

На правах рукописи



A blue handwritten signature in cursive script.

Смаль Александр Владимирович

**Доказательство нижних оценок
на размер формул для булевых функций
методами коммуникационной сложности**

Специальность 01.01.06 —
«Математическая логика, алгебра и теория чисел»

Автореферат
диссертации на соискание учёной степени
кандидата физико-математических наук

Санкт-Петербург — 2022

Работа выполнена в лаборатории математической логики Санкт-Петербургского отделения Математического института им. В. А. Стеклова РАН.

- Научный руководитель: **Гирш Эдуард Алексеевич**
доктор физико-математических наук,
профессор РАН
- Официальные оппоненты: **Верещагин Николай Константинович**,
доктор физико-математических наук,
профессор,
Московский государственный университет
им. М.В. Ломоносова, профессор
- Ромащенко Андрей Евгеньевич**,
кандидат физико-математических наук,
Институт проблем передачи информации
им. А.А. Харкевича РАН,
старший научный сотрудник
- Ведущая организация: Федеральное государственное автономное
образовательное учреждение высшего
образования «Уральский федеральный
университет имени первого Президента
России Б.Н. Ельцина»

Защита диссертации состоится 9 марта 2022 г. в 17:30 на заседании Диссертационного совета Д 002.202.02 в Санкт-Петербургском отделении Математического института им. В.А.Стеклова РАН по адресу: 191023, Санкт-Петербург, наб. р. Фонтанки, д. 27.

С диссертацией можно ознакомиться в библиотеке Санкт-Петербургского отделения Математического института им. В.А. Стеклова РАН,
<http://www.pdmi.ras.ru/>.

Автореферат разослан _____ января 2022 года.
Телефон для справок: +7 (812) 312-40-58.

Ученый секретарь
диссертационного совета
Д 002.202.02,
доктор физико-математических наук Пономаренко Илья Николаевич

Общая характеристика работы

Актуальность темы и степень её разработанности.

Определение. *Формула Де Моргана ϕ от n переменных* — это корневое двоичное дерево с пометками, в котором каждая внутренняя вершина имеет ровно два потомка и помечена одной из логических связок $\{\wedge, \vee\}$, а листья помечены *литералами* $\{x_1, x_2, \dots, x_n, \neg x_1, \neg x_2, \dots, \neg x_n\}$. Вычисление формулы ϕ на входе $x \in \{0,1\}^n$ заключается в подстановке значений соответствующих битов x в листья и последовательном вычислении значений для каждой внутренней вершины от листьев к корню в соответствии с пометками в этих вершинах. *Значение формулы ϕ на входе x* определяется как значение в корне, полученное в результате вычисления ϕ на x . Будем говорить, что формула ϕ *вычисляет* булеву функцию $f_n : \{0,1\}^n \rightarrow \{0,1\}$, если для всех $x \in \{0,1\}^n$ значение ϕ на входе x совпадает с $f_n(x)$. *Размером формулы ϕ* называется количество листьев, а *глубиной формулы ϕ* — высота дерева, т.е. количество рёбер в самом длинном простом пути от корня до некоторого листа.

В следующих определениях и в контексте нижних оценок под булевой функцией $f : \{0,1\}^n \rightarrow \{0,1\}$ часто будет подразумеваться не конкретная функция для некоторого фиксированного n , а бесконечная последовательность функций f_1, f_2, \dots , где $f_i : \{0,1\}^i \rightarrow \{0,1\}$.

Определение. Будем говорить, что булева функция $f : \{0,1\}^n \rightarrow \{0,1\}$ *вычисляется формулами Де Моргана размера $s(n)$* , если для каждого $i \in \mathbb{N}$ существует формула Де Моргана размера $s(i)$, вычисляющая f_i . *Формульной сложностью $L(f)$ функции f* называется минимальная функция s , такая что f вычисляется формулами Де Моргана размера $s(n)$.

