ФГБОУ ВО Московский государственный университет
имени М. В. Ломоносова
Механико-математический факультет

На правах рукописи

УДК 519.7

Подольская Ольга Викторовна

Оценки сложности булевых функций в некоторых бесконечных базисах

01.01.09 — дискретная математика и математическая кибернетика

ДИССЕРТАЦИЯ
на соискание учёной степени
кандидата физико-математических наук

Научный руководитель:
доктор физико-математических наук,
профессор О. М. Касим-Заде

Москва — 2017

Содержание

Введение

Общая характеристика работы

Актуальность темы

Данная диссертация относится к теории синтеза и сложности управляющих систем — одному из основных направлений дискретной математики и математической кибернетики. Задача синтеза управляющих систем — это одна из важнейших задач математической кибернетики. В общем виде эта задача сформулирована, например, в [45] и может быть описана следующим образом. Заданы множество базисных элементов и правила построения из них более сложных объектов, называемых управляющими системами. В качестве управляющих систем могут рассматриваться, например, схемы из функциональных элементов, формулы, контактные схемы и т.д. Каждый базисный элемент реализует некоторую функцию, и определено правило, согласно которому всякой построенной из этих элементов управляющей системе сопоставляется реализуемая ею функция. Возникает задача построения для каждой функции управляющей системы в заданном базисе, реализующей эту функцию. В такой формулировке задача решается неоднозначно: может быть построено несколько различных управляющих систем, реализующих одну и ту же функцию, но обладающих различными особыми характеристиками (такими как сложность, стоимость, временная задержка и т.д.). Поэтому задача естественным образом уточняется: для каждой функции требуется построить управляющую систему, которая была бы наилучшей с точки зрения некоторой заданной характеристики. В качестве такой характеристики чаще всего рассматривается некоторая мера сложности управляющей системы — неотрицательное число, которое характеризует систему. Счи-

тается, что чем меньше значение этой характеристики у управляющей системы, тем эта система «лучше» с точки зрения данной меры сложности.

Окончательно задача синтеза может быть сформулирована так: требуется построить по любой заданной функции такую управляющую систему, которая реализует эту функцию и обладает минимально возможным значением сложности (в предположении, что указанный минимум достигается — в противном случае задача соответствующим образом модифицируется). Это минимальное значение называется сложностью функции.

В диссертации изучается задача о реализации булевых функций схемами из функциональных элементов в бесконечных базисах. В данной работе *базисом* называется произвольное функционально полное множество булевых функций, т. е. такое множество, что всякая булева функция выражается через функции из этого множества с помощью операции суперпозиции. Будем называть базис *бесконечным*, если для всякого натурального числа k существует функция в этом базисе, которая существенно зависит не менее чем от k переменных; иначе будем называть базис конечным (см., например, [9]).

Мы используем обычное определение понятия схемы из функциональных элементов, (см., например, [25, 30]), подробно оно приведено в главе 1.

В работе изучается характеристика схемы, называемая сложностью схемы, которая определяется следующим образом. Каждой схеме S в заданном базисе B ставится в соответствие неотрицательное число $L_B(S)$, которое равно числу элементов в этой схеме; $L_B(S)$ называется *сложностью схемы* S в базисе B. Для каждой булевой функции f ее *сложность* в базисе B обозначается через $L_B(f)$ и определяется следующим образом: $L_B(f) = \min L_B(S)$, где минимум берется по всем схемам S, реализующим функцию f в этом базисе (подробнее об этих и других понятиях см., например, в [25, 46, 47, 61, 62]).

Известны и другие меры сложности, относящиеся к различным существующим классам управляющих систем: например, для контактных схем — число контактов, для схем из функциональных элементов — сумма весов

(стоимость) элементов, глубина, задержка, мощность и другие (см., например, [1,16,23,28,67]). Отметим, что в данной работе изучается только одна мера сложности: сложность схемы как число функциональных элементов в этой схеме, и другие меры сложности не рассматриваются.

Как правило, существует тривиальное решение задачи о нахождении сложности функции в определенном базисе методом перебора всех схем заданной сложности, но на практике оно оказывается малоэффективным, поскольку обладает большой алгоритмической сложностью. В связи с этим для описания сложности схем вводится соответствующая базису B функция Шеннона $L_B(n)$, определяемая следующим соотношением: $L_B(n) = \max L_B(f)$, где максимум берется по всем булевым функциям f, зависящим от n переменных, и изучается поведение этой функции. По существу, $L_B(n)$ есть наименьшее число элементов, достаточное для реализации любой булевой функции от n переменных схемами в базисе B (подробнее см., например, [25]). Такой подход был предложен К. Э. Шенноном в [67], где был впервые применен для контактных схем. Нахождение функции Шеннона в точном виде в большинстве случаев оказывается практически невозможным. Отсюда возникают задачи приближенного вычислений этой функции, нахождение ее порядка роста, и в некоторых случаях удается найти асимптотику роста этой функции.

Для описания асимптотического поведения действительнозначных функций, сравнения порядков их роста в работе используются обычные понятия асимптотического равенства (неравенства) [31], равенства (неравенства) по порядку и другие. Подробно эти понятия и обозначения для них введены в главе 1.

Известно, что для всех конечных базисов порядки роста функции Шеннона одинаковы и равны $\frac{2^n}{n}$ [59]. Асимптотически точно поведение порядков роста функции Шеннона для всех конечных базисов с положительными весами элементов было исчерпывающе описано О. Б. Лупановым [30]: в случае произвольного конечного базиса B было показано, что $L_B(n) \sim \rho \cdot \frac{2^n}{n}$, где ρ — константа, зависящая только от базиса.

Бесконечные базисы с точки зрения вопросов сложности изучены значительно меньше, чем конечные. Поведение функций Шеннона в них гораздо более разнообразно. Дадим краткий обзор истории предыдущих исследований, относящихся к тематике сложности схем в бесконечных базисах. Данный обзор отражает основные моменты и не претендует на исчерпывающую полноту.

В одной из первых работ, имеющих отношение к проблеме синтеза схем в бесконечных базисах, Е. Ю. Захарова [2] изучала сложность реализации булевых функций в классе схем, в котором допускается реализация булевых функций элементами и простым «склеиванием» проводников (так называемое, «проводное "и"»). Фактически, эта задача предшествует задаче синтеза схем в бесконечных базисах. Для такого класса схем (в [2] он называется классом схем из ламповых элементов) было показано, что асимптотика функции Шеннона в некоторых базисах может быть существенно уменьшена по сравнению с классом обычных схем из функциональных элементов.

Согласно основому тезису об управляющих системах, сформулированному С. В. Яблонским [45], для каждой физической управляющей системы может быть построена математическая управляющая система, адекватно изображающая схемно-функциональные характеристики этой физической управляющей системы. В этом смысле схемы из функциональных элементов в бесконечных базисах могут рассматриваться как математические модели некоторых физических управляющих систем. Например, на практике встречаются задачи, в которых число входов элемента может быть сравнимо со сложностью схемы, то есть теоретически число входов базисных элементов потенциально не ограничено. Одна из наиболее разработанных моделей с такими свойствами — схемы из пороговых функциональных элементов, которые определены ниже.

Булева функция $f(x_1, \ldots, x_n)$ называется *пороговой*, если существуют действительные числа $w_1, \ldots, w_n, h$ такие, что $w_1x_1 + \ldots + w_nx_n \geqslant h$ тогда и только тогда, когда $f(x_1, \ldots, x_n) = 1$; схема из функциональных элементов, каждому

элементу которой приписана некоторая пороговая функция, называется *схемой из пороговых элементов*, а ее элементы — *пороговыми элементами* [29].

По существу, пороговые функциональные элементы могут рассматриваться как простейшая модель нейронов в нервной системе живых организмов. Первой формальной моделью нейронных сетей является модель, предложенная У. Мак-Каллоком и У. Питтсом [60], ее уточнил и развил затем С. К. Клини [57].

Задачей о сложности реализации булевых функций схемами в базисе, состоящем из всех пороговых функций, занимались многие авторы, при этом, вообще говоря, рассматривались разные меры сложности схем (число элементов схемы [29, 36, 40, 71], сумма абсолютных значений весов переменных во всех пороговых элементах схемы [3]). Э. И. Нечипорук [36] установил порядок роста функции Шеннона сложности схем в этом базисе. Полное решение задачи об асимптотике функции Шеннона было получено О. Б. Лупановым: в [29] было доказано, что $L_T(n) \sim 2 \cdot \left(\frac{2^n}{n}\right)^{1/2}$, где T — базис всех пороговых функций.

Известны результаты о конечных базисах из нетривиальных элементов с нулевыми весами, которые естественным образом соответствуют некоторым бесконечным базисам. В частности, в [33, 55] рассматривались схемы в базисах, в которых элементам, реализующим конъюнкции и дизъюнкции, приписывался нулевой вес, а инвертору, то есть элементу, реализующему отрицание, — единичный, и изучалась задача синтеза схем для заданных функций с минимально возможным суммарным весом всех элементов схемы. Интерес к изучению указанной меры сложности, которая обычно называется *инверсионной сложностью*, возник в связи с тем, что на практике в некоторых технологиях изготовления реальных электронных схем элементы, реализующие отрицание, более дороги и менее надежны, чем элементы, которые реализуют другие функции [55].

Начало изучению инверсионной сложности было положено работой Э. Н. Гилберта [55], где рассматривалась соответствующая задача синтеза в классе контактных схем. В [55] было показано, что порядок роста функции Шеннона инверсионной сложности равен $\log_2 n$. А. А. Марков [33] получил точ-

ное выражение для инверсионной сложности булевой функции: $\lceil \log_2(r(f)+1) \rceil$, где $r(f)$ — максимальное число перемен значений функции f с 1 на 0, максимум берется по всем возрастающим цепям наборов значений переменных. При этом он получил точное выражение для функции Шеннона инверсионной сложности: $\lfloor \log_2(n+1) \rfloor$. Также А. А. Марковым была установлена точная формула для инверсионной сложности произвольной системы булевых функций [34]. По-видимому, это были первые результаты, прямо связанные с бесконечными базисами: указанному базису из элементов с нулевыми весами соответствует, например, бесконечный базис, состоящий из всех монотонных булевых функций и их отрицаний, функция Шеннона в этом базисе асимптотически совпадает с функцией Шеннона инверсионной сложности.

Э. И. Нечипорук рассматривал задачу о синтезе схем в базисах, содержащих элементы с нулевыми весами, в общей постановке: он изучал сложность схем из функциональных элементов в базисах, часть которых составляют элементы с произвольными положительными весами, а оставшуюся часть — элементы с нулевыми весами [35,37]. В [35], в частности, была найдена асимптотика функции Шеннона вида $\sim \sqrt{2} \cdot 2^{n/2}$ для базиса, в котором дизъюнкция двух переменных имеет вес 0, а отрицание — вес 1. Та же асимптотика имеет место для бесконечного базиса, состоящего из функции отрицания и всевозможных дизъюнкций переменных.

Отметим также работы [20, 21], где изучалась вопросы сложности реализации булевых функций схемами в конечных базисах с произвольными ненулевыми весами элементов.

До сих пор говорилось о постановке задачи синтеза схем, реализующих произвольные функции, и об оценках функции Шеннона. При синтезе схем выделяют более узкие специальные классы функций и для них рассматривают постановку задачи синтеза «шенноновского» типа: изучают поведение наибольшей сложности функций от заданного числа переменных из определенного класса.

Одним из наиболее изученных с точки зрения такой постановки задачи является класс всех симметрических булевых функций [27].

Функция называется *симметрической*, если при любой перестановке своих переменных она не изменяется. Всюду далее, говоря «симметрические функции», мы будем иметь в виду симметрические булевы функции.

Первые результаты о реализации симметрических функций были получены К. Э. Шенноном для класса контактных схем [66], позднее они развивались и усиливались (см., например, [27,67]). В классе схем из функциональных элементов О. Б. Лупановым [26] было показано, что всякая симметрическая функция реализуется с линейной относительно числа переменных сложностью в любом конечном базисе.

Для базиса B_2, состоящего из всех булевых функций, существенно зависящих от не более чем двух переменных, из [26] известна верхняя оценка $5n$ сложности произвольной симметрической булевой функции n переменных, в [52] эта оценка была улучшена и понижена до $4.5n$. Что касается нижних оценок сложности симметрических функций в этом базисе, то, по-видимому, наилучшей из известных является оценка $2.5n$, доказанная для симметрических функций от n переменных специального вида [68]. Подробнее об этих и других результатах см. [44, 51, 53, 72].

Отметим также результат для базиса U_2, состоящего из всех элементов, реализующих нелинейные функции, существенно зависящие от двух переменных: по-видимому, наилучшая известная нижняя оценка сложности реализации симметрических функций от n переменных в этом базисе (полученная для некоторых симметрических функций специального вида [74]) составляет $4n$.

Также для базиса T всех пороговых функций известна асимптотика функции Шеннона $L_T(\Sigma^n) = \max L_T(f)$, где максимум берется по всем симметрическим функциям f от n переменных, полученная О. Б. Лупановым [29]: $L_T(\Sigma^n) \sim 2 \cdot (\frac{n}{\log_2 n})^{1/2}$.

Одними из важнейших симметрических функций являются линейные функции и функции голосования. Эти функции представляют особый интерес и на протяжении многих лет изучались различными авторами.

Здесь и далее *линейной функцией* называется булева функция, определяемая соотношением $l_n(x_1, \ldots, x_n) = x_1 + \ldots + x_n \pmod 2$; булева функция $m_n(x_1, \ldots, x_n)$, принимающая значение 1 на тех и только тех наборах, в которых число единиц не меньше $\frac{n}{2}$, называется *функцией голосования.*

В ряде работ были получены точные формулы, выражающие сложность линейной функции и ее отрицания в некоторых конечных и бесконечных базисах. В частности, были установлены точные формулы для классического базиса $\{\&, \vee, \neg\}$ [41]: $L_{\{\&,\vee,\neg\}}(l_n) = L_{\{\&,\vee,\neg\}}(\overline{l_n}) = 4n - 4$, для базиса «штрих Шеффера» [14, 42]: $L_{x|y}(l_n) = 4n - 4$, $L_{x|y}(\overline{l_n}) = 4n - 3$, а также для базиса U_2 [64]: $L_{U_2}(l_n) = L_{U_2}(\overline{l_n}) = 3n - 3$ (по сути, в упомянутой выше работе [74] содержится обобщение этого результата).

Что касается бесконечных базисов, то одними из первых в этом направлении были получены точные формулы сложности линейной функции и ее отрицания в базисе B обобщенных «стрелок Пирса» $\{\overline{x_1 \vee \ldots \vee x_k}\}$, $k \in \{2, 3, \ldots\}$ [58]: $L_B(l_n) = L_B(\overline{l_n}) = 3n - 2$ при всех $n \geqslant 3$, $L_B(l_2) = 5$, $L_B(\overline{l_2}) = 4$. Этот результат переносится на двойственный базису B базис B^*, состоящий из обобщенных «штрихов Шеффера» $\{\overline{x_1 \& \ldots \& x_k}\}$, $k \in \{2, 3, \ldots\}$ [58]: $L_{B^*}(l_n) = L_{B^*}(\overline{l_n}) = 3n - 2$ при всех $n \geqslant 3$. В англоязычной литературе базисы B и B^* часто обозначают NOR и $NAND$ соответственно.

В [73] изучалась сложность линейной функции и ее отрицания в базисе U_∞, состоящем из элементов, которые реализуют функции вида $(x_1^{\sigma_1} \& \ldots \& x_k^{\sigma_k})^\beta$, где $k \in \{2, 3, \ldots\}$, $\sigma_1, \ldots, \sigma_k, \beta \in \{0, 1\}$, x^α равно x при $\alpha = 1$ и $\overline{x}$ при $\alpha = 0$. Было доказано [73], что $2n - 1 \leqslant L_{U_\infty}(l_n) \leqslant \left\lceil \frac{5(n-1)}{2} \right\rceil$ при всех $n \geqslant 2$, и то же верно для $L_{U_\infty}(\overline{l_n})$. Верхняя оценка для l_n была затем улучшена в [15], где доказана оценка $L_{U_\infty}(l_n) \leqslant \left\lceil \frac{7n-4}{3} \right\rceil$.

В [73] также установлено точное равенство сложности линейной функции и ее отрицания в базисе T пороговых функций: $L_T(l_n) = L_T(\overline{l_n}) = \lceil \log_2(n+1) \rceil$.

Кроме того, известно значительное число результатов, относящихся к реализации симметрических функций формулами и схемами ограниченной глубины, которые также могут рассматриваться как схемы специального вида в бесконечных базисах. Однако, в данной работе эти результаты не приводятся, поскольку основное внимание в диссертации сосредоточено на вопросах реализации функций схемами из функциональных элементов без ограничений. Укажем лишь на известные результаты о сложности реализации симметрических функций формулами [43], функции голосования монотонными формулами [70], а также результаты о схемах ограниченной глубины для функции голосования [39, 65] и линейной функции [49, 50, 54]. Также следует упомянуть важные результаты об оценках сложности схем в неполных базисах (см., например, [38]).

Наряду с числом элементов (весом) схем, одна из важнейших мер их сложности — глубина (задержка). *Глубиной* схемы называется наибольшее число функциональных элементов, составляющих ориентированную цепь, ведущую от входов схемы к ее выходу; соответствующую функцию Шеннона для схем в заданном базисе B принято обозначать через $D_B(n)$ (см., например, [10–12, 18, 19, 22, 28]). Для любого конечного базиса B булевых функций О. Б. Лупановым [28] было показано, что $D_B(n) \sim C \cdot n$, где C — некоторая константа конкретного вида, зависящая только от базиса.

В первых работах, посвященных изучению глубины в случае бесконечных базисов, в основном были установлены асимптотики и порядки роста функции Шеннона глубины для конкретных базисов, причем во всех примерах эти порядки роста оказывались равными либо 1 (например, для базиса всех булевых функций или для базиса пороговых функций [29]), либо $\log_2 n$ (см., например, [22]). О. М. Касим-Заде [10, 11] установил, что функция Шеннона глубины для любого бесконечного базиса булевых функций по порядку роста равна либо 1, либо $\log_2 n$; эти результаты были усилены затем в [12].

А. В. Кочергин, по-видимому, первым начал исследовать поведение функции Шеннона глубины для случая конечных и бесконечных базисов, состоящих из функций k-значной логики, где $k \geqslant 3$, и ему удалось полностью описать качественную картину асимптотического поведения функции Шеннона глубины в этом случае [18, 19]. В [19] было установлено, что для произвольного конечного базиса B функций k-значной логики $D_B(n) \sim \widetilde{C} \cdot n$, где константа $\widetilde{C}$ выражается через логарифм некоторого алгебраического числа и зависит только от базиса, а также предложен алгоритм нахождения по базису указанной константы. Что касается бесконечных базисов, то в [18] было доказано, что порядок роста функции Шеннона глубины либо равен 1, либо равен $\log_2 n$. Тем самым было показано что эффекты, описанные для случая булевых функций, распространяются и на случай функций k-значной логики, где $k \geqslant 3$.

Вернемся к изучаемой в диссертации характеристике схемы — сложности. В работе Н. А. Карповой [4] рассматривались бесконечные базисы, в которых каждому базисному элементу приписан произвольный неотрицательный вес, а сложность схемы определяется как сумма весов входящих в нее элементов, и исследовался следующий вопрос: какие числовые функции могут быть функциями Шеннона в таких базисах? Нахождение точного и полного ответа на этот вопрос представляется практически невозможным, поэтому задача рассматривалась с точки зрения асимптотической характеризации функций Шеннона. Н. А. Карпова установила необходимые и достаточные условия, которым должна удовлетворять числовая функция, асимптотически равная функции Шеннона в некотором бесконечном базисе из элементов с произвольными неотрицательными весами. Таким образом, была дана полная характеризация функций, асимптотически равных функциям Шеннона в таких бесконечных базисах [4]. Отметим, что задача нахождения по заданному бесконечному базису функции Шеннона сложности в этом базисе Н. А. Карповой в указанной работе не рассматривалась.

Вообще говоря, не известно какого-либо общего метода, с помощью которого по произвольному бесконечному базису можно найти порядок роста соответствующей функции Шеннона или хотя бы оценить ее с некоторой точностью, например, с точностью до полиномиальной эквивалентности (функции $a(n)$ и $b(n)$ называются *полиномиально эквивалентными*, если существуют такие многочлены $P_1(x)$, $P_2(x)$, что при всех достаточно больших n выполнено: $a(n) \leqslant P_1(b(n))$, $b(n) \leqslant P_2(a(n))$) [7].

Как известно, в большинстве случаев нижние оценки функций Шеннона в различных классах управляющих систем устанавливаются *мощностным методом*. Этот метод, по сути, основан на сравнении количества схем заданной сложности и количества функций, допускающих реализацию схемами этой сложности. Такой метод, по-видимому, впервые был использован в работе Дж. Риордана и К. Шеннона [63].

О. М. Касим-Заде [8] предложил новый метод получения двусторонних оценок функций Шеннона в произвольных бесконечных базисах, который позволяет при достаточно слабых ограничениях оценивать рост функций Шеннона с точностью до полиномиальной эквивалентности. Метод получения нижних оценок в [8] основан на «мощностных» соображениях и восходит к [29,36]. Что касается верхних оценок, то предложенный в [8] метод позволяет получать верхние оценки функции Шеннона, сопоставимые с ее мощностной нижней оценкой. Эти результаты получили развитие в [9], где были получены более точные оценки.

В общих чертах качественная картина поведения порядков роста функций Шеннона в бесконечных базисах была описана О. М. Касим-Заде в [13]. Для дальнейшего изложения введем еще два определения.

Если выполнено соотношение $a(n) = O(b(n))$, то, следуя [13], *интервалом* между функциями $a(n)$ и $b(n)$ будем называть множество всех действительнозначных функций $c(n)$ натурального аргумента, принимающих положительные значения при всех достаточно больших n и удовлетворяющих условиям $c(n) = \Omega(a(n))$ и $c(n) = O(b(n))$. Если функция $c(n)$ лежит в интервале между

функциями $a(n)$ и $b(n)$ и по порядку роста не совпадает ни с одной из них, то будем говорить, что функция $c(n)$ лежит *строго в интервале* между функциями $a(n)$ и $b(n)$.

В [7] О. М. Касим-Заде доказал, что для всякого бесконечного базиса B выполняется соотношение $L_B(n) = O(2^{n/2})$. С точностью до константы эта оценка является, вообще говоря, не улучшаемой: из работы Э. И. Нечипорука [35], в частности, известен пример бесконечного базиса, в котором порядок роста функции Шеннона равен $2^{n/2}$. Результаты работ Э. Н. Гилберта [55] и А. А. Маркова [33] дают пример бесконечного базиса с порядком роста функции Шеннона равным $\log_2 n$. Результаты Э. И. Нечипорука [36] и О. Б. Лупанова [29] о схемах в базисе пороговых функций дают пример бесконечного базиса с порядком роста функции Шеннона равным $(\frac{2^n}{n})^{1/2}$. Отметим еще базис B, состоящий из всех булевых функций, для которого $L_B(n) = 1$ при всех натуральных n.

Согласно классификации, описанной в [13], для любого бесконечного базиса порядок роста функции Шеннона либо равен 1, либо лежит в одном из двух интервалов: или между функциями $\log_2 n$ и n, или между функциями n и $2^{n/2}$.

Таким образом, для всякого бесконечного базиса порядок роста функции Шеннона либо равен 1, либо не меньше $\log_2 n$. Иначе говоря, не существует базиса, для которого порядок роста функции Шеннона лежит строго в интервале между функциями 1 и $\log_2 n$ [13].

В [13] установлено, что существуют базисы с порядком роста функции Шеннона равным n. Из этого факта и приведенных выше результатов следует, что границы 1, $\log_2 n$, n и $2^{n/2}$ каждого из интервалов, указанных в классификации порядков роста функций Шеннона [13], достижимы.

Отметим, что порядок роста функции Шеннона $(\frac{2^n}{n})^{1/2}$, относящийся к базису пороговых функций, лежит строго в интервале между функциями n и $2^{n/2}$. Можно показать, что число базисов с различными порядками роста функций Шеннона в этом интервале бесконечно; обширное семейство таких базисов построено в работе [13].

Содержательно (подробнее см. [13]) *классом* L называется множество функций от одной действительной переменной, состоящее из тождественной функции x, всех действительных констант, и такое, которое вместе с любыми двумя функциями $f(x)$, $g(x)$ содержит все функции, финально эквивалетные функциям $f(x)+g(x)$, $f(x)-g(x)$, $f(x)g(x)$, $e^{f(x)}$, $g(x)/f(x)$, $\log_2|f(x)|$ (финальная эквивалентность означает равенство функций для всех значений аргумента, начиная с некоторого числа).

В [13] показано, что для любой функции λ, принадлежащей классу L и удовлетворяющей условиям: $\lambda(n) = \Omega(n), \log_2 \lambda(n) = O(n^{1/2})$, существует бесконечный базис, в котором функция Шеннона по порядку роста равна функции λ. В частности, из этого результата вытекает, что порядками роста функции Шеннона являются, например, функции $n \log_2 n$, $n \log_2 \log_2 n$, n^2, $n^{\frac{3}{2}}$, $n^{\sqrt{2}}$, $2^{\sqrt[3]{n}}$ и другие (подробнее см. [13]).

Что касается интервала между функциями $\log_2 n$ и n, то ответ на вопрос «существуют ли базисы, в которых порядки роста функций Шеннона лежат строго в этом интервале?» до сих пор оставался неизвестным.

Упоминавшийся выше метод получения оценок, предложенный в [8], в частности, дает следующий результат: если полученная посредством него мощностная нижняя оценка функции Шеннона в данном бесконечном базисе по порядку не ниже линейной (и тем самым функция Шеннона попадает в интервал от n до $2^{n/2}$), то функция Шеннона по порядку заключена между этой нижней оценкой и ее квадратом. В интервале от $\log_2 n$ до n это свойство, вообще говоря, не выполняется, зачастую для таких бесконечных базисов получение достаточно точных нижних оценок их функций Шеннона требует привлечения иных соображений. По-видимому, впервые этот эффект был обнаружен при изучении базиса антицепных функций.

