее из S наборов с номерами, не превосходящими $S-1$. Про такое множество будем говорить, что оно состоит из первых S наборов множества $\{0,1\}^n$. Пусть $f : \boldsymbol{S} \to \{0,1\}$ и $1 \leqslant R \leqslant S$. По функции f определим функцию $f^R : \boldsymbol{S} \to \{0,1\}^R$ так, что для любого $\boldsymbol{\sigma}$ из $\boldsymbol{S}$

$$f^R(\boldsymbol{\sigma}) = (f(\boldsymbol{\sigma}), f(\boldsymbol{\sigma}_1), \ldots, f(\boldsymbol{\sigma}_{R-1})),$$

где $|\boldsymbol{\sigma}_i| = |\boldsymbol{\sigma}| + i \pmod S$. Будем говорить, что f^R вычисляет значения f на R последовательных наборах.

Теорема 4.1. *Пусть* $n \to \infty$, $\boldsymbol{S}$ *состоит из первых* S *наборов* $\{0,1\}^n$, $2^{n-1} < S \leqslant 2^n$, $R \ll S/\log_2^2 S$. *Тогда для любой* n*-местной булевой функции* $f : \boldsymbol{S} \to \{0,1\}$

$$L(f^R) \lesssim \frac{S}{\log_2 S}.$$

Доказательство. Значения n-местной функции f запишем в таблице T из 2^k строк и $\lceil S/2^k \rceil$ столбцов, поставив в соответствие i-й строке таблицы двоичный набор $(\sigma_1, \ldots, \sigma_k)$, являющийся двоичным представлением числа $i-1$, а j-му столбцу — набор $(\sigma_{k+1}, \ldots, \sigma_n)$ — двоичное представление числа $j-1$. В таблице на пересечении i-й строки и j-го столбца поставим значение $f(\sigma_1, \ldots, \sigma_k, \sigma_{k+1}, \ldots, \sigma_n)$ — значение f на $((j-1)2^k+i)$-м наборе из $\boldsymbol{S}$. Последний столбец будет состоять из $S - 2^k(\lceil S/2^k \rceil - 1)$ элементов и поэтому может оказаться короче остальных. Полагая, что $R < 2^k$, к каждому столбцу таблицы T, кроме последнего, снизу припишем первые $R-1$ элементов следующего столбца. К последнему столбцу припишем первые $R-1$ элементов первого столбца, дополнив оставшиеся позиции нулями. В результате получим таблицу H из 2^k+R-1 строк и $\lceil S/2^k \rceil$ столбцов, в которой в j-м столбце R последовательных элементов с i-го по $(i+R-1)$-й, где $i \leqslant 2^k$ (для последнего столбца $i \leqslant S - 2^k(\lceil S/2^k \rceil - 1)$), являются значениями f на R последовательных наборах, начиная с $f(\sigma_1, \ldots, \sigma_k, \sigma_{k+1}, \ldots, \sigma_n)$.

Пусть $h_i(x_{k+1}, \ldots, x_n)$ — булева функция, вектор значений которой совпадает с i-й строкой H. Тогда для любого булева набора $(\sigma_{k+1}, \ldots, \sigma_n)$ набор $\big(h_i(\sigma_{k+1}, \ldots, \sigma_n)\big)_{i=1}^{2^k+R-1}$ совпадает с j-м столбцом таблицы H. Таким образом, для вычисления f на R последовательных наборах, начиная с набора $(\sigma_1, \ldots, \sigma_n)$, достаточно вычислить значения всех функций $h_i(\sigma_{k+1}, \ldots, \sigma_n)$ и выделить в получившемся наборе R последовательных значений, начиная с j-й позиции, где $j = 1 + \sum\limits_{t=1}^{k} \sigma_t 2^{t-1}$.

Вычисляющую значения функции f_R схему S представим в виде трех независимых подсхем.

1. Множество первых $\lceil S/2^k \rceil$ булевых наборов $(\sigma_{k+1}, \ldots, \sigma_n)$ разобьем на $\lceil \lceil S/2^k \rceil / p \rceil$ подмножеств K_i, каждое из которых, кроме, быть может, последнего, состоит из p последовательных элементов. Здесь полагаем, что $S/2^k p \gg 1$. Подсхема S_1 для каждого K_i вычисляет все возможные функции $g(x_{k+1}, \ldots, x_n)$, равные нулю вне K_i. Нетрудно видеть, что

$$L(\mathsf{S}_1) = \mathcal{O}\left(\frac{S2^p}{2^k p}\right). \tag{4.1}$$

2. Подсхема S_2 из вычисленных подсхемой S_1 функций g вычисляет функции h_i. Так как каждая функция h_i является дизъюнкцией не более чем $\lceil \lceil S/2^k \rceil / p \rceil$ функций g, то

$$L(\mathsf{S}_2) \leqslant \frac{\lceil S/2^k \rceil}{p} \cdot \left(2^k + R - 1\right) \leqslant \frac{S}{p} + \frac{1}{p}\left(\frac{SR}{2^k} + 2^k + R\right). \tag{4.2}$$

3. Подсхема S_3 по значениям $\sigma_1, \ldots, \sigma_k$ переменных $x_1, \ldots, x_k$ из вычисленного подсхемой S_2 набора значений $2^k + R - 1$ функций h_i выделяет R последовательных значений, первым из которых является значение

функции h_j, где $j = 1 + \sum_{t=1}^{k} \sigma_t 2^{t-1}$. Такие схемы неоднократно рассматривались различными авторами. По-видимому, одним из первых это сделал О. Б. Лупанов в [4], показав, что сложность схемы с точностью до постоянного множителя не превосходит произведения длины набора и его логарифма. Схема (подробное описание представлено в [6]) состоит в реализации последовательных сдвигов набора на $\sigma_t 2^{t-1}$ позиций для $t = 1, 2, \ldots, k$. В результате этих сдвигов требуемые R последовательных позиций набора попадают в заранее определенное место. Таким образом,

$$L(\mathsf{S}_3) = \mathcal{O}\left((2^k + R - 1)\log_2(2^k + R - 1)\right). \tag{4.3}$$

Суммируя (4.1)–(4.3) и учитывая неравенство $R \leqslant 2^k$, видим, что

$$L(\mathsf{S}) \leqslant \frac{S}{p} + \mathcal{O}\left(\frac{SR}{p2^k} + \frac{S2^p}{p2^k} + k2^k\right) \tag{4.4}$$

при выполнении условия $S/2^k p \gg 1$.

Положим

$$k = \left\lceil \log_2 S - 2\log_2\log_2 S - \log_2\log_2 \frac{S}{R\log_2^2 S} \right\rceil,$$
$$p = \lfloor \log_2 S - 4\log_2\log_2 S \rfloor.$$

При таких k и p справедливо неравенство $S/2^k p \geqslant \log_2 S \gg 1$, а из условия $R \ll S/\log_2^2 S$ следует, что $\dfrac{S}{R\log_2^2 S} \gg 1$. Поэтому нетрудно видеть, что при $n \to \infty$ для слагаемых в правой части неравенства (4.4) справедливы соотношения

$$\frac{S}{p} \sim \frac{S}{\log_2 S},$$
$$k2^k \asymp \frac{S\log_2 S}{\log_2^2 S \cdot \log_2 \frac{S}{R\log_2^2 S}} \ll \frac{S}{\log_2 S},$$
$$\frac{SR}{p2^k} \asymp \frac{S}{\log_2 S} \cdot \frac{R\log_2^2 S}{S} \cdot \log_2 \frac{S}{R\log_2^2 S} \ll \frac{S}{\log_2 S},$$
$$\frac{S2^p}{p2^k} \asymp \frac{S}{\log_2 S} \cdot \frac{S\log_2^2 S}{S\log_2^4 S} \cdot \log_2 \frac{S}{R\log_2^2 S} \ll \frac{S}{\log_2 S},$$

подставляя которые в (4.4), видим, что

$$L(\mathsf{S}) \lesssim \frac{S}{\log_2 S}.$$

Теорема доказана.

4.3. Произвольный базис. Будем рассматривать вычисление булевых функций схемами в произвольном полном конечном базисе $B = \{\varphi_i\}$, в котором каждой базисной функции φ_i приписан вес $\varrho_i > 0$. В этом случае сложностью схемы называется сумма весов ее элементов. Нетрудно показать, что для любых полных конечных базисах B и B' существуют такие константы c_1 и c_2, что для любой булевой функции f

$$c_1 L_{B'}(f) \leqslant L_B(f) \leqslant c_2 L_{B'}(f).$$

Далее, как правило, без специального упоминания будем пользоваться этими равенствами при оценке сложности схем в произвольном базисе, если их сложность оценивается с точностью до постоянного множителя, а конструкция аналогичных схем в стандартном базисе очевидна.

Пусть базисная функция φ_i зависит от r_i аргументов. Величина

$$\varrho = \min_i \frac{\varrho_i}{r_i - 1},$$

где минимум берется по всем более чем одноместным элементам базиса, называется минимумом приведенных весов этого базиса. В [4] показано, что вычисление произвольной булевой функции можно организовать так, что вычисляющая эту функцию схема будет почти полностью состоять из элементов с минимальным приведенным весом. Основываясь на этом результате, технике и других результатах из [4, 6], установим справедливость следующей теоремы.

Т е о р е м а 4.2. *Пусть $n \to \infty$, $\boldsymbol{S}$ состоит из первых S наборов $\{0,1\}^n$, $2^{n-1} < S \leqslant 2^n$, $R \ll S/\log_2^2 S$. Тогда для любого полного конечного базиса B с минимальным приведенным весом ϱ и любой n-местной булевой функции $f : \boldsymbol{S} \to \{0,1\}$*

$$L_B(f^R) \lesssim \varrho \cdot \frac{S}{\log_2 S}.$$

Докажем лемму 4.1 — утверждение из [4] об обобщенном разложении булевой функции. На этом разложении основано доказательство следующей леммы 4.2, на которой, в свою очередь, основано доказательство теоремы 4.2, играющей исключительную роль в доказательстве всех последующих теорем.

Л е м м а 4.1. *Пусть булева функция $F(x_0, \ldots, x_{K-1})$, где $K \geqslant 2^n$, существенно зависит от всех своих переменных. Тогда существуют такие булевы функции*

$$\begin{aligned} &\psi_i(y_1, \ldots, y_n, z), \quad \text{где} \quad 0 \leqslant i < 2^n, \\ &\chi_i(y_1, \ldots, y_n), \quad \text{где} \quad 2^n \leqslant i < K - 1, \end{aligned}$$

что любая булева функция $f(y_1, \ldots, y_n, z_1, \ldots, z_m)$ может быть представлена в виде:

$$\begin{aligned} f(y_1, \ldots, y_n, z_1, \ldots, z_m) = \\ = F(&\psi_0(y_1, \ldots, y_n, f(0, \ldots, 0, z_1, \ldots, z_m)), \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ &\psi_{|\boldsymbol{\alpha}|}(y_1, \ldots, y_n, f(\alpha_1, \ldots, \alpha_n, z_1, \ldots, z_m)), \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ &\psi_{2^n-1}(y_1, \ldots, y_n, f(1, \ldots, 1, z_1, \ldots, z_m), \\ &\chi_{2^n}(y_1, \ldots, y_n), \ldots\ldots, \chi_{K-1}(y_1, \ldots, y_n)). \end{aligned} \tag{4.5}$$

Д о к а з а т е л ь с т в о. Функция F существенно зависит от каждой своей переменной, поэтому для каждого $0 \leqslant j < K - 1$ найдутся такие постоянные α_{ji}, что

$$F(\alpha_{j,0}, \ldots, \alpha_{j,j-1}, x_j, \alpha_{j,j+1}, \ldots, \alpha_{j,K-1}) = x_j \oplus \alpha_{j,j}. \tag{4.6}$$

Функции ψ_i при $0 \leqslant i < 2^n$ и функции χ_i при $2^n \leqslant i < K-1$ определим следующими равенствами:

$$\psi_i(\beta_1, \ldots, \beta_n, z) = \psi_i(\boldsymbol{\beta}, z) = \begin{cases} \alpha_{|\boldsymbol{\beta}|,i}, & \text{если } i \neq |\boldsymbol{\beta}|, \\ z \oplus \alpha_{|\boldsymbol{\beta}|,|\boldsymbol{\beta}|}, & \text{если } i = |\boldsymbol{\beta}|, \end{cases}$$

$$\chi_i(\beta_1, \ldots, \beta_n) = \chi_i(\boldsymbol{\beta}) = \alpha_{|\boldsymbol{\beta}|,i}.$$

Тогда при $\boldsymbol{z} = (z_1, \ldots, z_m)$ из (4.6) видим, что для любого $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$

$$\begin{aligned} F(\psi_0(\boldsymbol{\alpha}, f(\boldsymbol{0}, \boldsymbol{z})), \ldots, \psi_{|\boldsymbol{\alpha}|}(\boldsymbol{\alpha}, f(\boldsymbol{\alpha}, \boldsymbol{z})), \ldots \\ \ldots, \psi_{2^n-1}(\boldsymbol{\alpha}, f(\boldsymbol{1}, \boldsymbol{z})), \chi_{2^n}(\boldsymbol{\alpha}), \ldots, \chi_{K-1}(\boldsymbol{\alpha})) = \\ = F(\alpha_{|\boldsymbol{\alpha}|,0}, \ldots, f(\boldsymbol{\alpha}, \boldsymbol{z}) \oplus \alpha_{|\boldsymbol{\alpha}|,|\boldsymbol{\alpha}|}, \ldots \\ \ldots, \alpha_{|\boldsymbol{\alpha}|,2^n-1}, \alpha_{|\boldsymbol{\alpha}|,2^n}, \ldots, \alpha_{|\boldsymbol{\alpha}|,K-1}) = \\ = \big(f(\boldsymbol{\alpha}, \boldsymbol{z}) \oplus \alpha_{|\boldsymbol{\alpha}|,|\boldsymbol{\alpha}|}\big) \oplus \alpha_{|\boldsymbol{\alpha}|,|\boldsymbol{\alpha}|} = f(\alpha_1, \ldots, \alpha_n, z_1, \ldots, z_m). \end{aligned}$$

Лемма доказана.

Разложение

$$f(y_1, \ldots, y_n, z_1, \ldots, z_m) = \bigvee_{\alpha_1, \ldots, \alpha_n} f(\alpha_1, \ldots, \alpha_n, z_1, \ldots, z_m) \cdot y_1^{\alpha_1} \cdot \ldots \cdot y_n^{\alpha_n}$$

булевой функции f по первым n переменным является частным случаем формулы (4.5), в которой

$$\begin{aligned} F(x_0, \ldots, x_{2^n-1}) &= x_0 \vee x_1 \vee \cdots \vee x_{2^n-1}, \\ \psi_{|\boldsymbol{\alpha}|}(y_1, \ldots, y_n, f(\alpha_1, \ldots, \alpha_n, z_1, \ldots, z_m)) &= \\ &= f(\alpha_1, \ldots, \alpha_n, z_1, \ldots, z_m) \cdot y_1^{\alpha_1} \cdot \ldots \cdot y_n^{\alpha_n}. \end{aligned}$$

Воспользуемся леммой 4.1 для доказательства следующего утверждения, аналогичного лемме Д.8 из [6].

Лемма 4.2. *Пусть $m \to \infty$, $\boldsymbol{S}$ состоит из первых S наборов $\{0,1\}^m$, $2^{m-1} < S \leqslant 2^m$, $1 \ll \log_2 S - \log_2 \log_2 R \ll \log_2 R$. Тогда для любых R m-местных булевых функций $f_i \colon \boldsymbol{S} \to \{0,1\}$*

$$L_B(f_1, \ldots, f_R) \lesssim \varrho \cdot \frac{RS}{\log_2 RS}.$$

Доказательство. Введем параметры k и l так, что $m = k + l$. Множество переменных $\boldsymbol{x} = \{x_1, \ldots, x_m\}$ функций f_i разобьем на два подмножества $\boldsymbol{y} = \{x_1, \ldots, x_k\}$ и $\boldsymbol{z} = \{x_{k+1}, \ldots, x_{k+l}\}$, полагая, что $f_i(\boldsymbol{x}) = f_i(\boldsymbol{y}, \boldsymbol{z})$ для каждого i.

Пусть $(r+1)$-местная функция φ имеет минимальный приведенный вес среди всех не менее чем двуместных функций базиса B. Введем функции $\Phi_1 = \varphi$ и

$$\begin{aligned} \Phi_t(y_0, \ldots, y_{tr}) &= \Phi_{t-1}(y_0, \ldots, y_{(t-1)r-1}, \varphi(y_{(t-1)r}, \ldots, y_{tr}))) = \\ &= \varphi(y_0, \ldots, y_{r-1}, \varphi(y_r, \ldots, y_{2r}(\ldots, \varphi(y_{(t-1)r}, \ldots, y_{tr}))\ldots)) \end{aligned}$$

для t, бóльших единицы. Индукцией по t нетрудно показать, что каждая функция Φ_t существенно зависит от всех своих $tr+1$ переменных.

Положим $S_k = \left\lceil \frac{S}{2^k} \right\rceil$, $s = \left\lceil \frac{S_k}{r} \right\rceil$. Так как $L_B(\varphi) = \varrho r$, то для сложности Φ_s справедливо неравенство

$$L_B(\Phi_s) \leqslant sL_B(\varphi) = \varrho \cdot sr. \tag{4.7}$$

Множество первых S_k значений переменных $\boldsymbol{z}$ лексикографически упорядочим и разобьем на $q = \left\lceil \frac{S_k}{p} \right\rceil$ подмножеств I_j, каждое из которых, кроме, возможно, последнего, состоит из p последовательных наборов. Затем каждую функцию $f_i(\boldsymbol{y}, \boldsymbol{z})$ представим в виде дизъюнкции q функций $f_{i,j}(\boldsymbol{y}, \boldsymbol{z})$, где для каждой $f_{i,j}(\boldsymbol{y}, \boldsymbol{z})$ ее значение $f_{i,j}(\boldsymbol{\alpha}, \boldsymbol{\beta})$ равно нулю при $\boldsymbol{\beta} \notin I_j$. Тогда

$$f_i(\boldsymbol{y}, \boldsymbol{z}) = \bigvee_{j=1}^{q} f_{i,j}(\boldsymbol{y}, \boldsymbol{z}). \tag{4.8}$$

Каждую функцию $f_{i,j}(\boldsymbol{y}, \boldsymbol{z})$ из этого разложения в силу леммы 4.1 разложим по первым k переменным и представим формулой

$$\begin{aligned} f_{i,j}(\boldsymbol{y}, \boldsymbol{z}) = \Phi_s(&\psi_0(\boldsymbol{y}, f_{i,j}(\boldsymbol{0}, \boldsymbol{z})), \ldots, \psi_{|\boldsymbol{\alpha}|}(\boldsymbol{y}, f_{i,j}(\boldsymbol{\alpha}, \boldsymbol{z})), \ldots \\ &\ldots, \psi_{2^k-1}(\boldsymbol{y}, f_{i,j}(\boldsymbol{1}, \boldsymbol{z}), \chi_{2^k}(\boldsymbol{y}), \ldots, \chi_{sr}(\boldsymbol{y})), \end{aligned} \tag{4.9}$$

в которой, в свою очередь, каждую функцию $\psi_{|\boldsymbol{\alpha}|}(\boldsymbol{y}, f_{i,j}(\boldsymbol{\alpha}, \boldsymbol{z}))$ разложим по последней переменной:

$$\psi_{|\boldsymbol{\alpha}|}(\boldsymbol{y}, f_{i,j}(\boldsymbol{\alpha}, \boldsymbol{z})) = \psi_{|\boldsymbol{\alpha}|}(\boldsymbol{y}, 0)\overline{f_{i,j}(\boldsymbol{\alpha}, \boldsymbol{z})} \vee \psi_{|\boldsymbol{\alpha}|}(\boldsymbol{y}, 1) f_{i,j}(\boldsymbol{\alpha}, \boldsymbol{z}). \tag{4.10}$$

Нетрудно видеть, что число различных функций $\psi_j(\boldsymbol{y}, \alpha)$ не превосходит 2^{k+1}, а число функций $\chi_j(\boldsymbol{y})$ — не более r. Так как каждая функция $f_{i,j}(\boldsymbol{\alpha}, \boldsymbol{z})$ равна нулю вне множества I_j, то число таких функций не превосходит $2^p q$. Следовательно, общее число произведений $\psi_{|\boldsymbol{\alpha}|}(\boldsymbol{y}, 0)\overline{f_{i,j}(\boldsymbol{\alpha}, \boldsymbol{z})}$ и $\psi_{|\boldsymbol{\alpha}|}(\boldsymbol{y}, 1) f_{i,j}(\boldsymbol{\alpha}, \boldsymbol{z})$ не больше чем $2^{k+1} 2^p q$, а общее число различных функций $\psi_{|\boldsymbol{\alpha}|}(\boldsymbol{y}, f_{i,j}(\boldsymbol{\alpha}, \boldsymbol{z}))$ в (4.10) при всех i, j и $\boldsymbol{\alpha}$ не больше $2^k 2^p q$.

Схему S, вычисляющую функции $f_1, \ldots, f_R$, построим в соответствии с разложением (4.8)–(4.10).