Определение. Будем говорить, что булева функция $f : \{0,1\}^n \rightarrow \{0,1\}$ *вычисляется формулами Де Моргана глубины $d(n)$* , если для каждого $i \in \mathbb{N}$ существует формула Де Моргана глубины $d(i)$, вычисляющая f_i . *Формульной глубиной $D(f)$ функции f* называется минимальная функция d , такая что f вычисляется формулами Де Моргана глубины $d(n)$.

Эти две характеристики булевых функций тесно связаны.

Утверждение. *Существует такая константа $c > 1$, что для любой булевой функции $f : \{0,1\}^n \rightarrow \{0,1\}$ выполняется*

$$\log_2 L(f) \leq D(f) \leq c \cdot \log_2 L(f).$$

Первое неравенство верно в силу того, что высота двоичного дерева ограничена снизу двоичным логарифмом от числа листьев. Второе неравенство имеет место, т.к. формулы Де Моргана можно сбалансировать с небольшим увеличением размера (подробнее см. [11]).

Доказательство нижних оценок на формульную сложность булевых функций — это одна из классических задач теории сложности вычислений. Ещё в 1942 году Риордан и Шеннон [17] доказали, что почти все булевы функции от n переменных имеют формульную сложность не менее $2^n / \log n$.

Теорема (Риордан, Шеннон). *Для любого $\epsilon > 0$ доля функций $f : \{0,1\}^n \rightarrow \{0,1\}$, для которых $L(f) \leq (1 - \epsilon) \cdot 2^n / \log n$, не превосходит $2^{-2^n \cdot (\epsilon - o(1))}$.*

Другими словами, если выбрать функцию случайно, то с вероятностью близкой к единице она будет иметь экспоненциальную формульную сложность. Однако неизвестны явно заданные функции (из классов **P** или **NP**) большой сложности. Более сорока лет исследователи развивали методы для доказательства нижних оценок: начиная с работ Субботовской [3] и Храпченко [4] вплоть до знаменитой статьи Хостада [9], в которой он доказал кубическую нижнюю оценку на формульную сложность функции Андреева [1; 2]. Эту нижнюю оценку не удаётся превзойти уже более 20 лет. Результат Хостада был улучшен Талом в работе [18], но улучшение коснулось только членов второго порядка, т.е. оценка осталась кубической.

Если изначальный подход к формульной сложности можно охарактеризовать как комбинаторный, то в дальнейшем стали появляться альтернативные методы анализа. В работе [13] Карчмером и Вигдерсоном было замечено, что формулы в базисе Де Моргана имеют очень тесную взаимосвязь с задачами коммуникационной сложности, предложенной Яо [19] за 10 лет до этого для совершенно других целей. В частности эта взаимосвязь позволяет получать оценки на формульную сложность и формульную глубину булевых функций через доказательство оценок на размер и глубину коммуникационных протоколов. В дальнейшем была сформулирована гипотеза Карчмера — Раза — Вигдерсона [12] и предложен план исследований, реализация которого может привести к доказательству суперкубической или даже суперполиномиальной нижней оценки на формульную сложность явной булевой функции. Первые шаги этого плана были реализованы в работах [5; 6; 8; 10]. Основной инструментарий этих работ — это изучение коммуникационной сложности и теоретико-информационные методы.

Целью данной работы является разработка и совершенствование новых подходов к доказательству нижних оценок на формульную сложность булевых функций с использованием методов коммуникационной сложности.

Научная новизна. Все полученные результаты являются новыми. Теоремы о предсказании семействами сертификатов и попарно несовместных свидетелей улучшают известные до этого оценки, делая их точными. Идея рассмотрения полудуплексных моделей коммуникации является

новой. Все полученные верхние и нижние оценки на полудуплексную коммуникационную сложность до этого были неизвестны. Основным результатом последней главы про нижнюю оценку на композицию универсального отношения и некоторой функции является первой нетривиальной оценкой такого рода. Кроме самих результатов, новыми являются представленные в последней главе методы доказательства нижних оценок на коммуникационную сложность, основанные сведениях между задачами классической, недетерминированной и полудуплексной коммуникации.

Теоретическая и практическая значимость. Диссертация имеет теоретический характер. Полученные результаты и разработанные методы могут быть использованы для дальнейшего изучения формульной сложности булевых функций и коммуникационной сложности.