Введем некоторые определения, которые потребуются для дальнейшего изложения.

Рассмотрим булев куб $\{0,1\}^n$ как частично упорядоченное множество наборов с естественным порядком декартова произведения. *Антицепью* булева куба будем называть всякое подмножество булева куба, состоящее из попарно несравнимых наборов. Булева функция, принимающая значение 1 лишь на некоторой антицепи, называется *антицепной*.

Множество всех антицепных функций образует бесконечный базис, который обозначается через AC (см. [5]). В базис AC также включаются функции-константы 0 и 1, по соглашению не имеющие переменных. С содержательной точки зрения им соответствуют функциональные элементы без входов, реализующие на выходе константы 0 и 1 соответственно. Множество AC замкнуто относительно операций подстановки констант и отождествления переменных, и всякая булева функция выражается через функции из множества AC с помощью операции суперпозиции (система AC полна, поскольку, например, функции $\overline{x}$, $x\&y$ являются антицепными, а их совокупность, как известно [31], образует базис). Особый интерес к базису AC вызван, в частности, причинами, о которых рассказано в данном введении на с. 21 – 22. На необходимость изучения теоретико-сложностных свойств базиса AC обращал внимание О. Б. Лупанов (см. [5]).

Изучение базиса антицепных функций началось с работ О. М. Касим-Заде [5, 6]. В [5] была доказана нижняя оценка $\Omega(n^{1/3})$ сложности линейной функции от n переменных, из которой очевидным образом была установлена нижняя оценка функции Шеннона $L_{AC}(n)$ такого же порядка. Также в [5] была установлена простейшая верхняя оценка $n+1$ для сложности произвольной булевой функции от n переменных. В [6] О. М. Касим-Заде доказал нижнюю оценку $\Omega((n/\ln n)^{1/2})$ сложности линейной функции от n переменных, тем самым улучшив предыдущую нижнюю оценку функции Шеннона.

Также для дальнейшего изложения потребуется следующее понятие. Когда мы говорим, что какое-то свойство выполнено для *почти всех функций* от n переменных, имеется в виду, что отношение числа функций, для которых это

свойство выполняется, к числу всех функций от n переменных стремится к единице при $n \longrightarrow \infty$.

Цель работы

Основной целью данной диссертации является исследование поведения функции Шеннона сложности булевых функций при реализации схемами в бесконечном базисе антицепных функций и некоторых других связанных с ним базисах, разработка новых методов получения оценок сложности булевых функций в базисе антицепных функций и улучшение известных ранее оценок, выявление нетривиальных новых эффектов сложности.

Основные методы исследования

В диссертации используются методы дискретной математики и математической кибернетики, комбинаторного анализа, теории вероятностей.

Научная новизна

Все основные результаты работы являются новыми и получены автором самостоятельно. Основные результаты диссертации заключаются в следующем.

1. Доказана новая верхняя оценка функции Шеннона в базисе антицепных функций (базис AC): $L_{AC}(n) \leqslant n$.

2. Доказана нижняя оценка порядка $\sqrt{n}$ для сложности реализации почти всех булевых функций от n переменных схемами в базисе AC.

3. Получена точная формула, выражающая сложность произвольной симметрической булевой функции в базисе AC. Как следствие, в этом базисе установлены точные формулы для сложности линейной функции l_n, ее от-

рицания $\overline{l_n}$ и функции голосования m_n от n переменных: $L_{AC}(l_n) = \left\lfloor \frac{n+1}{2} \right\rfloor$, $L_{AC}(m_n) = L_{AC}(\overline{l_n}) = \left\lceil \frac{n+1}{2} \right\rceil$ при любом $n \geqslant 2$.

4. Для базиса AC установлен порядок роста функции Шеннона: $L_{AC}(n) = \Theta(n)$.

5. Установлено, что в базисе, состоящем из всех антицепных функций и линейных функций от любого числа переменных, порядок роста функции Шеннона равен $\sqrt{n \log_2 n}$. Тем самым, по-видимому, впервые показано, что существует базис, для которого порядок роста функции Шеннона лежит строго в интервале между функциями $\log_2 n$ и n.

Теоретическая и практическая ценность

Работа носит теоретический характер. Результаты диссертации могут найти применение в теории синтеза и сложности управляющих систем и в других разделах дискретной математики и математической кибернетики.

Апробация диссертации

Результаты по теме диссертации неоднократно докладывались автором на научно-исследовательских семинарах «Математические вопросы кибернетики» и «Синтез и сложность управляющих систем» под руководством профессора О. М. Касим-Заде (МГУ, 2013 – 2016 гг.).

Результаты по теме диссертации докладывались автором на следующих всероссийских и международных конференциях:

1) IX и X «Молодежные научные школы по дискретной математике и ее приложениям» (г. Москва, Институт прикладной математики им. М. В. Келдыша РАН, 2013, 2015 гг.);

2) конференция «Ломоносовские чтения» (г. Москва, МГУ, 2013 г.);

3) Индо-Российская конференция по алгебре, теории чисел, дискретной математике и их приложениям (г. Москва, МГУ, 2014 г.);

4) Международные научные конференции студентов, аспирантов и молодых ученых «Ломоносов-2013» и «Ломоносов-2015» (г. Москва, МГУ, 2013, 2015 гг.);

5) XII Международный семинар «Дискретная математика и ее приложения» им. академика О. Б. Лупанова (г. Москва, МГУ, 2016 г.).

Публикации

Основные результаты диссертации опубликованы автором в 6 печатных работах [75–80], из них 3 [75–77] в научных журналах из перечня, рекомендованного ВАК.

Структура и объем диссертации

Диссертация состоит из введения, пяти глав, заключения и списка литературы. Основные утверждения работы сформулированы в виде теорем, вспомогательные — в виде лемм. Утверждения пронумерованы парой чисел, где первое означает номер главы, а второе — номер утверждения внутри главы. Общий объем работы — 106 страниц.

Содержание диссертации

Во введении приведена краткая история задачи и кратко изложены основные результаты диссертации.

В главе 1 введены основные понятия, используемые в работе, и доказаны некоторые вспомогательные утверждения.

Глава 2 посвящена доказательству верхней оценки функции Шеннона в базисе антицепных функций. Основной результат главы можно сформулировать в виде теоремы.

Теорема 1 (2.1). *Для любого n имеет место верхняя оценка функции Шеннона $L_{AC}(n) \leqslant n$.*

Таким образом, улучшена верхняя оценка $L_{AC}(n) \leqslant n + 1$ из работы [5]. Для доказательства теоремы 1 был разработан специальный метод, который впоследствии был обобщен и использован в работе автора [76], где, в частности, получена верхняя оценка сложности реализации произвольной симметрической булевой функции в базисе AC.

В главе 3 доказывается следующее утверждение.

Теорема 2 (3.1). *Для почти всех булевых функций f от n переменных $L_{AC}(f) > \frac{\sqrt{n}}{2\sqrt{2}}$.*

Для полноты изложения в главу 3 включены также нижние оценки порядка $\sqrt{n}$ сложности реализации линейной функции и функции голосования от n переменных в базисе AC, доказанные тем же методом, что и теорема 2. Позднее эти нижние оценки были усилены в работе автора [76] (см. теорему 4 ниже).

Для дальнейшего изложения введем еще некоторые понятия и обозначения. *Слоем* булева куба называется множество всех наборов куба, содержащих одинаковое количество единиц. Ясно, что всякий слой является антицепью. Для симметрической функции f через $k(f)$ будем обозначать количество слоев куба, на которых функция f равна 1.

В главе 4 установлена точная формула, выражающая сложность реализации произвольной симметрической функции в базисе антицепных функций.

Теорема 3 (4.1). *Для произвольной симметрической функции f, существенно зависящей от всех своих $n \geqslant 2$ переменных, выполнено равенство:* $L_{AC}(f) = \min(k(f),\, n - k(f) + 2)$.

В дополнение к теореме 3 заметим, что сложность функций $f \equiv 0$ и $f \equiv 1$ равна 1, сложность функции $f = x_i$ равна 0 (схема состоит из одного полюса), сложность функции $f = \overline{x}_i$ равна 1. Тем самым получено исчерпывающее описание сложности всех симметрических функций в базисе AC.

Как следствие из теоремы 3, установлены точные формулы для сложности линейной функции, ее отрицания и функции голосования.

Теорема 4 (4.2). *Для линейной функции l_n, ее отрицания $\overline{l_n}$ и функции голосования m_n от n переменных выполнены равенства*

$$L_{AC}(l_n) = \left\lfloor \frac{n+1}{2} \right\rfloor,\ L_{AC}(m_n) = L_{AC}(\overline{l_n}) = \left\lceil \frac{n+1}{2} \right\rceil$$

при всех $n \geqslant 2$.

Теоремы 1 и 4 позволяют установить порядок роста функции Шеннона в базисе антицепных функций. Этот результат формулируется в виде следующей теоремы.

Теорема 5 (4.3). $L_{AC}(n) = \Theta(n)$.

Важно отметить, что нижняя оценка функции Шеннона $L_{AC}(n)$ получена здесь не мощностным методом: она следует из доказанных иным методом нижних оценок сложности конкретных булевых функций — линейных функций или функций голосования.

Как известно, количество антицепей булева куба заданной размерности равно числу мотононных булевых функций, зависящих от того же числа переменных [5]. С учетом этого, мощностная нижняя оценка функции Шеннона $L_{AC}(n)$ устанавливается в [5] аналогично мощностной нижней оценке инверсионной сложности, полученной Э. Н. Гилбертом [55], и имеет вид: $L_{AC}(n) \gtrsim \frac{1}{2}\log_2 n$.

Таким образом порядок роста функции Шеннона $L_{AC}(n) = \Theta(n)$ оказывается экспоненциальным по отношению к указанной мощностной нижней оценке. По-видимому, впервые такой эффект был обнаружен в работе О. М. Касим-Заде [5], где была получена нижняя оценка функции Шеннона $L_{AC}(n) = \Omega(n^{1/3})$

как следствие из установленной в этой работе нижней оценки сложности реализации линейных функций (см. также [6]). В данной диссертации результаты [5,6] в этом направлении значительно усилены.

Заметим, что и нижняя оценка порядка $\sqrt{n}$ для почти всех булевых функций из теоремы 2 также экспоненциально превышает мощностную нижнюю оценку функции Шеннона.

Интересно отметить, что точная формула для функции Шеннона инверсионной сложности, полученная А А. Марковым [33], также устанавливается на некоторой последовательности конкретных функций и превосходит мощностную нижнюю оценку порядка $\log_2 n$ (но всего асимптотически в два раза).

Выше говорилось, что до сих пор оставался открытым вопрос о существовании базисов, для которых порядки роста функций Шеннона лежат строго в интервале между функциями $\log_2 n$ и n. В главе 5 построен, по-видимому, первый пример такого бесконечного базиса.

Определим следующее множество функций. Будем обозначать через ACL множество, состоящее из всех антицепных функций и всех линейных функций от любого числа переменных. Аналогично AC, множество ACL является бесконечным базисом.

Основной результат главы 5 содержится в следующем утверждении.

Теорема 6 (5.1). $L_{ACL}(n) = \Theta(\sqrt{n \log_2 n})$.

Верхняя оценка доказана в разделе 5.3 (теорема 5.2). Нижняя оценка в теореме 6 получается не мощностным методом. В разделе 5.4 показано, что порядок роста функции Шеннона достигается на последо- вательности функций голосования: $L_{ACL}(m_n) = \Omega(\sqrt{n \log_2 n})$ (теорема 5.3).

Из теоремы 4 следует, что линейные функции и функции голосования в базисе AC обладают наибольшей по порядку роста сложностью. Базис ACL получен добавлением к базису антицепных функций всех линейных функций. Теорема 6 показывает, что такое расширение базиса AC понижает порядок роста функции

Шеннона, при этом функция голосования в новом базисе по-прежнему остается самой сложной по порядку.

Естественно исследовать, как изменится поведение функции Шеннона при добавлении к базису антицепных функций всех функций голосования. Изучению этого вопроса посвящен раздел 5.5. Бесконечный базис, состоящий из всех антицепных функций и всех функций голосования от любого числа переменных, обозначается через ACM.

В разделе 5.5 доказано следующее утверждение.

Теорема 7 (5.5). $L_{ACM}(n) = \Theta(\log_2 n)$.

Таким образом, из результатов главы 5 следует, что несмотря на то, что в обоих базисах ACL и ACM наблюдается существенное, по сравнению с базисом AC, понижение порядка роста функции Шеннона, тем не менее порядки роста функций Шеннона в этих базисах значительно различаются, то есть добавление различных функций с почти одинаковой и притом наибольшей по порядку роста сложностью оказывает существенно различное влияние на поведение функции Шеннона.

Благодарности

Автор выражает искреннюю благодарность своему научному руководителю доктору физико-математических наук, профессору О. М. Касим-Заде за постановку задач и постоянное внимание к работе. Автор благодарит участников семинаров «Синтез и сложность управляющих систем» и «Математические вопросы кибернетики» в МГУ за полезные обсуждения.

Глава 1

Предварительные сведения

В этой главе для полноты изложения формулируется ряд известных понятий, на которые мы опираемся в диссертации. Также вводятся некоторые обозначения, которые будут использоваться на протяжении всего текста диссертации.

Определим обычным образом понятие *схемы из функциональных элементов*, которое вводится с помощью вспомогательного объекта — «сети» (см., например, [25, 30]).

Процитируем из [30] определения понятия сети, схемы из функциональных элементов и функции, реализуемой схемой (некоторые обозначения изменены).

«"Сеть" строится из полюсов и элементов. <...> Каждый элемент имеет несколько входов, занумерованных числами $1, 2, \ldots$ и один выход (в частности, допускаются элементы без входов). <...>

В приводимом ниже определении индуктивно определяется "сеть" и множество ее вершин.

I. Полюс есть сеть. Он является (единственной) вершиной этой "сети".

II. Если S_1 и S_2 — сети без общих вершин, то их объединение есть «сеть». Вершинами этой "сети" являются вершины исходных "сетей".

III. Если S — сеть и e — элемент, все выходы и выходы которого не являются вершинами сети S, то результат присоединения (т. е. отождествления) всех входов элемента e к некоторым вершинам "сети" S есть "сеть"; при этом к одной вершине "сети" могут присоединяться различные входы, но

каждый вход присоединяется только к одной вершине. Вершинами новой " сети" являются вершины "сети" S и выход элемента e» [30].

Отметим, что допускаются элементы, не имеющие входов, но имеющие выход. Если выход такого элемента не является вершиной сети, то результат добавления такого элемента к сети есть сеть, вершинами которой являются вершины исходной сети и выход этого элемента.

«*Схемой из функциональных элементов* называется "сеть", в которой

1) каждому полюсу приписана одна из переменных $x_1, \ldots, x_n, \ldots$, причем разным полюсам — разные переменные. Полюсы называются также *входами схемы*;

2) каждому элементу e с r входами поставлена в соответствие некоторая булева функция $\phi_e(y_1, \ldots, y_r)$, существенно зависящая от r аргументов (при $r = 0$ функция ϕ_e есть константа) и называемая функцией элемента e; элемент e с сопоставленной ему функцией ϕ_e называется *функциональным элементом*;

3) некоторой вершине приписано число 1; некоторой вершине (быть может, совпадающей с первой) приписано число 2 и т.д.; некоторой вершине приписано число m. Вершины, которым приписано хотя бы одно из чисел, отмечены символом *. Эти вершины называются *выходами* схемы; l-м выходом будем называть (единственный) выход, которому приписано число l (и, может быть, другие числа)» [30].

«Функции, реализуемые схемой, определяются следующим образом (будет указан процесс сопоставления функций вершинам схемы):

1) каждому входу схемы сопоставляется функция, равная переменной, приписанной этому входу;

2) пусть всем вершинам, к которым присоединены входы элемента e схемы, уже сопоставлены функции. Тогда выходу этого элемента сопоставляется

функция $\phi_e(f^{(1)}, \ldots, f^{(r)})$, где $\phi_e(y_1, \ldots, y_r)$ — функция элемента e, а $f^{(j)}$ — функция, сопоставленная той вершине, с которой соединен j-й вход элемента e.

В результате этого процесса каждой вершине схемы будет сопоставлена некоторая функция.

Схема по определению реализует упорядоченную систему функций (вектор-функцию) $(f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n))$, где $f_l(x_1, \ldots, x_n)$ — функция, сопоставленная l-му выходу. Такие системы функций будем называть (n, m)-функциями» [30].

Мы будем рассматривать случай $m = 1$ и считать, что схема реализует одну функцию. Подробнее эти и другие понятия изложены в [30].

Если функции всех элементов схемы S принадлежат множеству B, то будем говорить, что схема S есть схема в базисе B [30].

Схема из функциональных элементов называется *приведенной*, если различные входы всякого элемента присоединены к различным вершинам схемы, а на выходе всякого элемента реализуется функция, отличная от константы (см. [6]). Отметим, что для любой схемы в базисе AC сложности s, реализующей функцию, отличную от константы, существует приведенная схема в базисе AC сложности не больше s, реализующая ту же функцию.

Нетрудно убедиться, что это верно и для базиса ACL: для любой схемы в базисе ACL сложности s, реализующей функцию, отличную от константы, существует приведенная схема в базисе ACL сложности не больше s, реализующая ту же функцию.

Отметим, что для базиса ACM аналогичное утверждение неверно (для доказательства результатов об этом базисе данный факт не используется).

Нумерация элементов схемы называется *правильной*, если на входы каждого элемента могут подаваться выходы элементов с меньшими номерами или

входы схемы. Известно [24], что такую нумерацию можно задать в любой схеме (возможно, несколькими способами).

Символы переменных $x_1, x_2, \ldots, x_n$, которые приписаны n входам схемы, будем называть *входными переменными* схемы.

Обозначим через $\boldsymbol{x}$ произвольный набор значений аргументов $(x_1, \ldots, x_n)$.

Элементы схемы будем обозначать символом e, элемент с номером i — через e_i. Как правило (если не сказано иное), через g_i будем обозначать антицепную функцию, которая соответствует элементу e_i, а через h_i — функцию, которая реализуется на выходе элемента e_i. Значение функции h_i при подаче на входы схемы набора $\boldsymbol{x}$ будем обозначать через $h_i(\boldsymbol{x})$.

Пусть среди переменных $x_1, \ldots, x_n$ выделены t переменных. Зафиксируем произвольным образом значения этих t переменных, а остальным переменным будем присваивать произвольные значения. Полученное множество наборов называется *подкубом* булева куба $\{0,1\}^n$ размерности $n - t$.

Максимальный набор куба $\{0,1\}^n$ — набор $\mathbf{1} = (1, \ldots, 1)$ будем называть *верхним* набором куба, а минимальный — $\mathbf{0} = (0, \ldots, 0)$, соответственно, *нижним*. Аналогично для всякого подкуба меньшей размерности верхним и нижним наборами будем называть соответственно максимальный и минимальный наборы этого подкуба.

Множество чисел $\{1, 2, \ldots, n\}$ будем обозначать через $[n]$.

Для любого $P \subseteq [n]$ через $\boldsymbol{x}^P$ обозначим такой двоичный набор $\boldsymbol{x} = (x_1, \ldots, x_n)$, что для любого $p \in [n]$ $x_p = 1$ тогда и только тогда, когда $p \in P$.

Напомним, что под *характеристической функцией* множества наборов $A \subseteq \{0,1\}^n$ понимается функция, принимающая значение 1 на тех и только тех наборах, которые лежат в множестве A. Таким образом, каждая функция, входящая в AC, есть характеристическая функция некоторой антицепи булева куба соответствующей размерности.

Приведем также для полноты изложения ряд известных понятий и обозначений, которые используются в работе для описания асимптотического поведения действительнозначных функций.

Пусть две действительнозначные функции $a(n)$ и $b(n)$ натурального аргумента при всех достаточно больших n принимают положительные значения. Будем говорить, что *порядок роста* функции $a(n)$ *не больше* $b(n)$ и обозначать это через $a(n) = O(b(n))$, если существует такая константа $c > 0$, что $a(n) \leqslant cb(n)$ при всех достаточно больших n. Будем также говорить, что порядок роста функции $b(n)$ *не меньше* $a(n)$, и обозначать это через $b(n) = \Omega(a(n))$. Если одновременно $a(n) = \Omega(b(n))$ и $a(n) = O(b(n))$, то будем говорить, что порядок роста $a(n)$ *равен* $b(n)$, и обозначать это через $a(n) = \Theta(b(n))$.

Если выполнено соотношение $\overline{\lim}_{n\to\infty} \frac{a(n)}{b(n)} \leqslant 1$, то будем говорить, что $a(n)$ *асимптотически не больше* $b(n)$ и обозначать это через $a(n) \lesssim b(n)$, а если выполнено соотношение $\lim_{n\to\infty} \frac{a(n)}{b(n)} = 1$, то будем говорить, что $a(n)$ *асимптотически равно* $b(n)$ и обозначать это через $a(n) \sim b(n)$ [31].

Глава 2

Верхняя оценка функции Шеннона в базисе AC

В данной главе мы докажем верхнюю оценку функции Шеннона в базисе антицепных функций. Доказательство этой теоремы приведено в работе автора [78].

Теорема 2.1. *Для любого n имеет место верхняя оценка функции Шеннона* $L_{AC}(n) \leqslant n$.

Эта теорема улучшает известный ранее результат: $L_{AC}(n) \leqslant n + 1$ [5].

Доказательство. В начале для произвольной булевой функции f от n переменных будет показано, как построить схему сложности не более $n + 2$, а затем мы поясним, как сложность этой схемы может быть уменьшена.

Напомним, что набор длины n, состоящий из нулей, мы обозначаем через $\mathbf{0}$, набор длины n, состоящий из единиц, — через $\mathbf{1}$, а набор $(x_1, \ldots, x_n)$ через $\boldsymbol{x}$.

Для всякой булевой функции f от n переменных зададим функции $H_0^f, \ldots, H_n^f$ от n переменных следующим образом. Для всякого $t \in \{0, 1, \ldots, n\}$ положим $H_t^f(\boldsymbol{x}) = 1$ на тех и только тех наборах $\boldsymbol{x}$, для которых $\sum\limits_{k=1}^{n} x_k = t$ и $f(\boldsymbol{x}) = 1$. Заметим, что так заданные функции H_t^f являются антицепными.

Определим функцию g от $n+1$ переменной $y_1, \ldots, y_{n+1}$ следующим образом: положим ее равной единице на всех наборах, в которых ровно одна единица, а на всех остальных наборах — равной нулю. Легко видеть, что так заданная функция g является антицепной.

Нетрудно убедиться, что

$$g(H_0^f(\boldsymbol{x}), \ldots, H_n^f(\boldsymbol{x})) = f(\boldsymbol{x}). \tag{2.1}$$

Для произвольной булевой функции f от n переменных, согласно выражению (2.1) построим схему, реализующую эту функцию. Указанная схема имеет сложность не более $n + 2$.

Опишем два приема, с помощью которых можно уменьшить полученную верхнюю оценку.

Первый прием опирается на следующее соображение. Заметим, что если $f(\mathbf{0}) = 0$, то из схемы, построенной в соответствии с выражением (2.1), можно удалить элемент, который реализует функцию H_0^f. Если $f(\mathbf{1}) = 0$, то из указанной схемы можно удалить элемент, который реализует функцию H_n^f. В самом деле, в обоих случаях указанные элементы реализуют константу 0. При этом в обоих случаях при удалении соответствующих элементов получается схема сложности не более $n + 1$.

Если $f(\mathbf{1}) = f(\mathbf{0}) = 1$, то применяя указанные выше соображения, мы можем построить схему для $\overline{f}$ сложности не более n, а затем подать выход этой схемы на элемент, реализующий отрицание. Тем самым получится схема, реализующую функцию f, сложности не более $n + 1$. Таким образом, для произвольной булевой функции от n переменных можем получить схему сложности не более $n + 1$.

Идея второго приема заключается в следующем: мы можем в определенном смысле эффективнее использовать элемент схемы, соответствующий функции g (в схеме сложности не более $n + 1$), подав на его входы «дополнительно» входные переменные $x_1, \ldots, x_n$. Поясним, что это значит, для частного случая функции f, такой что $f(\mathbf{1}) = 1, f(\mathbf{0}) = 0$.

Зададим функцию g' от $2n-1$ переменной $y_1, \ldots, y_{n-1}, x_1, \ldots, x_n$ следующим образом. Пусть функция g' принимает значение 1 лишь на наборах двух типов:

1) существует номер j, такой что $y_j = 1$, для всякого $i \neq j$ $y_i = 0$, $\sum\limits_{k=1}^{n} x_k = j$ и $f(x_1, \ldots, x_n) = 1$;

2) для всякого j $y_j = 0$, для всякого i $x_i = 1$.

Реализуем функцию f следующим образом:

$$f(\boldsymbol{x}) = g'(H_1^f, \ldots, H_{n-1}^f, x_1, \ldots, x_n). \tag{2.2}$$

Справедливость выражения (2.2) проверяется прямым перебором возможных значений входных наборов. Схема, соответствующая этому равенству, имеет сложность n.

Оставшиеся три случая, которые определяются значениями функции f на наборах $\mathbf{0}$ и $\mathbf{1}$, рассматриваются аналогично посредством комбинирования приемов, указанных выше. При этом, нетрудно понять, что в случае функции f, такой что $f(\mathbf{0}) = f(\mathbf{1}) = 0$, мы можем получить схему сложности не более $n-1$.

Таким образом мы доказали верхнюю оценку n сложности реализации произвольной булевой функции f от n переменных схемами в базисе AC. ■

Глава 3

Нижняя оценка для почти всех булевых функций в базисе AC

3.1 Результаты главы 3

В данной главе будут доказаны следующие теоремы.