1. Подсхема S_1 вычисляет все функции $\psi_j(\boldsymbol{y}, \alpha)$ и $\chi_j(\boldsymbol{y})$. Так как сложность каждой из этих функций не превосходит 2^k, то

$$L(\mathsf{S}_1) = \mathcal{O}\left(2^{2k}\right). \tag{4.11}$$

2. Подсхема S_2 вычисляет первые S_k элементарных конъюнкций переменных $\boldsymbol{z}$ и собирает из них все функции $f_{i,j}(\boldsymbol{\alpha}, \boldsymbol{z})$ (вместе с их отрицаниями $\overline{f_{i,j}(\boldsymbol{\alpha}, \boldsymbol{z})}$). Нетрудно видеть, что

$$L(\mathsf{S}_2) = \mathcal{O}\left(S_k m + 2^p qp\right). \tag{4.12}$$

3. Используя функции $\psi_j(\boldsymbol{y}, \alpha)$, вычисленные подсхемой S_1, и функции $f_{i,j}(\boldsymbol{\alpha}, \boldsymbol{z})$ и $\overline{f_{i,j}(\boldsymbol{\alpha}, \boldsymbol{z})}$, вычисленные подсхемой S_2, подсхема S_3, в соответствии с формулой (4.10), вычисляет все функции $\psi_{|\boldsymbol{\alpha}|}(\boldsymbol{y}, f_{i,j}(\boldsymbol{\alpha}, \boldsymbol{z}))$. Для вычисления каждой из этих функций достаточно конечного числа элементов, не превосходящего $2L_B(\&) + L_B(\vee)$. Поэтому

$$L(\mathsf{S}_3) = \mathcal{O}\left(2^k 2^p q\right). \tag{4.13}$$

4. Используя вычисленные подсхемами S_1 и S_3 функции $\chi_j(\boldsymbol{y})$ и $\psi_{|\boldsymbol{\alpha}|}(\boldsymbol{y}, f_{i,j}(\boldsymbol{\alpha}, \boldsymbol{z}))$, подсхема S_4 в соответствии с разложением (4.9) вычисляет все функции $f_{i,j}(\boldsymbol{y}, \boldsymbol{z})$ Из (4.7)–(4.9) видим, что

$$L(\mathsf{S}_4) \leqslant \varrho \cdot sr \cdot Rq. \tag{4.14}$$

5. Подсхема S_5 из вычисленных подсхемой S_4 функций $f_{i,j}(\boldsymbol{y}, \boldsymbol{z})$ в соответствии с (4.8) собирает все функции $f_i(\boldsymbol{y}, \boldsymbol{z})$. Нетрудно видеть, что

$$L(\mathsf{S}_5) = \mathcal{O}\left(Rq\right). \tag{4.15}$$

Суммируя неравенства (4.11)–(4.15) и подставляя в получившуюся сумму параметры $S_k = \left\lceil \frac{S}{2^k} \right\rceil$, $s = \left\lceil \frac{S_k}{r} \right\rceil$ и $q = \left\lceil \frac{S_k}{p} \right\rceil$, видим, что

$$L(\mathsf{S}) \leqslant \varrho \cdot \left\lceil \frac{2^k}{r} \right\rceil r \cdot R \left\lceil \frac{\lceil S2^{-k} \rceil}{p} \right\rceil + \mathcal{O}\left(2^{2k} + \lceil S2^{-k} \rceil m + \right.$$
$$\left. + 2^p \left\lceil \frac{\lceil S2^{-k} \rceil}{p} \right\rceil p + 2^k 2^p \left\lceil \frac{\lceil S2^{-k} \rceil}{p} \right\rceil + R \left\lceil \frac{\lceil S2^{-k} \rceil}{p} \right\rceil \right).$$

Далее параметры k и p выберем так, чтобы при $m \to \infty$ выполнялись асимптотические неравенства

$$2^k \gg 1, \quad S \gg 2^k, \quad S_k \gg p, \tag{4.16}$$

которые обеспечивают в последней выключенной формуле неограниченный рост всех функций вида $\lceil \cdot \rceil$. Поэтому при таких значениях k и p схема S определена корректно и для ее сложности справедливо асимптотическое неравенство

$$L(\mathsf{S}) \lesssim \varrho \cdot \frac{2^k}{r} r \cdot R \frac{S2^{-k}}{p} +$$
$$+ \mathcal{O}\left(2^{2k} + S2^{-k}m + 2^p \frac{S2^{-k}}{p} p + 2^k 2^p \frac{S2^{-k}}{p} + R\frac{S2^{-k}}{p}\right) \sim$$
$$\sim \varrho \cdot \frac{RS}{p} + \mathcal{O}\left(2^{2k} + S2^{-k}m + 2^p S2^{-k} + 2^p \frac{S}{p} + \frac{RS}{2^k p}\right). \tag{4.17}$$

Положим

$$k = \lfloor \log_2 S - \log_2 \log_2 R - \log_2(\log_2 S - \log_2 \log_2 R) \rfloor,$$
$$p = \lfloor \log_2 R - \log_2 \log_2 R \rfloor.$$

Тогда из условия леммы $1 \ll \log_2 S - \log_2 \log_2 R \ll \log_2 R$ следуют асимптотические оценки

$$\log_2 S \ll \log_2 R \sim \log_2 RS \sim p \tag{4.18}$$

и справедливость условий (4.16):

$$1 \ll 2^k \asymp \frac{S}{\log_2 R \cdot (\log_2 S - \log_2 \log_2 R)} \ll \frac{S}{\log_2 R} \ll S,$$
$$S_k \sim S2^{-k} \asymp \frac{S \log_2 R \cdot (\log_2 S - \log_2 \log_2 R)}{S} \gg \log_2 R \sim p.$$

Также нетрудно видеть, что при выбранных значениях k и p

$$\begin{aligned}
2^{2k} &\ll \left(\frac{S}{\log_2 R}\right)^2 \ll \frac{RS}{\log_2^2 R} \ll \frac{RS}{\log_2 RS},\\
S2^{-k}m &\ll Sm \asymp S\log_2 S \ll \frac{RS}{\log_2 RS},\\
2^p S2^{-k} &\ll 2^p S \asymp \frac{RS}{\log_2 R} \sim \frac{RS}{\log_2 RS},\\
2^p\frac{S}{p} &\ll 2^p S \asymp \frac{RS}{\log_2 RS},\\
\frac{RS}{2^k p} &\ll \frac{RS}{p} \sim \frac{RS}{\log_2 R} \sim \frac{RS}{\log_2 RS}.
\end{aligned} \tag{4.19}$$

Подставив оценки (4.18) и (4.19) в неравенство (4.17), видим, что при $m\to\infty$

$$L(\mathsf{S}) \lesssim \varrho\cdot\frac{RS}{\log_2 RS}.$$

Лемма доказана.

Доказательство теоремы 4.2 во многом следует доказательству теоремы 4.1. Значения n-местной функции f запишем в таблице T из 2^k строк и $\lceil S/2^k\rceil$ столбцов, поставив в соответствие i-й строке таблицы двоичный набор $(\sigma_1,\ldots,\sigma_k)$, являющийся двоичным представлением числа $i-1$, а j-му столбцу — набор $(\sigma_{k+1},\ldots,\sigma_n)$ — двоичное представление числа $j-1$. В таблице на пересечении i-й строки и j-го столбца поставим значение $f(\sigma_1,\ldots,\sigma_k,\sigma_{k+1},\ldots,\sigma_n)$ — значение f на $((j-1)2^k+i)$-м наборе из $\boldsymbol{S}$. Последний столбец будет состоять из $S-2^k(\lceil S/2^k\rceil-1)$ элементов и поэтому может оказаться короче остальных. Полагая, что $R<2^k$, к каждому столбцу таблицы T, кроме последнего, снизу припишем первые $R-1$ элементов следующего столбца. К последнему столбцу припишем первые $R-1$ элементов первого столбца, дополнив оставшиеся позиции нулями. В результате получим таблицу H из 2^k+R-1 строк и $\lceil S/2^k\rceil$ столбцов, в которой в j-м столбце R последовательных элементов с i-го по $(i+R-1)$-й, где $i\leqslant 2^k$ (для последнего столбца $i\leqslant S-2^k(\lceil S/2^k\rceil-1)$), являются значениями f на R последовательных наборах, начиная с $f(\sigma_1,\ldots,\sigma_k,\sigma_{k+1},\ldots,\sigma_n)$. Пусть $h_i(x_{k+1},\ldots,x_n)$ — булева функция, вектор значений которой совпадает с i-й строкой H. Тогда для вычисления f на R последовательных наборах, начиная с набора $(\sigma_1,\ldots,\sigma_n)$, достаточно вычислить значения всех функций $h_i(\sigma_{k+1},\ldots,\sigma_n)$ и выделить в получившемся наборе R последовательных значений, начиная с j-й позиции, где $j=1+\sum\limits_{t=1}^{k}\sigma_t 2^{t-1}$.

Вычисляющую значения функции f схему S представим в виде двух независимых подсхем S_1 и S_2.

1. Подсхема S_1, конструкция которой приведена в доказательстве леммы 4.2, вычисляет все определенные выше функции h_i. Так как каждая из этих 2^k+R-1 функций зависит от $n-k$ переменных, то для того, чтобы воспользоваться конструкцией из леммы 4.2, достаточно показать, что при $n-k\to\infty$

$$2\log_2\log_2\left(2^k+R-1\right) \leqslant n-k \ll \log_2\left(2^k+R-1\right). \tag{4.20}$$

Положим $k = \left\lfloor n - 2\log_2 n - \log_2\log_2 \frac{2^n}{Rn^2} \right\rfloor$. Так как $2^{n-1} < S \leqslant 2^n$ и $R \ll S/\log_2^2 S$, то $R \ll 2^n / n^2$ и, следовательно,

$$n - k \leqslant n - n + 2\log_2 n + \log_2\log_2 \frac{2^n}{Rn^2} + 1 \leqslant$$
$$\leqslant 3\log_2 n + 1 \ll \log_2 \frac{2^{n-1}}{n^2 \log_2 \frac{2^n}{Rn^2}} \leqslant \log_2 2^k \leqslant \log_2 \left(2^k + R - 1\right).$$

С другой стороны, из неравенства $R \ll 2^n / n^2$ следует, что

$$\frac{2^k}{R} \asymp \frac{2^n}{Rn^2} \Big/ \log_2 \frac{2^n}{Rn^2} \gg 1. \tag{4.21}$$

Поэтому

$$n - k \geqslant n - n + 2\log_2 n + \log_2\log_2 \frac{2^n}{Rn^2} \geqslant 2\log_2 n \geqslant$$
$$\geqslant 2\log_2 \left\lfloor n - 2\log_2 n - \log_2\log_2 \frac{2^n}{Rn^2} + 1 \right\rfloor \geqslant$$
$$\geqslant 2\log_2(k+1) = 2\log_2\log_2 2^{k+1} \geqslant 2\log_2\log_2 \left(2^k + R - 1\right).$$

Таким образом, неравенства (4.20) выполняются, схема S_1 вычисляет все функции h_i и в силу леммы 4.2 для ее сложности справедливо асимптотическое неравенство

$$L(\mathsf{S}_1) \lesssim \varrho \cdot \frac{\left(2^k + R - 1\right)\lceil S/2^k \rceil}{\log_2\left(\left(2^k + R - 1\right)\lceil S/2^k \rceil\right)} \sim \varrho \cdot \frac{S}{\log_2 S}. \tag{4.22}$$

2. Подсхема S_3 по значениям $\sigma_1, \ldots, \sigma_k$ переменных $x_1, \ldots, x_k$ из вычисленного подсхемой S_1 набора значений $2^k + R - 1$ функций h_i выделяет R последовательных значений, первым из которых является значение функции h_j, где $j = 1 + \sum\limits_{t=1}^{k} \sigma_t 2^{t-1}$. Из (4.3) и (4.21) следует, что

$$L(\mathsf{S}_2) \asymp (2^k + R - 1)\log_2(2^k + R - 1) \asymp$$
$$\asymp \frac{2^n}{n^2 \log_2 \frac{2^n}{Rn^2}} \log_2 \frac{2^n}{n^2 \log_2 \frac{2^n}{Rn^2}} \asymp \frac{2^n}{n \log_2 \frac{2^n}{Rn^2}} \ll \frac{S}{\log_2 S}. \tag{4.23}$$

Объединяя неравенства (4.22) и (4.23), получаем требуемую оценку:

$$L(\mathsf{S}) = L(\mathsf{S}_1) + L(\mathsf{S}_2) \lesssim \varrho \cdot \frac{S}{\log_2 S}.$$

Теорема доказана.

Тривиальным следствием доказанной теоремы является теорема Лупанова (теорема 4.3) о сложности вычисления произвольной булевой функции схемами в произвольном полном конечном базисе из [4].

Т е о р е м а 4.3. *Пусть $B = \{\varphi_i\}$ — полный конечный базис, ϱ — минимальный приведенный вес B. Тогда при $n \to \infty$ для любой n-местной булевой функции f*

$$L_B(f) \lesssim \varrho \cdot \frac{2^n}{n}.$$

Комбинируя доказательства теоремы 4.2 и леммы 4.2, нетрудно доказать следующее утверждение, являющееся полезным дополнением к теореме 4.2 при применении принципа локального кодирования.

Т е о р е м а 4.4. *Пусть $n \to \infty$, B — полный конечный базис, ϱ — минимальный приведенный вес B, $\boldsymbol{S}$ состоит из первых S наборов $\{0,1\}^n$, $2^{n-1} < S \leqslant 2^n$, $n - \log_2 \log_2 R \gg 1$. Тогда для любых R n-местных булевых функций $f_i : \boldsymbol{S} \to \{0,1\}$*

$$L_B(f_1, \ldots, f_R) \lesssim \varrho \cdot \frac{RS}{\log_2 RS}.$$

§ 5. Частичные функции ограниченного веса

В этом разделе рассматривается сложность вычисления частичных булевых функций ограниченного веса схемами в произвольном полном конечном базисе. Представленные здесь оценки доказывают справедливость неравенства (1.1) для широкого диапазона значений параметров N и D. Аналогичные результаты для схем в базисе B_2 были опубликованы ранее в [14, 18].

5.1. Почти равновесные функции. Пусть $n \to \infty$ и $\boldsymbol{D} \subseteq \{0,1\}^n$. Булеву функцию $f : \boldsymbol{D} \to \{0,1\}$ назовем почти равновесной функцией, если она равна единице на N наборах из области $\boldsymbol{D}$ и $\log_2 N \sim \log_2 D$. Для сложности почти равновесных булевых функций справедлива теорема 5.1, которая обобщает утверждение теоремы 2.1 о сложности частичных булевых функций на более широкий класс схем — схемы в произвольном полном конечном базисе и на более широкий класс частичных функций — почти равновесные функции.

Т е о р е м а 5.1. *Пусть $n \to \infty$, B — полный конечный базис с минимальным приведенным весом ϱ, $\boldsymbol{D} \subseteq \{0,1\}^n$, функция $f : \boldsymbol{D} \to \{0,1\}$ равна единице не более чем на N наборах из области $\boldsymbol{D}$. Если $\log_2 N \sim \log_2 D$, то*

$$L_B(f) \lesssim \varrho \cdot \frac{\log_2 \binom{D}{N}}{\log_2 \log_2 \binom{D}{N}} + \mathcal{O}(n).$$

Доказательство теоремы 5.1 во многом повторяет доказательство теоремы 2.1, отличаясь от последнего иным доказательством существования хорошего доопределяющего множества и несколько более сложным, по сравнению с доказательством леммы 2.2, доказательством ее аналога — леммы 5.3, выполненного при помощи метода локального кодирования.

5.2. Доопределения. Следующее утверждение установлено в [13], где рассматривалась сложность вычисления частичных булевых функций формулами.

Л е м м а 5.1. *Пусть $\boldsymbol{A}$ — множество наборов из $\{0,1,*\}^m$, каждый из которых содержит s булевых элементов, среди которых t единиц и $s-t$ нулей. Существует доопределение множества $\boldsymbol{A}$, состоящее не более чем из $m^2 \binom{s}{t}$ наборов.*

Доказательство. Нетрудно видеть, что множество $\boldsymbol{A}$ состоит ровно из $\binom{m}{s}\binom{s}{t}$ элементов. Составим таблицу T из $\binom{m}{k}$ строк и $\binom{m}{s}\binom{s}{t}$ столбцов. Каждой строке поставим в соответствие набор из $\{0,1\}^m$, содержащий ровно k единиц, а столбцу — недоопределенный набор из $\boldsymbol{A}$. В этой таблице на пересечении i-й строки, соответствующей набору $\boldsymbol{\beta}_i$, и j-го столбца, соответствующего набору $\boldsymbol{\alpha}_j$, поставим единицу, если $\boldsymbol{\beta}_i$ будет доопределением $\boldsymbol{\alpha}_j$, и нуль в противном случае. В такой таблице в каждой строке стоит ровно $\binom{k}{t}\binom{m-k}{s-t}$ единиц, а в каждом столбце — $\binom{m-s}{k-t}$ единиц.

Будем говорить, что i-я строка покрывает j-й столбец, если на их пересечении стоит единица. Для доказательства леммы достаточно показать, что в T найдется набор, состоящий не более чем из $2m^2\binom{s}{t}$ строк, покрывающих в совокупности все ее столбцы. Такой набор будем формировать последовательно, произвольно выбрав строку на первом шаге и добавляя в него на каждом следующем шаге строку, покрывающую максимальное число еще не покрытых столбцов.

Положим $A_0=\binom{m}{s}\binom{s}{t}$, и пусть A_r — число столбцов, остающихся непокрытыми после r шагов алгоритма. Допустим, что для A_r имеет место неравенство

$$A_r \leqslant A_0\left(1-\binom{m-s}{k-t}\Big/\binom{m}{k}\right)^r,$$

справедливость которого при $r=0$ очевидна. На каждом шаге в каждом непокрытом столбце находится ровно $\binom{m-s}{k-t}$ единиц (все единицы непокрытого столбца находятся в еще невыбранных строках). Поэтому общее число единиц в непокрытых столбцах равно $A_r\binom{m-s}{k-t}$ и, следовательно, найдется строка, в которой число единиц не меньше их среднего числа. Такая строка покрывает не менее

$$A_r\binom{m-s}{k-t}\Big/\left(\binom{m}{k}-r\right) \geqslant A_r\binom{m-s}{k-t}\Big/\binom{m}{k}$$

столбцов. Выбрав эту строку в качестве $(r+1)$-й строки формируемого набора, видим, что в этом случае

$$\begin{aligned} A_{r+1} &\leqslant A_r - A_r\binom{m-s}{k-t}\Big/\binom{m}{k} = A_r\left(1-\binom{m-s}{k-t}\Big/\binom{m}{k}\right) \leqslant \\ &\leqslant A_0\left(1-\binom{m-s}{k-t}\Big/\binom{m}{k}\right)^{r+1}. \end{aligned} \tag{5.1}$$

Далее рассмотрим равенство

$$\binom{m}{k}=\sum_{i=0}^{k}\binom{s}{i}\binom{m-s}{k-i},$$

в котором биномиальные коэффициенты с отрицательными нижними индексами полагаем равными нулю. 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

$$i = \left\lfloor \frac{(s+1)(k+1)}{m+2} \right\rfloor. \tag{5.2}$$

Рассматривая правую часть в (5.2) 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 $i = t$. Тогда

$$\binom{m-s}{k-t}\Big/\binom{m}{k} = \binom{m-s}{k-t}\Big/\left(\sum_{i=0}^{s}\binom{s}{i}\binom{m-s}{k-i}\right) \geqslant \\ \geqslant \binom{m-s}{k-t}\Big/\left((s+1)\binom{s}{t}\binom{m-s}{k-t}\right) \geqslant \left(m\binom{s}{t}\right)^{-1}.$$

Следовательно, в силу (5.1)

$$A_r \leqslant A_0\left(1 - \left(m\binom{s}{t}\right)^{-1}\right)^r < A_0 2^{-r/\left(m\binom{s}{t}\right)} = \binom{m}{s}\binom{s}{t}2^{-r/\left(m\binom{s}{t}\right)}.$$

Пусть $r = \left\lceil m\binom{s}{t}\log_2\binom{m}{s}\right\rceil$. Тогда после r шагов алгоритма в таблице останется меньше чем

$$\binom{m}{s}\binom{s}{t}2^{-\left\lceil m\binom{s}{t}\log_2\binom{m}{s}\right\rceil/\left(m\binom{s}{t}\right)} \leqslant \binom{s}{t}\binom{m}{s}2^{-\log_2\binom{m}{s}} = \binom{s}{t}$$

непокрытых столбцов, которые, очевидно, можно покрыть не более чем $\binom{s}{t}$ строками. Следовательно, число строк в покрытии не превосходит

$$r + \binom{s}{t} - 1 \leqslant m\binom{s}{t}\log_2\binom{m}{s} + \binom{s}{t} = \\ = \binom{s}{t}\left(m\log_2\binom{m}{s} + 1\right) \leqslant \binom{s}{t}\left(m(m-1)+1\right) < m^2\binom{s}{t}.$$

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

Доказательство. Множество $\boldsymbol{A}$ разобьем на классы, поместив в класс $\boldsymbol{A}(s,t)$, $t\leqslant s$, все наборы с s булевыми компонентами, t из которых равны единице. Из леммы 5.1 следует, что для множества $\boldsymbol{A}(s,t)$ существует доопределение $\boldsymbol{B}(s,t)$, состоящее не более чем из $m^2\binom{s}{t}$ наборов. Пусть $\boldsymbol{\alpha}\in\boldsymbol{A}(s,t)$. 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 (не превосходящее число возможных значений параметров s и t) не превосходит m^2. Поэтому множество $\cup_{s,t}\boldsymbol{B}(s,t)$ состоит не более чем из $m^5 2^R$ наборов и по построению является доопределением множества $\boldsymbol{A}$. Лемма доказана.

5.3. Доказательство теоремы 5.1.

Лемма 5.3. *Пусть $n\to\infty$, B — полный конечный базис с минимальным приведенным весом ϱ, $\boldsymbol{D}\subseteq\{0,1\}^n$, функция $f:\boldsymbol{D}\to\{0,1\}$ равна единице не более чем на N наборах из области $\boldsymbol{D}$. Если параметры n, D, N такие, что $N\leqslant\frac{1}{2}D$ и $\log_2\log_2\binom{D}{N}\sim n$, то*

$$L_B(f)\lesssim\varrho\cdot\frac{\log_2\binom{D}{N}}{\log_2\log_2\binom{D}{N}}.$$

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 j-му столбцу таблицы двоичный набор $(\sigma_1,\ldots,\sigma_k)$, являющийся двоичным представлением числа $j-1$, а i-й строке — набор $(\sigma_{k+1},\ldots,\sigma_n)$, являющийся двоичным представлением числа $i-1$. В таблице на пересечении j-го столбца и i-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 2^{2k-1} классов, поместив в класс $\boldsymbol{P}_{ij}$ наборы, начинающиеся в i-й и заканчивающиеся в j-й позициях.

Из леммы 5.2 следует, что для множества элементарных наборов класса $\boldsymbol{P}_{ij}$ существует множество их доопределений, которое состоит не более чем из $2^{5k}2^R$ 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 $\boldsymbol{H}$, состоящее не более чем из $2^{7k}2^R$ наборов $\boldsymbol{\beta}$ длины 2^k. Перенумеруем $\boldsymbol{\beta}$ из $\boldsymbol{H}$

целыми неотрицательными числами от нуля до $2^{7k}2^R-1$, присвоив нулевому набору нулевой номер.

Преобразуем таблицу T_f в новую таблицу T_h. Для этого для каждого i заменим в T_f i-ю строку, состоящую из элементарных наборов $\boldsymbol{\alpha}_{ij}$, дизъюнкцией $\boldsymbol{\beta}_i = \vee_j \boldsymbol{\beta}_{ij}$ их доопределений $\boldsymbol{\beta}_{ij}$ из $\boldsymbol{H}$. Преобразованная таблица T_h будет таблицей значений некоторой n-местной функции h, являющейся доопределением функции f.

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

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

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

$$h(x_1,\ldots,x_n)=\bigvee_{\boldsymbol{\sigma}=(\sigma_{k+1},\ldots,\sigma_n)}\Big(\bigvee_{g\in G} g(x_1,\ldots,x_k)\Big)x_{k+1}^{\sigma_{k+1}}\cdot\ldots\cdot x_n^{\sigma_n}. \tag{5.3}$$

Оценим число функций g в (5.3). Сделаем это так же, как и в доказательстве леммы 3.1. Заметим, что число функций, соответствующих наборам $\boldsymbol{\alpha}$ с $I(\boldsymbol{\alpha})<R$, не превосходит числа строк таблицы 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 $\sum\limits_{i=1}^{p} s_i\leqslant D$, $\sum\limits_{i=1}^{p} t_i\leqslant N$ и по условию леммы $N\leqslant\frac{1}{2}D$, то

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

Таким образом, общее число элементарных наборов в T_f, а следовательно, и функций g в (5.3) не превосходит

$$\log_2\binom{D}{N}\Big/R+2^{n-k}. \tag{5.4}$$

Перенумеруем элементарные наборы $\boldsymbol{\alpha}$ целыми неотрицательными числами от нуля до $2^{7k}2^R-1$, присвоив каждому набору номер его доопределения $\boldsymbol{\beta}$ из T_h. Теперь из таблицы T_f построим вектор $\boldsymbol{T}$ следующим образом: в T_f заменим все элементарные наборы $\boldsymbol{\alpha}$, на которые разбиты ее строки, их номерами $\boldsymbol{t}$ — двоичными наборами длины

$$m=\lceil\log_2 2^{7k}2^R\rceil\leqslant R+7k+1,$$

и затем, начиная с первой строки $\boldsymbol{T}_1$, выпишем все строки $\boldsymbol{T}_i$ новой таблицы одну за другой в виде вектора $\boldsymbol{T}=(\boldsymbol{T}_1\ldots\boldsymbol{T}_i\ldots\boldsymbol{T}_{2^{n-k}})$, где $\boldsymbol{T}_i=(\boldsymbol{t}_{i1}\ldots\boldsymbol{t}_{ij}\ldots\boldsymbol{t}_{il_i})$. Из (5.4) следует, что длина $\boldsymbol{T}$ удовлетворяет неравенству

$$\begin{aligned}T&\leqslant\left(\log_2\binom{D}{N}\Big/R+2^{n-k}\right)(R+7k+1)=\\&=\log_2\binom{D}{N}\left(1+\frac{7k+1}{R}\right)+2^{n-k}(R+7k+1).\end{aligned}$$

При этом, так как длина каждого элементарного набора не меньше $\log_2 R$, нетрудно видеть, что каждый вектор $\boldsymbol{T}_i$ состоит не более чем из q номеров, а его длина T_i не превосходит s, где

$$q = \left\lceil \frac{2^k}{\log_2 R} \right\rceil, \quad s \leqslant \left\lceil \frac{2^k}{\log_2 R} \right\rceil (R + 7k + 1).$$

Положим $\boldsymbol{l} = (l_1, \ldots, l_i, \ldots, l_{2^{n-k}})$, где l_i — число номеров $\boldsymbol{t}_{ij}$ в векторе $\boldsymbol{T}_i$, $\boldsymbol{r} = (r_1, \ldots, r_i, \ldots, r_{2^{n-k}})$, где r_i — номер позиции, начиная с которой в векторе $\boldsymbol{T}$ располагается вектор $\boldsymbol{T}_i$. Далее вектор $\boldsymbol{T}$ будем рассматривать как вектор значений частичной $\lceil \log_2 T \rceil$-местной булевой функции t, определенной на первых T наборах $\lceil \log_2 T \rceil$-мерного куба (здесь T — длина $\boldsymbol{T}$), векторы $\boldsymbol{l}$ и $\boldsymbol{r}$ — как векторы значений функции

$$l : \{0,1\}^{n-k} \to \{0,1\}^{\lceil \log_2 q \rceil} \quad \text{и} \quad r : \{0,1\}^{n-k} \to \{0,1\}^{\lceil \log_2 T \rceil}$$

соответственно. Пусть, кроме того,

$$g : \{0,1\}^{\lceil \log_2 p \rceil} \to \{0,1\}^{2^k}$$

— функция, преобразующая номер набора $\boldsymbol{t}$ в соответствующий этому набору вектор $\boldsymbol{\beta}$ из $\boldsymbol{H}$. Теперь покажем, как при помощи функций t, l, r и g вычислить функцию h. Вычисляющую функцию h схему S представим в виде пяти независимых подсхем.