Методология и методы исследования. Для получения результатов второй главы и части результатов третьей применяется теоретико-информационный аппарат энтропии Шеннона. Для получения результатов третьей главы использовались обобщения известных методов доказательства оценок на коммуникационную сложность, а также специально разработанный метод элиминации раундов. Кроме того, для решения задачи нелинейной оптимизации в третьей главе применялись численные методы. В четвёртой главе применяются новые методы доказательства нижних оценок на коммуникационную сложность, основанные на сведениях между задачами классической, недетерминированной и полудуплексной коммуникации.

Основные положения, выносимые на защиту:

1. Доказано, что если случайная величина X , распределённая на $\{0,1\}^n$, имеет энтропию $H(X) \geq n - k$, то средняя вероятность того, что в X встречается сертификат для X_i размера $q < n$ не превосходит $\frac{k \cdot (q+1)}{n}$.
2. Доказаны верхние оценки на полудуплексную коммуникационную сложность для функции равенства EQ_n : $n/\log_2 5 + O(\log n)$ для модели с тишиной и $n/\log_2 3 + O(\log n)$ для модели с нулём, а также верхняя оценка $n/2 + O(1)$ на функцию дизъюнктивности DIS_n в модели с тишиной.
3. Доказаны нижние оценки на полудуплексную коммуникационную сложность функции внутреннего произведения IP_n : $n/2$ для модели с тишиной, $n/1.39$ для модели с нулём и $n/\log_2(7/3)$ для модели с противником.
4. Доказаны верхние оценки на количество информации, которым игроки могут обменяться за один раунд полудуплексной коммуникации: 2 бита в модели с тишиной и 1.389 бита в модели с нулём. Для случая, когда частные распределения на входах игроков являются независимыми, доказаны более сильные оценки: 1.67 бита в модели с тишиной и 1.234 бита в модели с нулём. На основе этого

доказаны нижние оценки на полудуплексную коммуникационную сложность игр Карчмера — Вигдерсона для функций подсчёта.

- Доказана нижняя оценка $1.5n - o(n)$ на коммуникационную сложность композиции универсального отношения и некоторой функции для случаев XOR-композиции и блочной композиции.

Достоверность полученных результатов обеспечивается их публикацией в рецензируемых научных изданиях, индексируемых международными базами данных.

Апробация работы. Основные результаты работы докладывались и обсуждались на следующих семинарах и конференциях.

- Семинар по теории сложности в Санкт-Петербургском отделении Математического института им. В.А. Стеклова РАН (Россия, 2018 и 2020).
- Традиционная зимняя сессия МИАН–ПОМИ, посвященная теме «Математическая логика» (Россия, 2018).
- Международная конференция «The 29th International Symposium on Algorithms and Computation» (Тайвань, 2018).
- Семинар по теории сложности в Математическом институте Чешской академии наук (Чехия, 2018 и 2021).
- Семинар «Laboratoire d’Informatique, de Robotique et de Micro-électronique de Montpellier» (Франция, 2019).
- Колмогоровский семинар по сложности вычислений и сложности определений (онлайн, 2020).
- Международная конференция «The 47th International Conference on Current Trends in Theory and Practice of Computer Science» (онлайн, 2021).
- Международная конференция «The Computational Complexity Conference» (онлайн, 2021).

Публикации. Основные результаты по теме диссертации изложены в четырёх работах [A1—A4], все из которых изданы в журналах, рекомендованных ВАК, и индексируемых Web of Science и Scopus.

Личный вклад. В работе [A4] постановка задачи принадлежит соавтору. Обсуждение идей, которые могут использоваться в доказательстве, велось совместно. Автору принадлежит доказательство теоремы 2, являющейся основным результатом статьи. В работе [A2] постановка задачи, основные определения, а также доказательства теорем 6–9, 15, 20 и 23 были разработаны совместно с И.А. Михайлиным. Кроме этого, автору принадлежат теоремы 14, 16 и 19. В работе [A1] автору принадлежат постановка задачи и теорема 4. В работе [A3] постановка задачи принадлежит соавтору. Автору принадлежит доказательство теоремы 9. Схема доказательства основных результатов была выработана авторами совместно.