Теорема 3.1. *Для почти всех булевых функций f от n переменных $L_{AC}(f) > \frac{\sqrt{n}}{2\sqrt{2}}$.*

Теорема 3.2. *Для линейной функции l_n и функции голосования m_n от n переменных выполнены оценки: $L_{AC}(l_n) > \frac{n-3}{\sqrt{3n}}$, $L_{AC}(m_n) > \frac{n-3}{\sqrt{3n}}$.*

Отметим, что доказательство теоремы 3.2 приводится для полноты изложения, поскольку оно без дополнительных усилий получается тем же методом, каким будет доказана теорема 3.1. В главе 4 установлены более сильные нижние оценки сложности линейной функции и функции голосования.

Способ доказательства нижних оценок, предлагаемый в этой главе, состоит в развитии и модификации методов, использованных в [5]. Доказательство нижней оценки, приведенное в [5], основано на комбинировании двух методов. Первый из них — это известный метод подстановки констант. Второй метод, впервые предложенный в работе [5], связан с элиминацией элементов при последовательном сужении области определения функции. Более точная нижняя оценка в работе [6] была получена путем усовершенствования методов из [5].

Изложение доказательств в этой главе будет устроено следующим образом. Вначале в разделе 3.2 мы введем некоторые необходимые определения и дока-

жем вспомогательные утверждения, которые потребуются в дальнейших рассуждениях. Затем в разделе 3.3 мы докажем общее утверждение о нижней оценке сложности схемы, реализующей произвольную функцию от n переменных в базисе AC. Из этого доказательства выведем теоремы 3.1 и 3.2.

Тем самым в базисе AC будут установлены нижние оценки порядка $\sqrt{n}$ для сложности почти всех булевых функций от n переменных, а также для линейной функции и функции голосования от n переменных.

3.2 Вспомогательные сведения

Множество принадлежащих кубу $\{0,1\}^n$ наборов, на которых функция f от n переменных принимает значение 1 (носитель функции), будем обозначать через $N^n(f)$.

Для доказательства основного результата главы нам потребуется вероятностное распределение специального вида на булевом кубе $\{0,1\}^n$. Зададим *вероятность* произвольного набора булева куба $\boldsymbol{\alpha}$ следующим образом:

$$\rho_n(\boldsymbol{\alpha}) = \frac{1}{C_n^{|\boldsymbol{\alpha}|} \cdot (n+1)},$$

где $|\boldsymbol{\alpha}|$ — количество единиц в наборе $\boldsymbol{\alpha}$.

Напомним, что *слоем* булева куба называется множество всех наборов куба, содержащих одинаковое количество единиц. Ясно, что всякий слой булева куба представляет собой антицепь.

Разобьем булев куб $\{0,1\}^n$ на слои $A_0, A_1, \ldots, A_n$ так, что слой A_t состоит из наборов, содержащих ровно t единиц. Количество этих слоев равно $n+1$.

Вероятность произвольного набора в t-м слое равна

$$\frac{1}{C_n^t \cdot (n+1)}.$$

Ясно, что вероятность слоя с номером t равна $\rho_n(A_t) = \frac{1}{n+1}$, и тогда выполнено основное свойство вероятности: $\sum\limits_{k=0}^{n} \rho_n(A_k) = 1$.

Рассмотрим произвольную антицепь в булевом кубе $\{0,1\}^n$, состоящую из s наборов: $A = \{\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_s\}$.

Лемма 3.1. *Для произвольной антицепи $A = \{\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_s\}$ в булевом кубе $\{0,1\}^n$ выполнено:*

$$\sum_{i=1}^{s} \frac{1}{C_n^{|\boldsymbol{\alpha}_i|}} \leqslant 1.$$

Доказательство этого утверждения можно найти, например, в [48]. Из леммы 3.1 нетрудно вывести

Следствие 3.2. *Для произвольной антицепи A в булевом кубе $\{0,1\}^n$ выполнено неравенство:*

$$\rho_n(A) \leqslant \frac{1}{n+1}\,.$$

Доказательство. Пусть $A = \{\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_s\}$. Тогда

$$\rho_n(A) = \sum_{i=1}^{s} \frac{1}{C_n^{|\boldsymbol{\alpha_i}|}} \cdot \frac{1}{(n+1)} \leqslant \frac{1}{n+1}.$$

■

Посмотрим, что происходит с вероятностью множества единиц функции при отбрасывании несущественных переменных этой функции.

Лемма 3.3. *Пусть у функции $f(x_1, \ldots, x_n)$ переменные $x_{s+1}, \ldots, x_n$ несущественные. Тогда*

$$\rho_n(N^n(f)) = \rho_s(N^s(f_{n-s})),$$

где f_{n-s} — функция от s переменных, получаемая из f отбрасыванием ее $n-s$ несущественных переменных.

Доказательство. Достаточно доказать утверждение для случая $s = n-1$, тогда для любого $s \leqslant n-1$ последовательно выведем

$$\rho_n(N^n(f)) = \rho_{n-1}(N^{n-1}(f_1)) = \ldots = \rho_s(N^s(f_{n-s})).$$

В случае $s = n-1$ отбросим у функции $f(x_1, \ldots, x_n)$ несущественную переменную x_n. Получим функцию f_1 от $n-1$ переменной.

В заданном распределении

$$\rho_n(N^n(f)) = \sum_{\boldsymbol{\alpha} \in N^n(f)} \rho_n(\boldsymbol{\alpha}). \tag{1}$$

Аналогично

$$\rho_{n-1}(N^{n-1}(f_1)) = \sum_{\boldsymbol{\beta} \in N^{n-1}(f_1)} \rho_{n-1}(\boldsymbol{\beta}). \tag{2}$$

При этом вероятность набора $\boldsymbol{\gamma} = (\gamma_1, \ldots, \gamma_{n-1})$ есть $\rho_{n-1}(\boldsymbol{\gamma}) = \frac{1}{C_{n-1}^{|\boldsymbol{\gamma}|} \cdot n}$.

Для удобства введем обозначение: $z = |\boldsymbol{\gamma}|$.

Рассмотрим сумму $\rho_n(\boldsymbol{\gamma}\mathbf{0}) + \rho_n(\boldsymbol{\gamma}\mathbf{1})$ (под $\boldsymbol{\gamma}\mathbf{0}$ понимается набор $(\gamma_1, \ldots, \gamma_{n-1}, 0)$ длины n). Имеем

$$\rho_n(\boldsymbol{\gamma}\mathbf{0}) + \rho_n(\boldsymbol{\gamma}\mathbf{1}) = \frac{1}{C_n^z \cdot (n+1)} + \frac{1}{C_n^{z+1} \cdot (n+1)} =$$

$$= \frac{1}{n+1} \cdot \left(\frac{C_n^{z+1} + C_n^z}{C_n^z \cdot C_n^{z+1}} \right) = \frac{1}{n+1} \cdot \frac{C_{n+1}^{z+1}}{C_n^z \cdot C_n^{z+1}} = \frac{1}{C_{n-1}^z \cdot n} = \rho_{n-1}(\boldsymbol{\gamma}),$$

где первое и последнее равенства получены по определению вероятности, а третье и четвертое — по свойствам биномиальных коэффициентов. Заметим, что условие $\boldsymbol{\gamma} \in N^{n-1}(f_1)$ равносильно тому, что $\boldsymbol{\gamma}\mathbf{0}, \boldsymbol{\gamma}\mathbf{1} \in N^n(f)$, поэтому

$$\rho_n(N^n(f)) = \rho_{n-1}(N^{n-1}(f_1)).$$

Лемма доказана. ■

Введем еще несколько определений и обозначений, которые нам потребуются в дальнейшем.

Частичной функцией $f\,(x_1, x_2, ..., x_n)$ называется функция, определенная на подмножестве A единичного булева куба, $f : A \to \{0,1\}^n$. Вне множества A функция не определена. Множество всех таких функций обозначается $P_2^n(A)$.

Если $A \subseteq B \subseteq \{0,1\}^n$ и $f \in P_2^n(B)$, то функция $g \in P_2^n(A)$, совпадающая с f на всех наборах из множества A, называется *сужением* функции f на множество A и обозначается через $f|_A$.

Сужение констант 0, 1 на множество A будем обозначать через $0|_A, 1|_A$.

Для всякой функции $f(x_1, \ldots, x_n)$ рассмотрим $\sigma_r(f)$ — минимальное число, такое, что для любого подмножества переменных T мощности $p \leqslant r$ этим переменным можно присвоить такие значения $a_{i_1}, \ldots, a_{i_p}$, где $p \leqslant r$, что для любого подмножества $A \subseteq \{0,1\}^{n-p}$, имеющего вероятность $\rho_{n-p}(A) > \sigma_r(f)$, выполнено соотношение

$$f(x_1, \ldots, a_{i_1}, \ldots, a_{i_p}, \ldots, x_n)|_A \notin \{0|_A, 1|_A\}.$$

Докажем верхнюю оценку величины σ_r для линейной функции от n переменных l_n.

Лемма 3.4. *Для всякого $r \leqslant n-3$ справедливо неравенство $\sigma_r(l_n) \leqslant \frac{2}{3}$.*

Доказательство. Рассмотрим линейную функцию от n переменных l_n. Выберем любое подмножество переменных мощности p не больше r и рассмотрим подмножество $A \subseteq \{0,1\}^{n-p}$, имеющее вероятность $\rho_{n-p}(A) > \frac{2}{3}$. Фиксировав значения выбранного подмножества переменных нулями, получим линейную функцию l_{n-p}.

Достаточно доказать, что $l_{n-p}(x_1, \ldots, a_{i_1}, \ldots, a_{i_p}, \ldots, x_n)|_A \notin \{0|_A, 1|_A\}$, где $a_{i_1} = \ldots = a_{i_p} = 0$.

Предположим, что $l_{n-p} = 0$. Рассмотрим случай четного $n-p$. Линейная функция принимает чередующиеся значения на слоях булева куба. В частности, на слоях $A_0, A_2, A_4, \ldots, A_{n-p}$ линейная функция равна нулю. Рассмотрим множество

$$\boldsymbol{A} = \bigcup_i A_{2i}.$$

Вероятность этого множества равна $\rho_{n-p}(\boldsymbol{A}) = (\frac{n-p}{2}+1)\cdot\frac{1}{n-p+1} \leqslant \frac{2}{3}$. Следовательно, для любого множества $A \subseteq \{0,1\}^n$, такого, что $l_{n-p}|_A = 0|_A$, вероятность A будет не больше чем $\frac{2}{3}$. Противоречие.

В случаях нечетного $n-p$ и константы 1 доказательство повторяет изложенное. ■

Аналогичная лемма справедлива и для функции голосования от n переменных m_n.

Лемма 3.5. *Для всякого $r \leqslant n-3$ справедливо неравенство $\sigma_r(m_n) \leqslant \frac{2}{3}$.*

Доказательство леммы для функции голосования проводится так же, как и для линейной функции, с той лишь разницей, что значения половины выбранного подмножества переменных следует фиксировать нулями, а другой половины — единицами.

Докажем следующее утверждение о величине σ_r случайной булевой функции f

Лемма 3.6. *Вероятность $\boldsymbol{P}\left(\sigma_r(f) \leqslant \frac{3}{4}\right)$ по случайной функции f от n переменных при $r = n/2$ стремится к единице при $n \longrightarrow \infty$.*

Доказательство. Пусть $f(x_1,\ldots,x_n)$ — случайная булева функция. Сначала зафиксируем подмножество индексов переменных мощности $p \leqslant n/2$, и зафиксируем нулями значения переменных с индексами из этого подмножества. Докажем для любого подмножества переменных мощности $p \leqslant n/2$, что при фиксировании их нулями вероятность того, что существует подмножество $A \subseteq \{0,1\}^{n-p}$, имеющее вероятность $\rho_{n-p}(A) > \frac{3}{4}$, мала. Отсюда мы выведем, что вероятность того, что такое подмножество переменных существует, также мала.

Будем рассматривать f как функцию от оставшихся $n-p$ переменных. Без ограничения общности будем считать, что это переменные $x_1,\ldots,x_{n-p}$.

Введем обозначение $s = n - p$. Рассмотрим разбиение куба $\{0,1\}^s$ на слои $A_0, A_1, \ldots, A_s$, как было описано выше. По определению вероятностного распределения ρ_s, оно равномерно на этих слоях.

Оценим $\mathbf{P}\left(\left|\rho_s(N^s(f)) - \frac{1}{2}\right| > \frac{1}{4}\right)$ — вероятность события, что $\rho_s(N^s(f))$ отличается от своего среднего значения более чем на $\frac{1}{4}$.

Определим множество $I \subseteq \{0, \ldots, s\}$ так: $I = \{i \,|\, i < \lfloor \frac{s-1}{8} \rfloor$ или $i > \lceil \frac{7s}{8} \rceil\}$, и пусть $|I| = q$. Ясно, что $\frac{s+1}{6} \leqslant q \leqslant \frac{s+1}{4}$ для достаточно больших s. Определим также объединение слоев

$$\boldsymbol{A} = \bigcup_{i \in I} A_i,$$

где A_i — слои булева куба.

Тогда

$$N^s(f) \setminus \boldsymbol{A} = \bigcup_{i \notin I} N^s(f) \cap A_i.$$

Заметим, что

$$\left|\rho_s(N^s(f)) - \frac{1}{2}\right| \leqslant \left|\rho_s(N^s(f) \cap \boldsymbol{A}) - \frac{1}{2} \cdot \frac{q}{s+1}\right| + \left|\rho_s(N^s(f) \setminus \boldsymbol{A}) - \frac{1}{2} \cdot \frac{s+1-q}{s+1}\right|.$$

Ясно, что

$$0 \leqslant \rho_s(N^s(f) \cap \boldsymbol{A}) \leqslant \rho_s(\boldsymbol{A}) = \frac{q}{s+1}.$$

Поэтому

$$\left|\rho_s(N^s(f) \cap \boldsymbol{A}) - \frac{1}{2} \cdot \frac{q}{s+1}\right| \leqslant \frac{q}{2(s+1)} \leqslant \frac{1}{8}.$$

Таким образом,

$$\mathbf{P}\left(\left|\rho_s(N^s(f)) - \frac{1}{2}\right| > \frac{1}{4}\right) \leqslant \mathbf{P}\left(\left|\rho_s(N^s(f) \setminus \boldsymbol{A}) - \frac{1}{2} \cdot \frac{s+1-q}{s+1}\right| > \frac{1}{8}\right),$$

и достаточно оценить сверху последнюю вероятность, а именно вероятность того, что отклонение от среднего на центральных слоях больше $\frac{1}{8}$.

Если такое отклонение имеет место, то для хотя бы одного k такого, что $\lfloor \frac{s-1}{8} \rfloor \leqslant k \leqslant \lceil \frac{7s}{8} \rceil$, верно неравенство

$$\left|\rho_s(N^s(f) \cap A_k) - \frac{1}{2(s+1)}\right| > \frac{1}{8(s+1-q)},$$

т.е. на одном из слоев происходит отклонение от среднего больше, чем на $\frac{1}{8(s+1-q)}$, что не меньше чем $\frac{3}{20(s+1)}$. Оценим вероятность события

$$\mathbf{P}\left(\left|\rho_s(N^s(f)\cap A_k)-\frac{1}{2(s+1)}\right|>\frac{3}{20(s+1)}\right).$$

Для оценки этого воспользуемся следующим утверждением (см., например, [69]).

Теорема 3.3. (*Следствие из неравенства Чернова*). *Пусть* $X=t_1+\ldots+t_n$, *где* t_i — *независимые случайные величины из* $\{0,1\}$. *Тогда для любого* $\varepsilon>0$ *выполнено неравенство*

$$\boldsymbol{P}\{|X-\boldsymbol{E}(X)|\geqslant\varepsilon\cdot\boldsymbol{E}(X)\}\leqslant 2e^{-\min\{\varepsilon^2/4,\,\varepsilon/2\}\boldsymbol{E}(X)}.$$

В нашем случае в качестве t_i выступают значения функции в точках антицепи (слоя) A_k, где $\lfloor\frac{s-1}{8}\rfloor\leqslant k\leqslant\lceil\frac{7s}{8}\rceil$. Величины t_i равны единице с вероятностью $\frac{1}{2}$ и нулю с вероятностью $\frac{1}{2}$, X — это сумма $\sum\limits_{i=1}^{C_s^k}t_i$, математическое ожидание этой величины есть $\mathbf{E}\sum\limits_{i=1}^{C_s^k}t_i=\frac{1}{2}\cdot C_s^k$. Таким образом,

$$\mathbf{P}\left(\left|\rho_s(N^s(f)\cap A_k)-\frac{1}{2(s+1)}\right|>\frac{3}{20(s+1)}\right)=$$

$$=\mathbf{P}\left(\left|\sum_{i=1}^{C_s^k}t_i-\frac{1}{2}\cdot C_s^k\right|>\frac{3}{10}\left(\frac{1}{2}\cdot C_s^k\right)\right)\leqslant 2e^{-\tau\cdot C_s^k}\leqslant 2e^{-\tau\cdot 2^{\lambda s}},$$

где $\tau,\lambda>0$ — некоторые константы.

Таким образом мы оценили вероятность указанного отклонения на k-м слое при фиксированных значениях переменных величиной $2e^{-\tau\cdot 2^{\lambda s}}$. Ясно тогда, что для оценки вероятности отклонения для слоев по всему кубу следует домножить эту величину на оценку количества слоев $s+1$, а для оценки вероятности события $\mathbf{P}\left(\sigma_r(f)>\frac{3}{4}\right)$ добавить еще множитель 2^n, оценивающий количество подмножеств индексов переменных мощности p, которые мы выбирали в начале доказательства леммы. В результате получится следующая оценка:

$$\mathbf{P}\left(\sigma_r(f)>\frac{3}{4}\right)\leqslant 2^n\cdot(s+1)\cdot 2e^{-\tau\cdot 2^{\lambda s}},$$

где величина в правой части неравенства стремится к нулю при $n \longrightarrow \infty$, поскольку $s \geqslant n/2$. ■

Докажем еще одно вспомогательное утверждение, прежде чем приступить к доказательству основного результата.

Лемма 3.7. *Пусть функция $f(x_1, \ldots, x_k)$ антицепная и существенно зависит от всех своих переменных. Рассмотрим функцию $f'(x_{m+1}, \ldots, x_k) = f(c_1, \ldots, c_m, x_{m+1}, \ldots, x_k)$. Тогда либо f' зависит от переменных $x_{m+1}, \ldots, x_k$ существенно, либо $f' \equiv 0$.*

Доказательство. От противного. Пусть существует набор $\boldsymbol{\beta} = (\beta_{m+1}, \ldots, \beta_k)$, такой, что $f'(\boldsymbol{\beta}) = 1$, и, например, от x_k функция f' не зависит существенно. Тогда $f'(\beta_{m+1}, \ldots, \beta_{k-1}, 0) = f'(\beta_{m+1}, \ldots, \beta_{k-1}, 1) = 1$.

Рассмотрим исходную функцию f. Ясно, что

$$f(c_1, \ldots, c_m, \beta_{m+1}, \ldots, \beta_{k-1}, 0) = f(c_1, \ldots, c_m, \beta_{m+1}, \ldots, \beta_{k-1}, 1) = 1.$$

Получено противоречие с тем, что f — антицепная функция. ■

3.3 Доказательство нижней оценки

Перейдем к доказательству ключевого утверждения, из которого будут следовать заявленные результаты главы 3.

Лемма 3.8. *Пусть n, s, r — натуральные числа, f — булева функция от n переменных. Пусть S — схема в базисе AC, реализующая функцию f. Тогда*

$$L_{AC}(S) > \min\{\frac{r}{s}, (s+1)(1-\sigma_r(f))\}.$$

Доказательство. Введем обозначение $t = \min\{\frac{r}{s}, (s+1)(1-\sigma_r(f))\}$. Доказывать будем от противного: предположим, что $L_{AC}(S) \leqslant t$.

Будем считать, что в схеме S все входные переменные схемы (определение см. в главе 1), которые подаются на входы элементов, являются существенными для функций, реализуемых этими элементами.

Введем на схеме правильную нумерацию элементов (определение см. в главе 1): $e_1, \ldots, e_t$. Для каждого элемента e_i рассмотрим функцию h_{e_i}, реализуемую подсхемой схемы S с выходом e_i; множество входных переменных, которые подаются на входы элемента e_i, обозначим через X_{e_i}.

Определим некоторое множество переменных F. Будем строить его следующим образом. Вначале полагаем $F = \emptyset$. Начинаем обход элементов схемы в порядке заданной нумерации. Для каждого элемента схемы e_i смотрим, сколько переменных содержится в множестве $X_{e_i} \setminus F$. Если $|X_{e_i} \setminus F| < s$, то полагаем $F := F \cup X_{e_i}$. Если $|X_{e_i} \setminus F| \geqslant s$, то переходим к следующему по порядку элементу схемы. После того, как пройдем один раз все элементы схемы, мы получим множество F, которое обозначим через F_1. Так же совершим второй проход элементов схемы и получим новое множество переменных, которое обозначим через F_2. И так далее.

Будем совершать проходы до тех пор, пока не получим, что $F_{k-1} = F_k$, т. е. новые переменные на k-м проходе уже не добавились. Ясно, что $k \leqslant t$, а $|F_k| < s \cdot t \leqslant r$. Полагаем $F = F_k$. Обозначим мощность множества F через p.

Поскольку $p < r$, то можно зафиксировать переменные из F значениями $a_{i_1}, \ldots, a_{i_p}$ из определения величины $\sigma_r(f)$ и далее рассматривать схему S как схему от оставшихся входных переменных, значения которых не зафиксированы. Тогда для любого элемента схемы S имеем следующее:

1) либо значения всех входных переменных, которые присоединены к его входам, зафиксированы;

2) либо у элемента не менее s входов, которые являются переменными, не входящими в F, а значит, их значения не зафиксированы, а остальные входные переменные зафиксированы. Тогда, по лемме 3.7, получаем, что соответству-

ющая функция h_{e_i} либо тождественно равна нулю, либо существенно зависит от не менее чем s переменных.

Для удобства обозначим $n - p$ через n_1. Рассмотрим наборы булева куба, в которых все переменные из множества F равны нулю. Они образуют подкуб $\{0,1\}^{n_1}$. Рассмотрим вероятностное распределение ρ_{n_1} на этом подкубе.

Мы будем доказывать, что для каждого i, $1 \leqslant i \leqslant t$, можно найти множество $C_i \subseteq \{0,1\}^{n_1}$, такое что

$$\rho_{n_1}(C_i) \geqslant 1 - i \cdot \frac{1}{s+1} \tag{3.1}$$

и

$$h_{e_1}|_{C_i} = \text{const}, \ldots, h_{e_{i-1}}|_{C_i} = \text{const}. \tag{3.2}$$

Рассуждение будет проходить по индукции по i.

Положим $C_0 = \{0,1\}^{n_1}$. Тогда условие (3.1) выполнено.

Пусть мы нашли множество C_{i-1}, такое, что выполнены условия (3.1) и (3.2). Рассмотрим элемент e_i. Для него возможны 2 случая:

1) либо все входные переменные, которые присоединены к его входам, принадлежат множеству F, а значит, они зафиксированы некоторыми значениями и функция h_{e_i} — константа на множестве C_{i-1}. Тогда полагаем $C_i = C_{i-1}$;

2) либо не менее s его входов присоединены к входным переменным схемы, не лежащими в F, а значения остальных переменных, которые подаются ему на вход, зафиксированы. Тогда, по лемме 3.7, функция h_{e_i}

   a) либо тождественно равна нулю,

   b) либо зависит не менее чем от s переменных существенно.

В случае 2a полагаем $C_i = C_{i-1}$.

Случай 2b изучим подробнее. Мы рассматриваем функцию от n_1 переменных, не менее s из которых существенные. Оценим сверху число наборов, на которых функция h_{e_i} принимает значение 1.

Базис AC замкнут относительно подстановки констант, поэтому, если отбросим у h_{e_i} несущественные переменные, то получим равную ей антицепную функцию $H(x_{i_1}, \ldots, x_{i_s})$, существенно зависящую не менее чем от s переменных, которые являются входными переменными схемы, поскольку все элементы e_k, где $k < i$, реализуют константы.

По лемме 3.3, имеем: $\rho_{n_1}(N^{n_1}(h_{e_i})) = \rho_s(N^s(H))$. Далее, поскольку функция H — антицепная, то множество $N^s(H)$ представляет собой антицепь. Значит, согласно следствию 3.2, справедлива оценка

$$\rho_{n_1}(N^{n_1}(h_{e_i})) = \rho_s(N^s(H)) \leqslant \frac{1}{s+1}.$$

Итак, в условиях случая 2b положим $C_i = C_{i-1} \setminus N^{n_1}(h_{e_i})$. Тогда

$$\rho_{n_1}(C_i) = \rho_{n_1}(C_{i-1} \setminus N^{n_1}(h_{e_i})) \geqslant \rho_{n_1}(C_{i-1}) - \rho_{n_1}(N^{n_1}(h_{e_i})) \geqslant \rho_{n_1}(C_{i-1}) - \frac{1}{s+1}.$$

Таким образом строим множества C_i, по индукции находим C_t. Для множества C_t получим:

$$\rho_{n_1}(C_t) \geqslant \rho_{n_1}(C_0) - \frac{t}{s+1} = 1 - \frac{t}{s+1}.$$

Следовательно, $\rho_{n_1}(C_t) > \sigma_r(f)$. Функция h_{e_t} — константа на множестве C_t. Получаем противоречие с определением $\sigma_r(f)$. Отсюда следует, что $L_{AC}(S) > t$. ■

Завершим доказательства теорем 3.1 и 3.2.

Для схем, реализующих почти все булевы функции от n переменных, положим $s = \lfloor\sqrt{2n}\rfloor, r = n/2$. Тогда, по лемме 3.8, получим, что $L_{AC}(S) > \frac{\sqrt{n}}{2\sqrt{2}}$.

Для произвольной схемы S, реализующей линейную функцию или функцию голосования от n переменных, положим $s = \lfloor\sqrt{3n}\rfloor, r = n - 3$. Получаем, что $L_{AC}(S) > \frac{n-3}{\sqrt{3n}}$.