1. Подсхема S_1 вычисляет $l_i = l(x_{k+1}, \ldots, x_n)$ и $r_i = r(x_{k+1}, \ldots, x_n)$. Из теоремы 4.3 следует, что

$$L(\mathsf{S}_1) = \mathcal{O}\left(\frac{2^{n-k}(\log_2 q + \log_2 T)}{n-k} \right) = \mathcal{O}\left(\frac{2^{n-k} \log_2 T}{n-k} \right). \tag{5.5}$$

2. Подсхемы S_2 и S_3 по вычисленным значениям l_i и r_i находят вектор $\boldsymbol{T}_i = \boldsymbol{t}_{i1} \ldots \boldsymbol{t}_{ij} \ldots \boldsymbol{t}_{il_i}$. Сначала подсхема S_2 вычисляет значения функции t на s последовательных наборах, начиная с r_i-го. Затем подсхема S_3 оставляет в вычисленном подсхемой S_2 векторе первые $l_i m$ значений и дополняет получившийся вектор нулями до вектора длины qm. Из теоремы 4.2 следует, что при выполнении условия $s \ll T / \log_2^2 T$ справедливы неравенства

$$L(\mathsf{S}_2) \lesssim \varrho \cdot \frac{T}{\log_2 T}, \quad L(S_3) \leqslant \mathcal{O}(s). \tag{5.6}$$

3. Подсхема S_4 разбивает вычисленный подсхемой S_3 вектор на блоки длины m — номера $\boldsymbol{t}_{ij}$, на каждом из этих номеров вычисляет значения функции g — набор длины 2^k. Затем S_4 вычисляет покомпонентную дизъюнкцию этих наборов, результатом чего является строка h_i таблицы H.

Нетрудно видеть, что основная сложность в S_4 приходится на вычисление q значений функции g. Поэтому в силу теоремы 4.3

$$L(\mathsf{S}_4) = \mathcal{O}\left(\lceil 2^k / R \rceil \cdot \frac{2^k \cdot 2^{7k+1} 2^R}{\log_2 (2^{7k+1} 2^R)} \right) = \mathcal{O}\left(\frac{2^{9k} 2^R}{R(R+7k)} \right).$$

4. Подсхема S_5 по значениям $\sigma_1, \ldots, \sigma_k$ переменных $x_1, \ldots, x_k$ выделяет из вычисленного подсхемой S_4 набора h_i его $|\boldsymbol{\sigma}|$-й элемент, — значение $h_i(\boldsymbol{\sigma})$. Нетрудно видеть, что

$$L(\mathsf{S}_5) = \mathcal{O}\left(2^k\right). \tag{5.7}$$

Суммируя неравенства (5.5)–(5.7), видим, что

$$L(\mathsf{S}) \lesssim \varrho \cdot \frac{T}{\log_2 T} + \mathcal{O}\left(\frac{2^{n-k}\log_2 T}{n-k} + \frac{2^k}{\log_2 R} + \frac{2^{9k}2^R}{R(R+7k)} + 2^k\right), \tag{5.8}$$

где

$$T \leqslant \log_2 \binom{D}{N}\left(1 + \frac{9k+1}{R}\right) + 2^{n-k}(R+7k+1), \tag{5.9}$$

и неравенство (5.8) справедливо при выполнении условия

$$s \asymp \frac{2^k}{\log_2 R}(R+7k) \ll \frac{T}{\log_2^2 T}. \tag{5.10}$$

Положим

$$k = \left\lceil n - \log_2\log_2\binom{D}{N} + 2\log_2\log_2\log_2\binom{D}{N}\right\rceil,$$
$$R = \left\lfloor \log_2\log_2\binom{D}{N} - 9k - 2\log_2\log_2\log_2\binom{D}{N}\right\rfloor.$$

Тогда, учитывая неравенство $\log_2 T \leqslant n$ и условие $\log_2\log_2\binom{D}{N} \sim n$, имеем

$$\begin{aligned} R &\sim \log_2\log_2\binom{D}{N}, \quad k \ll \log_2\log_2\binom{D}{N}, \\ R + 9k &\leqslant \log_2\log_2\binom{D}{N} - 2\log_2\log_2\log_2\binom{D}{N}, \\ n - k &\leqslant \log_2\log_2\binom{D}{N} - 2\log_2\log_2\log_2\binom{D}{N}. \end{aligned} \tag{5.11}$$

Из конструкции вектора $\boldsymbol{T}$ легко следует справедливость (5.10). Подставляя оценки из (5.11) в (5.8), после несложных преобразований получаем требуемую оценку сложности схемы S:

$$L(\mathsf{S}) \lesssim \varrho \cdot \frac{\log_2\binom{D}{N}}{\log_2\log_2\binom{D}{N}}.$$

Лемма доказана.

Следуя доказательству теоремы 2.1, распространим результат предыдущей леммы на области меньшего размера. Сделаем это, как и в доказательстве теоремы 2.1, при помощи линейных операторов из лемм 2.3–2.6, разделяющих и почти разделяющих множества нулей и единиц вычисляемых функций. Так как $L_B(\mathscr{L}) \leqslant L_B(\oplus) \cdot L_{B_2}(\mathscr{L})$ для любого полного конечного базиса B и любого линейного оператора $\mathscr{L}$, то все верхние оценки сложности линейных операторов в леммах 2.3–2.6 справедливы и для схем в базисе B.

Следующее утверждение является аналогом леммы 2.8 из доказательства теоремы 2.1.

Лемма 5.4. *Пусть $n \to \infty$, B — полный конечный базис с минимальным приведенным весом ϱ, $\boldsymbol{D} \subseteq \{0,1\}^n$, функция $f : \boldsymbol{D} \to \{0,1\}$ равна*

единице не более чем на N наборах из области $\boldsymbol{D}$. Если $\log_2 N \sim \log_2 D$, $N \leqslant \frac{1}{2}D$ *и* $\frac{1}{3}n \leqslant \log_2 D \leqslant n - 4\log_2 n$, *то*

$$L_B(f) \lesssim \varrho \cdot \frac{\log_2 \binom{D}{N}}{\log_2 \log_2 \binom{D}{N}}. \tag{5.12}$$

Доказательство. Положим $k = 3\log_2 n$, $\boldsymbol{D}_0 = \{\boldsymbol{x} \in \boldsymbol{D} \mid f(\boldsymbol{x}) = 0\}$, $\boldsymbol{D}_1 = \{\boldsymbol{x} \in \boldsymbol{D} \mid f(\boldsymbol{x}) = 1\}$. К областям $\boldsymbol{D}_0$ и $\boldsymbol{D}_1$ применим лемму 2.5, полагая, что $\boldsymbol{A} = \boldsymbol{D}_1$ и $\boldsymbol{B} = \boldsymbol{D}_0$. В результате для $m = \lceil \log_2 D_0 + 3\log_2 n \rceil$ найдется такой линейный оператор $\mathscr{L}\colon \{0,1\}^n \to \{0,1\}^m$, что множество

$$\boldsymbol{C} = \{(\boldsymbol{x}, \boldsymbol{y}) \mid \boldsymbol{x} \in \boldsymbol{D}_0, \boldsymbol{y} \in \boldsymbol{D}_1, \mathscr{L}(\boldsymbol{x}) = \mathscr{L}(\boldsymbol{y})\}$$

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

$$g(\boldsymbol{z}) = \begin{cases} 1, & \text{если } \exists\, \boldsymbol{x} \in \boldsymbol{D}_1 \text{ такой, что } \boldsymbol{z} = \mathscr{L}(\boldsymbol{x}), \\ & \quad \text{и } \nexists\, \boldsymbol{y} \in \boldsymbol{D}_0 \text{ такой, что } \boldsymbol{z} = \mathscr{L}(\boldsymbol{y}), \\ 0 & \text{в противном случае,} \end{cases}$$

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

$$L_B(f) \leqslant L_B(g) + L_B(h) + L_B(\mathscr{L}) + L_B(\oplus). \tag{5.13}$$

Оценим сложность функции g. Из оценок

$$\left(\frac{D}{N}\right)^N \leqslant \binom{D}{N} \leqslant \left(\frac{3 \cdot D}{N}\right)^N$$

биномиального коэффициента следуют верхняя и нижняя оценки его повторного логарифма

$$\log_2 N + \log_2 \log_2 \frac{D}{N} \leqslant \log_2 \log_2 \binom{D}{N} \leqslant \log_2 N + \log_2 \log_2 \frac{3 \cdot D}{N},$$

которые отличаются не более чем постоянным слагаемым. Учитывая условия леммы, приходим к асимптотическим равенствам

$$\log_2 \log_2 \binom{D}{N} \sim \log_2 N \sim \log_2 D \sim m.$$

Поэтому для оценки сложности функции g можно воспользоваться леммой 5.3. Из этой леммы следует, что

$$L_B(g) \lesssim \varrho \cdot \frac{\log_2 \binom{D}{N}}{\log_2 \log_2 \binom{D}{N}}. \tag{5.14}$$

Для вычисления функции h воспользуемся ее совершенной дизъюнктивной формой, полагая, что вне области $\boldsymbol{D}$ эта функция равна нулю. Так как в силу условий леммы $N \leqslant \log_2 \binom{D}{N}$ и $\log_2 N = \Omega(n)$, то

$$L_B(h) = \mathcal{O}\left(\frac{Nn}{\log_2^3 N}\right) = \mathcal{O}\left(\frac{N}{\log_2^2 N}\right) \ll \frac{\log_2 \binom{D}{N}}{\log_2 \log_2 \binom{D}{N}}. \tag{5.15}$$

Сложность оператора $\mathscr{L}$ по порядку не превосходит $\frac{n^2}{\log_2 n}$. Поэтому из условий леммы следует неравенство $L_B(\mathscr{L}) \ll L_B(g)$, которое вместе с (5.13)–(5.15) доказывает справедливость (5.12). Лемма доказана.

Далее докажем лемму 5.5 — аналог леммы 2.9 из доказательства теоремы 2.1.

Лемма 5.5. *Пусть $n \to \infty$, B — полный конечный базис с минимальным приведенным весом ϱ, $\boldsymbol{D} \subseteq \{0,1\}^n$, функция $f : \boldsymbol{D} \to \{0,1\}$ равна единице не более чем на N наборах из области $\boldsymbol{D}$. Если $\log_2 N \sim \log_2 D$, $N \leqslant \frac{1}{2} D$ и $\log_2 D \leqslant \frac{1}{3} n$, то*

$$L_B(f) \lesssim \varrho \cdot \frac{\log_2 \binom{D}{N}}{\log_2 \log_2 \binom{D}{N}} + \mathcal{O}(n).$$

Доказательство. Положим $m = \lfloor 2 \log_2 D \rfloor$. К области $\boldsymbol{D}$ применим лемму 2.6. В результате найдется инъективный на $\boldsymbol{D}$ линейный оператор $\mathscr{L} : \{0,1\}^n \to \{0,1\}^m$, для которого

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

Далее введем определенную на области $\mathscr{L}(\boldsymbol{D})$ частичную m-местную булеву функцию

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

Нетрудно видеть, что функция g равна единице не более чем на N наборах из $\mathscr{L}(\boldsymbol{D})$ и $f(\boldsymbol{x}) = g(\mathscr{L}(\boldsymbol{x}))$. Так как $m = \lfloor 2 \log_2 D \rfloor$, то можно воспользоваться леммой 5.4. В силу этой леммы

$$L_B(g) \lesssim \varrho \cdot \frac{\log_2 \binom{D}{N}}{\log_2 \log_2 \binom{D}{N}}.$$

Следовательно,

$$L_B(f) \lesssim \varrho \cdot \frac{\log_2 \binom{D}{N}}{\log_2 \log_2 \binom{D}{N}} + \mathcal{O}\left(\frac{n \log_2 D}{\log_2 n}\right). \tag{5.16}$$

Если $D > n^3$, то при $n \to \infty$ первое слагаемое в правой части (5.16) растет быстрее второго слагаемого, а если $n \leqslant D \leqslant n^3$, то второе слагаемое в (5.16) есть $\mathcal{O}(n)$. Лемма доказана.

Теперь доказательство теоремы 5.1 легко получается из лемм 5.3, 5.4 и 5.5. Если $\log_2 D \geqslant \frac{1}{3}n$, то утверждение теоремы следует из леммы 5.3 и леммы 5.4. Если $\log_2 D \leqslant \frac{1}{3}n$, то утверждение теоремы следует из леммы 5.5.

5.4. Полностью определенные функции. Следующая теорема 5.2 — это классическая теорема О. Б. Лупанова [6] о сложности булевых функций с данным числом единиц. Формулировка теоремы 5.2 слегка отличается от теоремы Лупанова, так как в [6] неравенство (5.17) доказывается для функций, равных единице ровно на N наборах. Однако нетрудно видеть, что справедливость (5.17) для функций, у которых число единичных наборов не превосходит N, следует из монотонности его правой части при $N \leqslant 2^{n-1}$ и справедливости этого неравенства для функций, у которых ровно N единичных наборов.

Как и в [6] доказательство теоремы 5.2 разбито на три части для разных, но частично пересекающихся интервалов значений N. Для двух из этих интервалов, рассмотренных в леммах 5.7 и 5.8, приводимые доказательства близки к соответствующим доказательствам из [6], отличаясь от последних некоторыми техническими деталями.

Теорема 5.2. *Пусть $n \to \infty$, B — полный конечный базис, ϱ — минимальный приведенный вес B, n-местная функция f равна единице не более чем на N наборах и $\log_2 n \ll N \leqslant 2^{n-1}$. Тогда*

$$L_B(f) \lesssim \varrho \cdot \frac{\log_2 \binom{2^n}{N}}{\log_2 \log_2 \binom{2^n}{N}}. \tag{5.17}$$

При больших N для почти равновесных полностью определенных функций справедливость теоремы 5.2 следует непосредственно из леммы 5.3, так как в рассматриваемом случае теорема 5.2 является частным случаем этой леммы. Сформулируем это следствие леммы 5.3 для полностью определенных функций в виде следующего утверждения.

Лемма 5.6. *Пусть $n \to \infty$. Если n-местная булева функция f равна единице на N наборах, где $\log_2 \log_2 \binom{2^n}{N} \sim n$, то*

$$L_B(f) \lesssim \varrho \cdot \frac{\log_2 \binom{2^n}{N}}{\log_2 \log_2 \binom{2^n}{N}}.$$

При меньших значениях веса справедливость теоремы 5.2 следует из лемм 5.7 и 5.8.

Лемма 5.7. *Пусть $n \to \infty$. Если n-местная булева функция f равна единице на N наборах, где $\log_2^4 n \ll N$ и $\log_2 n \ll \log_2 \frac{2^n}{N}$, то*

$$L_B(f) \lesssim \varrho \cdot \frac{\log_2 \binom{2^n}{N}}{\log_2 \log_2 \binom{2^n}{N}}.$$

Доказательство. Оценим правую часть неравенства леммы. Так как

$$\left(\frac{2^n}{N}\right)^N \leqslant \binom{2^n}{N} \leqslant \left(\frac{3\cdot 2^n}{N}\right)^N,$$

то

$$N\log_2\frac{2^n}{N} \leqslant \log_2\binom{2^n}{N} \leqslant N\log_2\frac{2^n}{N} + N\log_2 3.$$

Также нетрудно видеть, что при $n\to\infty$ и $\log_2 n \ll \log_2\frac{2^n}{N}$

$$\log_2\log_2\frac{2^n}{N} \sim \log_2 n, \quad \text{если } N < n^{\log_2 n},$$
$$\log_2\log_2\frac{2^n}{N} \ll \log_2 N, \quad \text{если } N \geqslant n^{\log_2 n}.$$

Поэтому

$$\begin{aligned}\log_2\log_2\binom{2^n}{N} &\sim \log_2\left(N\log_2\frac{2^n}{N}\right) = \\ &= \log_2 N + \log_2\log_2\frac{2^n}{N} \sim \log_2 N + \log_2 n.\end{aligned} \tag{5.18}$$

Следовательно, для правой части неравенства леммы справедливо асимптотическое равенство

$$\frac{\log_2\binom{2^n}{N}}{\log_2\log_2\binom{2^n}{N}} \sim \frac{N\log_2\frac{2^n}{N}}{\log_2 N + \log_2 n}, \tag{5.19}$$

правую часть которого будем далее использовать для оценки сложности функции f.

Пусть f удовлетворяет условиям леммы. Определим набор данных, знание которых позволит достаточно «экономным» способом вычислить ее значение.

Пусть $\boldsymbol{\alpha}_1,\ldots,\boldsymbol{\alpha}_N$ — наборы, на которых f равна единице. Положим $t_1 = |\boldsymbol{\alpha}_1|$ и $t_i = |\boldsymbol{\alpha}_i| - |\boldsymbol{\alpha}_{i-1}|$ для $i = 2,\ldots,N$. Каждое t_i представим набором $\boldsymbol{t}_i$ коэффициентов его двоичного представления длины l_i, в котором старший (правый) разряд равен единице, т. е. $|\boldsymbol{t}_i| = t_i$, и так как $t_i < 2^n$, то $l_i \leqslant n$. Также для каждого $i = 1,\ldots,N$ введем двоичный вектор $\boldsymbol{l}_i$ длины $\lceil\log_2(n+1)\rceil$, для которого $|\boldsymbol{l}_i| = l_i$.

Пусть $\boldsymbol{T} = (\boldsymbol{t}_1\ldots\boldsymbol{t}_i\ldots\boldsymbol{t}_N)$, $\boldsymbol{L} = (\boldsymbol{l}_1\ldots\boldsymbol{l}_i\ldots\boldsymbol{l}_N)$. Вектор $\boldsymbol{T}$ разобьем на

$$q = \left\lceil\frac{N}{p}\right\rceil \tag{5.20}$$

блоков $\boldsymbol{T}_j = (\boldsymbol{t}_{(j-1)p+1}\ldots\boldsymbol{t}_{jp})$, каждый из которых, кроме, возможно, последнего, состоит из p последовательных наборов $\boldsymbol{t}$. Значение параметра p определим позднее. Аналогичным образом разобьем вектор $\boldsymbol{L}$ на блоки $\boldsymbol{L}_j = (\boldsymbol{l}_{(j-1)p+1}\ldots\boldsymbol{l}_{jp})$. Будем говорить, что блок $\boldsymbol{T}_j$ соответствует набору $\boldsymbol{\sigma}$, если

$$|\boldsymbol{\alpha}_{(j-1)p+1}| \leqslant |\boldsymbol{\sigma}| < |\boldsymbol{\alpha}_{jp+1}|,$$

т. е. $\boldsymbol{\sigma}$ находится между $((j-1)p+1)$-м и jp-м единичными наборами f. Наконец введем величины r_i — номера позиций, начиная с которых в век-

торе $\boldsymbol{T}$ располагаются блоки $\boldsymbol{T}_i$, и их двоичные представления — наборы $\boldsymbol{r}_i$ длины $\lceil \log_2 T \rceil$, т. е. $r_i = |\boldsymbol{r}_i|$.

Далее вектор $\boldsymbol{T}$ будем рассматривать как вектор значений частичной $\lceil \log_2 T \rceil$-местной булевой функции t, определенной на первых T наборах $\lceil \log_2 T \rceil$-мерного куба (здесь T — длина $\boldsymbol{T}$), вектор $\boldsymbol{L}$ — как вектор значений функции $l : \{0,1\}^{\lceil \log_2 L \rceil} \to \{0,1\}$, а величины r_i — как значения некоторой функции $r : \{0,1\}^{\lceil \log_2 q \rceil} \to \{0,1\}^{\lceil \log_2 T \rceil}$.

Векторы $\boldsymbol{T}$ и $\boldsymbol{L}$ полностью определяют функцию f, и от их длин зависит сложность вычисления f. Для длины L вектора $\boldsymbol{L}$ справедливо неравенство

$$L = N\lceil \log_2(n+1) \rceil \leqslant N + N \log_2(n+1) \sim N \log_2 n. \tag{5.21}$$

Оценим сверху длину T вектора $\boldsymbol{T}$. Так как длина каждого $\boldsymbol{t}_i$ не превосходит $\lceil \log_2(t_i+1) \rceil \leqslant 1 + \log_2 t_i$, то $T \leqslant \sum\limits_{i=1}^{N} (1 + \log_2 t_i)$, где в силу неравенства Йенсена

$$\frac{1}{N} \sum_{i=1}^{N} \log_2 t_i \leqslant \log_2 \frac{\sum\limits_{i=1}^{N} t_i}{N} \leqslant \log_2 \frac{2^n}{N}.$$

Следовательно,

$$T \leqslant N + N \log_2 \frac{2^n}{N} \sim N \log_2 \frac{2^n}{N}. \tag{5.22}$$

Далее без ограничения общности будем полагать, что в (5.22) достигается асимптотическое равенство, т. е. $T \sim N \log_2 \frac{2^n}{N}$. Также отметим необходимую далее очевидную оценку $T_i \leqslant pn$ длины каждого блока $\boldsymbol{T}_i$.

Теперь покажем, как при помощи функций t, l и r вычислить значение функции f на произвольном наборе $\boldsymbol{\sigma}$. Выполняющую необходимые вычисления схему S представим в виде восьми независимых подсхем.