Содержание работы

Во **введении** обосновывается актуальность исследований, проводимых в рамках данной диссертации, приводится краткий обзор положения дел в рассматриваемой области, формулируется цель, ставятся задачи, описывается научная новизна и значимость представляемой работы.

Первая глава содержит основные определения и факты, необходимые для понимания последующих глав. В **разделе 1.2** излагаются основы классической теории информации. В **подразделе 1.2.1** определяется *энтропия Шеннона* и перечисляются основные её свойства.

Определение (Шеннон, 1948). Пусть случайная величина α принимает значения из множества $\{a_1, a_2, \dots, a_k\}$ с вероятностями $\{p_1, p_2, \dots, p_k\}$, $p_i \geq 0$, $\sum_i p_i = 1$. *Энтропия Шеннона* случайной величины α определяется как

$$H(\alpha) = \sum_{i=1}^k p_i \cdot \log \frac{1}{p_i}$$

(при $p_i = 0$ мы полагаем в этой сумме $p_i \cdot \log \frac{1}{p_i} = 0$).

На основе этого определения вводятся понятия *энтропии совместного распределения нескольких величин* и *условной энтропии одной случайной величины относительно другой*. В **подразделе 1.2.2** определяется *взаимная информация двух случайных величин* и *взаимная информация двух случайных величин при условии третьей*. Все эти понятия потребуются во второй и третьей главах.

Раздел 1.3 посвящён базовым определениям классической коммуникационной сложности, а также методам доказательства нижних оценок на коммуникационную сложность функций. В **подразделе 1.3.1** описывается классическая коммуникационная модель для двух игроков. Пусть X , Y и Z — конечные множества, и пусть задана некоторая функция $f : X \times Y \rightarrow Z$. Два игрока, будем называть их Алиса и Боб, решают *коммуникационную задачу для функции f* , если:

1. множества X , Y , Z и функция f известны обоим игрокам,
2. Алиса знает некоторый $x \in X$,
3. Боб знает некоторый $y \in Y$,
4. Алиса и Боб стремятся вычислить $f(x, y)$.

Для решения этой коммуникационной задачи Алиса и Боб могут пересылать друг другу битовые сообщения. Задача считается решённой, если оба игрока знают $f(x, y)$. *Коммуникационную сложность функции f* определяют как минимальное количество битов, которое необходимо и достаточно переслать для вычисления $f(x, y)$ для любой пары $(x, y) \in X \times Y$, и обозначают $CC(f)$. Для формализации этой игры вводится понятие *коммуникационного протокола*, который представляет собой двоичное дерево

с пометками, описывающее общение игроков на всех парах входов (x, y) . Эти определения можно обобщить на случай тернарного отношения $R \subseteq X \times Y \times Z$ — в этом случае игроки должны будут найти некоторый $z \in Z$, для которого $(x, y, z) \in R$.

Подраздел 1.3.2 описывает методы для доказательства нижних оценок на коммуникационную сложность. **Подраздел 1.3.3** вводит несколько классических функций вида $\{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}$, которые изучают в контексте коммуникационной сложности:

- функция равенства $\text{EQ}_n(x, y) = 1 \iff x = y$,
- функция внутреннего произведения $\text{IP}_n(x, y) = \sum_i x_i y_i \pmod 2$,
- функция дизъюнктивности $\text{DISJ}_n(x, y) = 1 \iff \sum_i x_i y_i = 0$.

В подразделе **1.3.4** даются базовые определения и оценки для недетерминированной коммуникационной сложности, которые потребуются в четвёртой главе.

Раздел 1.4 рассказывает о связи коммуникационных протоколов и формул Де Моргана. В подразделе **1.4.1** определяется игра Карчмера — Вигдерсона для функции $f : \{0,1\}^n \rightarrow \{0,1\}$, являющаяся коммуникационной задачей для отношения

$$\text{KW}_f = \{(x, y, i) \mid x \in f^{-1}(0), y \in f^{-1}(1), x_i \neq y_i\},$$

которое называется *отношением Карчмера — Вигдерсона* для функции f . В работе [13] неявно доказана следующая теорема.