Глава 4

Сложность симметрических функций в базисе AC

4.1 Результаты главы 4

В этой главе изучается сложность реализации симметрических булевых функций схемами из функциональных элементов в базисе AC.

Раздел 4.2 посвящен доказательству точной формулы, выражающей сложность реализации произвольной симметрической функции схемами в базисе AC. Напомним, что для симметрической функции f через $k(f)$ обозначается количество слоев куба (т.е. всех наборов куба, содержащих одинаковое количество единиц), на которых функция f равна 1.

Теорема 4.1. *Для произвольной симметрической функции f, существенно зависящей от всех своих $n \geqslant 2$ переменных, выполнено равенство:*

$$L_{AC}(f) = \min\left(k(f),\, n - k(f) + 2\right).$$

Замечание. *В базисе AC сложность функций $f \equiv 0$ и $f \equiv 1$ равна 1, сложность функции $f = x_i$ равна 0 (схема состоит из единственного полюса), сложность функции $f = \overline{x}_i$ равна 1.*

С использованием теоремы 4.1 нетрудно установить точные значения сложности реализации функции четности и функции голосования от n переменных схемами в базисе AC.

Теорема 4.2. *Для линейной функции l_n, ее отрицания $\overline{l_n}$ и функции голосования m_n от n переменных выполнены равенства*

$$L_{AC}(l_n) = \left\lfloor \frac{n+1}{2} \right\rfloor,\ L_{AC}(m_n) = L_{AC}(\overline{l_n}) = \left\lceil \frac{n+1}{2} \right\rceil$$

при всех $n \geqslant 2$.

Доказательство этого результата изложено в разделе 4.3.

Следует отметить, что в работе автора [76], где изложено доказательство теорем 4.1 и 4.2, из формулировок утверждений выпало условие о том, что $n \geqslant 2$.

В главе 2 установлена верхняя оценка функции Шеннона $L(n) \leqslant n$. Эта оценка и нижняя оценка, вытекающая из теоремы 4.2, в совокупности устанавливают порядок роста функции Шеннона в базисе AC.

Теорема 4.3. $L_{AC}(n) = \Theta(n)$.

4.2 Доказательство теоремы 4.1

Докажем по отдельности две леммы.

Лемма 4.1. *Для произвольной симметрической функции $f(x_1 \ldots, x_n)$, существенно зависящей от всех своих $n \geqslant 2$ переменных, выполнено: $L_{AC}(f) \geqslant \min(k(f),\, n - k(f) + 2)$.*

Лемма 4.2. *Для произвольной симметрической функции $f(x_1 \ldots, x_n)$, существенно зависящей от всех своих $n \geqslant 2$ переменных, выполнено: $L_{AC}(f) \leqslant \min(k(f),\, n - k(f) + 2)$.*

Вначале мы коротко опишем идею доказательства леммы 4.1, а затем изложим подробное полное рассуждение. Далее мы докажем лемму 4.2 (доказательство опубликовано в работе автора [78]).

Доказательства лемм 4.1 и 4.2 в совокупности дадут доказательство теоремы 4.1.

Идея доказательства леммы 4.1

Мы изложим здесь идею доказательства нижней оценки из леммы 4.1 на примере частного случая. Здесь и далее в главе 4 доказательство нижних оценок будем вести для приведенных схем с произвольно фиксированной правильной нумерацией элементов (определения см. в главе 1). Для произвольной симметрической функции f рассмотрим все схемы, которые реализуют эту функцию и обладают следующим свойством: на входы любого элемента схемы подаются все входы схемы. (В дальнейшем — см. доказательство леммы 4.2 — будет показано, что всякую симметрическую функцию можно реализовать схемой такого вида.) Для любой схемы S_f с описанным свойством покажем, что нижняя оценка ее сложности имеет вид $L_{AC}(S_f) \geqslant k(f)$. Данный частный случай удобен, чтобы продемонстрировать идею доказательства леммы 4.1 грубо, в самых общих чертах. В общем случае, при доказательстве леммы 4.1, описанное свойство схем, разумеется, не предполагается.

В рассматриваемом частном случае введем понятие первого ненулевого элемента на данном наборе. Пусть при подаче на входы схемы произвольного набора $\boldsymbol{\alpha} \in \{0,1\}^n$ элементы $e_{i_1}, \ldots, e_{i_l}$ есть все такие элементы схемы S_f, что $h_{i_j}(\boldsymbol{\alpha}) = 1$ для всех $j \in [l]$ (напомним, что согласно обозначениям, введенным в главе 1, через h_j обозначается функция, которая реализуется на выходе элемента e_j). Тогда элемент e_m, обладающий минимальным номером среди элементов $e_{i_1}, \ldots, e_{i_l}$, будем называть первым ненулевым элементом на наборе $\boldsymbol{\alpha}$. Отметим, что это определение соответствует интуитивному представлению.

Возьмем произвольную цепь $\widetilde{C}$, состоящую из $n+1$ различного набора куба $\{0,1\}^n$. Цепь $\widetilde{C}$ обладает следующим свойством: никакой элемент схемы S_f не будет дважды первым ненулевым на наборах этой цепи. Действительно, предположим обратное: некоторый элемент e_t является первым ненулевым на наборах $\boldsymbol{\beta}$ и $\boldsymbol{\gamma}$ цепи $\widetilde{C}$. Без ограничения общности будем считать, что набор $\boldsymbol{\beta}$ меньше набора $\boldsymbol{\gamma}$. По определению первого ненулевого элемента, все элементы с номерами

меньше t выдают 0 на наборах $\boldsymbol{\beta}$ и $\boldsymbol{\gamma}$. Таким образом, получаем, что антицепная функция g_t, которая соответствует элементу e_t, выдает 1 на некоторой паре сравнимых наборов. Это противоречит тому, что функция g_t — антицепная.

Из доказанного свойства цепи следует, что сложность схемы S_f не меньше количества наборов этой цепи, на которых в схеме есть первый ненулевой элемент. Заметим, что если функция f выдает 1 на каком-то наборе, то в схеме S_f есть первый ненулевой элемент на этом наборе. Отсюда и вытекает нижняя оценка сложности схемы: $L_{AC}(S_f) \geqslant k(f)$.

При доказательстве свойства цепи используется тот факт, что схема S_f имеет особый вид: на входы элемента e_t, которому приписана антицепная функция g_t, непосредственно подаются все входы схемы. В общем случае схема не обладает указанным свойством, и аналогичное утверждение не получится доказать для произвольно выбранной цепи; потребуется построить специальную цепь, следуя определенному правилу. Кроме того, в общем случае понятие первого ненулевого элемента будет определено несколько более сложным образом. Указанные технические изменения позволят доказать лемму 4.1 в общем случае, опираясь на изложенные выше основные идеи.

Основная конструкция

Доказательство. Рассмотрим произвольную симметрическую функцию $f(x_1, \ldots, x_n)$, которая равна 1 на $k(f)$ различных слоях куба $\{0,1\}^n$ (по условию также считаем, что f зависит от всех своих $n \geqslant 2$ переменных существенно). Рассмотрим произвольную схему S в базисе AC, реализующую функцию f. Пусть $L_{AC}(S) = s$ и $e_1, \ldots, e_s$ — все элементы схемы (считаем, что задана правильная нумерация элементов схемы, определение см. в главе 1). Элементам приписаны соответственно антицепные функции $g_1, \ldots, g_s$. Докажем оценку $s \geqslant \min(k(f),\, n - k(f) + 2)$.

Для доказательства построим цепь C, состоящую из $n+1$ различного набора куба $\{0,1\}^n$. В качестве крайних наборов цепи C возьмем верхний и нижний наборы куба: $\mathbf{0}, \mathbf{1} \in \{0,1\}^n$ (см. определение в главе 1). Оставшаяся часть раздела посвящена построению промежуточных наборов цепи.

Говоря неформально, промежуточные наборы цепи мы будем получать, двигаясь по кубу с двух сторон: спускаясь от верхнего набора или поднимаясь от нижнего. «Спуск» от верхнего набора осуществляется так: по определенному алгоритму в текущем наборе выбирается одна из единичных компонент, значение которой изменяется на 0. Полученный набор добавляется в цепь. Значение входной переменной, соответствующей выбранной компоненте, далее считается зафиксированным значением 0 и более не изменяется. Аналогично осуществляется «подъем» от нижнего набора: значение определенной нулевой компоненты текущего набора изменяется на 1, и, тем самым, получается очередной набор цепи; соответствующая входная переменная фиксируется значением 1. Всякий раз при фиксировании значения очередной входной переменной происходит переход к подкубу размерности на единицу меньше, и далее рассматриваются его верхний и нижний наборы (определение подкуба см. в главе 1).

Вернемся к подробному описанию процесса построения цепи. Чтобы построить цепь, будем рассматривать элементы схемы S в порядке заданной правильной нумерации, начиная с элемента e_1. Процесс построения будет характеризоваться следующими параметрами.

- Номер шага $i \in [s]$; он определяется номером элемента схемы, с которого начинается данный шаг.

- Одновременно с цепью строятся два множества: F_i, $T_i \subseteq [n]$. Это множества номеров тех входных переменных схемы, значения которых после i-го шага зафиксированы нулями (F_i) и единицами (T_i, соответственно).

  Входную переменную схемы будем называть *свободной относительно множества* A, где $A \subseteq [n]$, если номер этой переменной принадлежит

множеству $[n] \setminus A$. В процессе построения цепи мы будем рассматривать свободные переменные относительно множеств вида $F_i \cup T_i$: неформально, это те переменные, значения которых в определенный момент времени еще не зафиксированы значениями 0 или 1. Входы схемы будем называть *свободными относительно множества* A, где $A \subseteq [n]$, если этим входам приписаны переменные, свободные относительно множества A.

На i-м шаге рассматривается подкуб с верхним и нижним наборами $\boldsymbol{x}^{[n]\setminus F_{i-1}}$ и $\boldsymbol{x}^{T_{i-1}}$ и строится новый подкуб — с верхним и нижним наборами $\boldsymbol{x}^{[n]\setminus F_i}$ и $\boldsymbol{x}^{T_i}$ (обозначения см. в главе 1).

- E_i — множество таких элементов схемы из множества $\{e_1, \ldots, e_i\}$, на входы которых могут подаваться только выходы элементов с меньшими номерами и входы схемы, соответствующие входным переменным с номерами из множества $F_i \cup T_i$. Для каждого i имеем: $E_i \subseteq \{e_1, \ldots, e_i\}$. Элемент схемы помещается в множество E_i на i-м шаге, если его входы не присоединены ко входам схемы, свободным относительно множества $F_i \cup T_i$.

Отметим, что с ростом номера i множества F_i, T_i и E_i не уменьшаются. В начале построения полагаем $i = 0$, $F_0 = T_0 = \emptyset$, $E_0 = \emptyset$ и, как уже было сказано, $C = \{\mathbf{0}, \mathbf{1}\}$.

Определим основное понятие, на котором основано рассуждение.

Определение 4.1. *Пусть задано множество элементов $E \subseteq \{e_1, \ldots, e_s\}$. Подадим на входы схемы S произвольный набор $\boldsymbol{\alpha} \in \{0,1\}^n$. Пусть $e_{r_1}, \ldots, e_{r_l}$ — это все такие элементы схемы, что для всякого $j \in [l]$ выполнено:*

1. $h_{r_j}(\boldsymbol{\alpha}) = 1$;
2. $e_{r_j} \in \{e_1, \ldots, e_s\} \setminus E$.

Элемент e_m, обладающий минимальным номером среди элементов $e_{r_1} \ldots, e_{r_l}$, называется первым ненулевым элементом на наборе $\boldsymbol{\alpha}$ относительно множества E.

Иногда, говоря о первом ненулевом элементе на некотором наборе, мы не будем указывать явно, относительно какого множества он рассматривается, так как это будет понятно из контекста.

Будем строить цепь таким образом, чтобы для любого i после i-го шага были выполнены следующие **свойства**.

1. Для всех $t, p \leqslant i$: $F_t \cap T_p = \emptyset$ (т. е. нельзя зафиксировать переменную, например, единицей, а позже — нулем; неформально об этом свойстве говорилось ранее).

2. Для всякого элемента $e_j \in \{e_1, \ldots, e_i\} \setminus E_i$ и для функции h_j, которая вычисляется на выходе элемента e_j, выполнено равенство:

$$h_j(\boldsymbol{x}^{[n]\setminus F_i}) = h_j(\boldsymbol{x}^{T_i}) = 0.$$

   Свойство 2 — ключевое в процессе построения цепи. Неформально говоря, оно означает, что после i-го шага при подаче на входы схемы верхнего и нижнего наборов текущего подкуба все элементы вплоть до i-го, кроме элементов из множества E_i, выдают на этих наборах 0.

Процедура построения цепи разбивается на два этапа.

Этап I. На этапе будет s шагов по числу элементов схемы. Предположим, было совершено i шагов, опишем $(i+1)$-й шаг.

По окончании i-го шага рассмотрены первые i элементов схемы: $e_1, e_2, \ldots, e_i$. Построено некоторое множество F_i, содержащее номера входных переменных схемы, зафиксированных значением 0. Также построено множество T_i, содержащее номера входных переменных схемы, зафиксированных значением 1. Цепь C содержит наборы $\mathbf{0}, \mathbf{1} \in \{0,1\}^n$, а также наборы, полученные одновременно с построением множеств F_i и T_i. Построено множество элементов E_i. Рассматривается подкуб размерности $n - |F_i| - |T_i|$ с верхним и нижним наборами $\boldsymbol{x}^{[n]\setminus F_i}$ и $\boldsymbol{x}^{T_i}$, соответственно.

Итак, начиная $(i+1)$-й шаг, переходим к элементу e_{i+1}. Возможны следующие случаи (отметим, что они не могут реализоваться одновременно).

1. Пусть на входы элемента e_{i+1} не подаются непосредственно входы схемы, свободные относительно множества $F_i \cup T_i$. Тогда полагаем $E_{i+1} = E_i \cup \{e_{i+1}\}$, $F_{i+1} = F_i$, $T_{i+1} = T_i$. На этом $(i+1)$-й шаг закончен.

2. Иначе: пусть на какой-либо вход элемента e_{i+1} непосредственно подается хотя бы один из входов схемы, свободный относительно множества $F_i \cup T_i$. Пусть этому входу приписана некоторая переменная x_m, где $m \in [n] \setminus (F_i \cup T_i)$. Проверим, выполнено ли свойство 2 для элемента e_{i+1}: $h_{i+1}(\boldsymbol{x}^{[n]\setminus F_i}) = h_{i+1}(\boldsymbol{x}^{T_i}) = 0$.

   2.1. Если свойство 2 выполнено, то полагаем $E_{i+1} = E_i$, $F_{i+1} = F_i$, $T_{i+1} = T_i$, и $(i+1)$-й шаг закончен.

   2.2. Пусть свойство 2 для e_{i+1} не выполнено на верхнем наборе подкуба: $h_{i+1}(\boldsymbol{x}^{[n]\setminus F_i}) = 1$ (случай нижнего набора будет разобран позже). Для удобства разобьем изложение этого случая на два подэтапа.

      2.2.1. Вначале мы работаем с элементом e_{i+1}. Из условия случая 2.2 следует, что элемент e_{i+1} является первым ненулевым на наборе $\boldsymbol{x}^{[n]\setminus F_i}$ относительно множества E_i. Зафиксируем значение указанной выше переменной x_m нулем.

      Будем использовать вспомогательные обозначения: F^r_{i+1}, E^r_{i+1} и, в дальнейшем, T^r_{i+1}, где r — натуральный параметр.

      Для $r = 1$ полагаем $F^1_{i+1} = F_i \cup \{m\}$; также полагаем $T_{i+1} = T_i$. Тем самым, мы переходим к подкубу размерности на единицу меньше (размерности $n - |F^1_{i+1}| - |T_{i+1}|$). Добавляем в цепь C верхний набор этого подкуба — $\boldsymbol{x}^{[n]\setminus F^1_{i+1}}$. Положим множество E^1_{i+1} равным объединению множества E_i и множества всех элементов e_j, где $j \leq i+1$, на входы которых после фиксирования

переменной x_m более не подаются непосредственно входы схемы, свободные относительно множества $F^1_{i+1} \cup T_{i+1}$.

2.2.2. Далее мы работаем с элементами e_j, где $j \leqslant i+1$. Вначале проведем рассуждение, по-прежнему считая значение r равным 1. Рассмотрим элементы e_j, где $j \leq i+1$ и $e_j \notin E^r_{i+1}$, и проверим, выполнено ли для них свойство 2 на наборе $\boldsymbol{x}^{[n]\setminus F^r_{i+1}}$. Пусть нашлись элементы, для которых свойство 2 не выполнено, и пусть e_l — элемент с минимальным номером среди них.

Лемма 4.3. *Хотя бы на один из входов указанного элемента e_l подается непосредственно какой-либо вход схемы, свободный относительно множества $F^r_{i+1} \cup T_{i+1}$.*

Доказательство. Для функции h_l, которая реализуется на выходе элемента e_l, имеем: $h_l(\boldsymbol{x}^{[n]\setminus F^r_{i+1}}) = 1$, $h_l(\boldsymbol{x}^{T_{i+1}}) = 0$. Значение антицепной функции g_l, соответствующей элементу e_l, определяется значениями на некоторых входах схемы, а также значениями на выходах элементов двух типов:

A. таких элементов e_u, что $e_u \notin E^r_{i+1}$, где $u < l$,

B. таких элементов e_u, что $e_u \in E^r_{i+1}$, где $u < l$.

Значения на выходах элементов 2-го типа определяются значениями на выходах элементов 1-го типа. В силу минимальности l, все элементы e_j 1-го типа на верхнем и нижнем наборах подкуба выдают 0. Следовательно, значения на выходах элементов 2-го типа на указанных двух наборах одинаковы. Получаем, что функция g_l выдает различные значения на некоторой паре наборов со следующим свойством: в этих наборах компоненты, соответствующие значениям на выходах элементов с меньшими номерами, совпадают. Следовательно, значения каких-то из оставшихся компонент в этих наборах должны различаться. Таким

образом, хотя бы один из входов схемы, свободный относительно множества $F^r_{i+1} \cup T_{i+1}$, подается непосредственно на один из входов элемента e_l. Лемма 4.3 доказана. ■

Продолжим основное рассуждение. По лемме 4.3 получаем, что элемент e_l является первым ненулевым элементом на наборе $\boldsymbol{x}^{[n]\setminus F^r_{i+1}}$ относительно множества E^r_{i+1}. Рассмотрим произвольный вход схемы, свободный относительно множества $F^r_{i+1} \cup T_{i+1}$, который подается непосредственно на некоторый вход элемента e_l. Зафиксируем переменную, которая приписана этому входу схемы, значением 0. Тем самым, мы добавим номер этой входной переменной в множество F^r_{i+1}. Обозначим полученное множество через F^{r+1}_{i+1}. Мы вновь перешли к подкубу размерности на единицу меньше. Верхний набор этого подкуба $\boldsymbol{x}^{[n]\setminus F^{r+1}_{i+1}}$ добавляем в цепь C.

Полагаем множество E^{r+1}_{i+1} равным объединению множества E^r_{i+1} и множества всех элементов e_j, где $j \leqslant i+1$, на входы которых после фиксирования указанной выше переменной более не подаются непосредственно входы схемы, свободные относительно множества $F^{r+1}_{i+1} \cup T_{i+1}$.

Далее мы действуем по циклу: вновь выполняем процесс, описанный в пункте 2.2.2, для всех $r = 2, \ldots, q$, где q — это такое значение параметра r, при котором свойство 2 будет выполнено для всех элементов e_j, где $j \in [i+1]$ и $e_j \notin E^q_{i+1}$.

Отметим важное свойство, которое потребуется в дальнейшем.

Лемма 4.4. *Любой элемент e_p, где $p \in [i+1]$, добавленный в множество E^r_{i+1}, где $r \leq q$, в рамках описанного в пункте 2.2 процесса, будет выдавать 0 на всех наборах подкуба размерности*

$n - |F^r_{i+1}| - |T_{i+1}|$, *на которых элементы* e_a, *где* $a < p$, $e_a \notin E^r_{i+1}$, *выдают* 0.

Доказательство. На входы элемента e_p не подаются входы схемы, свободные относительно множества $F^r_{i+1} \cup T_{i+1}$, поэтому на всех указанных наборах этот элемент выдает одно и то же значение. На нижнем наборе подкуба он выдает 0 (т. к. $T_{i+1} = T_i$). Значит, на всех описанных наборах подкуба он также выдает 0. Лемма 4.4 доказана. ■

После того, как описанные действия выполнены, полагаем $F_{i+1} = F^q_{i+1}$, $E_{i+1} = E^q_{i+1}$, и $(i+1)$-й шаг закончен.

Рассмотрим оставшийся случай.

2.3. Пусть свойство 2 для e_{i+1} не выполнено на нижнем наборе подкуба: $h_{i+1}(\boldsymbol{x}^{T_i}) = 1$.

Лемма 4.5. *Случаи 2.2 и 2.3 не могут произойти одновременно.*

Доказательство. Предположим противное. При этом имеем: для всех $e_j \notin E_i$, где $j < i+1$, функции h_j на наборах $\boldsymbol{x}^{[n]\setminus F_i}$ и $\boldsymbol{x}^{T_i}$ выдают 0; для всех $e_j \in E_i$, где $j < i+1$, функции h_j на этих наборах выдают одно и то же значение. Наборы $\boldsymbol{x}^{[n]\setminus F_i}$ и $\boldsymbol{x}^{T_i}$ сравнимы, и, по условию случая 2.2, какой-либо из входов элемента e_{i+1} присоединен ко входу схемы, на котором на этих наборах будут различные значения. Значит, функция g_{i+1} выдает 1 на некоторой паре сравнимых наборов, отличающихся по крайней мере в одной компоненте. Получаем противоречие с тем, что g_{i+1} — антицепная функция. Лемма 4.5 доказана. ■

Итак, вернемся к случаю 2.3: он двойственен случаю 2.2, и мы действуем аналогично, с той лишь разницей, что входные переменные фиксируются значением 1. Итак, вначале зафиксируем указанную

в пункте 2 переменную x_m единицей, и положим $T^1_{i+1} = T_i \cup \{m\}$ (следуя обозначениям, введенным в 2.2). Положим $F_{i+1} = F_i$. Таким образом, переходим к подкубу размерности $n - |F_{i+1}| - |T^1_{i+1}|$. Помещаем в цепь C набор $\boldsymbol{x}^{T^1_{i+1}}$. Далее, аналогично случаю 2.2, выполняем цикл, описанный в 2.2.2, получая, соответственно, множества $T^2_{i+1}, T^3_{i+1}, \ldots$ до тех пор, пока для некоторого v свойство 2 не будет выполнено для всех элементов e_j, где $j \leqslant i+1$ и $e_j \notin E^v_{i+1}$. После этого полагаем $T_{i+1} = T^v_{i+1}, E_{i+1} = E^v_{i+1}$, и $(i+1)$-й шаг закончен.

Если мы совершали шаги этапа I и зафиксировали значения всех входных переменных, то, таким образом, цепь, состоящая из $n+1$ набора, построена, и процесс заканчивается.

Пусть мы совершили s шагов, описанных в случаях 1 и 2 этапа I, т. е. рассмотрели последовательно все элементы схемы S, однако искомая цепь еще не построена. После s-го шага получены множества F_s, T_s и E_s — для краткости далее опустим индексы и будем писать F, T и E, соответственно. Переходим к этапу II.

Этап II. Исходный куб размерности n сужен до подкуба размерности $n - |F| - |T|$ так, что все элементы схемы $e_1, \ldots, e_s$, кроме элементов из E, выдают 0 на верхнем и нижнем наборах этого подкуба — $\boldsymbol{x}^{[n]\setminus F}$ и $\boldsymbol{x}^T$. Положим $T^0 = T$. Будем добавлять в T^0 номера переменных из $[n] \setminus (F \cup T)$, получая множества T^1, T^2 и т. д., следующим образом: для любого $i \geqslant 0$,

1. если на наборе $\boldsymbol{x}^{T^i}$ нет первого ненулевого элемента относительно множества E, то добавляем в множество T^i номер произвольной переменной из множества $[n]\setminus(F\cup T^i)$. Получаем множество T^{i+1} и набор $\boldsymbol{x}^{T^{i+1}}$, который помещаем в цепь;

2. если на наборе $\boldsymbol{x}^{T^i}$ есть первый ненулевой элемент относительно множества E, то, аналогично доказательству леммы 4.3, нетрудно показать, что

какой-либо из входов этого элемента присоединен ко входу схемы, свободному относительно множества $[n] \setminus (F \cup T^i)$. Зафиксируем единицей входную переменную, которая соответствует этому входу. Получаем множество T^{i+1} и набор $\boldsymbol{x}^{T^{i+1}}$, который помещаем в цепь.

Если в рамках описанного процесса при добавлении номера какой-либо переменной в множество T^i входы некоторого элемента e_d более не присоединены ко входам схемы, свободным относительно множества $F \cup T^i$, то полагаем $E = E \cup \{e_d\}$. Нетрудно понять, что для всех таких элементов выполняется свойство, аналогичное лемме 4.4. Отметим, что первый ненулевой элемент рассматривается всякий раз относительно текущего множества E.

Повторяем описанный процесс до тех пор, пока все входные переменные не будут зафиксированы, то есть, пока не будет построена искомая цепь C. Отметим, что на этапе 2 множество T выбрано для определенности: можно было выбрать множество F и, соответственно, фиксировать переменные значением 0.

При построении цепи C на входы схемы подаются только наборы $\boldsymbol{x}^T$ и $\boldsymbol{x}^{[n]\setminus F}$(для краткости индексы опущены). Эти наборы сравнимы, т. к. на каждом шаге $T \subseteq [n] \setminus F$. Таким образом, множество C действительно является цепью.

Завершение доказательства леммы 4.1

Цепь C обладает следующим свойством.