1. Подсхема S_1 вычисляет номер i блока $\boldsymbol{T}_i$, который соответствует набору $\boldsymbol{\sigma}$. Для этого S_1 сравнивает $\boldsymbol{\sigma}$ с наборами $\boldsymbol{\alpha}_{p+1}, \ldots, \boldsymbol{\alpha}_{(q-1)p+1}$ и определяет пару, для которой $|\boldsymbol{\alpha}_{(i-1)p+1}| \leqslant |\boldsymbol{\sigma}| < |\boldsymbol{\alpha}_{ip+1}|$. Результат представляется двоичным вектором длины q с единственной единичной компонентой на i-м месте. Затем этот вектор преобразуется в двоичное число i. В силу (5.20) нетрудно видеть, что

$$L(\mathsf{S}_1) \asymp qn \asymp \frac{Nn}{p}. \tag{5.23}$$

2. Подсхема S_2 по номеру i вычисляет длину T_i блока $\boldsymbol{T}_i$ и позицию r_i, начиная с которой в векторе $\boldsymbol{T}$ располагается блок $\boldsymbol{T}_i$. Длина блока $\boldsymbol{T}_i$ вычисляется как значение $\lceil \log_2 q \rceil$-местной функции с n компонентами, а позиция r_i — как значение $\lceil \log_2 q \rceil$-местной функции с $\lceil \log_2 T \rceil$ компонентами. Из теоремы 4.3 и (5.20) легко следует, что

$$L(\mathsf{S}_2) \asymp \frac{qn}{\log_2 q} + \frac{q \log_2 T}{\log_2 q} \asymp \frac{Nn}{p \log_2 \frac{N}{p}}. \tag{5.24}$$

3. Подсхема S_3 по вычисленному подсхемой S_2 значению r_i находит вектор $\boldsymbol{T}_i = (\boldsymbol{t}_{(i-1)p+1} \ldots \boldsymbol{t}_{ip})$. Для этого S_3 сначала вычисляет значения функции t

на pn последовательных наборах, начиная с набора $\boldsymbol{r}_i$. Затем в вычисленном векторе S_3 оставляет первые T_i значений и дополняет получившийся вектор нулями до вектора длины qn. Из теоремы 4.2, равенства (5.22) и неравенства (5.18) следует, что при выполнении условия $pn \ll T/\log_2^2 T$ справедливы неравенства

$$L(\mathsf{S}_3) \lesssim \varrho \cdot \frac{T}{\log_2 T} + \mathcal{O}(qn) \lesssim \varrho \cdot \frac{N \log_2 \frac{2^n}{N}}{\log_2 N + \log_2 n} + \mathcal{O}\Big(\frac{Nn}{p}\Big). \tag{5.25}$$

4. Подсхема S_4 по вычисленному подсхемой S_1 номеру блока i находит вектор $\boldsymbol{L}_i = (\boldsymbol{l}_{(i-1)p+1} \ldots \boldsymbol{l}_{ip})$. Для этого S_4 вычисляет значения функции l на $p\lceil\log_2(n+1)\rceil$ последовательных наборах, начиная с набора с номером $(\lceil\log_2(n+1)\rceil((i-1)p+1))$. Из (5.21) следует, что при выполнении условия $p \log_2 n \ll L/\log_2^2 L$ это можно сделать со сложностью

$$L(\mathsf{S}_4) \asymp \frac{L}{\log_2 L} \sim \frac{N \log_2 n}{\log_2 N + \log_2 \log_2 n}. \tag{5.26}$$

5. Подсхема S_5 разбивает вектор $\boldsymbol{L}_i$ на p блоков $\boldsymbol{l}_{(i-1)p+j}$ длины $\lceil\log_2(n+1)\rceil$, вычисляет суммы $a_k = r_i + \sum\limits_{j=1}^{k} l_{(i-1)p+j}$ и таким образом определяет в блоке $\boldsymbol{T}_i$ позиции, в которых начинаются наборы $\boldsymbol{t}_{(i-1)p+1}, \ldots \boldsymbol{t}_{(i-1)p+k}, \ldots \boldsymbol{t}_{ip}$. Легко видеть, что

$$L(\mathsf{S}_5) \asymp pn. \tag{5.27}$$

6. Подсхема S_6 состоит из $p-1$ одинаковых подсхем S_{6k}, где $k \in \{2, \ldots, p\}$, S_{6k} выделяет из $\boldsymbol{T}_i$ его k-й набор $\boldsymbol{t}_{(i-1)p+k}$ и дополняет его справа нулями до набора $\boldsymbol{d}_k$ длины n. Из (4.3) следует, что

$$L(\mathsf{S}_6) \asymp p \cdot n \cdot p \log_2 p = p^2 n \log_2 p. \tag{5.28}$$

7. Подсхема S_7 по номеру i блока $\boldsymbol{T}_i$ вычисляет набор $\boldsymbol{\alpha}_{(i-1)p+1}$. Затем S_7 вычисляет суммы $b_k = |\boldsymbol{\alpha}_{(i-1)p+1}| + \sum\limits_{j=2}^{k} |\boldsymbol{d}_j|$, двоичные представления которых являются единичными наборами $|\boldsymbol{\alpha}_{(i-1)p+k}|$ функции f из i-го блока. Вычисляя $\boldsymbol{\alpha}_{(i-1)p+1}$ как значение $\lceil\log_2 q\rceil$-местной функции с n компонентами, видим, что

$$L(\mathsf{S}_7) \asymp \frac{Nn}{p \log_2 \frac{N}{p}} + pn. \tag{5.29}$$

8. Подсхема S_8 сравнивает $\boldsymbol{\sigma}$ с вычисленными предыдущей подсхемой единичными наборами $\boldsymbol{\alpha}_{(i-1)p+1}, \ldots, \boldsymbol{\alpha}_{ip}$. Если $\boldsymbol{\sigma}$ совпадает с одним из этих наборов, то $f(\boldsymbol{\sigma}) = 1$, если нет, то $f(\boldsymbol{\sigma}) = 0$. Легко видеть, что

$$L(\mathsf{S}_8) \asymp pn. \tag{5.30}$$

Суммируя неравенства (5.23)–(5.30), приходим к асимптотическому неравенству

$$\begin{aligned} L(\mathsf{S}) \lesssim \varrho \cdot \frac{N \log_2 \frac{2^n}{N}}{\log_2 N + \log_2 n} + \mathcal{O}\Bigg(\frac{Nn}{p} + \frac{Nn}{p \log_2 \frac{2^n}{N}} + \frac{Nn}{p} + \\ + \frac{N \log_2 n}{\log_2 N + \log_2 \log_2 n} + pn + p^2 n \log_2 p + \frac{Nn}{p \log_2 \frac{N}{p}} + pn \Bigg). \end{aligned} \tag{5.31}$$

Неравенство (5.31) после очевидных упрощений преобразуется в неравенство

$$L(\mathsf{S}) \lesssim \varrho \cdot \frac{N \log_2 \frac{2^n}{N}}{\log_2 N + \log_2 n} + \mathcal{O}\left(\frac{Nn}{p} + \frac{N \log_2 n}{\log_2 N + \log_2 \log_2 n} + p^2 n \log_2 p\right), \quad (5.32)$$

справедливое, как и (5.31), при выполнении условий

$$pn \ll \frac{N \log_2 \frac{2^n}{N}}{(\log_2 N + \log_2 n)^2}, \qquad p \log_2 n \ll \frac{N \log_2 n}{(\log_2 N + \log_2 \log_2 n)^2},$$

обеспечивающих справедливость оценок (5.25) и (5.26). Нетрудно показать, что в условиях доказываемой леммы справедливость последних неравенств следует из неравенств

$$p \ll \frac{N \log_2 \frac{2^n}{N}}{n(\log_2 N + \log_2 n)^2}, \qquad p \ll \frac{N}{\log_2^2 N}. \quad (5.33)$$

Параметр p подберем так, чтобы при $n \to \infty$ каждое слагаемое в аргументе «$\mathcal{O}$» в (5.32) росло медленнее первого слагаемого в правой части этого неравенства. Для этого достаточно, чтобы выполнялись следующие три условия:

$$\begin{aligned} \frac{Nn}{p} &\ll \frac{N \log_2 \frac{2^n}{N}}{\log_2 N + \log_2 n}, \\ \frac{N \log_2 n}{\log_2 N + \log_2 \log_2 n} &\ll \frac{N \log_2 \frac{2^n}{N}}{\log_2 N + \log_2 n}, \\ p^2 n \log_2 p &\ll \frac{N \log_2 \frac{2^n}{N}}{\log_2 N + \log_2 n}. \end{aligned} \quad (5.34)$$

Первое и последнее из этих условий следуют из неравенств

$$\begin{aligned} p &\gg \frac{n(\log_2 N + \log_2 n)}{\log_2 \frac{2^n}{N}}, \\ p &\ll \left(\frac{N \log_2 \frac{2^n}{N}}{n(\log_2 N + \log_2 n)^2}\right)^{1/2}, \end{aligned} \quad (5.35)$$

а среднее не зависит от p. Так как из условия $\log_2 n \ll \log_2 \frac{2^n}{N}$ доказываемой леммы легко следует, что $N \log_2 n \ll N \log_2 \frac{2^n}{N}$, то среднее неравенство в (5.34) выполняется автоматически.

Суммируя сказанное выше, видим (см. (5.19)), что сложность схемы S асимптотически не превосходит

$$\varrho \cdot \frac{N \log_2 \frac{2^n}{N}}{\log_2 N + \log_2 n} \sim \varrho \cdot \frac{\log_2 \binom{2^n}{N}}{\log_2 \log_2 \binom{2^n}{N}},$$

если (см. (5.33) и (5.35)) найдется такое p, что

$$p \gg \frac{n(\log_2 N + \log_2 n)}{\log_2 \frac{2^n}{N}}, \tag{5.36}$$

$$p \ll \left(\frac{N \log_2 \frac{2^n}{N}}{n(\log_2 N + \log_2 n)^2} \right)^{1/2}, \tag{5.37}$$

$$p \ll \frac{N \log_2 \frac{2^n}{N}}{n(\log_2 N + \log_2 n)^2}, \tag{5.38}$$

$$p \ll \frac{N}{\log_2^2 N}. \tag{5.39}$$

Покажем, что такое p существует. Сделаем это для двух случаев в зависимости от величины N:

1. $N \geqslant n^6$;
2. $\varepsilon(n) \log_2^4 n \ll N < n^6$, где $\varepsilon(n) \to \infty$ при $n \to \infty$.

В первом случае (5.36) следует из неравенств

$$p \gg n \log_2 N \gg \frac{n(\log_2 N + \log_2 n)}{\log_2 \frac{2^n}{N}},$$

а неравенства (5.38) и (5.39) являются следствиями неравенства (5.37), которое, в свою очередь, следует из неравенств

$$p \ll \left(Nn^{-3}\right)^{1/2} \ll \left(\frac{N \log_2 \frac{2^n}{N}}{n(\log_2 N + \log_2 n)^2} \right)^{1/2}.$$

Легко видеть, что в рассматриваемом случае найдется p, удовлетворяющее неравенствам

$$n \log_2 N \ll p \ll \left(Nn^{-3}\right)^{1/2},$$

и следовательно, при таком p справедливы неравенства (5.36)—(5.39).

Во втором случае (5.36) следует из неравенств

$$p \gg \log_2 n \geqslant \frac{n(\log_2 N + \log_2 n)}{\log_2 \frac{2^n}{N}}.$$

Из соотношений

$$\left(\frac{N \log_2 \frac{2^n}{N}}{n(\log_2 N + \log_2 n)^2} \right)^{1/2} \asymp \left(\frac{N}{\log_2^2 n} \right)^{1/2} \ll \frac{N}{\log_2^2 N}$$

следует, что неравенства (5.38) и (5.39), как и в первом случае, являются следствиями неравенства (5.37). Поэтому, если параметр p удовлетворяет неравенствам

$$\log_2 n \ll p \ll \left(\frac{N}{\log_2^2 n} \right)^{1/2}, \tag{5.40}$$

то справедливы неравенства (5.36)—(5.39). Так как в рассматриваемом случае N ограничено снизу функцией $\varepsilon(n) \log_2^4 n$, то (5.40) будет следовать из неравенств

$$\log_2 n \ll p \ll \left(\frac{\varepsilon(n) \log_2^4 n}{\log_2^2 n} \right)^{1/2} = \sqrt{\varepsilon(n)} \log_2 n,$$

которые, очевидно, имеют непустое решение. Лемма доказана.

Лемма 5.8. *Пусть* $n \to \infty$. *Если* n*-местная булева функция* f *равна единице на* N *наборах, где* $\log_2 n \ll N$ *и* $\log_2 N \ll \log_2 n$, *то*

$$L_B(f) \lesssim \varrho \cdot \frac{\log_2 \binom{2^n}{N}}{\log_2 \log_2 \binom{2^n}{N}}.$$

Доказательство. Пусть $\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_N$ — наборы, на которых f равна единице. Индукцией по числу наборов нетрудно показать, что найдутся N компонент, в которых наборы $\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_N$ различаются. Без ограничения общности будем считать, что такими компонентами будут первые N компонент. Из этих компонент наборов $\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_N$ составим наборы $\boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_N$ так, что каждый $\boldsymbol{\beta}_i$ будет началом $\boldsymbol{\alpha}_i$ длины N. Составим таблицу T из n строк и N столбцов, в которой i-му столбцу соответствует двоичный набор $\boldsymbol{\gamma}$ длины $\lceil \log_2 N \rceil$, $|\boldsymbol{\gamma}| = i - 1$, сам столбец совпадает с набором $\boldsymbol{\alpha}_i$, а j-ю строку таблицы будем рассматривать как вектор значений $\lceil \log_2 N \rceil$-местной функции f_j, определенной на первых N наборах $\lceil \log_2 N \rceil$-мерного булева куба.

Пусть $\boldsymbol{\sigma} \in \{0,1\}^n$ и $\boldsymbol{\tau} \in \{0,1\}^N$ — начало $\boldsymbol{\sigma}$. Покажем, как, используя наборы $\boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_N, \boldsymbol{\tau}$ и функции $f_1, \ldots, f_n$, вычислить значение $f(\boldsymbol{\sigma})$.

Выполняющую необходимые вычисления схему S представим в виде трех независимых подсхем.

1. Подсхема S_1 сравнивает набор $\boldsymbol{\tau}$ с наборами $\boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_N$ и в результате сравнения определяет индекс i так, что

$$i = \begin{cases} 0, & \text{если } \boldsymbol{\tau} \notin \{\boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_N\}; \\ j, & \text{если } \boldsymbol{\tau} = \boldsymbol{\beta}_j. \end{cases}$$

Так как $\log_2 N \ll \log_2 n$, то нетрудно видеть, что

$$L(\mathsf{S}_1) \asymp N^2 \asymp 2^{o(\log_2 n)} \ll \frac{Nn}{\log_2 n}. \tag{5.41}$$

2. Подсхема S_2 по номеру i (если $i > 0$) вычисляет набор $\boldsymbol{\alpha}_i$, началом которого является набор $\boldsymbol{\beta}_i$. Для этого S_2 находит значения функций $f_1, \ldots, f_n$ на наборе $\boldsymbol{\gamma}$ таком, что $|\boldsymbol{\gamma}| = i - 1$. Для построения подсхемы S_2 можно воспользоваться леммой 4.2 (или теоремой 4.4). Полагая $n = R$ и $N = S$, видим, что условия $1 \ll \log_2 N - \log_2 \log_2 n \ll \log_2 n$ леммы 4.2 легко следуют из условий $\log_2 n \ll N$ и $\log_2 N \ll \log_2 n$ доказываемой леммы. Следовательно,

$$L(\mathsf{S}_2) \lesssim \varrho \cdot \frac{Nn}{\log_2 Nn}. \tag{5.42}$$

3. Подсхема S_3 вычисляет $f(\boldsymbol{\sigma})$, сравнивая вычисленный подсхемой S_2 набор $\boldsymbol{\alpha}_i$ с набором $\boldsymbol{\sigma}$. Если наборы совпали, то $f(\boldsymbol{\sigma}) = 1$, если нет, то $f(\boldsymbol{\sigma}) = 0$. Очевидно, что

$$L(\mathsf{S}_3) \asymp n \ll \frac{Nn}{\log_2 n}. \tag{5.43}$$

Суммируя неравенства (5.41)–(5.43) и учитывая равенство (5.19), видим, что

$$\begin{aligned} L(\mathsf{S}) &\lesssim \varrho \cdot \frac{Nn}{\log_2 Nn} + o\left(\frac{Nn}{\log_2 n}\right) + \mathcal{O}(n) \sim \\ &\sim \varrho \cdot \frac{Nn}{\log_2 Nn} \sim \varrho \cdot \frac{N \log_2 \frac{2^n}{N}}{\log_2 N + \log_2 n} \sim \varrho \cdot \log_2 \binom{2^n}{N} \Big/ \log_2 \log_2 \binom{2^n}{N}. \end{aligned} \tag{5.44}$$

Лемма доказана.

Следующую лемму приведем без доказательства. Утверждение леммы 5.9 является простым следствием доказательства леммы 5.8, в котором при условии $N = \mathcal{O}(\log_2 n)$ изменяются только неравенства (5.41) и (5.42), правые части которых превращаются в $\mathcal{O}(n)$.

Лемма 5.9. *Пусть $n \to \infty$. Если n-местная булева функции f равна единице на $N = \mathcal{O}(\log_2 n)$ наборах, то*

$$L_B(f) = \mathcal{O}(n).$$

Доказательство теоремы 5.2. Сначала докажем справедливость (5.17) для функций, у которых ровно N единичных наборов. Сделаем это, показав, что для любого N, удовлетворяющего условиям теоремы, справедливы условия хотя бы одной из лемм 5.6–5.8.

1. Пусть $2^n / n^{\log_2 n} \leqslant N \leqslant 2^{n-1}$. Тогда при $n \to \infty$

$$\log_2 \log_2 \binom{2^n}{N} \geqslant \log_2 \left(N \log_2 \frac{2^n}{N} \right) \geqslant \log_2 \left(\frac{2^n}{n^{\log_2 n}} \log_2 n^{\log_2 n} \right) =$$

$$= \log_2 \frac{2^n \log_2^2 n}{n^{\log_2 n}} = n - \log_2^2 n + 2 \log_2 \log_2 n \sim n.$$

В этом случае (5.17) следует из леммы 5.6.

2. Пусть $\log_2^4 n \ll N < 2^n / n^{\log_2 n}$. Тогда

$$\log_2 \frac{2^n}{N} \geqslant \log_2 n^{\log_2 n} = \log_2^2 n \gg \log_2 n.$$

В этом случае (5.17) следует из леммы 5.7.

3. Пусть $\log_2 n \ll N < \log_2^5 n$. Тогда $\log_2 N \ll \log_2 n$ и (5.17) следует из леммы 5.8.

Таким образом, установлена справедливость (5.17) для функций, у которых ровно N единичных наборов. Теперь утверждение теоремы следует из монотонности правой части (5.17) по N при $N \leqslant 2^{n-1}$. Теорема доказана.

Сформулируем простое следствие теоремы 5.2 и леммы 5.9, убрав из формулировки теоремы 5.2 ограничения на N.

Теорема 5.3. *Пусть $n \to \infty$, B — полный конечный базис, ϱ — минимальный приведенный вес B, n-местная функция f равна единице не более чем на N наборах. Тогда*

$$L_B(f) \lesssim \varrho \cdot \frac{\log_2 \binom{2^n}{N}}{\log_2 \log_2 \binom{2^n}{N}} + \mathcal{O}(n).$$

5.5. Общий случай. Главным результатом этого раздела является теорема 5.4 о сложности частичных булевых функций ограниченного веса.

Теорема 5.4. *Пусть $n \to \infty$, B — полный конечный базис с минимальным приведенным весом ϱ, $\boldsymbol{D} \subseteq \{0,1\}^n$, функция $f : \boldsymbol{D} \to \{0,1\}$ равна единице не более чем на N наборах из области $\boldsymbol{D}$. Если параметры n, D, N такие, что $D \geqslant n$ и $\log_2 \log_2 D \ll N \leqslant \frac{1}{2} D$, то*

$$L_B(f) \lesssim \varrho \cdot \frac{\log_2 \binom{D}{N}}{\log_2 \log_2 \binom{D}{N}} + \mathcal{O}\left(\frac{n \log_2 D}{\log_2 n} \right).$$

Доказательство теоремы 5.4 похоже на доказательство теоремы 5.1 и разбивается на три случая, которые рассматриваются в следующих леммах. Первая из этих лемм — простое следствие теоремы 5.1.

Лемма 5.10. *Пусть $n \to \infty$, B — полный конечный базис с минимальным приведенным весом ϱ, $\boldsymbol{D} \subseteq \{0,1\}^n$, функция $f : \boldsymbol{D} \to \{0,1\}$ равна единице не более чем на N наборах из области $\boldsymbol{D}$. Если параметры n, D, N такие, что $D \geqslant 2^{n/3}$ и $Dn^{-\log_2 n} \leqslant N \leqslant \frac{1}{2}D$, то*

$$L_B(f) \lesssim \varrho \cdot \frac{\log_2 \binom{D}{N}}{\log_2 \log_2 \binom{D}{N}} + \mathcal{O}\left(\frac{n \log_2 D}{\log_2 n}\right).$$

Доказательство. Так как

$$\log_2 D > \log_2 N \geqslant \log_2 D - \log_2 n^{-\log_2 n} \sim \log_2 D,$$

то $\log_2 N \sim \log_2 D$ и утверждение леммы следует из теоремы 5.1. Лемма доказана.

Вторая лемма — аналог леммы 5.4 из доказательства теоремы 5.1.

Лемма 5.11. *Пусть $n \to \infty$, B — полный конечный базис с минимальным приведенным весом ϱ, $\boldsymbol{D} \subseteq \{0,1\}^n$, функция $f : \boldsymbol{D} \to \{0,1\}$ равна единице не более чем на N наборах из области $\boldsymbol{D}$. Если параметры n, D, N такие, что $D \geqslant 2^{n/3}$ и $\log_2 \log_2 D \ll N \leqslant Dn^{-\log_2 n}$, то*

$$L_B(f) \lesssim \varrho \cdot \frac{\log_2 \binom{D}{N}}{\log_2 \log_2 \binom{D}{N}} + \mathcal{O}\left(\frac{n \log_2 D}{\log_2 n}\right).$$

Доказательство. Положим $\boldsymbol{D}_0 = \{\boldsymbol{x} \mid f(\boldsymbol{x}) = 0\}$, $\boldsymbol{D}_1 = \{\boldsymbol{x} \mid f(\boldsymbol{x}) = 1\}$ и $k = 3\log_2 n$. К областям $\boldsymbol{D}_0$ и $\boldsymbol{D}_1$ применим лемму 2.5, полагая, что $\boldsymbol{A} = \boldsymbol{D}_1$, $\boldsymbol{B} = \boldsymbol{D}_0$. Так как $D_0 < D$ и $D_1 \leqslant N$, то в силу этой леммы для $m = \lceil \log_2 D + 3\log_2 n \rceil$ найдется такой линейный оператор $\mathscr{L} : \{0,1\}^n \to \{0,1\}^m$, что

$$L_B(\mathscr{L}) = \mathcal{O}\left(\frac{n \log_2 D}{\log_2 n}\right), \tag{5.45}$$

а множество

$$\boldsymbol{C} = \{(\boldsymbol{x}, \boldsymbol{y}) \mid \boldsymbol{x} \in \boldsymbol{D}_0, \boldsymbol{y} \in \boldsymbol{D}_1, \mathscr{L}(\boldsymbol{x}) = \mathscr{L}(\boldsymbol{y})\}$$

состоит не более чем из Nn^{-3} пар наборов. Далее введем определенную на $\{0,1\}^m$ m-местную булеву функцию

$$g(\boldsymbol{z}) = \begin{cases} 1, & \text{если } \exists\, \boldsymbol{x} \in \boldsymbol{D}_1 \text{ такой, что } \boldsymbol{z} = \mathscr{L}(\boldsymbol{x}), \\ & \quad \text{и } \nexists\, \boldsymbol{y} \in \boldsymbol{D}_0 \text{ такой, что } \boldsymbol{z} = \mathscr{L}(\boldsymbol{y}), \\ 0 & \text{в противном случае} \end{cases}$$

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

$$L_B(f) \leqslant L_B(g) + L_B(h) + L_B(\mathscr{L}) + L_B(\oplus). \tag{5.46}$$

Оценим сложность функции g. В силу неравенств $N \gg \log_2 n > \log_2 m$ для этого можно воспользоваться теоремой 5.2. Из этой теоремы, неравенства $D/N \geqslant n^{\log_2 n}$ и неравенств

$$\log_2 \binom{2^m}{N} \leqslant \log_2 \binom{2Dn^3}{N} \leqslant N \log_2 \frac{3 \cdot 2Dn^3}{N} = \\ = N \log_2 \frac{D}{N} + 3N \log_2 n + N \log_2 6 \sim N \log_2 \frac{D}{N}$$

следует, что

$$L_B(g) \lesssim \varrho \cdot \frac{\log_2 \binom{2^m}{N}}{\log_2 \log_2 \binom{2^m}{N}} \lesssim \varrho \cdot \frac{N \log_2 \frac{D}{N}}{\log_2 N + \log_2 \log_2 \frac{D}{N}}. \tag{5.47}$$

С другой стороны,

$$\log_2 \binom{D}{N} \geqslant \log_2 \left(\frac{D}{N}\right)^N = N \log_2 \frac{D}{N}.$$

Поэтому в силу (5.47)

$$L_B(g) \lesssim \varrho \cdot \frac{\log_2 \binom{D}{N}}{\log_2 \log_2 \binom{D}{N}}. \tag{5.48}$$

Для вычисления функции h (если она отлична от тождественного нуля) воспользуемся ее совершенной дизъюнктивной формой, полагая, что вне области $\boldsymbol{D}$ эта функция равна нулю. Так как $N \leqslant \log_2 \binom{D}{N}$ при $N \leqslant \frac{1}{2}D$, то

$$L_B(h) = \mathcal{O}\left(\frac{Nn}{n^3}\right) = \mathcal{O}\left(\frac{N}{n^2}\right) \ll \frac{\log_2 \binom{D}{N}}{\log_2 \log_2 \binom{D}{N}}. \tag{5.49}$$

Таким образом, в силу (5.45), (5.46), (5.48) и (5.49)

$$L_B(f) \lesssim \varrho \cdot \frac{\log_2 \binom{D}{N}}{\log_2 \log_2 \binom{D}{N}} + \mathcal{O}\left(\frac{n \log_2 D}{\log_2 n}\right). \tag{5.50}$$

Лемма доказана.