Лемма 4.6. *Никакой элемент схемы S не был первым ненулевым элементом (относительно соответствующих множеств) на двух различных наборах цепи C в процессе ее построения.*

Доказательство. Будем вести доказательство методом «от противного». Пусть, без ограничения общности, набор $\boldsymbol{x}^P$ добавлен в цепь на шаге с номером b, а $\boldsymbol{x}^{P'}$— на шаге с номером c, где $b < c$. На этих шагах были построены мно-

жества E_b и E_c, причем $E_b \subseteq E_c$. И пусть существует $t \in [s]$ такой, что элемент e_t — первый ненулевой элемент на наборах x^P и $x^{P'}$ относительно соответствующих множеств. В частности, имеем: $h_t(\boldsymbol{x}^P) = h_t(\boldsymbol{x}^{P'}) = 1$. Для всякого элемента $e_j \notin E_c$, где $j < t$, по определению первого ненулевого элемента (относительно множества E_c, а следовательно, и E_b), выполнено: $h_j(\boldsymbol{x}^P) = h_j(\boldsymbol{x}^{P'}) = 0$. Также для всякого элемента $e_j \in E_c \setminus E_b$, где $j < t$, по свойству из леммы 4.4, имеем: $h_j(\boldsymbol{x}^P) = h_j(\boldsymbol{x}^{P'}) = 0$, а значения элементов $e_j \in E_b$, где $j < t$, определяются значениями остальных элементов с меньшими номерами. Следовательно, значения всякого элемента с номером меньше t будут одинаковыми на наборах $\boldsymbol{x}^{P'}$ и $\boldsymbol{x}^P$. При этом, по построению, набор $\boldsymbol{x}^{P'}$ отличается от набора $\boldsymbol{x}^P$ значением хотя бы одной компоненты, соответствующей входной переменной схемы, непосредственно подаваемой на один из входов элемента e_t.

Таким образом, для антицепной функции g_t, соответствующей элементу e_t, имеем: g_t выдает 1 на некоторой паре сравнимых наборов. Это противоречит тому, что g_t — антицепная функция. Лемма 4.6 доказана. ■

Завершим доказательство леммы 4.1. Напомним, что построенная цепь C содержит $n + 1$ набор куба $\{0, 1\}^n$. На всех наборах цепи, на которых в схеме S нет первого ненулевого элемента относительно соответствующего множества, значение на выходе схемы одинаковое, обозначим его через a, где $a \in \{0, 1\}$. На любом наборе цепи, на котором схема выдает $1 - a$, есть первый ненулевой элемент. Функция $f(x_1, \ldots, x_n)$ принимает значение 1 на $k(f)$ наборах этой цепи, а значение 0 — на $n + 1 - k(f)$ наборах. Возможны следующие случаи.

1. Пусть $a = 0$. Тогда для любого набора, на котором схема выдает 1, в схеме есть первый ненулевой элемент. То есть на $k(f)$ наборах цепи C есть первые ненулевые элементы. По лемме 4.6, все эти элементы различны. Отсюда получаем, что $L_{AC}(S) \geqslant k(f)$.

2. Пусть $a = 1$. Тогда для любого набора, на котором схема выдает 0, в схеме есть первый ненулевой элемент. То есть, на $n + 1 - k(f)$ наборах цепи C

есть первые ненулевые элементы. Аналогично, по лемме 4.6, получаем: $L_{AC}(S) \geqslant n + 1 - k(f)$. При этом, последний элемент схемы (элемент e_s) не является первым ненулевым, т. к. если на некотором наборе в схеме есть первый ненулевой элемент, то, по условию случая, схема выдает 0, т. е. элемент e_s выдает 0. Отсюда вытекает, что $L_{AC}(S) \geqslant n + 2 - k(f)$.

Итак, мы показали, что $L_{AC}(S) \geqslant \min(k(f), n - k(f) + 2)$. В силу произвольности схемы S, получаем аналогичное неравенство для величины $L_{AC}(f)$. Лемма 4.1 полностью доказана. ■

Отметим, что метод доказательства, использованный в главе 4, не позволяет получить для почти всех функций оценку лучше, чем доказанная оценка в главе 3.1.

Доказательство леммы 4.2

Рассмотрим произвольную симметрическую функцию $f(x_1, \ldots, x_n)$, существенно зависящую от всех своих $n \geqslant 2$ переменных. Разобьем доказательство на две части: в первой части докажем оценку $L_{AC}(f) \leqslant k(f)$, во второй — оценку $L_{AC}(f) \leqslant n - k(f) + 2$. Вместе эти оценки дают требуемое утверждение.

Доказательство. 1. Пусть функция f равна 1 на слоях булева куба с номерами $i_1, \ldots, i_{k(f)}$, причем $i_1 < \ldots < i_{k(f)}$ (по условию леммы, $f \not\equiv 0$, поэтому хотя бы один такой слой существует).

Напомним, что набор значений аргументов $(x_1, \ldots, x_n)$ обозначается через $\boldsymbol{x}$. Для функции f, для каждого $t \in \{i_1, \ldots, i_{k(f)}\}$ зададим функцию $h_t(\boldsymbol{x})$ так: $h_t(\boldsymbol{x}) = 1$ тогда и только тогда, когда $\sum\limits_{p=1}^{n} x_p = i_t$. Ясно, что функции h_t — антицепные, поскольку являются характеристическими функциями слоев куба.

Обозначим через $\boldsymbol{y}$ набор значений аргументов $(y_1, \ldots, y_{k(f)-1)})$.

Пусть M_1 — множество наборов $(\boldsymbol{y}, \boldsymbol{x})$ таких, что одновременно выполнены три условия: 1) существует такой номер $j \in [k(f) - 1]$, что $y_j = 1$; 2) для всех $q \neq j$ выполнено, что $y_q = 0$; 3) $\sum\limits_{p=1}^{n} x_p = i_j$. Пусть M_2 — множество наборов $(\boldsymbol{y}, \boldsymbol{x})$, удовлетворяющих следующим условиям: для всех $q \in [k(f) - 1]$ выполнено, что $y_q = 0$, и $\sum\limits_{p=1}^{n} x_p = i_{k(f)}$.

Зададим булеву функцию g от $k(f) - 1 + n$ переменных $y_1 \ldots, y_{k(f)-1}, x_1 \ldots, x_n$ так: $g(\boldsymbol{y}, \boldsymbol{x}) = 1$ лишь на наборах $(\boldsymbol{y}, \boldsymbol{x})$ из множества $M_1 \sqcup M_2$.

Нетрудно понять, что функция g — антицепная. Действительно, рассмотрим два набора из носителя g: $(\boldsymbol{y}_1, \boldsymbol{x}_1) \neq (\boldsymbol{y}_2, \boldsymbol{x}_2)$. Если $(\boldsymbol{y}_1, \boldsymbol{x}_1), (\boldsymbol{y}_2, \boldsymbol{x}_2) \in M_1$ и $\boldsymbol{y}_1 \neq \boldsymbol{y}_2$, то наборы несравнимы. Если $(\boldsymbol{y}_1, \boldsymbol{x}_1), (\boldsymbol{y}_2, \boldsymbol{x}_2) \in M_1$ и $\boldsymbol{y}_1 = \boldsymbol{y}_2$, то номера компонент, в которых стоят по i_j единиц в наборах $\boldsymbol{x}_1$ и $\boldsymbol{x}_2$, не совпадают. А значит, наборы $(\boldsymbol{y}_1, \boldsymbol{x}_1)$ и $(\boldsymbol{y}_2, \boldsymbol{x}_2)$ несравнимы. Если $(\boldsymbol{y}_1, \boldsymbol{x}_1), (\boldsymbol{y}_2, \boldsymbol{x}_2) \in M_2$, то, аналогично предыдущему случаю, легко видеть, что наборы несравнимы. Если, без ограничения общности, $(\boldsymbol{y}_1, \boldsymbol{x}_1) \in M_1$, $(\boldsymbol{y}_2, \boldsymbol{x}_2) \in M_2$, то $\boldsymbol{y}_1 > \boldsymbol{y}_2$, а в $\boldsymbol{x}_2$ больше единиц, чем в $\boldsymbol{x}_1$. Значит, наборы $(\boldsymbol{y}_1, \boldsymbol{x}_1)$, $(\boldsymbol{y}_2, \boldsymbol{x}_2)$ несравнимы.

Реализуем функцию $f(\boldsymbol{x})$ так:

$$f(\boldsymbol{x}) = g\left(h_1(\boldsymbol{x}), \ldots, h_{k(f)-1}(\boldsymbol{x}), \boldsymbol{x}\right). \tag{4.1}$$

То есть, мы подставляем в функцию g характеристические функции слоев булева куба, образующих в совокупности носитель функции f — все, кроме функции $h_{k(f)}$, — а также переменные, и получаем реализацию функции f.

Проверим равенство (4.1). Рассмотрим произвольный набор $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$. Возможны два случая.

(a) Пусть $f(\boldsymbol{\alpha}) = 1$, тогда $\sum\limits_{p=1}^{n} \alpha_p \in \{i_1, \ldots, i_{k(f)}\}$. Если $\sum\limits_{p=1}^{n} \alpha_p \leqslant i_{k(f)-1}$, то существует номер $j \in [k(f) - 1]$ такой, что $h_j(\boldsymbol{\alpha}) = 1$, для любого

$q \neq j : h_q(\boldsymbol{\alpha}) = 0$ и $\sum\limits_{p=1}^{n} \alpha_p = i_j$. Получаем, что набор $(\boldsymbol{y}, \boldsymbol{\alpha})$, где $(y_1, \ldots, y_{k(f)-1}, \boldsymbol{\alpha}) = \big(h_1(\boldsymbol{\alpha}), \ldots, h_{k(f)-1}(\boldsymbol{\alpha}), \boldsymbol{\alpha}\big)$, принадлежит множеству M_1. Значит, $g(\boldsymbol{y}, \boldsymbol{\alpha}) = 1$. Если $\sum\limits_{p=1}^{n} \alpha_p = i_{k(f)}$, то для любого $q \in [k(f) - 1]$, выполнено: $y_q = h_q(\boldsymbol{\alpha}) = 0$. Таким образом, набор $(\boldsymbol{y}, \boldsymbol{\alpha})$ принадлежит M_2, и следовательно, $g(\boldsymbol{y}, \boldsymbol{\alpha}) = 1$.

(b) Пусть $f(\boldsymbol{\alpha}) = 0$. Тогда для любого $j \in [k(f)]$ выполнено: $h_j(\boldsymbol{\alpha}) = 0$. В частности, $h_{k(f)}(\boldsymbol{\alpha}) = 0$, а значит, $\sum\limits_{p=1}^{n} \alpha_p \neq i_{k(f)}$. Отсюда получаем, что набор $(\boldsymbol{y}, \boldsymbol{\alpha}) = \big(h_1(\boldsymbol{\alpha}), \ldots, h_{k(f)-1}(\boldsymbol{\alpha}), \boldsymbol{\alpha}\big)$ не принадлежит ни M_1, ни M_2. Следовательно, $g(\boldsymbol{y}, \boldsymbol{\alpha}) = 0$.

Из (4.1) следует, что функция f может быть реализована схемой в базисе AC со сложностью не больше $k(f)$.

Получаем, что для всякой симметрической функции f, существенно зависящей от всех своих $n \geqslant 2$ переменных, существует схема S_f сложности $L_{AC}(S_f) \leqslant k(f)$, которая реализует функцию f и обладает следующим свойством: на входы всякого элемента схемы подаются все ее входы.

2. Напомним, что $f \not\equiv 1$. Из доказательства для случая 1 получаем, что для функции $\overline{f}$ выполнено: $L_{AC}(\overline{f}) \leqslant k(\overline{f})$, где $k(\overline{f}) = n + 1 - k(f)$. Таким образом, функция $\overline{f}$ может быть реализована схемой сложности не больше $n + 1 - k(f)$. Из всякой схемы для этой функции с помощью элемента отрицания легко получается схема для функции f, то есть $L_{AC}(f) \leqslant n - k(f) + 2$.

Итак, для произвольной симметрической функции f, существенно зависящей от $n \geqslant 2$ переменных, мы показали, что $L_{AC}(f) \leqslant \min\left(k(f), n - k(f) + 2\right)$. Тем самым лемма 4.2 доказана. ■

Доказательства лемм 4.1 и 4.2 дают в совокупности доказательство теоремы 4.1.

4.3 Доказательство теоремы 4.2

Для функции голосования имеем: $k(m_n) = \left\lceil \frac{n+1}{2} \right\rceil$ и, по теореме 4.1, получаем: $L_{AC}(m_n) = \left\lceil \frac{n+1}{2} \right\rceil$. Для линейной функции имеем: $k(l_n) = \left\lfloor \frac{n+1}{2} \right\rfloor$, соответственно, по теореме 4.1, получаем: $L_{AC}(l_n) = \left\lfloor \frac{n+1}{2} \right\rfloor$, что и доказывает теорему 4.2. ■

Отметим, что максимум верхней оценки из леммы 4.2 достигается: при нечетных n он равен сложности функций m_n, l_n и $\overline{l_n}$, а при четных n — сложности функций m_n и $\overline{l_n}$.

Глава 5

Оценки функции Шеннона в базисах ACL и ACM

5.1 Результаты главы 5

В данной главе построен пример бесконечного базиса, для которого порядок роста функции Шеннона лежит строго в интервале между функциями $\log_2 n$ и n.

Напомним, что через ACL обозначается бесконечный базис, состоящий из всех антицепных функций и всех линейных функций от любого числа переменных. В этой главе будет доказано следующее утверждение.

Теорема 5.1. $L_{ACL}(n) = \Theta(\sqrt{n \log_2 n})$.

Справедливость этого утверждения вытекает из сформулированных ниже верхней и нижней оценок функции Шеннона. Верхняя оценка доказана в разделе 5.3.

Теорема 5.2. $L_{ACL}(n) = O(\sqrt{n \log_2 n})$.

В разделе 5.4 доказана нижняя оценка сложности реализации функции голосования.

Теорема 5.3. $L_{ACL}(m_n) = \Omega(\sqrt{n \log_2 n})$.

Из этой теоремы вытекает нижняя оценка функции Шеннона.

Теорема 5.4. $L_{ACL}(n) = \Omega(\sqrt{n \log_2 n})$.

Также в данной главе рассматривается бесконечный базис ACM, состоящий из всех антицепных функций и всех функций голосования от любого числа переменных.

В разделе 5.5 приведено доказательство следующего утверждения.

Теорема 5.5. $L_{ACM}(n) = \Theta(\log_2 n)$.

5.2 Вспомогательные сведения

В этом разделе мы приведем определения понятий, формулировки и доказательства некоторых утверждений, которые потребуются для доказательства основных теорем данной главы.

При доказательстве теоремы 5.2 будет использовано следующее утверждение (доказательство см., например, в [48]).

Теорема 5.6. *Наибольшая мощность цепи в конечном частично упорядоченном множестве P равна наименьшему числу непересекающихся антицепей, на которые P может быть разложено.*

Также будут использованы некоторые результаты из теории кодирования. Приведенные ниже определения понятия линейного кода и некоторых других понятий подробнее можно найти, например, в [32]; мы дадим лишь их краткое изложение.

Пусть n и r, $r \leqslant n$, — некоторые натуральные числа, H — двоичная матрица, имеющая n столбцов. *Линейный код* длины n и размерности r с проверочной матрицей H состоит из всех двоичных векторов $\boldsymbol{x}$, таких что $H\boldsymbol{x} = 0$. Векторы $\boldsymbol{x}$ называются *кодовыми словами*. Если в матрице H имеется $n - r$ линейно независимых строк, то в линейном коде содержится 2^r кодовых слов. Число r называется *размерностью* кода. *Расстоянием (Хэмминга)* между двумя кодовыми словами называется число позиций, в которых эти слова различаются.

Минимальным расстоянием d кода называется минимальное расстояние между его словами. Код с минимальным расстоянием d может исправлять $\left\lfloor \frac{d-1}{2} \right\rfloor$ ошибок. Минимальное расстояние линейного кода равно минимальному весу ненулевых кодовых слов, где вес кодового слова — это число ненулевых позиций в нем. Любые $d-1$ столбцов проверочной матрицы линейного кода с минимальным расстоянием d линейно независимы.

Известно, что для существования линейного двоичного кода длины n, размерности r с минимальным расстоянием не менее d достаточно выполнения следующего неравенства:

$$\sum_{i=0}^{d-2} C_{n-1}^{i} < 2^{n-r}. \tag{5.1}$$

Это неравенство называют *границей Варшамова – Гилберта* [32].

Напомним известные оценки суммы биномиальных коэффициентов (см., например, [56]):

$$\left(\frac{t}{s}\right)^{s} \leqslant \sum_{i=0}^{s} C_{t}^{i} \leqslant \left(\frac{et}{s}\right)^{s}. \tag{5.2}$$

Используя второе неравенство из выражения (5.2) для $t = n-1$, $s = d-2$, нетрудно получить следующее достаточное условие для выполнения неравенства (5.1):

$$(d-2)\log_2 \frac{e(n-1)}{d-2} \leqslant n-r. \tag{5.3}$$

Таким образом, если неравенство (5.3) выполнено, то как следствие, выполнено неравенство (5.1), и значит, существует линейный двоичный код длины n, размерности r с минимальным расстоянием d.

Докажем лемму, которая потребуется при доказательстве теоремы 5.2.

Лемма 5.1. *Пусть* n *— натуральное число,* $k = \lfloor \sqrt{n \log_2 n} \rfloor$. *При всяком достаточно большом* n *для указанного* k *существует семейство непустых подмножеств* $R_1, \ldots, R_k \subseteq [n]$, *такое что любое семейство непустых попарно не пересекающихся подмножеств* $B_1, \ldots, B_k \subseteq [n]$ *обладает следующим свойством: хотя бы для одной пары* $i, j \in [n]$ *величина* $|B_j \cap R_i|$ *— нечетна.*

Доказательство. Рассмотрим двоичный линейный код длины n, размерности $n-k$ с минимальным расстоянием более $\frac{n}{k}$.

Нетрудно понять, что такой линейный код существует. Действительно, при $r = n-k$, $d = \lceil \frac{n}{k} \rceil$ неравенство (5.3) имеет вид: $\left(\lceil \frac{n}{k} \rceil - 2\right) \log_2 \frac{e(n-1)}{\lceil \frac{n}{k} \rceil - 2} \leqslant k$. Легко видеть, что при $k = \lfloor \sqrt{n \log_2 n} \rfloor$ последнее неравенство выполнено при всех достаточно больших n, что гарантирует существование описанного кода.

Рассмотрим проверочную матрицу этого кода, обозначим ее через H. Матрица имеет размер $k \times n$, ее строки — это упорядоченные наборы длины n, состоящие из нулей и единиц. Зададим подмножества $R_1, \ldots, R_k \subseteq [n]$ так: будем считать, что i-я строка матрицы H — это *характеристический вектор (набор) множества* R_i, а именно, множество R_i содержит элемент множества $[n]$, если на соответствующей этому элементу позиции в характеристическом векторе множества R_i стоит единица.

Далее, рассмотрим произвольное семейство непустых попарно не пересекающихся подмножеств $B_1, \ldots, B_k \subseteq [n]$. Сопоставим каждому из множеств B_j его характеристический вектор, будем обозначать его через $\boldsymbol{\chi}_{B_j} \in \{0,1\}^n$.

Требуется показать, что для указанного семейства множеств $R_1, \ldots, R_k$ и семейства множеств $B_1, \ldots, B_k$ найдется такое $j \in [k]$, что $H \cdot \boldsymbol{\chi}_{B_j} \neq \mathbf{0}$, где $\mathbf{0} \in \{0,1\}^n$.

Подмножества $B_1, \ldots, B_k$ попарно не пересекаются, это означает, что существует такое j_1, что для B_{j_1} выполнено: $|B_{j_1}| \leqslant \frac{n}{k}$. Матрица H является проверочной матрицей кода с минимальным расстоянием более $\frac{n}{k}$. Следовательно, выполнено: $H \cdot \boldsymbol{\chi}_{B_{j_1}} \neq \mathbf{0}$, где $\mathbf{0} \in \{0,1\}^n$, а значит, существует такое $i \in [k]$, что пересечение множеств R_i и B_{j_1} есть множество нечетной мощности. ■

Известно, что если существует двоичный линейный код длины n, исправляющий s ошибок и содержащий 2^r кодовых слов, то должно выполняться неравенство:

$$2^r \sum_{i=0}^{s} C_n^i \leqslant 2^n. \tag{5.4}$$

Обычно это неравенство называют *границей Хэмминга* (или «границей сферической упаковки») [32].

Используя первое неравенство в выражении (5.2), из условия (5.4) легко вывести следующее:

$$r + s \log_2 \frac{n}{s} \leqslant n. \tag{5.5}$$

Таким образом, если существует двоичный линейный код длины n, исправляющий s ошибок и содержащий 2^r кодовых слов, то выполняется неравенство (5.5).

При доказательстве теоремы 5.4 нам потребуется следующая лемма.

Лемма 5.2. *Пусть n — произвольное натуральное число. Для любого натурального $k \leqslant \lfloor \frac{1}{4}\sqrt{n \log_2 n} \rfloor$ и любого семейства непустых подмножеств $R_1, \ldots, R_k \subseteq [n]$ существует семейство непустых попарно не пересекающихся подмножеств $B_1, \ldots, B_k \subseteq [n]$, такое что*

1. *для любых $i, j \in [k]$ $|B_j \cap R_i|$ — четно;*
2. *для любого $j \in [k]$ выполнены неравенства: $\frac{n}{4k} \leqslant |B_j| \leqslant \frac{n}{2k}$.*

Доказательство. Пусть k, n — натуральные, $n' \geqslant \frac{n}{2}$, $k \leqslant \lfloor \frac{1}{4}\sqrt{n \log_2 n} \rfloor$, $k \in \mathbb{N}$.

В дальнейшем будет неоднократно использоваться следующий простой факт. Никакая двоичная матрица размера размера $k \times n'$, не может служить проверочной матрицей линейного двоичного кода длины n, исправляющего s ошибок и содержащего 2^r слов, где $r = n' - k$, $s = \left\lfloor \frac{n}{8k} \right\rfloor$. Действительно, нетрудно проверить, что при указанных значениях параметров неравенство (5.5) не выполняется.

Рассмотрим матрицу, строки которой есть характеристические векторы множеств $R_1, \ldots, R_k \subseteq [n]$ (подробнее см. в доказательстве леммы 5.1), обозначим ее через A. Отметим, что размер этой матрицы есть $k \times n$. Построим непустые попарно не пересекающиеся подмножества $B_1, \ldots, B_k \subseteq [n]$, удовлетворяющие условию леммы.

Поскольку матрица A не является проверочной матрицей кода с минимальным расстоянием больше $\frac{n}{4k}$, то существует подмножество $B \subset [n]$, такое что $|B| \leqslant \frac{n}{4k}$ и характеристический вектор этого множества $\boldsymbol{\chi}_B$ удовлетворяет уравнению

$$A \cdot \boldsymbol{\chi}_B = \mathbf{0}, \tag{5.6}$$

где $\mathbf{0} \in \{0,1\}^n$.

Удалим столбцы матрицы A, номера которых являются элементами множества B. Обозначим $n - |B|$ через n_1. После удаления столбцов мы получим новую матрицу A_1 размера $k \times n_1$. Заметим, что $n_1 \geqslant \frac{n}{2}$, значит, матрица A_1 также не является проверочной матрицей линейного двоичного кода размерности $r = n_1 - k$, исправляющего $s = \left\lfloor \frac{n}{8k} \right\rfloor$ ошибок.

Далее, проверим, выполнены ли неравенства: $\frac{n}{4k} \leqslant |B| \leqslant \frac{n}{2k}$. Ясно, что второе неравенство выполнено по построению.

1. Если первое неравенство выполнено, то полагаем $B_1 = B$.

2. Пусть первое неравенство не выполнено. Тогда, повторяя аналогичные рассуждения для матрицы A_1, получим множество B' и положим $B_1 = B' \cup B$. Заметим, что поскольку множества B и B' не пересекаются, то $\boldsymbol{\chi}_{B \cup B'} = \boldsymbol{\chi}_B + \boldsymbol{\chi}_{B'}$, и, в силу линейности, вектор $\boldsymbol{\chi}_{B \cup B'}$ удовлетворяет уравнению (5.6), при этом $|B' \cup B| \leqslant \frac{n}{2k}$. Повторяем процедуру до тех пор, пока не будет выполнено неравенство: $|B_1| \geqslant \frac{n}{4k}$. Заметим, что при таком построении величина $|B_1|$ не превысит верхнюю границу $\frac{n}{2k}$, так как размер шага, то есть мощность добавляемых множеств, не более $\frac{n}{4k}$.

Далее, проводя аналогичные рассуждения, строим множества $B_2, \ldots, B_k$. Нетрудно понять, что построение множеств возможно до тех пор, пока остается хотя бы $\frac{n}{2}$ столбцов исходной матрицы A, именно это условие гарантирует свойство 2, сформулированное в условии леммы.

■

5.3 Доказательство теоремы 5.2

В данном разделе мы покажем, что для произвольной булевой функции f от n переменных можно построить схему в базисе ACL, реализующую функцию f, сложности по порядку не больше $\sqrt{n \log_2 n}$.

Неформально опишем идею доказательства верхней оценки. Рассмотрим натуральное $k = \lfloor \sqrt{n \log_2 n} \rfloor$. Разобьем булев куб $\{0,1\}^n$ на аффинные подпространства (определение см., например, в [17]) с помощью специально заданных k линейных функций, обозначим их через $f_1, \ldots, f_k$. Разбиение будет устроено так, что каждое из этих подпространств не содержит цепей длины больше k. Вычислим систему функций $f_1, \ldots, f_k$, используя k элементов, реализующих линейные функции. Вычислим также отрицания этих функций, используя k элементов отрицания.

Далее, каждое из подпространств, заданных системой функций $f_1, \ldots, f_k$, разобьем на k не пересекающихся антицепей (это можно сделать по теореме 5.6).

Зададим k различных антицепных функций, в определенном смысле соответствующих этому разбиению, а именно так, что для фиксированного подпространства каждая из этих функций будет характеристической функцией одной из антицепей, на которые разбито пространство.

Обозначим набор $(f_1(\boldsymbol{x}), \ldots, f_k(\boldsymbol{x}), \overline{f_1}(\boldsymbol{x}), \ldots, \overline{f_k}(\boldsymbol{x}))$, где $\boldsymbol{x} \in \{0,1\}^n$, через $L(\boldsymbol{x})$. Если рассмотреть любые два набора $\boldsymbol{x}$, $\boldsymbol{y}$ из различных подпространств, то, во-первых, соответствующие наборы $L(\boldsymbol{x})$, $L(\boldsymbol{y})$ будут несравнимы, а во-вторых, каждый из этих наборов задает подпространство. Поэтому, используя значения вычисленных линейных функций $f_1, \ldots, f_k$ и их отрицаний, можно задать антицепные функции таким образом, чтобы одна антицепная функция отвечала антицепям из разных подпространств. Для этого будем строить указанные антицепные функции от $2k + n$ переменных: на первые k входов элемента, которому приписана соответствующая антицепная функция, будем пода-

вать выходы элементов, которым приписаны функции $f_1, \ldots, f_k$, на следующие k входов — их отрицания, а на оставшиеся n входов — входы схемы.

Наконец, с помощью еще одного антицепного элемента «соберем» окончательную схему, реализующую функцию f. Таким образом получим схему сложности не больше $3k + 1$, что при указанном k дает верхнюю оценку из теоремы 5.2.

Перейдем непосредственно к доказательству теоремы 5.2.

Доказательство. Рассмотрим натуральное $k = \lfloor \sqrt{n \log_2 n} \rfloor$ и рассмотрим k линейных функций от n переменных $x_1, \ldots, x_n$. Занумеруем эти линейные функции произвольным образом, обозначив их через $f_1, \ldots, f_k$ (для всякого $i \in [k]$ $f_i(x_1, \ldots, x_n) = l_n(x_1, \ldots, x_n) = x_1 + \ldots + x_n \pmod 2$).

Функции $f_1, \ldots, f_k$ разбивают куб $\{0,1\}^n$ на не более чем 2^k аффинных подпространств. Действительно, рассмотрим систему k уравнений:

$$\begin{cases} f_1(\boldsymbol{x}) = a_1 \\ \ldots \\ f_k(\boldsymbol{x}) = a_k, \end{cases} \tag{5.7}$$

где $\boldsymbol{x} \in \{0,1\}^n$, $a_i \in \{0,1\}$. Всякий набор $\boldsymbol{x}$ принадлежит аффинному подпространству, задаваемому соответствующим набором:

$$(a_1, \ldots, a_k) = (f_1(\boldsymbol{x}), \ldots, f_k(\boldsymbol{x}))\,.$$

Упорядочим наборы $(a_1, \ldots, a_k)$ по возрастанию (имеется в виду естественный лексикографический порядок при $0 \leqslant 1$) и занумеруем аффинные подпространства порядковыми номерами соответствующих наборов $(a_1, \ldots, a_k)$ С учетом этой нумерации обозначим указанные аффинные подпространства через $L_0, \ldots, L_{2^k-1}$.

Для всякого $i \in [k]$ обозначим через R_i, где $R_i \subseteq [n]$, непустое подмножество номеров существенных переменных функции l_i.

Предположим, что существует цепь, состоящая из $k+1$ различного двоичного набора n-мерного куба: $\boldsymbol{x}_0, \ldots, \boldsymbol{x}_k$, где $\boldsymbol{x}_0 \leqslant \ldots \leqslant \boldsymbol{x}_k$, и существует номер $t \in \{0, 1, \ldots, 2^k - 1\}$, такой что все эти наборы принадлежат одному аффинному подпространству L_t. Обозначим эту цепь через $\widetilde{X}$. Выведем необходимое условие того, что какое-либо аффинное подпространство содержит цепь длины больше k.

Для всякого $j \in [k]$ набор $\boldsymbol{x}_{j-1}$ цепи $\widetilde{X}$ отличается от набора $\boldsymbol{x}_j$ значениями некоторых компонент, которые в первом наборе равны 0, а во втором наборе равны 1. Обозначим через B_j подмножества номеров тех переменных, которые в наборе $\boldsymbol{x}_{j-1}$ равны 0, а в наборе $\boldsymbol{x}_j$ равны 1. Ясно, что так заданные множества B_j образуют непересекающиеся подмножества $[n]$.

Цепь $\widetilde{X}$ целиком содержится в аффинном пространстве L_t, следовательно, на каждом наборе этой цепи все уравнения системы (5.7) выдают один и тот же результат, а именно:

$$\begin{cases} l_1(\boldsymbol{x}_0) = l_1(\boldsymbol{x}_1) = \ldots = l_1(\boldsymbol{x}_k) = a_1 \\ \ldots \\ f_i(\boldsymbol{x}_0) = f_i(\boldsymbol{x}_1) = \ldots = f_i(\boldsymbol{x}_k) = a_i \\ \ldots \\ f_k(\boldsymbol{x}_0) = f_k(\boldsymbol{x}_1) = \ldots = f_k(\boldsymbol{x}_k) = a_k, \end{cases} \tag{5.8}$$

где набор $(a_1, \ldots, a_k)$ из правой части системы (5.8) соответствует числу t.

Для произвольных i, j рассмотрим равенство: $f_i(\boldsymbol{x}_{j-1}) = f_i(\boldsymbol{x}_j)$. Напомним, что B_j — это номера переменных, имеющих различные значения в наборах $\boldsymbol{x}_{j-1}$ к $\boldsymbol{x}_j$. Из указанного равенства следует, что количество переменных с номерами из множества B_j, от которых зависит линейная функция f_i — четно. Из системы (5.8) вытекает, что для любых i, j мощность пересечения $|B_j \cap R_i|$ — четна. Это и есть искомое необходимое условие.

Таким образом, для того чтобы k линейных функций разбивали пространство двоичных наборов длины n на 2^k аффинных подпространств так, чтобы ни

одно из них не содержало цепи длиннее k, необходимо, чтобы описанное условие не выполнялось. Ясно, что для этого достаточно взять число k, удовлетворяющее лемме 5.1.

Вернемся к основному рассуждению. По лемме 5.1, для $k = \lfloor \sqrt{n \log_2 n} \rfloor$ существует k непустых подмножеств множества $[n]$ с определенными свойствами; обозначим их через $R_1^*, \ldots, R_k^*$. Рассмотрим k различных линейных функций $f_1^*, \ldots, f_k^*$ от n переменных $x_1, \ldots, x_n$, таких что для всякого $i \in [k]$ функция f_i^* существенно зависит от всех переменных с номерами из подмножества $R_i^* \subseteq n$. Будем строить схему S, реализующую функцию f, следующим образом.

Считаем, что входам схемы S приписаны переменные $x_1, \ldots, x_n$. Рассмотрим элементы, реализующие функции $f_1^*, \ldots, f_k^*$, обозначим их через $e_1, \ldots, e_k$. Для всякого i подадим на входы элемента e_i переменные с номерами из множества R_i^*. Тем самым вычислим систему функций $f_1^*, \ldots, f_k^*$. Реализуем также отрицания функций $f_1^*, \ldots, f_k^*$, подав выходы элементов $e_1, \ldots, e_k$ на входы элементов $e_{k+1}, \ldots, e_{2k}$, реализующих отрицание.

Всякий двоичный набор $\boldsymbol{x} \in \{0,1\}^n$ лежит в одном из аффинных подпространств $L_0, \ldots, L_{2^k-1}$, на которые функции $f_1^*, \ldots, f_k^*$ разбивают пространство всех двоичных наборов длины n. На всяком наборе из фиксированного подпространства для любого i функция f_i^* принимает одно и то же значение.

Выберем произвольное подпространство L_t, где t определяется двоичным набором $(a_1, \ldots, a_k)$ из правой части системы (5.7). Рассмотрим L_t как частично упорядоченное множество (с обычным линейным порядком для сравнимых наборов).

Согласно выведенному выше необходимому условию, множество L_t не содержит цепи, состоящей из более чем k наборов. По теореме 5.6, множество L_t может быть разбито на k антицепей (некоторые из них могут быть пустыми). Обозначим антицепи, на которые разбивается множество L_t, через $A_1^t, \ldots, A_k^t$. Так, для всякого $t \in \{0, 1, \ldots, 2^k - 1\}$ имеем: $L_t = \bigsqcup_{i=1}^{k} A_i^t$.

Для всякого $j \in [k]$ определим антицепные функции h_j от $2k+n$ переменных $z_1, \ldots, z_k, y_1, \ldots, y_k, x_1, \ldots, x_n$ следующим образом.

Рассмотрим произвольный набор $(\gamma_1, \ldots, \gamma_k, \beta_1, \ldots, \beta_k, \boldsymbol{\alpha}) \in \{0,1\}^{2k+n}$. Существует единственный номер $t \in \{0, 1, \ldots, 2^k - 1\}$, такой что $\boldsymbol{\alpha} \in L_t$. Положим функцию h_j равной 1 на наборе $(\gamma_1, \ldots, \gamma_k, \beta_1, \ldots, \beta_k, \boldsymbol{\alpha})$ тогда и только тогда, когда одновременно выполнено:

$$\begin{cases} \boldsymbol{\alpha} \in A_j^t, \text{ где } (\gamma_1, \ldots, \gamma_k) \text{ — двоичная запись } t, \\ \text{для всех } i \in [k] : \ \beta_i = \overline{\gamma}_i, \\ f(\boldsymbol{\alpha}) = 1. \end{cases} \tag{5.9}$$

Во всех остальных случаях положим функцию h_j равной 0. Ясно, что так заданная функция h_j является антицепной. Антицепные элементы, реализующие функции $h_1, \ldots, h_k$, обозначим соответственно через $e_{2k+1}, \ldots, e_{3k}$.

Продолжим построение схемы S. На первые $2k$ входов элементов $e_{2k+1}, \ldots, e_{3k}$ подадим выходы элементов $e_1, \ldots, e_k$ (они реализуют функции $f_1^*, \ldots, f_k^*$) и выходы элементов $e_{k+1}, \ldots, e_{2k}$ (они реализуют функции $\overline{f}_1^*, \ldots, \overline{f}_k^*$), а на оставшиеся n входов — входы схемы $x_1, \ldots, x_n$.

Для всякого $j \in [k]$ обозначим функцию, которая реализуется на выходе элемента e_{2k+j} через H_j. Для произвольного набора $\boldsymbol{\alpha} \in \{0,1\}^n$ имеем:

$$H_j(\boldsymbol{\alpha}) = h_j\left(f_1^*(\boldsymbol{\alpha}), \ldots, f_k^*(\boldsymbol{\alpha}), \overline{f}_1^*(\boldsymbol{\alpha}), \ldots, \overline{f}_k^*(\boldsymbol{\alpha}), \boldsymbol{\alpha}\right).$$

Зададим функцию g от k переменных следующим образом: $g(v_1, \ldots, v_k)$ равна 1 лишь на таких двоичных наборах $(v_1, \ldots, v_k)$, в которых есть ровно одна единица. Ясно, что функция g является антицепной. Обозначим через e антицепной элемент, реализующий функцию g.

Нетрудно видеть, что для всякого набора $\boldsymbol{\alpha} \in \{0,1\}^n$

$$g(H_1(\boldsymbol{\alpha}), \ldots, H_k(\boldsymbol{\alpha})) = f(\boldsymbol{\alpha}). \tag{5.10}$$

Достроим схему S, согласно формуле (5.10): подадим на входы элемента e выходы элементов $e_{2k+1}, \ldots, e_{3k}$.

Таким образом, мы получили схему S, реализующую функцию f, причем $L_{ACL}(S) \leqslant 3k + 1 = O(\sqrt{n \log_2 n})$. Тем самым теорема 5.2 доказана. ■

5.4 Доказательство теоремы 5.3

В этом разделе мы докажем теорему 5.3 о нижней оценке сложности функции голосования в базисе ACL. Доказательство, изложенное ниже, является в некотором смысле развитием доказательства леммы 4.1 о нижней оценке сложности произвольной симметрической функции, приведенного в главе 4. Для полноты изложения и удобства чтения доказательство в данной главе приведено полностью, без отсылок к главе 4.

Некоторые определения

Напомним определение из главы 1. Пусть среди переменных $x_1, \ldots, x_n$ выделены t переменных. Зафиксируем произвольным образом значения этих t переменных, а остальным переменным будем присваивать произвольные значения. Полученное множество наборов называется *подкубом* булева куба $\{0,1\}^n$ размерности $n - t$.

Пусть среди переменных $x_1, \ldots, x_n$ выделены k непустых попарно не пересекающихся подмножеств. Зафиксируем произвольным образом значения всех переменных, не входящих ни в одно из этих подмножеств. Переменным из указанных подмножеств будем присваивать произвольные значения так, чтобы значения переменных внутри каждого подмножества были одинаковыми. Полученное множество наборов будем называть *обобщенным подкубом* размерности k булева куба $\{0,1\}^n$. Обобщенный подкуб размерности k состоит из 2^k наборов.

Напомним также, что согласно определениям из главы 1, *верхним* набором двоичного куба $\{0,1\}^n$ (его подкуба) называется максимальный набор, а *нижс-*

ним — минимальный. Для куба $\{0,1\}^n$ верхний набор состоит из единиц, будем обозначать его через $\mathbf{1}$, а нижний, состоящий из нулей, — через $\mathbf{0}$.

Начало основного рассуждения

Перейдем непосредственно к доказательству теоремы 5.3. Доказательство будем вести для приведенной схемы с произвольно фиксированной правильной нумерацией элементов (определения см. в главе 1).

Доказательство. Для функции голосования от n переменных докажем, что сложность произвольной схемы в базисе ACL, реализующей эту функцию, не меньше $\frac{1}{4} \cdot \left\lfloor \frac{1}{4}\sqrt{n \log_2 n} \right\rfloor$. Рассуждение будет построено методом «от противного».

Рассмотрим произвольную схему S, реализующую функцию голосования m_n. Пусть входам схемы приписаны символы переменных $x_1, x_2, \ldots, x_n$, (согласно обозначениям из главы 1, будем называть их входными переменными схемы). Обозначим сложность схемы S через s, а элементы схемы — через $e_1, \ldots, e_s$ (напомним, что введена правильная нумерация элементов).

Предположим, что $s < \frac{1}{4} \cdot \left\lfloor \frac{1}{4}\sqrt{n \log_2 n} \right\rfloor$. Обозначим количество элементов, которым приписаны линейные функции через p, а сами приписанные этим элементам функции соответственно через $l_1, \ldots, l_p$, где $p \leqslant s$. Для всякого $i \in [p]$ обозначим через R_i множество номеров входных переменных, подаваемых непосредственно на входы элемента, которому приписана линейная функция l_i.

В лемме 5.2 возьмем $k = \left\lfloor \frac{1}{4}\sqrt{n \log_2 n} \right\rfloor$. Рассмотрим семейство множеств $R_1, \ldots, R_k$, где $R_1, \ldots, R_p$ — указанные выше множества, а для всякого $i > p$ множество R_i — это произвольно выбранное фиксированное непустое подмножество $[n]$. По лемме 5.2, существует семейство непустых попарно не пересекающихся подмножеств $B_1, \ldots, B_k \subseteq [n]$ с описанными в лемме свойствами. Будем называть множества $B_1, \ldots, B_k$ *блоками*.

Введем натуральный *параметр* $a \leqslant \frac{n}{2}$. Значение параметра a будет определено в конце доказательства (в разделе 5.4), для текущего рассуждения можем считать, что оно произвольно и фиксировано.

В блоки $B_1, \ldots, B_k$ входят номера входных переменных, образующие непересекающиеся множества. Зафиксируем значения входных переменных с номерами вне блоков $B_1, \ldots, B_k$ следующим образом: произвольно выберем a из этих переменных и положим их равными 1, а остальные — равными 0. Для каждого блока B_i заменим все входные переменные с номерами из этого блока на y_i. Получим новые переменные $y_1, \ldots, y_k$. Обозначим через Γ всевозможные наборы куба $\{0,1\}^n$, которые получаются при подстановке произвольных значений переменных $y_1, \ldots, y_k$. Отметим, что Γ является обобщенным подкубом булева куба $\{0,1\}^n$.

Мы получили взаимно однозначное отображение куба $\{0,1\}^k$ на обобщенный подкуб $\Gamma \subseteq \{0,1\}^n$: всякому набору из множества Γ ставится в соответствие такой набор $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_k) \in \{0,1\}^k$, что для любого $i \in [k]$ α_i равно значению компонент набора из Γ с номерами из блока B_i. Через $\gamma(\boldsymbol{\alpha})$ будем обозначать набор множества Γ, соответствующий набору $\boldsymbol{\alpha} \in \{0,1\}^k$, и будем называть $\gamma(\boldsymbol{\alpha})$ γ-*образом* соответствующего набора.

Отметим, что построенное отображение γ сохраняет свойство сравнимости: если какие-то два набора $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \{0,1\}^k$ сравнимы ($\boldsymbol{\alpha} < \boldsymbol{\beta}$), то и наборы $\gamma(\boldsymbol{\alpha}), \gamma(\boldsymbol{\beta})$ сравнимы ($\gamma(\boldsymbol{\alpha}) < \gamma(\boldsymbol{\beta})$).

Определим взаимно-однозначное отображение $\hat{\gamma}$ подмножеств множества $[k]$ на подмножества множества $[n]$. Если подмножество $A \subseteq [k]$ задано своим характеристическим вектором $\boldsymbol{\chi}_A \in \{0,1\}^k$, то его $\hat{\gamma}$-образ — это подмножество множества $[n]$, которое задается характеристическим вектором $\gamma(\boldsymbol{\chi}_A) \in \Gamma$. Будем обозначать $\hat{\gamma}$-образ множества A через $\hat{\gamma}(A)$.

Далее мы будем строить цепь C в кубе $\{0,1\}^k$, состоящую из $k+1$ различного набора. Забегая вперед скажем, что нас будет интересовать множество

γ-образов ее наборов, которое представляет собой цепь в исходном кубе $\{0,1\}^n$. Будем обозначать эту цепь через $\Gamma(C)$.

Построение цепи

Начнем построение цепи C в кубе $\{0,1\}^k$. В качестве крайних наборов цепи C возьмем верхний и нижний наборы этого куба: $\mathbf{0}, \mathbf{1} \in \{0,1\}^k$. Оставшаяся часть раздела посвящена построению промежуточных наборов этой цепи.

Говоря неформально, промежуточные наборы цепи мы будем получать, двигаясь по кубу с двух сторон: спускаясь от текущего верхнего набора или поднимаясь от текущего нижнего. «Спуск» от текущего верхнего набора осуществляется так: по определенному алгоритму в этом наборе выбирается одна из единичных компонент, значение которой изменяется на 0. Значение переменной, соответствующей выбранной компоненте, далее считается зафиксированным значением 0 и более не изменяется. При фиксировании значения переменной происходит переход к подкубу размерности на единицу меньше. Его верхний набор становится текущими верхним набором. Этот набор добавляется в цепь.

Аналогично осуществляется «подъем» от текущего нижнего набора: значение определенной нулевой компоненты текущего нижнего набора изменяется на 1, и тем самым, получается очередной набор цепи; соответствующая входная переменная при этом фиксируется значением 1 и далее не изменяется.

Отметим, что фиксирование одной переменной в кубе размерности k соответствует фиксированию группы входных переменных исходного куба размерности n, при этом в исходном кубе происходит переход к соответствующему обобщенному подкубу.

Вернемся к подробному описанию процесса построения цепи. Чтобы построить цепь, будем рассматривать элементы схемы S в порядке заданной правильной нумерации, начиная с элемента e_1. Процесс построения характеризуется следующими параметрами.

- Номер шага $i \in [s]$; он определяется номером элемента схемы, с которого начинается данный шаг.

- Одновременно с цепью на каждом шаге строятся два множества: F_i, $T_i \subseteq [k]$. Множество F_i (или T_i) — это множество номеров переменных среди $y_1, \ldots, y_k$, которые после завершения i-го шага зафиксированы нулями (единицами соответственно). Отметим, что построение множества $F_i \subseteq [k]$ (или T_i) соответствует построению множества $\hat{\gamma}(F_i) \subseteq [n]$ (или $\hat{\gamma}(T_i)$ соответственно), состоящего из номеров входных переменных схемы, значения которых после i-го шага зафиксированы нулями (единицами).

  Входную переменную схемы будем называть *свободной относительно множества* A, где $A \subseteq [k]$, если номер этой переменной принадлежит множеству $\hat{\gamma}([k] \setminus A) \subseteq [n]$, то есть значение этой входной переменной еще не зафиксировано.

  В процессе построения цепи мы будем рассматривать свободные переменные относительно множеств вида $F_i \cup T_i$: неформально, это те переменные, значения которых в текущий момент еще не зафиксированы значениями 0 или 1. Как правило, говоря о свободных переменных, мы не будем явно указывать, относительно какого множества они рассматриваются, поскольку это будет ясно из контекста.

  Входы схемы будем называть *свободными относительно множества* A, где $A \subseteq [k]$, если этим входам приписаны переменные, свободные относительно множества A.

  Напомним, что для любого подмножества $P \subseteq [k]$ через $\boldsymbol{y}^P$ мы обозначаем такой двоичный набор $\boldsymbol{y} = (y_1, \ldots, y_k)$, что для любого номера $p \in [k]$ $y_p = 1$ тогда и только тогда, когда $p \in P$.

На i-м шаге рассматривается подкуб с текущими верхним и нижним наборами $\boldsymbol{y}^{[k]\setminus F_{i-1}}$ и $\boldsymbol{y}^{T_{i-1}}$ и строится новый подкуб — с текущим верхним и нижним наборами $\boldsymbol{y}^{[k]\setminus F_i}$ и $\boldsymbol{y}^{T_i}$.

- На каждом шаге строится множество E_i — это множество элементов схемы из $\{e_1, \ldots, e_i\}$, таких что
  - на их входы подаются только выходы элементов с меньшими номерами и входы схемы, соответствующие входным переменным с номерами из множества $\hat{\gamma}(F_i \cup T_i)$, или
  - этим элементам приписаны линейные функции из множества $\{l_1, \ldots, l_k\}$.

  Для каждого i имеем: $E_i \subseteq \{e_1, \ldots, e_i\}$. Элемент схемы помещается в множество E_i на i-м шаге, если его входы не присоединены ко входам схемы, свободным относительно множества $F_i \cup T_i$.

Отметим, что с ростом i множества F_i, T_i и E_i не уменьшаются. В начале построения полагаем $i = 0$, $F_0 = T_0 = \emptyset$, $E_0 = \emptyset$ и, как уже было сказано, цепь $C = \{\mathbf{0}, \mathbf{1}\}$.

Определим основное понятие, на котором основано рассуждение (здесь и далее, как обычно, через h_i обозначается функция, которая реализуется на выходе элемента e_i).

Определение 5.1. *Пусть задано множество элементов $E \subseteq \{e_1, \ldots, e_s\}$. Подадим на входы схемы S произвольный набор $\gamma(\boldsymbol{\alpha}) \in \Gamma$. Пусть $e_{r_1}, \ldots, e_{r_l}$ — это все такие элементы схемы, что для всякого $j \in [l]$ выполнено:*

1) $h_{r_j}(\gamma(\boldsymbol{\alpha})) = 1$;

2) $e_{r_j} \in \{e_1, \ldots, e_s\} \setminus E$.

Элемент e_m, обладающий минимальным номером среди элементов $e_{r_1} \dots, e_{r_l}$, называется первым ненулевым элементом на наборе $\gamma(\boldsymbol{\alpha})$ относительно множества E.

Иногда, говоря о первом ненулевом элементе на некотором наборе, мы не будем указывать явно, относительно какого множества он рассматривается, так как это будет понятно из контекста.

Будем строить цепь таким образом, чтобы для любого i после i-го шага были выполнены следующие **свойства**.

1. Для всех $t, q \leqslant i$: $F_t \cap T_q = \emptyset$ (т. е. нельзя зафиксировать переменную, например, единицей, а позже — нулем; неформально об этом свойстве говорилось ранее).

2. Значения любого элемента $e_j \in E_i$ одинаковы на всех γ-образах наборов цепи, на которых элементы e_t, где $t < j$, $e_t \notin E_i$ выдают 0.

3. Для всякого элемента $e_j \in \{e_1, \dots, e_i\} \setminus E_i$ и для функции h_j, которая вычисляется на выходе элемента e_j, выполнено равенство:

$$h_j(\gamma(\boldsymbol{y}^{[k]\setminus F_i})) = h_j(\gamma(\boldsymbol{y}^{T_i})) = 0.$$

   Свойство 3 — ключевое в процессе построения цепи. Неформально говоря, оно означает, что после i-го шага при подаче на входы схемы γ-образов верхнего и нижнего наборов текущего подкуба все элементы вплоть до i-го, кроме элементов из множества E_i, выдают на этих наборах 0.

Процедура построения цепи разбивается на два этапа.

Этап I. На этапе будет s шагов по числу элементов схемы. Предположим, было совершено i шагов, опишем $(i+1)$-й шаг.

Мы совершили i шагов, это означает, что рассмотрены первые i элементов схемы $e_1, e_2, \dots, e_i$ и построено некоторое множество F_i, такое что $\hat{\gamma}(F_i)$ содержит номера входных переменных схемы, зафиксированных значением 0. Также

построено множество T_i, такое что $\hat{\gamma}(T_i)$ содержит номера входных переменных схемы, зафиксированных значением 1. Цепь C к началу $i+1$ шага содержит наборы $\mathbf{0}, \mathbf{1} \in \{0,1\}^k$, а также наборы, которые получаются одновременно с построением множеств F_i и T_i. Построено множество элементов E_i. Рассматривается подкуб размерности $k - |F_i| - |T_i|$ с текущими верхним и нижним наборами $\boldsymbol{y}^{[k]\setminus F_i}$ и $\boldsymbol{y}^{T_i}$ соответственно.

Итак, начиная $(i+1)$-й шаг, переходим к элементу e_{i+1}. Возможны следующие случаи (отметим, что они не могут реализоваться одновременно).