Третья лемма — аналог леммы 5.5 из доказательства теоремы 5.1.

Лемма 5.12. *Пусть $n \to \infty$, B — полный конечный базис с минимальным приведенным весом ϱ, $\boldsymbol{D} \subseteq \{0,1\}^n$, функция $f : \boldsymbol{D} \to \{0,1\}$ равна единице не более чем на N наборах из области $\boldsymbol{D}$. Если параметры n, D, N такие, что $n \leqslant D \leqslant 2^{n/3}$ и $\log_2 \log_2 D \ll N \leqslant \frac{1}{2}D$, то*

$$L_B(f) \lesssim \varrho \cdot \frac{\log_2 \binom{D}{N}}{\log_2 \log_2 \binom{D}{N}} + \mathcal{O}\left(\frac{n \log_2 D}{\log_2 n}\right).$$

Доказательство. Положим $m = \lfloor 2\log_2 D \rfloor$. К области $\boldsymbol{D}$ применим лемму 2.6. В результате найдется инъективный на $\boldsymbol{D}$ линейный оператор $\mathscr{L}\colon \{0,1\}^n \to \{0,1\}^m$, для которого

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

Далее введем определенную на области $\mathscr{L}(\boldsymbol{D})$ частичную m-местную булеву функцию

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

Функция g равна единице не более чем на N наборах из области $\mathscr{L}(\boldsymbol{D})$ и $f(\boldsymbol{x}) = g(\mathscr{L}(\boldsymbol{x}))$. Так как $m = \lfloor 2\log_2 D \rfloor$, то в зависимости от величины N для оценки сложности g можно воспользоваться либо леммой 5.10, либо леммой 5.11. В каждом из этих случаев

$$L_B(g) \lesssim \varrho \cdot \frac{\log_2 \binom{D}{N}}{\log_2 \log_2 \binom{D}{N}} + \mathcal{O}\left(\frac{m\log_2 D}{\log_2 m}\right).$$

Следовательно,

$$L_B(f) \lesssim \varrho \cdot \frac{\log_2 \binom{D}{N}}{\log_2 \log_2 \binom{D}{N}} + \mathcal{O}\left(\frac{n\log_2 D}{\log_2 n}\right).$$

Лемма доказана.

Доказательство теоремы 5.4. Если $\log_2 D \geqslant \frac{1}{3}n$, то утверждение теоремы следует из леммы 5.10 и леммы 5.11. Если $\log_2 D \leqslant \frac{1}{3}n$, то утверждение теоремы следует из леммы 5.12.

§ 6. Частичные функции ограниченного веса — 2

В этом разделе в теореме 6.1 завершается доказательство верхней оценки сложности вычисления частичных булевых функций ограниченного веса схемами в произвольном полном конечном базисе для всех значений параметров N и D. Полученный результат, — неравенство (6.1), можно считать окончательным: если правая часть в (6.1) растет быстрее числа переменных, то оценка асимптотически точна, в противном случае точна по порядку.

6.1. Теорема о сложности частичных функций.

Теорема 6.1. *Пусть $n \to \infty$, B — полный конечный базис с минимальным приведенным весом ϱ, $\boldsymbol{D} \subseteq \{0,1\}^n$, функция $f\colon \boldsymbol{D} \to \{0,1\}$ равна единице не более чем на N наборах из области $\boldsymbol{D}$. Тогда*

$$L_B(f) \lesssim \varrho \cdot \frac{\log_2 \binom{D}{N}}{\log_2 \log_2 \binom{D}{N}} + \mathcal{O}(n). \tag{6.1}$$

Без ограничения общности будем считать*), что $D \geqslant n$ и $N \leqslant \frac{1}{2}D$. При таких параметрах для сложности любой удовлетворяющей условиям теоремы функции f из теоремы 5.4 следует неравенство

$$L_B(f) \lesssim \varrho \cdot \frac{\log_2 \binom{D}{N}}{\log_2 \log_2 \binom{D}{N}} + \mathcal{O}\left(\frac{n \log_2 D}{\log_2 n}\right), \tag{6.2}$$

которое отличается от неравенства теоремы 6.1 только вторым слагаемым. Это слагаемое определяется сложностью линейных операторов, используемых в доказательстве теоремы 5.4, и растет быстрее $\mathcal{O}(n)$, только если $\log_2 D \gg \log_2 n$. Определим, при каких значениях N второе слагаемое растет медленнее первого и его рост не оказывает заметного влияния на сумму в правой части (6.2).

Пусть $n^2 \ll N \leqslant D/2$. При таких N и D для слагаемых в (6.2) справедливы неравенства

$$\begin{gathered} \frac{\log_2 \binom{D}{N}}{\log_2 \log_2 \binom{D}{N}} \geqslant \frac{\log_2 \binom{2N}{N}}{\log_2 \log_2 \binom{2N}{N}} \geqslant \frac{N}{\log_2 N} \gg \frac{n^2}{\log_2 n} \gg n, \\ \frac{n \log_2 D}{\log_2 n} \leqslant \frac{n \log_2 2^n}{\log_2 n} \leqslant \frac{n^2}{\log_2 n}, \end{gathered} \tag{6.3}$$

из которых следует, что в (6.2) первое слагаемое растет быстрее второго и быстрее n и, следовательно, $L_B(f)$ асимптотически не превосходит первого слагаемого, т. е.

$$L_B(f) \lesssim \varrho \cdot \frac{\log_2 \binom{D}{N}}{\log_2 \log_2 \binom{D}{N}} + \mathcal{O}(n), \quad \text{где } n^2 \ll N \leqslant D/2. \tag{6.4}$$

Поэтому для доказательства теоремы 6.1 достаточно показать справедливость неравенства (6.1) только для небольших значений N, например **) для $N < n^3$.

Сделаем это, воспользовавшись фрагментами доказательства теоремы 5.4, в которых линейные операторы из лемм 2.4–2.6, разделяющие и почти разделяющие непересекающиеся множества, заменим их аналогами меньшей сложности. Новые операторы, обладая лишь немного худшими «разделяющими» возможностями, вычисляются схемами линейной сложности. Существование таких операторов было установлено в [26]. Как и в [26], каждый такой оператор является композицией двух операторов. Первый оператор, увеличивая размерность исходного пространства в четыре раза, преобразует любой ненулевой набор в набор, вес которого пропорционален его длине. Существование таких операторов было установлено в [25]. Ниже этот факт доказан в леммах 6.1–6.4, доказательство которых следует в основном работам [29, 30] и ранее было представлено в [16]. Затем в лемме 6.5 показывается, что для любой области, состоящей из наборов большого веса, существует «хороший» оператор, для которого только небольшое число наборов области может принадлежать его ядру и ранг которого

*) См. Введение.

**) Уменьшение N и/или привлечение неравенства $\log_2 D \gg \log_2 n$ не позволят заметно упростить приводимое далее доказательство теоремы 6.1.

близок к логарифму размера области. Наконец, в леммах 6.6–6.8 показывается, что на основе композиции линейных операторов из лемм 6.4 и 6.5 можно получить подходящие для вычисления частичных булевых функций линейные операторы, использование которых превращает второе слагаемое в неравенстве теоремы 5.4 в $\mathcal{O}(n)$.

6.2. Линейные операторы. Напомним, что i-я строка булевой матрицы покрывает ее j-й столбец, если в этой матрице на пересечении i-й строки и j-го столбца стоит единица.

Лемма 6.1. *Существует такая постоянная $\delta > 0$, что для любого достаточно большого n существует двоичная матрица $M_{2n,n}$ из $2n$ строк и n столбцов, в каждой строке которой находится ровно 7 единиц, и в которой*

$$\begin{aligned}&\text{для каждого } k, \text{ не превосходящего } 2n\delta, \text{ любые}\\ &k \text{ строк покрывают более чем } 4k \text{ столбцов.}\end{aligned} \tag{6.5}$$

Доказательство. Пусть R — множество всех матриц, состоящих из $2n$ строк и n столбцов, во всех строках которых находится ровно 7 единиц. Оценим величину N, равную отношению числа тех матриц из R, которые не обладают свойством (6.5), к числу всех матриц из R. Нетрудно видеть, что k строк, в которых единицы сосредоточены на пересечении не более чем с $4k$ столбцами, можно выбрать $\binom{2n}{k}$ способами, а соответствующие им столбцы — $\binom{n}{4k}$ способами, единицы в выбранных строках можно расставить не более чем $\binom{4k}{7}^k$ способами, в оставшихся строках это можно сделать $\binom{n}{7}^{2n-k}$ способами. Поэтому

$$\begin{aligned}N &\leqslant \sum_{k=1}^{2n\delta} \binom{2n}{k}\binom{n}{4k}\binom{4k}{7}^k\binom{n}{7}^{2n-k}\binom{n}{7}^{-2n} =\\ &= \sum_{k=1}^{2n\delta} \binom{2n}{k}\binom{n}{4k}\binom{4k}{7}^k\binom{n}{7}^{-k} \leqslant\\ &\leqslant \sum_{k=1}^{2n\delta}\left(\frac{3\cdot 2n}{k}\right)^k\left(\frac{3\cdot n}{4k}\right)^{4k}\left(\frac{4k(4k-1)\dots(4k-6)}{n(n-1)\dots(n-6)}\right)^k \leqslant\\ &\leqslant \sum_{k=1}^{2n\delta}\left(\frac{3\cdot 2n}{k}\right)^k\left(\frac{3n}{4k}\right)^{4k}\left(\frac{4k}{n}\right)^{7k} = \sum_{k=1}^{2n\delta} 3^{5k}2^{7k}\left(\frac{k}{n}\right)^{2k} < \sum_{k=1}^{2n\delta}\left(3^5 2^8\delta^2\right)^k.\end{aligned}$$

Нетрудно видеть, что при при выполнении неравенства $3^5 2^8\delta^2 \leqslant 2^{-1}$ (которое, очевидно, справедливо при $\delta < 2^{-9}$) отношение N будет меньше единицы и, следовательно, найдется матрица, удовлетворяющая условиям леммы. Лемма доказана.

Лемма 6.2. *Существует такая постоянная $\delta > 0$, что для любого достаточно большого n существует двоичная матрица $M_{2n,n}$ из $2n$ строк и n столбцов, в каждой строке которой находится ровно 7 единиц и в которой при любом k, не превосходящем $2n\delta$, в каждой подматрице, образованной k строками, есть более k столбцов содержащих ровно один единичный элемент.*

Доказательство. Пусть матрица M удовлетворяет условию (6.5) из леммы 6.1. В этой матрице произвольным образом выберем k строк и составим из них подматрицу M' матрицы M. Пусть R_1 обозначает число столбцов, покрываемых ровно одной из выбранных строк, а $R_{\geqslant 2}$ — число столбцов, покрываемых более чем одной такой строкой. Другими словами, R_1 равно числу столбцов подматрицы M', содержащих ровно по одному единичному элементу, а $R_{\geqslant 2}$ равно числу столбцов с более чем одним единичным элементом. В силу леммы 6.1 величины R_1 и $R_{\geqslant 2}$ удовлетворяют следующим неравенствам:

$$R_1 + R_{\geqslant 2} > 4k,$$
$$R_1 + 2R_{\geqslant 2} \leqslant 7k.$$

Исключая из этих неравенств $R_{\geqslant 2}$, имеем

$$R_1 > 4k - R_{\geqslant 2} \geqslant 4k - \frac{1}{2}\left(7k - R_1\right) = \frac{1}{2}k + \frac{1}{2}R_1,$$

т. е. $R_1 > k$. Лемма доказана.

Лемма 6.3. *Пусть $M_{2n,n}$ — матрица из леммы* 6.2. *Тогда для любого двоичного набора $\boldsymbol{v}$ веса k, где $k \leqslant 2n\delta$, произведение $\boldsymbol{v}\cdot M_{2n,n}$ содержит более k единичных элементов — $\|\boldsymbol{v}\cdot M_{2n,n}\| > \|\boldsymbol{v}\|$.*

Доказательство. Пусть в наборе $\boldsymbol{v}$ компоненты $v_{i_1}, \ldots, v_{i_k}$ — ненулевые. В матрице $M_{2n,n}$ рассмотрим подматрицу M, образованную строками с номерами $i_1, \ldots, i_k$. В силу леммы 6.2 в этой подматрице найдутся столбцы с номерами $j_1, \ldots, j_s$ где $s > k$, каждый из которых содержит ровно один единичный элемент. Легко видеть, что для любого j_i из $\{j_1, \ldots, j_s\}$ скалярное произведение $\boldsymbol{v}$ и j_i-го столба матрицы $M_{2n,n}$ равно единице. Следовательно, произведение $\boldsymbol{v}\cdot M_{2n,n}$ содержит $s > k$ единичных элементов. Лемма доказана.

Далее в леммах 6.4–6.8 оценивается сложность вычисления линейных операторов схемами в базисе $\{\oplus\}$ с точностью до постоянного множителя. Так как $L_B(\mathscr{L}) \leqslant L_B(\oplus)\cdot L_{\{\oplus\}}(\mathscr{L})$ для любого полного конечного базиса B и любого линейного оператора $\mathscr{L}$, то все верхние оценки сложности в леммах 6.4–6.8 справедливы и для схем в базисе B.

Лемма 6.4. *Существует такая постоянная $0 < \gamma < 1$, что для любого достаточно большого n найдется такой линейный оператор $\mathscr{G}_{n,4n}\colon \{0,1\}^n \to \{0,1\}^{4n}$ с матрицей $G_{n,4n}$, что $\|\boldsymbol{v}\cdot G_{n,4n}\| \geqslant \gamma n$ для любого ненулевого вектора $\boldsymbol{v}$ и $L_{\{\oplus\}}(\mathscr{G}_{n,4n}) = \mathcal{O}(n)$.*

Доказательство. Лемму докажем для $n = 2^k m$ индукцией по k. В основание индукции положим оператор $\mathscr{G}_{m,4m}(\boldsymbol{v}) = (\boldsymbol{v}, \boldsymbol{v}, \boldsymbol{v}, \boldsymbol{v})$, где m — минимально возможное, при котором существует матрица $M_{4m,2m}$ в лемме 6.1. Очевидно, что в этом случае $\gamma = 4/m$ и $L_{\{\oplus\}}(G_{m,4m}) = 0$.

Теперь допустим, что удовлетворяющий условиям линейный оператор $\mathscr{G}_{n,4n}$ с матрицей $G_{n,4n}$ существует при некотором $n \geqslant m$. Используя этот оператор, построим оператор $\mathscr{G}_{2n,8n}$. Пусть $\boldsymbol{v}$ — вектор длины $2n$, $\boldsymbol{v}' = \boldsymbol{v}\cdot M_{2n,n}$ — вектор длины n, $\boldsymbol{w} = \boldsymbol{v}'\cdot G_{n,4n}$ — вектор длины $4n$, $\boldsymbol{u} = \boldsymbol{w}\cdot M_{4n,2n}$ — вектор длины $2n$. Тогда оператор $\mathscr{G}_{2n,8n}$ определим равенством $\mathscr{G}_{2n,8n}(\boldsymbol{v}) = (\boldsymbol{v}, \boldsymbol{w}, \boldsymbol{u})$. Покажем, что для матрицы

$$G_{2n,8n} = \Big(E_{2n} \mid M_{2n,n}\cdot G_{n,4n} \mid M_{2n,n}\cdot\big(G_{n,4n}\cdot M_{4n,2n}\big)\Big)$$

такого оператора неравенство

$$\|\boldsymbol{v}\cdot G_{2n,8n}\|\geqslant 2n\gamma \tag{6.6}$$

справедливо для любого ненулевого вектора $\boldsymbol{v}$ длины $2n$ с постоянной $\gamma=\min\left(\delta,\frac{4}{m}\right)$, где δ — постоянная из леммы 6.3.

Если $\|\boldsymbol{v}\|\geqslant 2n\gamma$, то, очевидно, имеет место и неравенство (6.6). Если вес ненулевого вектора $\boldsymbol{v}$ меньше, чем $2n\gamma$, то в силу леммы 6.3 вес вектора $\boldsymbol{v}'$ больше нуля и в силу предположения индукции $\|\boldsymbol{w}\|\geqslant n\delta$. Если при этом справедливо более сильное неравенство $\|\boldsymbol{w}\|\geqslant 2n\gamma$, то (6.6) также справедливо. Если же $n\gamma<\|\boldsymbol{w}\|<2n\gamma$, то в силу леммы 6.3 вес вектора $\boldsymbol{u}$ больше веса вектора $\boldsymbol{w}$ и поэтому $\|\boldsymbol{v}\cdot G_{2n,8n}\|>\|\boldsymbol{w}\|+\|\boldsymbol{u}\|>2n\gamma$.

Покажем, что $L_{\{\oplus\}}(\mathscr{G}_{2n,8n})=\mathscr{O}(n)$. Допустим, что $L_{\{\oplus\}}(\mathscr{G}_{n,4n})\leqslant 42n$ при $n>m$. Так как сложность линейного оператора не превосходит числа единичных элементов его матрицы, а сложность композиции линейных операторов не превосходит суммы их сложностей, то $L_{\{\oplus\}}(\mathscr{M}_{2n,n})\leqslant 14n$ и для оператора $\mathscr{G}_{2n,8n}$ с матрицей

$$G_{2n,8n}=\left(E_{2n}\mid M_{2n,n}\cdot G_{n,4n}\mid\left(M_{2n,n}\cdot G_{n,4n}\right)\cdot M_{4n,2n}\right)$$

справедливо неравенство

$$\begin{aligned}L_{\{\oplus\}}(\mathscr{G}_{2n,8n})&\leqslant L_{\{\oplus\}}(\mathscr{M}_{2n,n})+L_{\{\oplus\}}(\mathscr{G}_{n,4n})+L_{\{\oplus\}}(\mathscr{M}_{4n,2n})\leqslant\\&\leqslant 14n+42n+28n=42\cdot 2n.\end{aligned}$$

Лемма доказана.

Доказательство следующей леммы близко к доказательству леммы 5.1, в котором используется такой же жадный алгоритм построения желаемого объекта. Более короткое вероятностное доказательство существования линейного оператора, аналогичного оператору из леммы 6.5, можно найти в [16].

Лемма 6.5. *Для любой постоянной $\gamma\in(0,1/2)$ и любой постоянной $\varepsilon>0$ существует такое натуральное N, что для каждого $n\geqslant N$ и любого множества $\boldsymbol{R}=\{\boldsymbol{r}_i\}\subseteq\{0,1\}^n$, в котором вес каждого набора не меньше $d=\gamma n$ и $R\geqslant n$, найдется такой линейный оператор $\mathscr{H}\colon\{0,1\}^n\to\{0,1\}^m$, что не более $2^{-(1-\varepsilon)m}R$ наборов из $\boldsymbol{R}$ принадлежат ядру $\mathscr{H}$ и $L_{\{\oplus\}}(\mathscr{H})=\mathscr{O}\left(m\frac{1}{\gamma}\log_2\frac{1}{\varepsilon}\right)$.*

Доказательство. Составим таблицу T из R столбцов, соответствующих наборам $\boldsymbol{r}$ из множества $\boldsymbol{R}$, и $\binom{n}{s}$ строк, соответствующих n-местным линейным булевым функциям $l(\boldsymbol{x})=\alpha_1x_1\oplus\ldots\oplus\alpha_nx_n$ с нечетным числом существенных аргументов s, где s — некоторая постоянная, значение которой определяется значением ε. На пересечении столбца, соответствующего набору $\boldsymbol{r}$, и строки, соответствующей функции l, поставим значение $l(\boldsymbol{r})$.

Для доказательства леммы достаточно показать, что в таблице T найдется набор из m строк, покрывающих в совокупности не менее чем $R-2^{-(1-\varepsilon)m}R$ столбцов, так как функции, соответствующие этим

строкам, сформируют требуемый оператор $\mathscr{H}$: если i-я строка покрывает j-й столбец, то i-я функция на j-м наборе равна единице, и этот набор не попадает в ядро. Такой набор строк будем формировать последовательно, взяв в качестве первой строки набора строку, покрывающую максимальное число столбцов, и добавляя в него на каждом шаге новую строку, покрывающую максимальное число еще не покрытых столбцов.

Оценим число единиц в T. Сделаем это, оценив число единиц в произвольном столбце таблицы. Пусть в наборе $\boldsymbol{r}_j$ содержится p единиц и q нулей, где $p \geqslant \gamma n$ и $p+q=n$. Тогда в j-м столбце таблицы находится

$$A = \sum_{\text{все четные } i} \binom{p}{s-i}\binom{q}{i} = \sum_{i=0}^{\min\left(\frac{s}{2}, \left\lfloor \frac{q}{2} \right\rfloor\right)} \binom{p}{s-2i}\binom{q}{2i}$$

единиц,

$$B = \sum_{\text{все нечетные } i} \binom{p}{s-i}\binom{q}{i} = \sum_{i=0}^{\min\left(\frac{s}{2}, \left\lfloor \frac{q}{2} \right\rfloor\right)} \binom{p}{s-2i+1}\binom{q}{2i-1}$$

нулей, и, очевидно, для суммы этих величин справедливо равенство

$$A + B = \binom{n}{s} = \binom{p+q}{s} = \sum_{i=0}^{\min(s,q)} \binom{p}{s-i}\binom{q}{i}. \tag{6.7}$$

Рассмотрим отношение

$$\binom{p}{s-i}\binom{q}{i} \Big/ \binom{p}{s-i-1}\binom{q}{i+1} = \frac{p-s+i+1}{s-i} \cdot \frac{i+1}{q-i} \tag{6.8}$$

двух соседних слагаемых в сумме из последнего равенства и определим значения параметра i, при которых это отношение не больше единицы. Из неравенства

$$\begin{aligned} 0 \geqslant (p-s+i+1)(i+1) - (s-i)(q-i) = \\ = i^2 + i(p-s+2) + (p-s+1) - i^2 + i(q+s) - qs = \\ = i(q+p+2) - qs + p - s + 1 = \\ = i(q+p+2) - (qs+q+s+1) + (p+q+2) = \\ = i(n+2) - (q+1)(s+1) + (n+2) \end{aligned}$$

следует, что отношение (6.8) не возрастает при

$$i \leqslant \frac{(q+1)(s+1)-(n+2)}{n+2} = \frac{(q+1)(s+1)}{n+2} - 1.$$

Положим

$$i_0 = \left\lfloor \frac{(q+1)(s+1)}{n+2} \right\rfloor. \tag{6.9}$$

Нетрудно видеть, что слагаемые в правой части равенства (6.7) возрастают при увеличении i, достигают максимума при $i = i_0$ и затем убывают. Воспользуемся этим свойством и оценим разность

$$A - B = \sum_{i=0}^{\min(s,q)} (-1)^i \binom{p}{s-i}\binom{q}{i} \tag{6.10}$$

при всех q, для которых $i_0 \leqslant 0$.