1. Пусть на входы элемента e_{i+1} не подаются непосредственно входы схемы, свободные относительно множества $F_i \cup T_i$, или элементу e_{i+1} приписана одна из линейных функций $l_1, \ldots, l_k$. Тогда полагаем $E_{i+1} = E_i \cup \{e_{i+1}\}$, $F_{i+1} = F_i$, $T_{i+1} = T_i$. На этом $(i+1)$-й шаг закончен.

   Лемма 5.3. *Свойство 2 для элемента e_{i+1} выполнено.*

   Доказательство. 1. Пусть на входы элемента e_{i+1} не подаются входы схемы, свободные относительно множества $F_{i+1} \cup T_{i+1}$. Тогда рассмотрим γ-образы наборов цепи, на которых элементы e_j, $j < i+1$, $e_j \notin E_{i+1}$, выдают 0. На этих γ-образах все элементы e_j, $j < i+1$, $e_j \in E_{i+1}$ выдают одно и то же значение, поскольку для них свойство 2 выполнено по построению. Значит, элемент e_{i+1} на всех указанных γ-образах выдает одно и то же значение, то есть свойство 2 выполнено.

2. Пусть элементу e_{i+1} приписана линейная функция $l_{i+1} \in \{l_1, \ldots, l_k\}$. Значения этого элемента определяются значениями элементов e_j, где $j < i+1$, $e_j \notin E_{i+1}$ и значениями на входах схемы с номерами из множества R_{i+1}, где R_{i+1} — подмножество номеров входных переменных, подаваемых непосредственно на входы элемента e_{i+1}.

   Рассмотрим два набора $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \{0,1\}^k$, содержащиеся в построенной части цепи C, такие что элементы e_j, где $j < i+1$, $e_j \notin E_{i+1}$, на $\gamma(\boldsymbol{\alpha})$

и $\gamma(\boldsymbol{\beta})$ выдают 0. Как уже было сказано, наборы цепи мы получаем одновременно с построением множеств F_{i+1} и T_{i+1} шаг за шагом: взяв текущий верхний или нижний наборы куба $\{0,1\}^k$, на первом шаге мы по некоторому правилу выбираем не более одной переменной и фиксируем ее значение нулем или единицей, тем самым получаем новый набор цепи. Номер зафиксированной переменной помещаем в множество $\gamma(F_1)$ или $\gamma(T_1)$ соответственно. Аналогично, на втором шаге получаются множества F_2 и T_2 и так далее.

Напомним, что любой переменной в рассматриваемом кубе размерности k соответствует группа отождествленных переменных исходного куба размерности n. Группы переменных заданы блоками номеров этих переменных — $B_1, \ldots, B_k \subseteq [n]$. Эти подмножества выбраны так, что они удовлетворяют лемме 5.2, то есть $B_1, \ldots, B_k$ попарно не пересекаются и всякое подмножество B_j пересекается с подмножеством R_{i+1} по множеству четной мощности. Значит, γ-образы любых двух наборов цепи C отличаются друг от друга значением компонент, таких что пересечение множества их номеров с множеством R_{i+1} четно. В частности, это верно для наборов $\gamma(\boldsymbol{\alpha})$ и $\gamma(\boldsymbol{\beta})$. Учитывая, что элементу e_{i+1} приписана линейная функция и при отождествлении переменных линейность сохраняется, получаем, что значение элемента e_{i+1} одинаково на наборах $\gamma(\boldsymbol{\alpha})$ и $\gamma(\boldsymbol{\beta})$.

■

Продолжим разбор случаев.

2. Пусть на какой-либо вход элемента e_{i+1} непосредственно подается хотя бы один из входов схемы, свободный относительно множества $F_i \cup T_i$ и элементу e_{i+1} не приписана ни одна из линейных функций $l_1, \ldots, l_p$. Пусть

указанному входу приписана некоторая переменная y_m, где $m \in [k] \setminus (F_i \cup T_i)$.

Проверим, выполнено ли свойство 3 для элемента e_{i+1}: $h_{i+1}(\gamma(\boldsymbol{y}^{[k]\setminus F_i})) = h_{i+1}(\gamma(\boldsymbol{y}^{T_i})) = 0$.

2.1. Если свойство 3 выполнено, то полагаем $E_{i+1} = E_i$, $F_{i+1} = F_i$, $T_{i+1} = T_i$, и $(i+1)$-й шаг закончен.

2.2. Пусть свойство 3 для e_{i+1} не выполнено для γ-образа текущего верхнего набора подкуба: $h_{i+1}(\gamma(\boldsymbol{y}^{[k]\setminus F_i})) = 1$ (случай нижнего набора будет разобран позже). Для удобства разобьем изложение этого случая на два подэтапа.

2.2.1. Вначале мы работаем с элементом e_{i+1}. Из условия случая 2.2 следует, что элемент e_{i+1} является первым ненулевым на наборе $\gamma(\boldsymbol{y}^{[k]\setminus F_i})$ относительно множества E_i. Зафиксируем значение указанной выше переменной y_m нулем.

Будем использовать вспомогательные обозначения: F^r_{i+1}, E^r_{i+1} и, в дальнейшем, T^r_{i+1}, где r — натуральный параметр.

Для $r = 1$ полагаем $F^1_{i+1} = F_i \cup \{m\}$; также полагаем $T_{i+1} = T_i$. Тем самым, мы переходим к подкубу размерности на единицу меньше (а именно, размерности $k - |F^1_{i+1}| - |T_{i+1}|$). Добавляем в цепь C верхний набор этого подкуба — $\boldsymbol{y}^{[k]\setminus F^1_{i+1}}$. Положим множество E^1_{i+1} равным объединению множества E_i и множества всех элементов e_j, где $j \leqslant i+1$, на входы которых после фиксирования переменной y_m более не подаются непосредственно входы схемы, свободные относительно множества $F^1_{i+1} \cup T_{i+1}$.

2.2.2. Далее мы работаем с элементами e_j, где $j \leqslant i+1$. Вначале проведем рассуждение, по-прежнему считая значение r равным 1.

Рассмотрим элементы e_j, где $j \leqslant i+1$ и $e_j \notin E^r_{i+1}$, и проверим, выполнено ли для них свойство 3 на наборе $\gamma(\boldsymbol{y}^{[k]\setminus F^r_{i+1}})$. Пусть на-

шлись элементы, для которых свойство 3 не выполнено, и пусть e_t — элемент с минимальным номером среди них. Справедливо следующее утверждение.

Лемма 5.4. *Хотя бы на один из входов указанного элемента e_t подается непосредственно какой-либо вход схемы, свободный относительно множества $F^r_{i+1} \cup T_{i+1}$.*

Доказательство. Для функции h_t, которая реализуется на выходе элемента e_t, имеем: $h_t(\gamma(\boldsymbol{y}^{[k]\setminus F^r_{i+1}})) = 1$, $h_t(\gamma(\boldsymbol{y}^{T_{i+1}})) = 0$. Значение антицепной функции g_t, соответствующей элементу e_t, определяется значениями на некоторых входах схемы, а также значениями на выходах элементов двух типов:

1) таких элементов e_u, что $e_u \notin E^r_{i+1}$, где $u < t$,

2) таких элементов e_u, что $e_u \in E^r_{i+1}$, где $u < t$.

Значения на выходах элементов 2-го типа определяются значениями на выходах элементов 1-го типа. В силу минимальности t, все элементы e_j 1-го типа на γ-образах текущего верхнего и нижнего наборов подкуба выдают 0. Следовательно, значения на выходах элементов 2-го типа на указанных двух наборах одинаковы. Получаем, что функция g_t выдает различные значения на некоторой паре наборов со следующим свойством: в этих наборах компоненты, соответствующие значениям на выходах элементов с меньшими номерами, совпадают. Следовательно, значения каких-то из оставшихся компонент в этих наборах должны различаться. Таким образом, хотя бы один из входов схемы, свободный относительно множества $F^r_{i+1} \cup T_{i+1}$, подается непосредственно на один из входов элемента e_t. Лемма 5.4 доказана. ■

Продолжим основное рассуждение. По лемме 5.4 получаем, что элемент e_t является первым ненулевым элементом на наборе

$\gamma(\boldsymbol{y}^{[k]\setminus F^r_{i+1}})$ относительно множества E^r_{i+1}. Рассмотрим произвольный вход схемы, свободный относительно множества $F^r_{i+1} \cup T_{i+1}$, который подается непосредственно на некоторый вход элемента e_t. Зафиксируем переменную, которая приписана этому входу схемы, значением 0. Тем самым, мы добавим номер соответствующей переменной в множество F^r_{i+1} (отметим, что это соответствует добавлению группы входных переменных в множество $\hat{\gamma}(F^r_{i+1})$). Обозначим полученное множество через F^{r+1}_{i+1}. Мы вновь перешли к подкубу размерности на единицу меньше (в терминах исходного куба $\{0,1\}^n$ — мы перешли к обобщенному подкубу). Верхний набор этого подкуба $\boldsymbol{y}^{[k]\setminus F^{r+1}_{i+1}}$ добавляем в цепь C.

Полагаем множество E^{r+1}_{i+1} равным объединению множества E^r_{i+1} и множества всех элементов e_j, где $j \leqslant i+1$, на входы которых после фиксирования указанной выше переменной более не подаются непосредственно входы схемы, свободные относительно множества $F^{r+1}_{i+1} \cup T_{i+1}$.

Далее мы действуем по циклу: вновь выполняем процесс, описанный в п. 2.2.2, для всех $r = 2, \ldots, q$, где q — это такое значение параметра r, при котором свойство 3 будет выполнено для всех элементов e_j, где $j \in [i+1]$ и $e_j \notin E^q_{i+1}$.

Докажем лемму, которая гарантирует выполнение свойства 2.

Лемма 5.5. *Любой элемент e_v, где $v \in [i+1]$, добавленный в множество E^r_{i+1}, где $r \leqslant q$, в рамках описанного в пункте 2.2 процесса, будет выдавать 0 на всех γ-образах наборов подкуба размерности $k - |F^r_{i+1}| - |T_{i+1}|$, на которых элементы e_a, где $a < v$, $e_a \notin E^r_{i+1}$, выдают 0.*

Доказательство. Аналогично доказательству случая 1 в лемме 5.3, на входы элемента e_v не подаются входы схемы, свободные относительно множества $F^r_{i+1} \cup T_{i+1}$, значит, на всех указанных в условии леммы 5.5 наборах этот элемент выдает одно и то же значение. На γ-образе нижнего набора подкуба он выдает 0 (т. к. $T_{i+1} = T_i$). Следовательно, на всех описанных наборах подкуба он также выдает 0. ■

После того, как описанные действия выполнены, полагаем $F_{i+1} = F^q_{i+1}$, $E_{i+1} = E^q_{i+1}$, и $(i+1)$-й шаг закончен.

Рассмотрим оставшийся случай.

2.3. Пусть свойство 3 для e_{i+1} не выполнено на γ-образе нижнего набора подкуба: $h_{i+1}(\gamma(\boldsymbol{y}^{T_i})) = 1$.

Лемма 5.6. *Случаи 2.2 и 2.3 не могут произойти одновременно.*

Доказательство. Предположим противное. При этом имеем: для всех $e_j \notin E_i$, где $j < i+1$, функции h_j на наборах $\gamma(\boldsymbol{y}^{[k]\setminus F_i})$ и $\gamma(\boldsymbol{y}^{T_i})$ выдают 0; для всех $e_j \in E_i$, где $j < i+1$, функции h_j на этих наборах выдают одно и то же значение. Наборы $\gamma(\boldsymbol{y}^{[k]\setminus F_i})$ и $\gamma(\boldsymbol{y}^{T_i})$ сравнимы, и, по условию случая 2.2, один из входов элемента e_{i+1} присоединен ко входу схемы, на котором на этих наборах будут различные значения. Значит, антицепная функция g_{i+1}, приписанная элементу e_{i+1}, выдает 1 на некоторой паре сравнимых наборов, отличающихся по крайней мере в одной компоненте. Получаем противоречие с тем, что g_{i+1} — антицепная функция. Лемма 5.6 доказана. ■

Итак, вернемся к случаю 2.3: он двойственен случаю 2.2, и мы действуем аналогично, с той лишь разницей, что входные переменные фиксируются значением 1. Итак, вначале зафиксируем указанную в пункте 2 переменную y_m единицей, и положим $T^1_{i+1} = T_i \cup \{m\}$ (следуя

обозначениям, введенным в 2.2). Положим $F_{i+1} = F_i$. Таким образом, переходим к подкубу размерности $k-|F_{i+1}|-|T^1_{i+1}|$. Помещаем в цепь C набор $\boldsymbol{y}^{T^1_{i+1}}$. Далее, аналогично случаю 2.2, выполняем цикл, описанный в 2.2.2, получая, соответственно, множества $T^2_{i+1}, T^3_{i+1}, \ldots$ до тех пор, пока для некоторого v свойство 3 не будет выполнено для всех элементов e_j, где $j \leqslant i+1$ и $e_j \notin E^v_{i+1}$. После этого полагаем $T_{i+1} = T^v_{i+1}, E_{i+1} = E^v_{i+1}$, и $(i+1)$-й шаг закончен.

Если мы совершали шаги этапа I и зафиксировали значения всех переменных среди $y_1, \ldots, y_k$ (и соответственно, всех входных переменных схемы), то, таким образом, цепь, состоящая из $k+1$ набора, построена, и процесс заканчивается.

Пусть мы совершили s шагов, описанных в случаях 1 и 2 этапа I, т. е. рассмотрели последовательно все элементы схемы S, однако искомая цепь еще не построена. После s-го шага получены множества F_s, T_s и E_s — для краткости далее опустим индексы и будем писать F, T и E, соответственно.

Переходим к этапу II.

Этап II. Исходный куб размерности k сужен до подкуба размерности $k - |F| - |T|$ так, что все элементы схемы $e_1, \ldots, e_s$, кроме элементов из E, выдают 0 на γ-образах верхнего и нижнего наборов этого подкуба: $\gamma(\boldsymbol{y}^{[k]\setminus F})$ и $\gamma(\boldsymbol{y}^T)$. Положим $T^0 = T$. Будем добавлять в T^0 номера переменных из $[k] \setminus (F \cup T)$, получая множества T^1, T^2 и так далее, следующим образом: для любого $i \geqslant 0$,

1) если на наборе $\gamma(\boldsymbol{y}^{T^i})$ нет первого ненулевого элемента относительно множества E, то добавляем в множество T^i номер произвольной переменной из множества $[k] \setminus (F \cup T^i)$. Получаем множество T^{i+1} и набор $\boldsymbol{y}^{T^{i+1}}$, который помещаем в цепь;

2) если на наборе $\gamma(\boldsymbol{y}^{T^i})$ есть первый ненулевой элемент относительно множества E, то, аналогично доказательству леммы 5.4, нетрудно показать, что

какой-либо из входов этого элемента присоединен ко входу схемы, свободному относительно множества $[k] \setminus (F \cup T^i)$. Зафиксируем единицей входную переменную, которая соответствует этому входу. Получаем множество T^{i+1} и набор $\boldsymbol{y}^{T^{i+1}}$, который помещаем в цепь.

Если в рамках описанного процесса при добавлении номера какой-либо переменной в множество T^i входы некоторого элемента e_d более не присоединены ко входам схемы, свободным относительно множества $F \cup T^i$, то полагаем $E = E \cup \{e_d\}$. Нетрудно понять, что для всех таких элементов выполняется свойство, аналогичное свойству, доказанному в лемме 5.5: они выдают 0 на всех γ-образах наборов подкуба соответствующей размерности, на которых элементы с меньшими номерами, не лежащие в текущем множестве E, выдают 0. Отметим, что первый ненулевой элемент рассматривается всякий раз относительно текущего множества E.

Повторяем описанный процесс до тех пор, пока все входные переменные не будут зафиксированы, то есть, пока не будет построена искомая цепь C. Отметим, что на этапе 2 множество T выбрано для определенности: можно было выбрать множество F и, соответственно, фиксировать переменные значением 0.

При построении цепи C на входы схемы подаются только наборы $\gamma(\boldsymbol{y}^T)$ и $\gamma(\boldsymbol{y}^{[k]\setminus F})$(для краткости индексы опущены). Эти наборы сравнимы, так как на каждом шаге $T \subseteq [k] \setminus F$. Таким образом, построенное множество C действительно является цепью.

Завершение доказательства теоремы 5.3

Цепь C обладает следующим свойством.

Лемма 5.7. *Никакой элемент схемы S не был первым ненулевым элементом (относительно соответствующих множеств) на γ-образах двух различных наборов цепи C в процессе ее построения.*

Доказательство. Будем вести доказательство методом «от противного». Пусть, без ограничения общности, набор $\boldsymbol{y}^P$ добавлен в цепь на шаге с номером b, а $\boldsymbol{y}^{P'}$— на шаге с номером c, где $b < c$. На этих шагах были построены множества элементов E_b и E_c, причем $E_b \subseteq E_c$. И пусть существует номер $t \in [s]$, такой что элемент e_t — первый ненулевой элемент на наборах $\gamma(\boldsymbol{y}^P)$ и $\gamma(\boldsymbol{y}^{P'})$ относительно соответствующих множеств. В частности, имеем: $h_t(\gamma(\boldsymbol{y}^P)) = h_t(\gamma(\boldsymbol{y}^{P'})) = 1$. Для всякого элемента $e_j \notin E_c$, где $j < t$, по определению первого ненулевого элемента (относительно множества E_c, а следовательно, и E_b), выполнено: $h_j(\gamma(\boldsymbol{y}^P)) = h_j(\gamma(\boldsymbol{y}^{P'})) = 0$. По свойству 2, значения любого элемента $e_j \in E_c$, $j < t$, одинаковы на наборах $\gamma(\boldsymbol{y}^{P'})$ и $\gamma(\boldsymbol{y}^P)$. При этом, по построению, набор $\gamma(\boldsymbol{y}^{P'})$ отличается от набора $\gamma(\boldsymbol{y}^P)$ значением хотя бы одной компоненты, соответствующей входной переменной схемы, непосредственно подаваемой на один из входов элемента e_t.

Таким образом, для антицепной функции g_t, приписанной элементу e_t, имеем: g_t выдает 1 на некоторой паре сравнимых наборов. Это противоречит тому, что g_t — антицепная функция. Лемма 5.7 доказана. ■

Обозначим через $\Gamma(C)$ множество γ-образов наборов цепи C. Ясно, что множество $\Gamma(C)$ является цепью, при этом, говоря неформально, цепь C в кубе $\{0,1\}^k$ «плотная», а цепь $\Gamma(C)$ в кубе $\{0,1\}^n$ — «разреженная», поскольку значения переменных при построении новых наборов менялись целыми блоками.

Вернемся к вопросу о том, каким нужно выбрать значение параметра a, введенного в начале доказательства. Напомним, что этот параметр определяет количество входных переменных с номерами вне блоков $B_1, \ldots, B_k$, которые в начале фиксируются единицами.

Будем называть нижней половиной булева куба $\{0,1\}^n$ все наборы, содержащие не более $\frac{n}{2}$ единиц, а верхней половиной — все наборы, содержащие более $\frac{n}{2}$ единиц.

Положим значение параметра a равным $\frac{n}{2} - \frac{k}{2} \cdot \frac{n}{4k}$. Покажем, что при таком значении a в обеих половинах куба содержится не менее $\xi \cdot k$ элементов цепи $\Gamma(C)$, где ξ — некоторая константа, $0 < \xi \leqslant 1$.

Напомним, что для каждого блока B_j, $j \in [k]$, имеем: $\frac{n}{4k} \leqslant |B_j| \leqslant \frac{n}{2k}$. Обозначим количество элементов цепи $\Gamma(C)$, которые могут располагаться в нижней половине куба, через A. С учетом неравенств на размеры каждого блока, получаем оценки на величину A

$$(\frac{n}{8})/(\frac{n}{2k}) \leqslant A \leqslant (\frac{n}{8})/(\frac{n}{4k}),$$

что равносильно следующему: $\frac{k}{4} \leqslant A \leqslant \frac{k}{2}$. Напомним, что $|\Gamma(C)| = k+1$, значит, в верхней половине куба окажется не менее $\frac{k}{2} + 1$ элементов цепи.

Для одной из половин куба на всяком наборе цепи $\Gamma(C)$, лежащем в этой половине, существует первый ненулевой элемент (относительно соответствующего множества). Действительно, предположим обратное: пусть $\gamma(\boldsymbol{\alpha}), \gamma(\boldsymbol{\beta}) \in \{0,1\}^n$ — наборы цепи, лежащие соответственно в верхней и нижней половине куба, такие что на обоих этих наборах в схеме нет первого ненулевого элемента относительно соответствующих множеств. Рассмотрим e_s — последний элемент схемы S, согласно введенной нумерации элементов. Нетрудно понять, что значение на выходе элемента e_s одинаково на наборах $\gamma(\boldsymbol{\alpha})$ и $\gamma(\boldsymbol{\beta})$, поскольку всякий элемент схемы, кроме элементов из множества E, на $\gamma(\boldsymbol{\alpha})$ и $\gamma(\boldsymbol{\beta})$ выдает 0. Получаем противоречие с тем, что на выходе элемента e_s реализуется функция голосования. При этом, по лемме 5.7, все первые ненулевые элементы на наборах цепи $\Gamma(C)$ различны.

Таким образом, получаем, что количество первых ненулевых элементов цепи либо не менее $\frac{1}{4} \cdot \left\lfloor \frac{1}{4}\sqrt{n \log_2 n} \right\rfloor$, если на каждом из элементов цепи из нижней половины куба есть первый ненулевой элемент, либо не менее $\frac{1}{2} \cdot \left\lfloor \frac{1}{4}\sqrt{n \log_2 n} \right\rfloor + 1$, если на каждом из элементов цепи из верхней половины куба есть первый ненулевой элемент. Следовательно, количество элементов схемы s не менее

$\frac{1}{4} \cdot \left\lfloor \frac{1}{4}\sqrt{n \log_2 n} \right\rfloor$, что противоречит предположению $s < \frac{1}{4} \cdot \left\lfloor \frac{1}{4}\sqrt{n \log_2 n} \right\rfloor$. Тем самым теорема 5.3 доказана.

■

5.5 Доказательство теоремы 5.5

Этот раздел посвящен доказательству теоремы 5.5. Разобьем эту теорему на две леммы и докажем каждую из них по отдельности.

Лемма 5.8. *Для произвольной булевой функции f от n переменных выполнено соотношение: $L_{ACM}(f) = O(\log_2 n)$.*

Лемма 5.9. $L_{ACM}(n) = \Omega(\log_2 n)$.

Обозначим через D бесконечный базис, состоящий из функции отрицания и монотонных функций от любого числа переменных. Докажем следующую лемму.

Лемма 5.10. *Для произвольной булевой функции f от n переменных выполнено неравенство: $L_D(f) \leqslant 4L_{ACM}(f)$.*

Доказательство. Для любой функции f рассмотрим произвольную схему S в базисе ACM, реализующую эту функцию. Покажем, что схему S можно преобразовать в схему S' в базисе D так, что ее сложность возрастет не более чем в 4 раза, и при этом схема S' по-прежнему реализует функцию f.

Всякому элементу схемы S приписана либо функция голосования, либо антицепная функция. Если элементу приписана функция голосования, то оставляем его без изменений. Если некоторому элементу e приписана антицепная функция, то заменим его на подсхему, состоящую из не более четырех элементов базиса D, следующим образом.

Пусть элементу e приписана антицепная функция g, которая принимает значение 1 на некоторой антицепи A. Определим функцию f_1: положим ее равной

единице на всех наборах, которые больше наборов цепи A, а на всех остальных наборах положим равной нулю. Ясно, что такая функция является монотонной. Определим также функцию f_2: положим ее равной единице на всех наборах, которые не меньше наборов цепи A, а на всех остальных наборах положим равной нулю. Нетрудно убедиться, что справедливо выражение: $g = \overline{f}_1 \& f_2$. Если в схеме S заменить элемент e на подсхему, соответствующую указанному выражению, то полученная схема по-прежнему реализует функцию f.

Если совершить описанную замену для каждого элемента в схеме S, которому приписана антицепная функция, то получим схему S', реализующую функцию f, в базисе D, причем $L_D(S') \leqslant 4L_{ACM}(S)$. В силу произвольности схемы S, получаем, что лемма доказана. ■

Из работы Э. Н. Гилберта [55] непосредственно вытекает, что порядок роста функции Шеннона в базисе D равен $\log_2 n$. Нетрудно видеть, что этот факт в совокупности с леммой 5.10 дают доказательство леммы 5.9.

Проведем некоторые вспомогательные рассуждения и затем докажем лемму 5.8.

Рассмотрим булев куб $\{0,1\}^n$. Обозначим функцию голосования m_n от n переменных через g_1. Определим функцию g_2 от n переменных: $g_2(x_1 \ldots, x_n)$ равна 1 в одном из двух случаев:

1. либо $\sum\limits_{i=1}^{n} x_i \geqslant \left\lfloor \frac{3n}{4} \right\rfloor$,
2. либо $\left\lfloor \frac{n}{4} \right\rfloor \leqslant \sum\limits_{i=1}^{n} x_i \leqslant \frac{n}{2}$.

Функция g_2 равна 1 тогда и только тогда, когда для произвольного набора $\boldsymbol{x} = (x_1 \ldots, x_n)$ выполнено неравенство

$$\sum_{i=1}^{n} x_i - \left\lfloor \frac{n}{2} \right\rfloor g_1(\boldsymbol{x}) \geqslant \left\lfloor \frac{n}{4} \right\rfloor . \tag{5.11}$$

Докажем верхнюю оценку сложности функции g_2.

Лемма 5.11. $L_{ACM}(g_2) \leqslant 3$.