При таких q (удовлетворяющих неравенству $q < \frac{n-s+1}{s+1}$) из условия $i_0 \leqslant 0$ следует, что слагаемые в (6.7) убывают с увеличением значения i при всех i. Положим $k = \min\left(\frac{s-1}{2}, \left\lfloor\frac{q}{2}\right\rfloor\right)$. Правую часть (6.10) представим в виде суммы

$$A - B = \sum_{i=0}^{k}\left(\binom{p}{s-2i}\binom{q}{2i} - \binom{p}{s-2i-1}\binom{q}{2i+1}\right),$$

где каждое слагаемое под знаком суммы неотрицательно, а в последней паре возможно отсутствует произведение из B. Следовательно, разность $A-B$ неотрицательна и A не меньше половины суммы (6.7):

$$A \geqslant \frac{1}{2}\binom{n}{s}. \tag{6.11}$$

Теперь оценим разность (6.10) при всех остальных возможных значениях q. В этом случае из неравенства $i_0 \geqslant 1$, равенства (6.9) и неравенства $p \geqslant \gamma n$ следует, что q ограничено снизу и не может быть очень маленьким:

$$\frac{n-s+1}{s+1} \leqslant q \leqslant (1-\gamma)n.$$

Пусть $\alpha = \frac{n-s+1}{n(s+1)}$. Тогда q можно представить произведением $q = \beta n$ с постоянной β, удовлетворяющей неравенствам $\alpha \leqslant \beta \leqslant 1-\gamma$. Так как при $p, q \to \infty$ и любых постоянных*) s и i

$$\binom{p}{s-i}\binom{q}{i}\Big/\binom{n}{s} \sim \frac{p^{s-i}}{(s-i)!}\cdot\frac{q^i}{i!}\cdot\frac{s!}{n^s} = \\ = \binom{s}{i}\left(1-\frac{q}{n}\right)^{s-i}\left(\frac{q}{n}\right)^i = \binom{s}{i}(1-\beta)^{s-i}\beta^i,$$

то A^Δ — доля единиц в столбце — асимптотически стремится к величине, не меньшей

$$A^\star = \sum_{\text{все четные } i}\binom{s}{i}(1-\beta)^{s-i}\beta^i,$$

а B^Δ — доля нулей — к величине, не большей

$$B^\star = \sum_{\text{все нечетные } i}\binom{s}{i}(1-\beta)^{s-i}\beta^i,$$

т. е. $A^\Delta \sim A^\star$ и $B^\Delta \sim B^\star$ при $n \to \infty$. Так как $A^\star + B^\star = 1$ и

$$A^\star - B^\star = \sum_{i=0}^{s}\binom{s}{i}(1-\beta)^{s-i}(-\beta)^i = (1-2\beta)^s,$$

то, учитывая неравенства $\beta \leqslant 1-\gamma$, $0 < \gamma < 1/2$ и нечетность s, видим, что

$$A^\star = \frac{1}{2}\left(1+(1-2\beta)^s\right) \geqslant \frac{1}{2}\left(1+(1-2(1-\gamma))^s\right) = \frac{1}{2}\left(1-(1-2\gamma)^s\right).$$

*) Нетрудно видеть, что следующее асимптотическое равенство будет справедливым также при всех $s, i \ll n^{1/3}$.

Поэтому для любого положительного δ и любой нечетной постоянной s, начиная с некоторого n,

$$A^{\triangle} \geqslant A^{\star} - \frac{\delta}{4} \geqslant \frac{1}{2}\left(1 - (1-2\gamma)^s\right) - \frac{\delta}{4}. \tag{6.12}$$

Далее, так как постоянная $\gamma \in (0, 1/2)$, т. е. $0 < 1 - 2\gamma < 1$, то для того же δ найдется такая нечетная постоянная s, что

$$(1-2\gamma)^s \leqslant \frac{\delta}{2}. \tag{6.13}$$

Тогда для A — числа единиц j-го столбца — справедливо независящее от индекса j неравенство

$$A \geqslant A^{\triangle}\binom{n}{s} \geqslant \left(\frac{1}{2}\left(1 - \frac{\delta}{2}\right) - \frac{\delta}{4}\right)\binom{n}{s} = \left(1-\delta\right)\frac{1}{2}\binom{n}{s}. \tag{6.14}$$

Таким образом, объединяя неравенства (6.11) и (6.14), заключаем, что найдутся такие натуральное N и нечетное s, для которых при каждом j и $n \geqslant N$

$$A \geqslant \left(1-\delta\right)\frac{1}{2}\binom{n}{s}.$$

Поэтому число единиц в таблице T не меньше чем

$$\left(1-\delta\right)\frac{1}{2}\binom{n}{s}R,$$

и, следовательно, существует строка, число единиц в которой не меньше среднего, т. е. не меньше чем

$$\left(1-\delta\right)\frac{1}{2}R.$$

Выбрав эту строку первой строкой набора, видим, что после первого шага в таблице останется не более

$$R_1 \leqslant R - \left(1-\delta\right)\frac{1}{2}R = \left(1+\delta\right)\frac{1}{2}R \tag{6.15}$$

непокрытых столбцов.

Пусть R_t — число столбцов, остающихся непокрытыми после выбора t строк. На каждом шаге в каждом непокрытом столбце находится не менее $\left(1-\delta\right)\frac{1}{2}R$ единиц (все единицы непокрытого столбца находятся в еще не выбранных строках). Поэтому общее число единиц в непокрытых столбцах не меньше $\left(1-\delta\right)\frac{1}{2}\binom{n}{s}R_t$, и, следовательно, найдется строка, в которой число единиц, лежащих в пересечении с еще непокрытыми столбцами, не меньше их среднего числа. Такая строка покрывает не менее

$$\left(1-\delta\right)\frac{1}{2}\binom{n}{s}R_t \Big/ \left(\binom{n}{s} - t\right) \geqslant \left(1-\delta\right)\frac{1}{2}\binom{n}{s}R_t \Big/ \binom{n}{s} = \left(1-\delta\right)\frac{1}{2}R_t$$

столбцов. Выбрав эту строку $(t+1)$-й строкой набора, видим, что в этом случае в таблице останется не более

$$R_{t+1} \leqslant R_t - \left(1-\delta\right)\frac{1}{2}R_t = \left(1 - \left(1-\delta\right)\frac{1}{2}\right)R_t = \left(1+\delta\right)\frac{1}{2}R_t \tag{6.16}$$

непокрытых столбцов. Оценим величину R_t индукцией по t. В основание индукции положим (6.15) и допустим, что $R_t \leqslant \left((1+\delta)\frac{1}{2}\right)^t R$. Тогда из (6.16) и предположения индукции следует неравенство

$$R_{t+1} \leqslant (1+\delta)\,\frac{1}{2}\cdot\left((1+\delta)\frac{1}{2}\right)^t R = \left((1+\delta)\frac{1}{2}\right)^{t+1} R,$$

доказывающее предположение индукции.

Пусть $\varepsilon = 2\delta$ и $m = t+1$. В этом случае из предыдущего неравенства

$$R_m \leqslant \left(\left((1+\delta)^{1/\delta}\right)^{\delta}\frac{1}{2}\right)^m R \leqslant 2^{2\delta m - m} R = 2^{-(1-\varepsilon)m} R.$$

Для выбранного δ из (6.12) определим минимальное n, при котором (6.12) справедливо, а из (6.13) найдем минимальное нечетное s, удовлетворяющее этому неравенству. Так как

$$\frac{\delta}{2} \geqslant (1-2\gamma)^s = \left((1-2\gamma)^{1/2\gamma}\right)^{2\gamma s} \geqslant 2^{-4\gamma s},$$

то $s = \mathcal{O}\left(\frac{1}{\gamma}\log_2\frac{1}{\delta}\right)$. Сложность системы линейных функций в базисе $\{\oplus\}$ не превосходит числа единиц в ее матрице, а в матрице сформированной системы $\mathscr{H}$ находится не более sm единиц и $s \asymp \frac{1}{\gamma}\log_2\frac{1}{\varepsilon}$. Поэтому $L_{\{\oplus\}}(\mathscr{H}) = \mathcal{O}\left(m\frac{1}{\gamma}\log_2\frac{1}{\varepsilon}\right)$. Лемма доказана.

Переформулируя лемму 6.5 для случая, когда множество $\boldsymbol{R}$ состоит из попарных сумм элементов двух непересекающихся множеств, получим следующее утверждение.

Лемма 6.6. *Для любой постоянной $\gamma \in (0, 1/2)$ и любой постоянной $\varepsilon > 0$ существует такое натуральное N, что для каждого $n \geqslant N$ и любых непересекающихся множеств $\boldsymbol{A}, \boldsymbol{B} \subseteq \{0,1\}^n$, для которых вес каждой суммы $\boldsymbol{x} \oplus \boldsymbol{y}$, где $\boldsymbol{x} \in \boldsymbol{A}, \boldsymbol{y} \in \boldsymbol{B}$, не меньше $d = \gamma n$, найдется такой линейный оператор $\mathscr{H}\colon \{0,1\}^n \to \{0,1\}^m$, что $L_{\{\oplus\}}(\mathscr{H}) = \mathcal{O}\left(m\frac{1}{\gamma}\log_2\frac{1}{\varepsilon}\right)$ и*

$$\left|\{(\boldsymbol{x},\boldsymbol{y}) \mid \boldsymbol{x}\in\boldsymbol{A}, \boldsymbol{y}\in\boldsymbol{B}, \mathscr{H}(\boldsymbol{x}) = \mathscr{H}(\boldsymbol{y})\}\right| \leqslant 2^{-(1-\varepsilon)m} AB.$$

Комбинируя утверждения лемм 6.4, 6.5 и 6.6, получим следующие две леммы — аналоги лемм 2.4 и 2.6.

Лемма 6.7. *Для любой постоянной $\varepsilon > 0$ существует такое натуральное N, что для каждого $n \geqslant N$ и любых непересекающихся множеств $\boldsymbol{A}, \boldsymbol{B} \subseteq \{0,1\}^n$ найдется такой линейный оператор $\mathscr{L}\colon \{0,1\}^n \to \{0,1\}^m$, что $L_{\{\oplus\}}(\mathscr{L}) = \mathcal{O}\left(n + m\log_2\frac{1}{\varepsilon}\right)$ и*

$$\left|\{(\boldsymbol{x},\boldsymbol{y}) \mid \boldsymbol{x}\in\boldsymbol{A}, \boldsymbol{y}\in\boldsymbol{B}, \mathscr{L}(\boldsymbol{x}) = \mathscr{L}(\boldsymbol{y})\}\right| \leqslant 2^{-(1-\varepsilon)m} AB.$$

Доказательство. Пусть γ — постоянная из условия леммы 6.4, $\mathscr{G}_{n,4n}$ — линейный оператор из леммы 6.4 такой, что $\|\mathscr{G}_{n,4n}(\boldsymbol{x})\| \geqslant 4\gamma n$ для каждого $\boldsymbol{x} \in \{0,1\}^n$ и $L_{\{\oplus\}}(\mathscr{G}_{n,4n}) = \mathcal{O}(n)$. Тогда $\|\mathscr{G}_{n,4n}(\boldsymbol{x}\oplus\boldsymbol{y})\| \geqslant 4\gamma n$

для любых $\boldsymbol{x} \in \boldsymbol{A}$ и $\boldsymbol{y} \in \boldsymbol{B}$. В силу леммы 6.6 для любой постоянной $\varepsilon > 0$ существует такой линейный оператор $\mathscr{H}_{4n,m} : \{0,1\}^{4n} \to \{0,1\}^m$, что $L_{\{\oplus\}}(\mathscr{H}_{4n,m}) = O\left(m\frac{1}{\gamma}\log_2\frac{1}{\varepsilon}\right)$ и

$$\left|\{(\boldsymbol{x},\boldsymbol{y}) \mid \boldsymbol{x} \in \mathscr{G}_{n,4n}(\boldsymbol{A}), \mathscr{G}_{n,4n}(\boldsymbol{y}) \in \boldsymbol{B}, \mathscr{H}_{4n,m}(\boldsymbol{x}) = \mathscr{H}_{4n,m}(\boldsymbol{y})\}\right| \leqslant 2^{-(1-\varepsilon)m}AB.$$

Легко видеть, что композиция $\mathscr{H}_{4n,m} \circ \mathscr{G}_{n,4n}$ будет требуемым оператором $\mathscr{L}$. Лемма доказана.

Лемма 6.8. *Пусть $\boldsymbol{D} \subseteq \{0,1\}^n$, $n \leqslant D < 2^{n/5}$. Существует такое натуральное N, что для каждого $n \geqslant N$ и $m = \lceil 4\log_2 D\rceil$ найдется такой линейный оператор $\mathscr{L}: \{0,1\}^n \to \{0,1\}^m$, что $L_{\{\oplus\}}(\mathscr{L}) = \mathscr{O}(n)$ и $\mathscr{L}(\boldsymbol{x}) \neq \mathscr{L}(\boldsymbol{y})$ для любых неравных $\boldsymbol{x}$ и $\boldsymbol{y}$ из $\boldsymbol{D}$.*

Доказательство. Пусть γ — постоянная из условия леммы 6.4, $\boldsymbol{R}$ — множество попарных сумм неравных наборов из $\boldsymbol{D}$, $\mathscr{G}_{n,4n}$ — линейный оператор из леммы 6.4 такой, что $\|\mathscr{G}_{n,4n}(\boldsymbol{x})\| \geqslant 4\gamma n$ для каждого $\boldsymbol{x} \in \{0,1\}^n$ и $L_{\{\oplus\}}(\mathscr{G}_{n,4n}) = \mathscr{O}(n)$. Тогда $\|\mathscr{G}_{n,4n}(\boldsymbol{x})\| \geqslant 4\gamma n$ для любого $\boldsymbol{x}$ из $\boldsymbol{R}$. В силу леммы 6.5 для $\varepsilon = 1/2$ существует такой линейный оператор $\mathscr{H}_{4n,m}: \{0,1\}^{4n} \to \{0,1\}^m$, что $L_{\{\oplus\}}(\mathscr{H}_{4n,m}) = O\left(m\frac{1}{\gamma}\right)$ и

$$\left|\{\boldsymbol{x} \mid \boldsymbol{x} \in \mathscr{G}_{n,4n}(\boldsymbol{R}), \mathscr{H}_{4n,m}(\boldsymbol{x}) = 0\}\right| < 2^{-\lceil 4\log_2 D\rceil/2}\frac{D^2}{2} \leqslant 2^{-2\log_2 D}\frac{D^2}{2} \leqslant \frac{1}{2}.$$

Легко видеть, что композиция $\mathscr{H}_{4n,m} \circ \mathscr{G}_{n,4n}$ будет требуемым оператором $\mathscr{L}$. Лемма доказана.

6.3. Доказательство теоремы 6.1. Выше было установлено в (6.2)–(6.4), что для доказательства теоремы достаточно показать справедливость неравенства (6.1) только для N, не превосходящих n^3. Сделаем это для каждого из следующих четырех различных условий, связывающих значения параметров D и N*):

1. $\log_2 D \sim n$;
2. $\log_2 D \lessdot n$, $\log_2 D \gg \log_2 N$, $N \gg \log_2 n$;
3. $\log_2 D \lessdot n$, $N \gg \log_2 n$;
4. $N = \mathscr{O}(\log_2 n)$.

Нетрудно видеть, что если $D \geqslant n$ и $N \leqslant n^3$, то при любом соотношении между такими параметрами справедливо хотя бы одно из условий 1–4.

1. Пусть $\log_2 D \sim n$. Тогда для любой сколь угодно малой положительной постоянной ε справедливы неравенства $2^n \leqslant D^{1+\varepsilon}$ и $3N^{2\varepsilon} \leqslant D^{\varepsilon}$. Следовательно,

$$\begin{aligned}\log_2\binom{2^n}{N} &\leqslant \log_2\binom{D^{1+\varepsilon}}{N} \leqslant \log_2\left(\frac{3D^{1+\varepsilon}}{N}\right)^N \leqslant \\ &\leqslant \log_2\left(\frac{3D^{\varepsilon}D^{1+\varepsilon}}{3N^{2\varepsilon}N}\right)^N = \log_2\left(\frac{D}{N}\right)^{(1+2\varepsilon)N} = \\ &= (1+2\varepsilon)\log_2\left(\frac{D}{N}\right)^N \leqslant (1+2\varepsilon)\log_2\binom{D}{N}.\end{aligned}$$

*) Неравенство $a(n) \lessdot b(n)$ означает, что $\overline{\lim}_{n\to\infty}\frac{a(n)}{b(n)} < 1$.

Поэтому, рассматривая f как полностью определенную функцию, видим, что в силу теоремы 5.3 для любой сколь угодно малой положительной постоянной ε выполняются неравенства

$$L_B(f) \lesssim \varrho \cdot \frac{\log_2 \binom{2^n}{N}}{\log_2 \log_2 \binom{2^n}{N}} + \mathcal{O}(n) \leqslant (1+2\varepsilon)\varrho \cdot \frac{\log_2 \binom{D}{N}}{\log_2 \log_2 \binom{D}{N}} + \mathcal{O}(n),$$

из которых и следует справедливость (6.4).

2. Пусть $\log_2 D \lessdot n$, $\log_2 N \ll \log_2 D$ и $N \gg \log_2 n$. В этом случае из асимптотического неравенства $\log_2 D \lessdot n$ следует существование положительной постоянной δ, для которой $D^{1+\delta} < 2^n$. Из второго неравенства $\log_2 N \ll \log_2 D$ следует, что существует функция $\varphi(n) \ll 1$, для которой $\log_2 N \ll \varphi(n) \log_2 D$. Поэтому для любой сколь угодно малой положительной постоянной ε

$$N \leqslant D^{\varphi(n)} \leqslant D^{\varepsilon}. \tag{6.17}$$

Из третьего неравенства $N \gg \log_2 n$ следует, что существует такая функция $\chi(n) \gg 1$, что

$$N \gg \chi(n) \log_2 n. \tag{6.18}$$

Покажем, что в рассматриваемом случае при $\varepsilon < \delta/8$

$$L_B(f) \lesssim (1+32\varepsilon)\varrho \cdot \frac{\log_2 \binom{D}{N}}{\log_2 \log_2 \binom{D}{N}} + \mathcal{O}\left(n + \log_2 \frac{1}{\varepsilon} \cdot \log_2 D\right). \tag{6.19}$$

Пусть $\boldsymbol{A} = \{\boldsymbol{x} \mid f(\boldsymbol{x}) = 1\}$, $\boldsymbol{B} = \{\boldsymbol{x} \mid f(\boldsymbol{x}) = 0\}$. Зафиксируем постоянную $\varepsilon < \delta/8$ и к областям $\boldsymbol{A}$ и $\boldsymbol{B}$ применим лемму 6.7. В силу этой леммы для данной постоянной ε существует линейный оператор $\mathscr{L}\colon \{0,1\}^n \to \{0,1\}^m$ такой, что

$$L_B(\mathscr{L}) = \mathcal{O}\left(n + m \log_2 \frac{1}{\varepsilon}\right) \tag{6.20}$$

и

$$\left|\{(\boldsymbol{x},\boldsymbol{y}) \mid \boldsymbol{x} \in \boldsymbol{A}, \boldsymbol{y} \in \boldsymbol{B}, \mathscr{L}(\boldsymbol{x}) = \mathscr{L}(\boldsymbol{y})\}\right| \leqslant 2^{-(1-\varepsilon)m} AB. \tag{6.21}$$

Положим $m = \lceil (1+4\varepsilon) \log_2 AB \rceil$. Тогда при $\varepsilon \leqslant 1/2$

$$\begin{aligned} -(1-\varepsilon)\lceil (1+4\varepsilon)\log_2 AB\rceil &\leqslant -(1-\varepsilon)(1+4\varepsilon)\log_2 AB \leqslant \\ &\leqslant -(1+3\varepsilon-4\varepsilon^2)\log_2 AB \leqslant -(1+\varepsilon)\log_2 AB \end{aligned}$$

и, следовательно,

$$2^{-(1-\varepsilon)m} AB \leqslant (AB)^{-1-\varepsilon} AB = (AB)^{-\varepsilon} < 1. \tag{6.22}$$

Таким образом, в силу (6.21) и (6.22) для любых $\boldsymbol{x} \in \boldsymbol{A}$ и $\boldsymbol{y} \in \boldsymbol{B}$ значения оператора $\mathscr{L}$ на таких наборах не совпадают: $\mathscr{L}(\boldsymbol{x}) \neq \mathscr{L}(\boldsymbol{y})$.

Отметим, что m определено так, что $m < n$. Действительно, так как $A = N$ и $B < D$, то с учетом (6.17) при $\varepsilon \leqslant 1/2$

$$\begin{aligned} m &= \lceil (1+4\varepsilon)\log_2 AB \rceil \leqslant \lceil (1+4\varepsilon)\log_2 ND \rceil \leqslant \\ &\leqslant \left\lceil (1+4\varepsilon)\log_2 D^{1+\varepsilon} \right\rceil \leqslant \lceil (1+4\varepsilon)(1+\varepsilon)\log_2 D \rceil \leqslant \\ &\leqslant \left\lceil (1+5\varepsilon+4\varepsilon^2)\log_2 D \right\rceil \leqslant \lceil (1+7\varepsilon)\log_2 D \rceil \leqslant \\ &\leqslant (1+8\varepsilon)\log_2 D < (1+\delta)\log_2 D < n. \end{aligned} \tag{6.23}$$

Введем определенную на $\{0,1\}^m$ m-местную булеву функцию

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

Нетрудно видеть, что g равна единице не более чем на N наборах из $\{0,1\}^m$, и $f(\boldsymbol{x}) = g(\mathscr{L}(\boldsymbol{x}))$. Поэтому

$$L_B(f) \leqslant L_B(g) + L_B(\mathscr{L}). \tag{6.24}$$

Так как $N \gg \log_2 n \geqslant \log_2 m$, то для оценки сложности функции g можно воспользоваться теоремой 5.2. Из этой теоремы и (6.23) следует, что

$$L_B(g) \lesssim \varrho \cdot \frac{\log_2 \binom{2^m}{N}}{\log_2 \log_2 \binom{2^m}{N}} \leqslant \varrho \cdot \frac{\log_2 \binom{D^{1+8\varepsilon}}{N}}{\log_2 \log_2 \binom{D^{1+8\varepsilon}}{N}}. \tag{6.25}$$

Из (6.17) и цепочки эквивалентных неравенств

$$N \leqslant D^{\varepsilon} \Longleftrightarrow D^{1-\varepsilon} \leqslant \frac{D}{N} \Longleftrightarrow D^{1+3\varepsilon-4\varepsilon^2} \leqslant \left(\frac{D}{N}\right)^{1+4\varepsilon}$$

следует, что при $\varepsilon \leqslant 1/2$

$$D^{1+\varepsilon} \leqslant D^{1+3\varepsilon-4\varepsilon^2} \leqslant \left(\frac{D}{N}\right)^{1+4\varepsilon}.$$

Поэтому, оценивая при $\varepsilon \leqslant 1/16$ и условии $\log_2 N \ll \log_2 D$ числитель в правой части (6.25), видим, что

$$\begin{aligned} \log_2 \binom{D^{1+8\varepsilon}}{N} &\leqslant \log_2 D^{(1+8\varepsilon)N} \leqslant \log_2 \left(\frac{D}{N}\right)^{(1+32\varepsilon)N} = \\ &= (1+32\varepsilon)\log_2 \left(\frac{D}{N}\right)^N \sim (1+32\varepsilon)\log_2 \binom{D}{N}. \end{aligned}$$

Подставляя получившееся неравенство в (6.25), убеждаемся в справедливости неравенства

$$L_B(g) \lesssim (1+32\varepsilon)\varrho \cdot \frac{\log_2 \binom{D}{N}}{\log_2 \log_2 \binom{D}{N}},$$

которое вместе с (6.24) и оценкой (6.20) доказывает в рассматриваемом случае справедливость (6.19):

$$L_B(f) \lesssim (1+32\varepsilon)\varrho \cdot \frac{\log_2 \binom{D}{N}}{\log_2 \log_2 \binom{D}{N}} + \mathscr{O}\left(n + \log_2 D \cdot \log_2 \frac{1}{\varepsilon}\right). \tag{6.19}$$

Далее покажем, что во втором слагаемом в (6.19) можно убрать зависимость от ε и заменить его на $\mathcal{O}(n)$. Сделаем это отдельно для двух вариантов роста значения параметра D: $\log_2 D \asymp n$; $\log_2 D \ll n$.

Пусть $\log_2 D \asymp n$. В этом случае найдется такая функция $\psi(n)$, что $\psi(n) \ll 1$, $\log_2 D \gg \psi(n)n$ и $\sqrt{\chi(n)}\psi(n) \geqslant 1$ для функции $\chi(n)$ из (6.18). Поэтому, учитывая неравенства $\log_2 N \ll \log_2 D$, $N \gg \chi(n)\log_2 n$ и $N < n^3$, находим нижнюю оценку первого слагаемого в (6.19):

$$\frac{\log_2 \binom{D}{N}}{\log_2 \log_2 \binom{D}{N}} \geqslant \frac{N \log_2 \frac{D}{N}}{\log_2 N + \log_2 \log_2 \frac{D}{N}} \gg \frac{\chi(n)\log_2 n \cdot \psi(n)n}{3\log_2 n + \log_2 n} \geqslant$$

$$\geqslant \frac{1}{4}\sqrt{\chi(n)}n \gg n \log_2 \frac{1}{\varepsilon} \geqslant \log_2 D \cdot \log_2 \frac{1}{\varepsilon}.$$

Таким образом, первое слагаемое в (6.19) растет быстрее второго и быстрее n. Поэтому уменьшение второго слагаемого до $\mathcal{O}(n)$ не меняет асимптотику всей суммы в (6.19) и превращает это неравенство в (6.1).

Пусть теперь $\log_2 D \ll n$. В этом случае найдется такая функция $\mu(n) \ll 1$, что $\log_2 D \ll \mu(n)n$, и тогда для второго слагаемого в (6.19) справедливы неравенства

$$\log_2 D \cdot \log_2 \frac{1}{\varepsilon} \ll \mu(n)n \log_2 \frac{1}{\varepsilon} \ll n,$$

в силу которых из (6.19) следует оценка (6.1).

3. Пусть $\log_2 D \prec n$ и $N \gg \log_2 n$. При этих условиях найдется такая функция $\chi(n) \gg 1$, что $N \gg \chi(n)\log_2 n$ и $\chi(n) \leqslant \frac{1}{5}\log_2 N$. Рассмотрим два интервала значений параметра D: $D \geqslant N^{\chi(n)}$; $D < N^{\chi(n)}$.

Если $D \geqslant N^{\chi(n)}$, то $\log_2 D \geqslant \chi(n)\log_2 N \gg \log_2 N$ и рассматриваемый случай является частным случаем предыдущего.

Если $D < N^{\chi(n)}$, то из леммы 6.8 следует, что для $\boldsymbol{D}$ и

$$m = \lceil 4\log_2 D \rceil \leqslant \lceil 4\chi(n)\log_2 N \rceil \leqslant \log_2^2 N$$

найдется линейный оператор $\mathscr{L}\colon \{0,1\}^n \to \{0,1\}^m$, для которого $L_B(\mathscr{L}) = \mathcal{O}(n)$ и $\mathscr{L}(\boldsymbol{x}) \neq \mathscr{L}(\boldsymbol{y})$ для любых неравных $\boldsymbol{x}$ и $\boldsymbol{y}$ из $\boldsymbol{D}$.

Введем определенную на $\mathscr{L}(\boldsymbol{D})$ частичную m-местную булеву функцию g так, что

$$g(\boldsymbol{y}) = f(\boldsymbol{x}), \text{ если } \boldsymbol{x} \in \boldsymbol{D} \text{ и } \boldsymbol{y} = \mathscr{L}(\boldsymbol{x}).$$

Нетрудно видеть, что $f(\boldsymbol{x}) = g(\mathscr{L}(\boldsymbol{x}))$, множество $\mathscr{L}(\boldsymbol{D})$ состоит из D наборов и функция g равна единице не больше чем на N наборах из $\mathscr{L}(\boldsymbol{D})$, где

$$N = 2^{\log_2 N} \geqslant 2^{\sqrt{m}} \gg m^3.$$

Следовательно, в силу (6.4)

$$L_B(f) \leqslant L_B(g) + L_B(\mathscr{L}) \lesssim \varrho \cdot \frac{\log_2 \binom{D}{N}}{\log_2 \log_2 \binom{D}{N}} + \mathcal{O}(n).$$

4. Пусть $N = \mathcal{O}(\log_2 n)$. При таких значениях N неравенство (6.1) следует из теоремы 5.3. Теорема доказана.

§ 7. Недоопределенные функции

Пусть $\boldsymbol{D}$, $\boldsymbol{M}$ — конечные множества, $\mathscr{P}(\boldsymbol{M})$ — множество всех непустых подмножеств $\boldsymbol{M}$. Набор $\boldsymbol{\alpha} = \{\alpha_1, \ldots, \alpha_n\}$ назовем M-ичным недоопределенным набором, если каждая его компонента α_i является элементом $\mathscr{P}(\boldsymbol{M})$. Набор $\boldsymbol{\beta}$ из $\boldsymbol{M}^n$ назовем доопределением недоопределенного набора $\boldsymbol{\alpha}$, если $\beta_i \in \alpha_i$ для всех i.

Функции из $\boldsymbol{D}$ в $\mathscr{P}(\boldsymbol{M})$ будем называть M-ичными недоопределенными функциями. Множество $\boldsymbol{S} = \{\boldsymbol{x} \in \boldsymbol{D} \mid f(\boldsymbol{x}) \neq \boldsymbol{M}\}$ назовем носителем f. Функцию $h\colon \boldsymbol{D} \to \boldsymbol{M}$ назовем доопределением недоопределенной функции f, если $h(\boldsymbol{x}) \in f(\boldsymbol{x})$ для любого $\boldsymbol{x} \in \boldsymbol{D}$, т. е. если вектор значений h является доопределением вектора значений f.

Пусть $\boldsymbol{\beta}$ — недоопределенный M-ичный набор длины N. Набор $\boldsymbol{k} = (k_1, k_2, \ldots, k_M)$ назовем характеристикой набора $\boldsymbol{\beta}$, если для каждого i число k_i равно количеству i-элементных компонент $\boldsymbol{\beta}$. На множестве недоопределенных наборов введем функцию I, показывающую степень определенности набора. Для набора $\boldsymbol{\alpha}$ с характеристикой $\boldsymbol{k} = (k_1, k_2, \ldots, k_M)$ положим

$$I(\boldsymbol{\alpha}) = \log_2 \left(\left(\frac{M}{1}\right)^{k_1} \left(\frac{M}{2}\right)^{k_2} \cdots \left(\frac{M}{M}\right)^{k_M} \right), \tag{7.1}$$

т. е. чем сильнее определен набор $\boldsymbol{\alpha}$, тем больше значение $I(\boldsymbol{\alpha})$. Нетрудно видеть, что недоопределенный M-ичный набор $\boldsymbol{\alpha}$ длины N с характеристикой $\boldsymbol{k} = (k_1, k_2, \ldots, k_M)$ имеет ровно

$$1^{k_1} 2^{k_2} \cdots M^{k_M} = M^N 2^{-I(\boldsymbol{\alpha})} \tag{7.2}$$

доопределений. Для недоопределенной функции f через $I(f)$ обозначим значение функции I на векторе значений f. Характеристикой функции f будем называть характеристику ее вектора значений.

7.1. Вычисление недоопределенных функций. Перенумеруем*) элементы множеств $\boldsymbol{D}$ и $\boldsymbol{M}$, и всем элементам из $\boldsymbol{D}$ и $\boldsymbol{M}$ поставим в соответствие булевы наборы длины $n = \lceil \log_2 D \rceil$ и $m = \lceil \log_2 M \rceil$ — двоичные представления их номеров. Используя это соответствие, будем представлять определенные на $\boldsymbol{D}$ и принимающие значения в $\boldsymbol{M}$ функции как n-местные m-значные булевы функции**) с областью определения в $\{0,1\}^n$ и областью значений в $\{0,1\}^m$ и, в соответствии с этим представлением, будем рассматривать вычисления функций из $\boldsymbol{D}$ в $\boldsymbol{M}$ схемами. Как и в случае частичных функций, сложностью $L_B(f)$ недоопределенной функции f называется сложность вычисления ее самого простого доопределения схемами в базисе B. Далее рассматривается сложность вычисления недоопределенных функций.

В упомянутой во введении работе [10] Нечипорук фактически рассмотрел частный случай вычисления недоопределенных функций с $M = 2$ и $\log_2 I(f) \sim n$, для которого получил асимптотически неулучшаемый результат. Л. А. Шоломов [20] распространил этот результат на случай $M = 2$

*) Далее будем отождествлять элементы множеств с их номерами.

**) Далее такие функции будем называть булевыми, опуская, как правило, упоминание о числе аргументов и числе компонент.

и $I(f) \geqslant n \log_2^{1+\delta} n$, где δ — сколь угодно малое положительное число. Продолжая начатое в [19] изучение сложности систем недоопределенных булевых функций, Шоломов в [21] получил решение для конечных значений M и $\log_2 I(f) \sim n$. Наконец, в работе [22] А. Е. Андреев получил окончательный результат для схем в базисе B_2 при слабых ограничениях на рост M и произвольных значениях $I(f)$. Далее в теореме 7.1 результат Андреева распространяется на схемы в произвольном полном конечном базисе. Доказательство ведется методом Шоломова из [20] и в целом мало отличается от доказательств теорем 2.1 и 5.1.

Рассмотрим множество $\boldsymbol{A}(M, \boldsymbol{D}, R)$, состоящее из всех недоопределенных M-ичных функций с областью определения $\boldsymbol{D}$ и таких, что $I(f) = R$ для каждой функции f из этого множества.

Теорема 7.1. *Пусть $D \to \infty$, B — полный конечный базис с минимальным приведенным весом ϱ, $\log_2 M \ll \log_2 R$ и $f \in \boldsymbol{A}(M, \boldsymbol{D}, R)$. Тогда*

$$L_B(f) \lesssim \varrho \cdot \frac{R}{\log_2 R} + \mathcal{O}(\log_2 D).$$

Утверждение теоремы следует из доказываемых в следующем разделе лемм 7.4, 7.5 и 7.6, в которых рассматриваются три частных случая вычисления произвольной недоопределенной функции f в зависимости от величины $I(f)$ — степени ее определенности.

Нижнюю оценку сформулируем для множеств $\boldsymbol{A}(M, \boldsymbol{D}, R, \boldsymbol{k})$, каждое из которых является подмножеством $\boldsymbol{A}(M, \boldsymbol{D}, R)$ и состоит из всех функций с характеристикой $\boldsymbol{k}$. Несмотря на то, что в $\boldsymbol{A}(M, \boldsymbol{D}, R, \boldsymbol{k})$ параметр R однозначно определяется характеристикой $\boldsymbol{k}$, он оставлен среди основных параметров множества $\boldsymbol{A}(M, \boldsymbol{D}, R, \boldsymbol{k})$, так как в нижней оценке в теореме 7.2 зависимость от $\boldsymbol{k}$ проявляется только косвенно, как зависимость от R.

Теорема 7.2. *Пусть $D \to \infty$, B — полный конечный базис с минимальным приведенным весом ϱ. В $\boldsymbol{A}(M, \boldsymbol{D}, R, \boldsymbol{k})$ найдется такая функция f, что*

$$L_B(f) \gtrsim \varrho \cdot \frac{R}{\log_2 R}.$$

Для доказательства теоремы 7.2 достаточно показать, что в любом доопределении множества $\boldsymbol{A}(M, \boldsymbol{D}, R, \boldsymbol{k})$ найдется функция, сложность которой удовлетворяет неравенству теоремы. Это можно легко сделать стандартным мощностным методом [6], используя доказанную ниже в лемме 7.3 нижнюю оценку числа функций в доопределении $\boldsymbol{A}(M, \boldsymbol{D}, R, \boldsymbol{k})$.

7.2. Доопределения. Множество $\boldsymbol{B} \subseteq \boldsymbol{M}^n$ назовем доопределением множества $\boldsymbol{A}$ недоопределенных M-ичных наборов, если для каждого недоопределенного набора $\boldsymbol{\alpha}$ из $\boldsymbol{A}$ в $\boldsymbol{B}$ найдется элемент $\boldsymbol{\beta}$, являющийся его доопределением. Следующую лемму — аналог лемм 2.1 и 5.2, как и эти леммы можно доказать, используя жадный алгоритм построения доопределения. Вместо этого дадим другое, более короткое доказательство, — доказательство существования из [17].

Лемма 7.1. *Пусть $\boldsymbol{A} = \{\boldsymbol{\alpha}\}$ — множество всех недоопределенных M-ичных наборов длины n с $I(\boldsymbol{\alpha}) \leqslant R$. Тогда существует доопределение множества $\boldsymbol{A}$, состоящее не более чем из $Mn2^R$ наборов.*

Доказательство. Допустим, что любое N-элементное подмножество множества $\{0, 1, \ldots, M-1\}^n$ не является доопределением множества $\boldsymbol{A}$. Тогда для каждого такого подмножества можно указать хотя бы один набор из $\boldsymbol{A}$, для которого в этом подмножестве нет доопределения. Поэтому число пар $(\boldsymbol{\alpha}, \boldsymbol{B})$, где $\boldsymbol{\alpha} \in \boldsymbol{A}$, а $\boldsymbol{B}$ — N-элементное подмножество множества $\boldsymbol{M}^n$, таких, что в $\boldsymbol{B}$ нет доопределения $\boldsymbol{\alpha}$, равно $\binom{M^n}{N}$. Так как $\boldsymbol{A}$ состоит менее чем из 2^{Mn} элементов, то в $\boldsymbol{A}$ найдется такой набор $\boldsymbol{\alpha}$, что более

$$\binom{M^n}{N} \Big/ 2^{Mn}$$

N-элементных подмножеств множества $\boldsymbol{M}^n$ не содержат доопределение $\boldsymbol{\alpha}$. С другой стороны, легко видеть, что для любого недоопределенного набора из $\boldsymbol{A}$ не более (см. (7.2))

$$\binom{M^n - M^n 2^{-R}}{N}$$

N-элементных подмножеств множества $\boldsymbol{M}^n$ не содержат его доопределение. Поэтому должно выполняться неравенство

$$\binom{M^n}{N} \Big/ \binom{M^n - M^n 2^{-R}}{N} < 2^{Mn}. \tag{7.3}$$

Оценивая левую часть (7.3), видим, что

$$\begin{aligned} 2^{Mn} &> \frac{M^n \cdots (M^n - N + 1)}{(M^n - M^n 2^{-R}) \cdots (M^n - M^n 2^{-R} - N + 1)} \geqslant \\ &\geqslant \left(\frac{M^n}{M^n - M^n 2^{-R}} \right)^N = \left(\frac{1}{1 - 2^{-R}} \right)^N \geqslant \\ &\geqslant \left(1 + 2^{-R} + 2^{-2R} \right)^N \geqslant 2^{N(2^{-R}(1+2^{-R}))}. \end{aligned}$$

Поэтому, логарифмируя полученные неравенства, заключаем, что

$$N < Mn2^R(1 + 2^{-R})^{-1} \leqslant Mn2^R(1 - 2^{-R-1}) \leqslant Mn2^R - 1. \tag{7.4}$$

Таким образом, из предположения, что любое N-элементное подмножество множества $\boldsymbol{M}^n$ не является доопределением множества $\boldsymbol{A}$, следует неравенство (7.4). Поэтому при N больших или равных правой части (7.4) среди N-элементных подмножеств множества $\boldsymbol{M}^n$ найдется хотя бы одно доопределение множества $\boldsymbol{A}$. Лемма доказана.

Лемма 7.2. *Пусть $\boldsymbol{A} = \{\boldsymbol{\beta}\}$ — множество недоопределенных M-ичных наборов длины n таких, что $I(\boldsymbol{\alpha}) \geqslant R$ и $I(\boldsymbol{\alpha}') < R$, где $\boldsymbol{\alpha}'$ — набор $\boldsymbol{\alpha}$ без последней компоненты. Тогда существует доопределение множества $\boldsymbol{A}$, состоящее не более чем из $nM^2 2^R$ наборов.*

Справедливость леммы 7.2 легко следует из леммы 7.1 и двух очевидных неравенств $2^{I(\boldsymbol{\alpha}')} < 2^R$ и $2^{I(\boldsymbol{\alpha})} \leqslant M2^{I(\boldsymbol{\alpha}')}$.

Лемма 7.3. *Пусть $\boldsymbol{A} = \{\boldsymbol{\alpha}\}$ — множество всех недоопределенных M-ичных наборов длины n с характеристикой $\boldsymbol{k} = (k_1, k_2, \ldots, k_M)$ и $I(\boldsymbol{\alpha}) = R$. Тогда любое доопределение множества $\boldsymbol{A}$ состоит не менее чем из 2^R наборов.*

Доказательство. Каждый недоопределенный набор из $\boldsymbol{A}$ имеет ровно $M^n 2^{-R}$ доопределений (7.2). Поэтому число пар $(\boldsymbol{\alpha}, \boldsymbol{\beta})$ таких, что $\boldsymbol{\alpha} \in \boldsymbol{A}$, $\boldsymbol{\beta} \in \boldsymbol{M}^n$ и $\boldsymbol{\beta}$ является доопределением $\boldsymbol{\alpha}$, равно $AM^n 2^{-R}$. Так как любые два M-ичных набора длины n являются доопределениями одного и того же числа недоопределенных наборов одинаковой характеристики $\boldsymbol{k}$, то каждый M-ичный набор длины n будет доопределением ровно $A2^{-R}$ наборов из $\boldsymbol{A}$. Следовательно, если множество $\boldsymbol{B}$ состоит менее чем из 2^R M-ичных наборов длины n, то оно содержит доопределения менее A наборов и поэтому не может быть доопределением множества $\boldsymbol{A}$. Лемма доказана.

7.3. Три частных случая. Первый случай — сильно определенные функции. Доказательство следующей леммы основано на принципе локального кодирования и аналогично доказательству леммы 5.3.

Лемма 7.4. *Пусть* $D \to \infty$, B *— полный конечный базис с минимальным приведенным весом* ϱ, $n = \lceil \log_2 D \rceil$, $\log_2 I(f) \sim n$, $\log_2 M \ll n$. *Тогда*

$$L_B(f) \lesssim \varrho \cdot \frac{I(f)}{\log_2 I(f)}.$$

Доказательство. Прежде всего отметим, что $I(f) \leqslant 2^n \log_2 M$ для любой f. И так как $\log_2 I(f) \leqslant n + \log_2 \log_2 M \sim n$, то все функции f с максимально возможными значениями $I(f)$ удовлетворяют условиям леммы.

Введем параметры K и k, значения которых определим позднее. Значения недоопределенной n-местной функции f запишем в таблице T_f и 2^k столбцов и 2^{n-k} строк, поставив в соответствие j-му столбцу таблицы двоичный набор $(\sigma_1, \ldots, \sigma_k)$, являющийся двоичным представлением числа $j-1$, а i-й строке — набор $(\sigma_{k+1}, \ldots, \sigma_n)$, являющийся двоичным представлением числа $i-1$. В таблице на пересечении j-го столбца и i-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 $I(\boldsymbol{\alpha}) \geqslant K$ и $I(\boldsymbol{\alpha}') < K$. Множество таких наборов разобьем на классы, поместив в класс $\boldsymbol{P}_{ij}$ 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 7.2 следует, что для множества элементарных наборов класса $\boldsymbol{P}_{ij}$ существует множество их доопределений, которое состоит не более чем из $2^k M^2 2^K$ 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 $\boldsymbol{H} = \{\boldsymbol{\beta}\}$, которое состоит не более чем из $M^2 2^{2k-1} 2^k 2^K$ наборов длины 2^k. Далее полагаем, что нулевой набор принадлежит $\boldsymbol{H}$. Перенумеруем $\boldsymbol{\beta}$ из $\boldsymbol{H}$ целыми неотрицательными числами от нуля до $M^2 2^{2k-1} 2^k 2^K - 1$, присвоив нулевому набору нулевой номер.

Преобразуем таблицу T_f в новую таблицу T_h. Для этого для каждого i заменим в T_f i-ю строку, состоящую из элементарных наборов $\boldsymbol{\alpha}_{ij}$, дизъюнкцией $\boldsymbol{\beta}_i = \vee_j \boldsymbol{\beta}_{ij}$ их доопределений $\boldsymbol{\beta}_{ij}$ из $\boldsymbol{H}$. В результате преобразованная таблица T_h будет таблицей значений некоторой n-местной функции h, являющейся доопределением функции f. Функцию h вычислим, используя теорему 4.2 (метод локального кодирования Лупанова).