Доказательство. Рассмотрим функцию голосования m_p, где $p = 2n + \lfloor \frac{n}{2} \rfloor$. Нетрудно понять, что

$$g_2(x_1, \ldots, x_n) = m_p(x_1, \ldots, x_n, \underbrace{\overline{g}_1, \ldots, \overline{g}_1}_{\lfloor \frac{n}{2} \rfloor}, \underbrace{1, \ldots, 1}_{n}). \tag{5.12}$$

Действительно, функция m_p равна 1 на наборе $\boldsymbol{x} = (x_1, \ldots, x_n)$ тогда и только тогда, когда $\sum\limits_{i=1}^{n} x_i - \lfloor \frac{n}{2} \rfloor g_1(\boldsymbol{x}) + n \geqslant \frac{1}{2}(2n + \lfloor \frac{n}{2} \rfloor)$, что равносильно неравенству (5.11). Из равенства (5.12) вытекает требуемая верхняя оценка сложности. ■

Далее, аналогично функции g_2, определим функцию g_3 от n переменных так: функция g_3 равна 1 на наборе $\boldsymbol{x} = (x_1, \ldots, x_n)$ тогда и только тогда, когда $\sum\limits_{i=1}^{n} x_i - \left\lfloor \frac{n}{2} \right\rfloor g_1(\boldsymbol{x}) - \left\lfloor \frac{n}{4} \right\rfloor g_2 \geqslant \left\lfloor \frac{n}{8} \right\rfloor$. Нетрудно показать, что $L_{ACM}(g_3) \leqslant 5$.

Считая $n + 1 = 2^k$, определим функцию g_k от n переменых следующим образом: положим g_k равной 1 лишь на тех наборах $\boldsymbol{x} = (x_1, \ldots, x_n)$, для которых

$$\sum_{i=1}^{n} x_i - \sum_{t=1}^{k-1} \left\lfloor \frac{n}{2^t} \right\rfloor g_t(\boldsymbol{x}) \geqslant \left\lfloor \frac{n}{2^k} \right\rfloor. \tag{5.13}$$

Докажем следующую лемму.

Лемма 5.12. $L_{ACM}(g_k) \leqslant 2k - 1$.

Доказательство. Рассмотрим функцию голосования m_s, где количество переменных s, от которых зависит эта функция, равно следующей сумме:

$$n + \left(\left\lfloor \frac{n}{2} \right\rfloor + \left\lfloor \frac{n}{4} \right\rfloor + \ldots + \left\lfloor \frac{n}{2^{k-1}} \right\rfloor \right) + \left(n + \left\lfloor \frac{n}{2} \right\rfloor + \left\lfloor \frac{n}{4} \right\rfloor + \ldots + \left\lfloor \frac{n}{2^{k-2}} \right\rfloor \right).$$

Скобки разделяют три группы слагаемых — в первой группе одно слагаемое n. Обозначим третью группу слагаемых $\left(n + \lfloor \frac{n}{2} \rfloor + \lfloor \frac{n}{4} \rfloor + \ldots + \lfloor \frac{n}{2^{k-2}} \rfloor \right)$ через N_3.

Докажем, что

$$g_k(x_1, \ldots, x_n) = m_s(x_1, \ldots, x_n, \underbrace{\overline{g}_1, \ldots, \overline{g}_1}_{\lfloor \frac{n}{2} \rfloor}, \underbrace{\overline{g}_2, \ldots, \overline{g}_2}_{\lfloor \frac{n}{4} \rfloor}, \ldots, \underbrace{\overline{g}_{k-1}, \ldots, \overline{g}_{k-1}}_{\lfloor \frac{n}{2^{k-1}} \rfloor}, \underbrace{1, \ldots, 1}_{N_3}). \tag{5.14}$$

Действительно, функция m_s равна 1 на произвольном наборе $\boldsymbol{x} = (x_1, \ldots, x_n)$ тогда и только тогда, когда

$$\sum_{i=1}^{n} x_i + \sum_{t=1}^{k-1} \left\lfloor \frac{n}{2^t} \right\rfloor g_t(\boldsymbol{x}) + N_3 \geqslant \frac{1}{2}\left(n + \left\lfloor \frac{n}{2} \right\rfloor + \left\lfloor \frac{n}{4} \right\rfloor + \ldots + \left\lfloor \frac{n}{2^{k-1}} \right\rfloor\right) + \frac{1}{2}N_3.$$

Последнее неравенство равносильно неравенству (5.13). Нетрудно видеть, что из равенства (5.14) следует оценка сложности $L_{ACM}(g_k) \leqslant 2k - 1$. ■

Сделаем еще одно важное замечание. Функция g_k равна 1 на слоях с номерами, идущими через один, причем $g_k(\mathbf{0}) = 0$. Следовательно, функция g_k есть линейная функция $l_n(x_1 \ldots, x_n) = x_1 + \ldots + x_n \pmod 2$. Отсюда имеем: $L_{ACM}(l_n) \leqslant 2k - 1 = 2\log_2(n+1) - 1$.

Итак, перейдем непосредственно к доказательству леммы 5.8.

Доказательство. Мы построим такую антицепную функцию h, зависящую от n переменных, что с помощью этой функции и функции g_k от n переменных можно вычислить любую функцию f от n переменных.

Для всякого $m \in \{1, \ldots, n+1\}$ определим функции $f_m(x_1, \ldots, x_n)$ следующим образом: если $\sum\limits_{i=1}^{n} x_i = m$, то $f_m(x_1, \ldots, x_n) = f(x_1, \ldots, x_n)$, в противном случае $f_m(x_1, \ldots, x_n) = 0$.

При всяком $\boldsymbol{x} = (x_1, \ldots, x_n)$ рассмотрим набор значений

$$G(\boldsymbol{x}) = \left(g_1(\boldsymbol{x}), \overline{g}_1(\boldsymbol{x}), g_2(\boldsymbol{x}), \overline{g}_2(\boldsymbol{x}), \ldots, g_k(\boldsymbol{x}), \overline{g}_k(\boldsymbol{x})\right).$$

Ясно, что для любых двух наборов $\boldsymbol{x}, \boldsymbol{x}'$ соотношение $G(\boldsymbol{x}) = G(\boldsymbol{x}')$ выполнено тогда и только тогда, когда $|\boldsymbol{x}| = |\boldsymbol{x}'|$ (как обычно, $|\boldsymbol{x}| = \sum\limits_{i=1}^{n} x_i$). То есть для любого $q = 1, \ldots, n+1$ можно определить значение G_q, которое соответствует слою с номером q.

Определим функцию h от $\lfloor 2\log_2(n+1) \rfloor + n$ переменных так, что $h(G(\boldsymbol{x}), \boldsymbol{x}) = 1$ тогда и только тогда, когда существует m, такое что $G(\boldsymbol{x})$ соответствует слою с номером m, то есть равно G_m, и $f_m(\boldsymbol{x}) = 1$.

Функция h является антицепной. Действительно, для любых двух наборов $\boldsymbol{\alpha}$ и $\boldsymbol{\alpha}'$, таких что $|\boldsymbol{\alpha}| = |\boldsymbol{\alpha}'|$, наборы $(G(\boldsymbol{\alpha}), \boldsymbol{\alpha})$ и $(G(\boldsymbol{\alpha}'), \boldsymbol{\alpha}')$ очевидно несравнимы, так как несравнимы сами наборы $\boldsymbol{\alpha}$ и $\boldsymbol{\alpha}'$. Если $|\boldsymbol{\alpha}| \neq |\boldsymbol{\alpha}'|$, то либо ни один из наборов $\boldsymbol{\alpha}$ и $\boldsymbol{\alpha}'$ не принадлежит слою с номером m и тогда $h = 0$, либо, без ограничения общности, $|\boldsymbol{\alpha}| = m$, но тогда $G(\boldsymbol{\alpha})$ несравним с $G(\boldsymbol{\alpha}')$.

Нетрудно понять, что для произвольного набора $\boldsymbol{\beta} \in \{0,1\}^n$ выполнено: $h(G(\boldsymbol{\beta}), \boldsymbol{\beta}) = f(\boldsymbol{\beta})$.

Итак, мы показали, что произвольная булева функция может быть реализована схемой в базисе ACM сложности не больше $\lfloor 2\log_2(n+1) \rfloor + 1$. Лемма 5.8 доказана. ■

Доказательства лемм 5.8 и 5.9 дают в совокупности доказательство теоремы 5.5.

Заключение

В диссертации получены оценки сложности булевых функций (в том числе, важнейших из них — линейной функции и функции голосования) и оценки функций Шеннона в некоторых бесконечных базисах.

В частности, в базисе антицепных функций AC получена новая верхняя оценка функции Шеннона, доказана новая нижняя оценка для почти всех булевых функций, найдена точная формула, выражающая сложность произвольной симметрической булевой функции, и установлен окончательный порядок роста функции Шеннона. Также построен, по-видимому, первый пример бесконечного базиса (базис ACL, состоящий из всех антицепных функций и линейных функций от любого числа переменных), для которого порядок роста функции Шеннона лежит строго в интервале между функциями $\log_2 n$ и n.

В то же время, остается неизвестным, сколько попарно различных порядков роста функции Шеннона лежит строго в указанном интервале, в частности, конечно или бесконечно их число. Одной из задач в направлении исследования этого вопроса является построение базисов с порядками роста функций Шеннона, лежащими строго в этом интервале и отличными от установленного в работе.

Для выяснения вопроса о влиянии базиса на поведение функции Шеннона перспективным представляется дальнейшее развитие методов исследования, предложенных в данной диссертации, применительно к базисам, получаемым путем расширения базиса AC с помощью добавления в него новых функций.

К нерешенным вопросам по направлениям, изучаемым в диссертации, можно отнести также исследование вопроса о возможности уточнения нижней оценки сложности для почти всех функций в базисе AC и получение оценок для почти всех булевых функций в базисе ACL.

Таким образом, область исследований задач, которым посвящена данная работа, представляется достаточно обширной и заслуживает дальнейшего изучения и развития.

Список литературы

1. *Вайнцвайг М. Н.* О мощности схем из функциональных элементов // ДАН СССР. — 1961. — Т. 139, № 2. — С. 320 – 323.

2. *Захарова Е. Ю.* Об одном обобщении электронно-ламповых схем // Проблемы кибернетики, вып. 7. — М.: Физматгиз, 1962. — С. 43 – 60.

3. *Захарова Е. Ю.* О синтезе схем из пороговых элементов // Проблемы кибернетики, вып. 9. — М.: Физматгиз, 1963. — С. 317 – 319.

4. *Карпова Н. А.* О некоторых свойствах функций Шеннона // Матем. заметки. — 1970. — Т. 8, вып. 5. — С. 663 – 674.

5. *Касим-Заде О. М.* О сложности схем в одном бесконечном базисе // Вестник Моск. ун-та. Сер. 1. Математика. Механика. — 1994. — № 6. — С. 40 – 44.

6. *Касим-Заде О. М.* О сложности реализации булевых функций схемами в одном бесконечном базисе // Дискретный анализ и исследование операций. — 1995. — Т. 2, № 1. — С. 7 – 20.

7. *Касим-Заде О. М.* Общая верхняя оценка сложности схем в произвольном бесконечном полном базисе // Вестник Моск. ун-та. Сер. 1. Математика. Механика. — 1997. — № 4. — С. 59 – 61.

8. *Касим-Заде О. М.* Об одном методе получения оценок сложности схем над бесконечными базисами // Математические вопросы кибернетики, вып. 11. — М.: Наука. Физматлит, 2002. — С. 247 – 254.

9. *Касим-Заде О. М.* Об одном методе получения оценок сложности схем над произвольным бесконечным базисом // Дискретный анализ и исследование операций. Сер. 1. — 2004. — Т. 11, № 2. — С. 41 – 65.

10. *Касим-Заде О. М.* О глубине булевых функций при реализации схемами над произвольным базисом // Вестник Моск. ун-та. Сер. 1. Математика. Механика. — 2007. — № 1. — С. 18 – 21.

11. *Касим-Заде О. М.* О глубине булевых функций над произвольным бесконечным базисом // Дискретный анализ и исследование операций. Сер. 1. — 2007. — Т. 14, № 1. — С. 45 – 69.

12. *Касим-Заде О. М.* О глубине булевых функций при реализации схемами над произвольным бесконечным базисом // Вестник Моск. ун-та. Сер. 1. Математика. Механика. — 2012. — № 6. — С. 55–57.

13. *Касим-Заде О. М.* О порядках роста функций Шеннона сложности схем над бесконечными базисами // Вестник Моск. ун-та. Сер. 1. Математика. Механика. — 2013. — № 3. — С. 55–57.

14. *Комбаров Ю. А.* О минимальных схемах в базисе Шеффера для линейных булевых функций // Дискретный анализ и исследование операций. — 2013. — Т. 20, № 4. — 65 – 87.

15. *Комбаров Ю. А.* Верхняя оценка сложности реализации линейных функций схемами в одном базисе из многовходовых элементов // Вестник Моск. ун-та. Сер. 1. Математика. Механика. — 2015. — № 5. — С. 47 – 50.

16. *Коршунов А. Д.* Об оценках сложности схем из объемных функциональных элементов и объемных схем из функциональных элементов // Проблемы кибернетики, вып. 19. — М.: Наука, 1967. — С. 275 – 284.

17. *Кострикин А. И.* Введение в алгебру. Часть II. Линейная алгебра / М.: Физико-математическая литература, 2000. — 368 с.

18. *Кочергин А. В.* О глубине функций k-значной логики в бесконечных базисах // Вестник Моск. ун-та. Сер. 1. Математика. Механика. — 2011. — № 1. — С. 22 – 26.

19. *Кочергин А. В.* О глубине функций k-значной логики в конечных базисах // Вестник Московского университета. Сер. 1. Математика. Механика. — 2013. — № 1. — С. 56–59.

20. *Краснова Т. И.* О сложности реализации булевых функций схемами с произвольными весами элементов // Вестник Самарского муниципального института управления. — Самара: САГМУ, 2013. — № 4, вып. 27. — С. 151 – 154.

21. *Краснова Т. И.* О реализации индивидуальных булевых функций схемами с произвольными весами элементов // Вестник Самарского муниципального института управления. — Самара: САГМУ, 2014. — № 1, вып. 28. — С. 97 – 100.

22. *Ложкин С. А.* Асимптотическое поведение функций Шеннона для задержек схем из функциональных элементов // Матем. заметки. — 1976. — Т. 19, № 6. — С. 939 – 951.

23. *Лупанов О. Б.* О вентильных и контактно-вентильных схемах // ДАН СССР. — 1956. — Т. 111, № 6. — С. 1171 – 1174.

24. *Лупанов О. Б.* Об одном методе синтеза схем // Известия высших учебных заведений. Радиофизика. — 1958. — Т. 1, № 1. — С. 120 – 140.

25. *Лупанов О. Б.* О синтезе некоторых классов управляющих систем // Проблемы кибернетики, вып. 10. — М.: Физматгиз, 1963. — С. 63 – 97.

26. *Лупанов О. Б.* О об одном подходе к синтезу управляющих систем — принципе локального кодирования // Проблемы кибернетики, вып. 14. — М.: Наука, 1965. — С. 31 – 110.

27. *Лупанов О. Б.* К вопросу о реализации симметрических функций алгебры логики контактными схемами // Проблемы кибернетики, вып. 15. — М.: Наука, 1965. — С. 85 – 100.

28. *Лупанов О. Б.* О схемах из функциональных элементов с задержками // Проблемы кибернетики, вып. 23. — М.: Наука, 1970. — С. 43 – 81.

29. *Лупанов О. Б.* О синтезе схем из пороговых элементов // Проблемы кибернетики, вып. 26. — М.: Наука, 1973. — С. 109 – 140.

30. *Лупанов О. Б.* Асимптотические оценки сложности управляющих систем / М.: Изд-во Московского университета, 1984. — 138 с.

31. *Лупанов О. Б.* Конспект лекций по курсу «Введение в математическую логику» / Под редакцией А. Б. Угольникова. М.: Изд-во ЦПИ при механико-математическом ф-те МГУ, 2007. — 192 с.

32. *Мак-Вильямс Ф. Дж.*, *Слоэн Н. Дж. А.* Теория кодов, исправляющих ошибки / М.: Радио и связь, 1979. — 744 с.

33. *Марков А. А.* Об инверсионной сложности систем функций // ДАН СССР. — 1957. — Т. 116, № 6. — С. 917 – 919.

34. *Марков А. А.* Об инверсионной сложности систем булевых функций // ДАН СССР. — 1963. — Т. 150, № 3. — С. 477 – 479.

35. *Нечипорук Э. И.* О сложности схем в некоторых базисах, содержащих нетривиальные элементы с нулевыми весами // Проблемы кибернетики, вып. 8. — М.: Физматгиз, 1962. — С. 123 – 160.

36. *Нечипорук Э. И.* О синтезе схем из пороговых элементов // Проблемы кибернетики, вып. 11. — М.: Наука, 1964. — С. 49 – 62.

37. *Нечипорук Э. И.* О синтезе логических сетей в неполных и вырожденных базисах // Проблемы кибернетики, вып. 14. — М.: Наука, 1965. — С. 111 – 160.

38. *Нигматуллин Р. Г.* Сложность булевых функций / М.: Наука, 1991. — 40 с.

39. *Разборов А. А.* Нижние оценки размера схем ограниченной глубины в полном базисе, содержащем функцию логического сложения // Матем. заметки. — 1987. — Т. 41, № 4. — С. 598 – 607.

40. *Редькин Н. П.* О синтезе схем из пороговых элементов для некоторых классов булевых функций // Кибернетика. — 1970. — № 5. — С. 6 – 9.

41. *Редькин Н. П.* Доказательство минимальности некоторых схем из функциональных элементов // Проблемы кибернетики, вып. 23. — М.: Наука, 1970. — С. 83 – 101.

42. *Редькин Н. П.* О минимальной реализации линейной функции схемой из функциональных элементов // Кибернетика. — 1971. — № 6. — С. 31 – 38.

43. *Храпченко В. М.* О сложности реализации симметрических функций формулами // Матем. заметки. — 1972. — Т. 11, № 1. — С. 109 – 120.

44. *Храпченко В. М.* Нижние оценки сложности схем из функциональных элементов // Кибернетический сборник, Сер. 2. — 1984. — Вып. 21. — С. 3 – 54.

45. *Яблонский С. В.* Основные понятия кибернетики // Проблемы кибернетики, вып. 2. — М.: Физматгиз, 1959. — С. 7 – 38.

46. *Яблонский С. В.* Дискретная математика и математические вопросы кибернетики. Т. 1 / Под ред. *С. В. Яблонского* и *О. Б. Лупанова*. — М.: Наука, 1974. — 313 с.

47. *Яблонский С. В.* Введение в дискретную математику / М.: Наука, 1986. — 384 с.

48. *Aigner M.* Combinatorial Theory / Springer Berlin Heidelberg. — 1979. — 483 p. (Русский перевод: Айгнер М. Комбинаторная теория / М.: Мир, 1982. — 558 с.)

49. *Ajtai M.* Σ_1^1-formulae on finite structures // Annals of Pure and Applied Logic. — 1983. — V. 24. — P. 1 – 48.

50. *Arora S., Barak B.* Computational complexity: a modern approach / Cambridge: Cambridge university press, 2009. — 549 p.

51. *Boppana R., Sipster M.* The complexity of finite functions // Handbook of Theoretical Computer Science. — Vol. A, Algorithms and Complexity. — Amsterdam: Elsevier, 1990. — P. 757 – 800.

52. *Demenkov E., Kojevnikov A., Kulikov A., Yaroslavtsev G.* New upper bounds on the Boolean circuit complexity of symmetric functions // Information Processing Letters. — 2010. — V. 110, № 7.1 — P. 264 –267.

53. *Dunne P. E.* The complexity of Boolean Networks / London: Academic Press, 1988.

54. *Furst M., Saxe J., Sipster M.* Parity, circuits and the polynomial time hierarchy // Mathematical Systems theory. —1984. — V. 17. — P. 13 – 27.

55. *Gilbert E. N.* Lattice theoretic properties of frontal switching functions // J. Math. Phys. — 1954. — V. 33, № 1. — P. 57 – 67. (Русский перевод: Гилберт Э.Н. Теоретико-структурные свойства замыкающих переключательных функций // Кибернетический сборник, вып. 1. — М.: ИЛ, 1960. — С. 175 – 188).

56. *Jukna S.* Extremal Combinatorics With Applications in Computer Science / Springer-Verlag Berlin Heidelberg, 2011. — 376 p.

57. *Kleene S. C.* Representation of events in nerve nets and finite automata // Automata Studies. Annals of Mathematics Studies, № 34. Edited by *Shannon C. E.*, *McCarthy J.* — Princeton University Press, 1956. — 285 p. (Русский перевод: Автоматы. Сборник статей / Под ред. А. А. Ляпунова. — М.: Изд-во иностр. лит-ры, 1956).

58. *Lai H.Ch., Muroga S.* Logic networks with a minimum number of NOR (NAND) gates for parity functions of n variables // IEEE Trans. Comput. — 1987. — C-36, № 2. — P. 157 – 166.

59. *Muller D. E.* Complexity in electronic switching circuits // IRE Trans. Electron. Comput. — 1956. — EC-5, № 1. — P. 15 – 19.

60. *McCulloch W. S.*, *Pitts W.* A logical calculus of the ideas immanent in nervous activity // Bull. Math. Biophys. — 1943. — V. 5. — P. 115 – 133. (Русский перевод: Автоматы. Сборник статей / Под ред. *А. А. Ляпунова.* — М.: Изд-во иностр. лит-ры, 1956).

61. *Savage J. E.* The Complexity of Computing / John Wiley & Sons Inc, 1977. (Русский перевод: Сэвидж Дж. Э. Сложность вычислений / М.: Изд.-во «Факториал», 1998. — 368 с.)

62. *Savage J. E.* Models of Computation: Exploring the Power of Computing / Addison-Wesley. — 1997.

63. *Riordan J., Shannon C. E.* The number of two-terminal series-parallel networks // J. Math. and Phys. — 1942. — V. 21, № 2. — P. 83 – 93. (Русский перевод: Шеннон К. Работы по теории информации и кибернетике / М.: ИЛ, 1963. — С. 46 – 58).

64. *Schnorr C. P.* Zwei lineare untere Schranken für die Komplexität Boolescher Funktionen // Computing. — 1974. — V. 13. № 2. — 155 – 171.

65. *Smolensky R.* Algebraic methods in the theory of lower bounds for Boolean circuit complexity / Proceedings of the nineteenth annual ACM symposium on Theory of computing. — 1987. — P. 77 – 82.

66. *Shannon C. E.* A symbolic analysis of relay and switching circuits // Trans. AIEE — 1938. — V. 51. — P. 713 – 722. (Русский перевод: Шеннон К. Э. Работы по теории информации и кибернетике / М.: ИЛ, 1963. — С. 9 – 45).

67. *Shannon C. E.* The synthesis of two-terminal switching circuits // Bell Syst. Techn. J. — 1949. — V. 28, № 1. — P. 59 – 98. (Русский перевод: Шеннон К. Э. Работы по теории информации и кибернетике / М.: ИЛ, 1963. — С. 59 – 101).

68. *Stockmeyer L. J.* On the combinational complexity of certain symmetric Boolean functions // Math. Systems Theory. — 1976. — Vol.10. — P. 323 – 336. (Русский перевод: Стокмейер Л. Дж. О комбинационной сложности некоторых симметрических булевых функций // Кибернетический сборник, Сер. 2. — 1979. — Вып. 16. — С. 45 – 61).

69. *Tao T., Vu V.* Additive combinatorics / Cambridge: Cambridge University Press, 2006. — 512 p.

70. *Valiant. L. G.* Short Monotone Formulae for the Majority Function // Journal of Algorithms. — 1984. — Vol. 5, № 3. — P. 363 – 366. (Русский перевод: Вэльянт Л. Простые монотонные формулы для функции голосования // Кибернетический сборник, Сер. 2. — 1987. — Вып. 24. — С. 97 – 100).

71. *Winder R. O.* Bounds on threshold gate realizability // IEEE Trans. Electron. Comput. — 1963. —EC-12, № 5. — P. 561 – 564.

72. *Wegener I.* The complexity of Boolean functions / Teubner, Stuttgart: Willey-Teubner Ser. Comput. Sci., 1987. — 470 p.

73. *Wegener I.* The complexity of the parity function in unbounded fan-in, unbounded depth circuits // Theor. Comput. Sci. — 1991. — V. 85, № 1. — P. 155 – 170.

74. *Zwick U.* A $4n$ lower bound on the combinational complexity of certain symmetric Boolean functions over the basis of unate dyadic Boolean functions // SIAM Journal on Computing. — 1991. — № 20. — P. 499 – 505.

Публикации автора по теме диссертации

75. *Подольская О. В.* О нижних оценках сложности схем в базисе антицепных функций // Вестник Моск. ун-та. Сер. 1. Математика. Механика. — 2013. — № 2. — С. 17 – 23.

76. *Подольская О. В.* Сложность реализации симметрических булевых функций схемами в базисе антицепных функций // Дискретная математика. — 2015. — Т. 27, вып. 3. — С. 95 – 107.

77. *Подольская О. В.* Сложность линейных функций и функции голосования в базисе антицепных функций // Вестник Моск. ун-та. Сер. 1. Математика. Механика. — 2016. — № 2. — С. 51 – 52.

78. *Подольская О. В.* Об оценках сложности схем в одном бесконечном базисе // Мат-лы IX Молодежной научной школы по дискретной математике и ее приложениям (Москва, 16 – 21 сентября 2013 г.). Под редакцией А. В. Чашкина. — М.: Изд-во ИПМ РАН, 2013. — С. 97 – 100.

79. *Подольская О. В.* О сложности реализации симметрических булевых функций в одном бесконечном базисе // Мат-лы X Молодежной научной школы по дискретной математике и ее приложениям (Москва, 5 – 11 октября

2015 г.). Под редакцией А. В. Чашкина. — М.: Изд-во ИПМ им. М. В. Келдыша, 2015. — С. 56 – 58.

80. *Подольская О. В.* Об оценках функций Шеннона сложности схем в некоторых бесконечных базисах // Мат-лы XII Междунар. семинара «Дискретная математика и ее приложения» имени академика О. Б. Лупанова (Москва, 20 – 25 июня 2016 г.). — М.: Изд-во механико-математического факультета МГУ, 2016. — С. 150 – 152.