Прежде всего оценим число наборов $\boldsymbol{\alpha}$, из которых состоит T_f. Заметим, что

$$I(f) = \sum_{\boldsymbol{\alpha}} I(\boldsymbol{\alpha}),$$

где сумма берется по всем наборам $\boldsymbol{\alpha}$, входящим в T_f. При этом число наборов с $I(\boldsymbol{\alpha}) < K$ не превосходит числа строк таблицы 2^{n-k}. Так как для каждого из оставшихся наборов $I(\boldsymbol{\alpha}) \geqslant K$, то, очевидно, что их число не превосходит $I(f)/K$. Таким образом, общее число наборов в T_f не превосходит

$$I(f) \Big/ K + 2^{n-k}. \tag{7.5}$$

Перенумеруем элементарные наборы $\boldsymbol{\alpha}$ целыми неотрицательными числами от нуля до $M^2 2^{3k-1} 2^K - 1$, присвоив каждому набору номер его доопределения $\boldsymbol{\beta}$ из T_h. Теперь из таблицы T_f построим вектор $\boldsymbol{T}$ следующим образом: в T_f заменим все элементарные наборы $\boldsymbol{\alpha}$, на которые разбиты ее строки, их номерами $\boldsymbol{t}$ — двоичными наборами длины

$$p = \lceil \log_2 M^2 2^{3k-1} 2^K \rceil \leqslant 2 \log_2 M + 3k + K,$$

и затем, начиная с первой строки $\boldsymbol{T}_1$, выпишем строки $\boldsymbol{T}_i$ новой таблицы одну за другой в виде вектора $\boldsymbol{T} = (\boldsymbol{T}_1 \ldots \boldsymbol{T}_i \ldots \boldsymbol{T}_{2^{n-k}})$, где $\boldsymbol{T}_i = (\boldsymbol{t}_{i1} \ldots \boldsymbol{t}_{ij} \ldots \boldsymbol{t}_{il_i})$. Из (7.5) следует, что длина T вектора $\boldsymbol{T}$ удовлетворяет неравенству

$$\begin{aligned} T &\leqslant (I(f)/K + 2^{n-k})(2 \log_2 M + 3k + K) = \\ &= I(f) \left(1 + \frac{2 \log_2 M + 3k}{K}\right) + (2 \log_2 M + 3k + K) 2^{n-k}. \end{aligned} \tag{7.6}$$

При этом, так как значение функции I на любой строке таблицы T_h не превосходит $2^k \log_2 M$, нетрудно видеть, что каждый вектор $\boldsymbol{T}_i$ состоит не более чем из q номеров, а его длина T_i не превосходит s, где

$$q = \left\lceil \frac{2^k \log_2 M}{K} \right\rceil, \quad s \leqslant \frac{(2 \log_2 M + 3k + K)(2^k \log_2 M + K)}{K}.$$

Положим $\boldsymbol{l} = (l_1, \ldots, l_i, \ldots, l_{2^{n-k}})$, где l_i — число номеров $\boldsymbol{t}_{ij}$ в векторе $\boldsymbol{T}_i$, $\boldsymbol{r} = (r_1, \ldots, r_i, \ldots, r_{2^{n-k}})$, где r_i — номер позиции, начиная с которой в векторе $\boldsymbol{T}$ располагается вектор $\boldsymbol{T}_i$. Далее вектор $\boldsymbol{T}$ будем рассматривать как вектор значений частичной $\lceil \log_2 T \rceil$-местной булевой функции t, определенной на первых T наборах $\lceil \log_2 T \rceil$-мерного булева куба, векторы $\boldsymbol{l}$ и $\boldsymbol{r}$ — как векторы значений функций

$$l : \{0,1\}^{n-k} \to \{0,1\}^{\lceil \log_2 q \rceil} \quad \text{и} \quad r : \{0,1\}^{n-k} \to \{0,1\}^{\lceil \log_2 T \rceil}$$

соответственно. Пусть, кроме того,

$$g : \{0,1\}^{\lceil \log_2 p \rceil} \to \{0,1\}^{2^k \lceil \log_2 M \rceil},$$

— функция, преобразующая номер $\boldsymbol{t}$ в соответствующий ему вектор $\boldsymbol{\beta}$ из $\boldsymbol{H}$, компоненты которого являются двоичными наборами длины $\lceil \log_2 M \rceil$. Покажем, как при помощи функций t, l, r и g вычислить функцию h. Вычисляющую функцию h схему S представим в виде пяти независимых подсхем.

1. Подсхема S_1 вычисляет $l_i = l(x_{k+1}, \ldots, x_n)$ и $r_i = r(x_{k+1}, \ldots, x_n)$. Из теоремы 4.3 следует, что

$$L(\mathsf{S}_1) = \mathcal{O}\left(\frac{2^{n-k}(\log_2 q + \log_2 T)}{n-k}\right) = \mathcal{O}\left(\frac{2^{n-k}\log_2 T}{n-k}\right). \tag{7.7}$$

2. Подсхемы S_2 и S_3 по вычисленным значениям l_i и r_i находят вектор $\boldsymbol{T}_i = (\boldsymbol{t}_{i1} \ldots \boldsymbol{t}_{ij} \ldots \boldsymbol{t}_{il_i})$. Сначала подсхема S_2 вычисляет значения функции t на s последовательных наборах, начиная с r_i-го набора. Затем подсхема S_3 оставляет в вычисленном подсхемой S_2 векторе первые $l_i p$ значений и дополняет получившийся вектор нулями до вектора длины qp. Из теоремы 4.2 следует, что при выполнении условия $s \ll T/\log_2^2 T$ справедливы неравенства

$$L(\mathsf{S}_2) \lesssim \varrho \cdot \frac{T}{\log_2 T}, \quad L(\mathsf{S}_3) \leqslant \mathcal{O}(s). \tag{7.8}$$

3. Подсхема S_4 разбивает вычисленный подсхемой S_3 вектор на q блоков длины p — номера $\boldsymbol{t}_{ij}$ и вычисляет значение $g(\boldsymbol{t}_{ij}) = \boldsymbol{\beta}_{ij}$ функции g на каждом из этих номеров, где результат $\boldsymbol{\beta}_{ij}$ — это набор из 2^k блоков $\boldsymbol{a}_{jv}$ длины $\lceil \log_2 M \rceil$, в котором блок $\boldsymbol{a}_{jv}$ является либо v-м элементом i-й строки таблицы H, если v-я позиция i-й строки попадает в j-й элементарный набор i-й строки таблицы T_f, либо нулевым набором в противном случае. Затем S_4 формирует 2^k векторов $\boldsymbol{b}_v$ длины $\lceil \log_2 M \rceil$ так, что вектор $\boldsymbol{b}_v$ вычисляется как покомпонентная дизъюнкция $\vee_j \boldsymbol{a}_{jv}$ блоков $\boldsymbol{a}_{jv}$ и в результате является v-м элементом вектора $\boldsymbol{\beta}_i = \vee_j \boldsymbol{\beta}_{ij}$, совпадающего с i-й строкой таблицы H.

Нетрудно видеть, что основная сложность в S_4 приходится на вычисление q значений $\lceil \log_2 p \rceil$-местной функции g. Поэтому в силу теоремы 4.3

$$\begin{aligned} L(\mathsf{S}_4) &= \mathcal{O}\left(\lceil 2^k \log_2 M / K \rceil \cdot 2^k \log_2 M \cdot \frac{M^2 2^{3k-1} 2^K}{\log_2(M^2 2^{3k-1} 2^K)}\right) = \\ &= \mathcal{O}\left(\frac{(\log_2 M)^2 M^2 2^{5k} 2^K}{K(3k + 2\log_2 M + K)}\right) = \mathcal{O}\left(\log_2 M \cdot M^2 2^{5k} 2^K K^{-1}\right). \end{aligned} \tag{7.9}$$

4. Подсхема S_5 по значениям переменных $x_1, \ldots, x_k$ выделяет из вычисленного подсхемой S_4 набора векторов $\boldsymbol{b}_v$ вектор, являющийся значением $h(\boldsymbol{x})$. Нетрудно видеть, что

$$L(\mathsf{S}_5) = \mathcal{O}\Big(2^k \log_2 M\Big). \tag{7.10}$$

Суммируя неравенства (7.7)–(7.10), видим, что

$$\begin{aligned} L(\mathsf{S}) \leqslant \varrho \cdot \frac{T}{\log_2 T} + \mathcal{O}\Bigg(&\frac{2^{n-k}\log_2 T}{n-k} + \\ &+ \log_2 M \cdot M^2 2^{5k} 2^K K^{-1} + 2^k \log_2 M + s \log_2 s\Bigg), \end{aligned} \tag{7.11}$$

где (см. (7.6))

$$T \leqslant I(f)\left(1 + \frac{2\log_2 M + 3k}{K}\right) + (2\log_2 M + 3k + K)2^{n-k}, \tag{7.12}$$

и неравенство (7.11) справедливо при выполнении условия

$$s \asymp \frac{(2\log_2 M + 3k + K)(2^k \log_2 M + K)}{K} \ll \frac{T}{\log_2^2 T}. \tag{7.13}$$

Положим

$$k = \lceil n - \log_2 I(f) + 2\log_2\log_2 I(f)\rceil,$$
$$K = \lfloor \log_2 I(f) - 2\log_2 M - 5k - 2\log_2\log_2 I(f)\rfloor.$$

Тогда при $n\to\infty$, учитывая условия $\log_2 I(f)\sim n$ и $\log_2 M \ll n$, имеем

$$\begin{aligned} K &\sim \log_2 I(f),\\ k &\ll \log_2 I(f),\\ K + 2\log_2 M + 5k &\leqslant \log_2 I(f) - 2\log_2\log_2 I(f),\\ n - k &\leqslant \log_2 I(f) - 2\log_2\log_2 I(f),\\ T &\lesssim I(f),\\ s &= 2^{o(\log_2 I(f))}. \end{aligned} \tag{7.14}$$

Из конструкции вектора $\boldsymbol{T}$ легко следует справедливость (7.13). Подставляя оценки из (7.14) в (7.12) и (7.11), после несложных преобразований получаем требуемую оценку сложности схемы S:

$$L(\mathsf{S}) \lesssim \varrho \cdot \frac{I(f)}{\log_2 I(f)}.$$

Лемма доказана.

Второй случай — средне определенные функции.

Л е м м а 7.5. *Пусть $D\to\infty$, B — полный конечный базис с минимальным приведенным весом ϱ, $n = \lceil \log_2 D\rceil$, $\log_2 I(f) \geqslant \frac{1}{4}n$, $\log_2 M \ll n$. Тогда*

$$L_B(f) \lesssim \varrho \cdot \frac{I(f)}{\log_2 I(f)}.$$

Д о к а з а т е л ь с т в о. Если $\log_2 I(f) \geqslant n - 2\log_2 M - 5\log_2 n$, то в этом случае $\log_2 I(f)\sim n$ и доказываемое неравенство следует из леммы 7.4. Поэтому далее полагаем, что $\log_2 I(f) \leqslant n - 2\log_2 M - 5\log_2 n$.

Пусть $(k_1, k_2, \ldots, k_M)$ — характеристика f. Прежде всего заметим, что, так как

$$2^{I(f)} = \left(\frac{M}{1}\right)^{k_1}\left(\frac{M}{2}\right)^{k_2}\cdots\left(\frac{M}{M}\right)^{k_M} \leqslant M^S,$$
$$2^{I(f)} \geqslant \left(\frac{M}{M-1}\right)^S \geqslant \left(1 + \frac{1}{M}\right)^S = \left(1 + \frac{1}{M}\right)^{M\cdot S/M} \geqslant 2^{S/M},$$

то из неравенств

$$\log_2 S - \log_2 M \leqslant \log_2 I(f) \leqslant \log_2 S + \log_2\log_2 M \tag{7.15}$$

и условий леммы легко следует, что

$$S \leqslant M \cdot I(f), \tag{7.16}$$
$$\log_2 I(f) \sim \log_2 S, \tag{7.17}$$
$$S \geqslant \frac{2^{n/4}}{\log_2 M}. \tag{7.18}$$

Положим $k = 3\log_2 n + \log_2 M$. К носителю функции f применим лемму 2.5. В результате для $s = \lfloor \log_2 S + 3\log_2 n + \log_2 M \rfloor < n$ найдется такой линейный оператор $\mathscr{L}\colon \{0,1\}^n \to \{0,1\}^s$, что множество

$$\boldsymbol{B} = \{(\boldsymbol{x}, \boldsymbol{y}) \mid \boldsymbol{x}, \boldsymbol{y} \in \boldsymbol{S}, \mathscr{L}(\boldsymbol{x}) = \mathscr{L}(\boldsymbol{y})\}$$

состоит не более чем из $Sn^{-3}M^{-1}$ пар наборов. Далее введем недоопределенную s-местную функцию

$$g(\boldsymbol{y}) = \begin{cases} f(\boldsymbol{x}), & \text{если } \exists \text{ единственный } \boldsymbol{x} \in \boldsymbol{S} \text{ такой, что } \boldsymbol{y} = \mathscr{L}(\boldsymbol{x}), \\ \boldsymbol{M} & \text{в противном случае,} \end{cases}$$

для которой значения $g(\mathscr{L}(\boldsymbol{x}))$ не совпадают со значениями $f(\boldsymbol{x})$ не более чем на $2Sn^{-3}M^{-1}$ наборах из $\{0,1\}^n$. Поэтому нетрудно видеть, что

$$2^{I(f)}M^{-S2n^{-3}M^{-1}} \leqslant 2^{I(g)} \leqslant 2^{I(f)}.$$

Следовательно, в силу условий леммы и неравенства (7.16)

$$I(f) - I(g) \leqslant \frac{2S\log_2 M}{n^3 M} = \\ = \mathcal{O}\left(\frac{I(f)\log_2 M}{n^3}\right) = \mathcal{O}\left(\frac{I(f)}{n^2}\right).$$

Таким образом, из предыдущего неравенства и (7.17)

$$\log_2 I(g) \sim \log_2 I(f) \sim s,$$

и для вычисления функции g можно воспользоваться леммой 7.4. Из этой леммы следует существование такого доопределение $\widehat{g}$ функции g, что

$$L_B(\widehat{g}) \lesssim \varrho \cdot \frac{I(f)}{\log_2 I(f)}.$$

Теперь заметим, что сложность линейного оператора $\mathscr{L}$ не превосходит n^2, и, следовательно, вычисление композиции $\widehat{g} \circ \mathscr{L}$ асимптотически не сложнее вычисления функции $\widehat{g}$:

$$L_B(\widehat{g} \circ \mathscr{L}) \lesssim \varrho \cdot \frac{I(f)}{\log_2 I(f)}.$$

Наконец, определим на $\{0,1\}^n$ полностью определенную функцию $h(\boldsymbol{x})$ так, чтобы покомпонентная сумма $h(\boldsymbol{x}) \oplus \widehat{g}(\mathscr{L}(\boldsymbol{x}))$ была доопределением $f(\boldsymbol{x})$, т. е. чтобы $h(\boldsymbol{x}) \oplus \widehat{g}(\mathscr{L}(\boldsymbol{x})) \in f(\boldsymbol{x})$. Для этого положим

$$h(\boldsymbol{x}) = \begin{cases} \boldsymbol{z}, & \text{если } \boldsymbol{x} \in \boldsymbol{S}, \text{ существует } \boldsymbol{y} \in \boldsymbol{S} \text{ такой,} \\ & \text{что } \mathscr{L}(\boldsymbol{y}) = \mathscr{L}(\boldsymbol{x}) \text{ и } \boldsymbol{z} \oplus \widehat{g}(\mathscr{L}(\boldsymbol{x})) \in f(\boldsymbol{x}), \\ \boldsymbol{0} & \text{в противном случае.} \end{cases}$$

Нетрудно видеть, что $h(\boldsymbol{x})$ отлична от нулевого набора не более чем на $2Sn^{-3}M^{-1}$ наборах из $\{0,1\}^n$. Поэтому, вычисляя компоненты h в со-

ответствии с их дизъюнктивными нормальными формами и учитывая условие $\log_2 M \ll n$ с неравенством (7.16), имеем

$$L_B(h) = \mathcal{O}\left(\frac{Sn\log_2 M}{n^3 M}\right) = \mathcal{O}\left(\frac{I(f)n\log_2 M}{n^3}\right) = o\left(\frac{I(f)}{\log_2 I(f)}\right).$$

Так как $L_B(f) \leqslant L_B(h) + L_B(\widehat{g}\circ\mathscr{L})$, то из двух последних выключенных неравенств следует, что $L_B(f) \sim L_B(\widehat{g}\circ\mathscr{L})$. Лемма доказана.

Третий случай — слабо определенные функции.

Лемма 7.6. *Пусть $D \to \infty$, B — полный конечный базис с минимальным приведенным весом ϱ, $n = \lceil \log_2 D \rceil$, $\log_2 I(f) \leqslant \frac{1}{3}n$ и $\log_2 M \ll \log_2 I(f)$. Тогда*

$$L_B(f) \lesssim \varrho \cdot \frac{I(f)}{\log_2 I(f)} + \mathcal{O}(n).$$

Доказательство. К носителю $\boldsymbol{S}$ применим лемму 2.6. В результате найдется такой линейный оператор $\mathscr{L}: \{0,1\}^n \to \{0,1\}^s$, где $s = \lfloor 2\log_2 S \rfloor < n$, для которого в области $\boldsymbol{S}$ нет таких элементов $\boldsymbol{x}$ и $\boldsymbol{y}$, что $\mathscr{L}(\boldsymbol{x}) = \mathscr{L}(\boldsymbol{y})$. Далее введем недоопределенную s-местную функцию

$$g(\boldsymbol{y}) = \begin{cases} f(\boldsymbol{x}), & \text{если } \exists\, \boldsymbol{x} \in \boldsymbol{S} \text{ такой, что } \boldsymbol{y} = \mathscr{L}(\boldsymbol{x}), \\ \boldsymbol{M} & \text{в противном случае.} \end{cases}$$

Нетрудно видеть, что в этом случае $f(\boldsymbol{x}) = g(\mathscr{L}(\boldsymbol{x}))$ и $I(g) = I(f)$. Так как $s \sim 2\log_2 S$ и (см. (7.15))

$$\log_2 S - \log_2 M \leqslant \log_2 I(f) \leqslant \log_2 S + \log_2\log_2 M,$$

то $\log_2 I(g) \sim \log_2 S \sim s/2$ и при достаточно больших n становится справедливым уже неасимптотическое неравенство $\log_2 I(g) \geqslant s/3$ и, следовательно, можно воспользоваться леммой 7.5. В силу этой леммы при $n \to \infty$

$$L_B(g) \lesssim \varrho \cdot \frac{I(f)}{\log_2 I(f)}. \tag{7.19}$$

Наконец, заметим, что для сложности линейного оператора $\mathscr{L}$ справедливо неравенство

$$L_B(\mathscr{L}) = \mathcal{O}\left(\frac{n(s+\log_2 n)}{\log_2 n}\right) = \mathcal{O}\left(\frac{n(\log_2 I(f) + \log_2 n)}{\log_2 n}\right). \tag{7.20}$$

Легко видеть, что при $n \to \infty$ сумма правых частей неравенств (7.19) и (7.20) не превосходит $\varrho \cdot \frac{I(f)}{\log_2 I(f)} + \mathcal{O}(n)$. Лемма доказана.

СПИСОК ЛИТЕРАТУРЫ

1. Андреев А. Е. О сложности реализации частичных булевых функций схемами из функциональных элементов // Дискретная математика. — 1989. — Т. 1, № 4. — С. 36–45.
2. Кричевский Р. Е. Сжатие и поиск информации. — М.: Радио и связь, 1989.

3. Лупанов О. Б. О вентильных и контактно-вентильных схемах // Доклады АН СССР. — 1956. — Т. 111, № 6. — С. 1171–1174.
4. Лупанов О. Б. Об одном методе синтеза схем // Известия высших учебных заведений. Серия радиофизика. — 1958. — № 1. — С. 120–140.
5. Лупанов О. Б. О принципе локального кодирования и реализации функций из некоторых классов схемами из функциональных элементов // Доклады АН СССР. — 1961. — Т. 140, № 2. — С. 322–325.
6. Лупанов О. Б. Об одном подходе к синтезу управляющих систем — принципе локального кодирования // Проблемы кибернетики. Вып. 14. — М.: Наука, 1965. — С. 31–110.
7. Лупанов О. Б. Асимптотические оценки сложности управляющих систем. — М.: Изд-во Московского университета, 1984. — (2-е издание: 2024 г.)
8. Лупанов О. Б. О некоторых случаях принципа локального кодирования // Discrete mathematics. Banach Center Publications. Vol. 7. — Warsaw: PWN, 1982. — P. 209–215. — DOI: 10.4064/-7-1-209-215.
9. Нечипорук Э. И. О синтезе вентильных схем // Проблемы кибернетики. Вып. 9. — М.: Физматгиз, 1963. — С. 37–44.
10. Нечипорук Э. И. О сложности вентильных схем, реализующих булевские матрицы с неопределенными элементами // Доклады АН СССР. — 1965. — Т. 163, № 1. — С. 40–42.
11. Нечипорук Э. И. О топологических принципах самокорректирования // Проблемы кибернетики. Вып. 21. — М.: Наука, 1969. — С. 5–102.
12. Чашкин А. В. Об одном методе вычисления частичных булевых функций // Математические вопросы кибернетики. Вып. 12. — М.: ФИЗМАТЛИТ, 2003. — С. 231–246.
13. Чашкин А. В. О сложности реализации булевых функций формулами // Дискретный анализ и исследование операций. — 2005. — Т. 12, № 2. — С. 56–72.
14. Чашкин А. В. Методы вычисления частичных булевых функций // Труды VII Международной конференции «Дискретные модели в теории управляющих систем» (Покровское, Московская область, 4–6 марта 2006 г.). — М.: МАКС Пресс, 2006. — С. 390–404.
15. Чашкин А. В. Дискретная математика. — М.: Академия, 2012.
16. Чашкин А. В. О линейных операторах, инъективных на произвольных подмножествах // Ученые записки Казанского университета. Серия Физико-математические науки. — 2014. — Т. 156, № 3. — С. 132–141.
17. Чашкин А. В. О средней сложности недоопределенных функций // Дискретная математика. — 2017. — Т. 29, № 2. — С. 133–159.
18. Чашкин А. В. Асимптотические оценки средней сложности булевых функций // Математические вопросы кибернетики. Вып. 20. — М.: ФИЗМАТЛИТ, 2022. — С. 257–306.
19. Шоломов Л. А. О функционалах, характеризующих сложность систем недоопределенных булевых функций // Проблемы кибернетики. Вып. 19. — М.: Наука, 1967. — С. 123–140.
20. Шоломов Л. А. О реализации недоопределенных булевых функций схемами из функциональных элементов // Проблемы кибернетики. Вып. 21. — М.: Наука, 1969. — С. 215–226.
21. Шоломов Л. А. Информационные свойства функционалов сложности для систем недоопределенных булевых функций // Проблемы кибернетики. Вып. 34. — М.: Наука, 1978. — С. 133–150.
22. Andreev A. E. Complexity of Nondeterministic Functions // BRICS Report Series. — 1994. — V. 1, No. 2. — DOI: 10.7146/brics.v1i2.21668.
23. 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 // Automata, Languages and Programming : LNCS. Vol. 1256 (ICALP 1997) / Ed. by P. Degano, R. Gorrieri, A. Marchetti-Spaccamela. — Berlin, Heidelberg : Springer, 1997. — P. 177–187.
24. 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 // Theoretical Computer Science. — 1999. — V. 221, No. 1/2. — P. 3–18. — DOI: 10.1016/s0304-3975(99)00024-9.
25. Gelfand S. I., Dobrushin R. L., Pinsker M. S. On the Complexity of Coding // Second International Symposium on Information Theory. — Akademiai Kiado, Budapest, 1973. — P. 177–184.

26. Miltersen P. B. Error correcting codes, perfect hashing circuits, and deterministic dynamic dictionaries // Proceedings of the Ninth Annual ACM-SIAM Symposium on Discrete Algorithms (San Francisco, California, USA, Jan. 25–27, 1998) / Ed. by H. J. Karloff. — ACM/SIAM, 1998. — P. 556–563. — URL: http://dl.acm.org/citation.cfm?id=314613.314845.
27. Miltersen P. B. On the Shannon function for partially defined Boolean functions // ICALP Workshops 2000, Proceedings of the Satelite Workshops of the 27th International Colloquium on Automata, Languages and Programming (Geneva, Switzerland, July 9–15, 2000) / Ed. by J. D. P. Rolim et al. — Carleton Scientific, Waterloo, Ontario, Canada, 2000. — P. 253–258.
28. Pippenger N. Information theory and the complexity of boolean functions // Mathematical Systems Theory. — 1976. — V. 10, No. 1. — P. 129–167. — DOI: 10.1007/bf01683269.
29. Spielman D. A. Linear-time encodable and decodable error-correcting codes // IEEE Transactions on Information Theory. — 1996. — V. 42, No. 6. — P. 1723–1731. — DOI: 10.1109/18.556668.
30. Sudan M. Essential Coding Theory. — 2002. — URL: http://people.csail.mit.edu/madhu/FT02/.

Поступило в редакцию 15 VI 2024