Теорема (Карчмер, Вигдерсон). *Для каждой формулы ϕ , вычисляющей функцию f , существует такой протокол Π_ϕ для отношения Карчмера — Вигдерсона KW_f , что его дерево совпадает с деревом, описывающим структуру формулы ϕ . Верно и обратное: если есть протокол для отношения KW_f , то есть и формула для f с такой же структурой.*

Существование такого сохраняющего структуру соответствия между протоколами и формулами позволяет использовать методы коммуникационной сложности для доказательства оценок на размер и глубину формул Де Моргана. В подразделе **1.4.2** изложен теоретико-информационный подход к доказательству нижних оценок на коммуникационную сложность игр Карчмера — Вигдерсона, основанный на оценке *информационного разглашения* — количества информации о своих входах, которое игроки разглашают в процессе общения. В подразделе **1.4.3** определяется *блочная композиция* двух булевых функций и формулируется гипотеза Карчмера — Раза — Вигдерсона из работы [12].

Определение. Пусть $f : \{0,1\}^m \rightarrow \{0,1\}$ и $g : \{0,1\}^n \rightarrow \{0,1\}$ — две произвольные булевы функции. *Блочная композиция* $f \diamond g : (\{0,1\}^n)^m \rightarrow \{0,1\}$ определяется соотношением

$$(f \diamond g)(x_1, \dots, x_m) = f(g(x_1), \dots, g(x_m)),$$

где $x_1, \dots, x_m \in \{0,1\}^n$.

Гипотеза (Карчмер, Раз, Вигдерсон). *Для любых непостоянных функций $f : \{0,1\}^m \rightarrow \{0,1\}$ и $g : \{0,1\}^n \rightarrow \{0,1\}$*

$$D(f \diamond g) \approx D(f) + D(g).$$

Если эта гипотеза верна, то существует вычислимая за полиномиальное время функция, которая не вычисляется формулами Де Моргана полиномиального размера, и следовательно, $\mathbf{P} \not\subseteq \mathbf{NC}^1$. Подход к разделению классов \mathbf{P} и \mathbf{NC}^1 путём доказательства этой гипотезы особенно привлекателен тем, что он, насколько нам известно, не нарушает ни один из известных на данный момент мета-математических барьеров вроде концепции «натуральных доказательств» Разборова и Рудича [16]. Стоит отметить, что у этой гипотезы есть множество различных переформулировок, из доказательства которых так же будет следовать $\mathbf{P} \not\subseteq \mathbf{NC}^1$. По теореме Карчмера — Вигдерсона коммуникационная сложность игры Карчмера — Вигдерсона для f совпадает с минимальной глубиной формулы Де Моргана для f . Эта взаимосвязь позволяет нам использовать методы коммуникационной сложности для доказательства нижних оценок на формульную глубину. В частности, гипотезу Карчмера — Раза — Вигдерсона можно переформулировать в терминах коммуникационной сложности игры Карчмера — Вигдерсона для блочной композиции двух произвольных булевых функций.

Гипотеза (Карчмер, Раз, Вигдерсон (переформулировка)). *Для любых непостоянных функций $f : \{0,1\}^m \rightarrow \{0,1\}$ и $g : \{0,1\}^n \rightarrow \{0,1\}$*

$$CC(KW_{f \diamond g}) \approx CC(KW_f) + CC(KW_g).$$

В последнем **подразделе 1.4.4** рассказывается про коммуникационные задачи для *универсального отношения* и отношения мультиплексера, обобщающие игры Карчмера — Вигдерсона.

Определение. *Универсальное отношение* длины n обозначается U_n и определяется соотношением

$$U_n = \{(x, y, i) \mid x, y \in \{0,1\}^n, i \in [n], x_i \neq y_i\} \cup \{(x, x, \perp) \mid x \in \{0,1\}^n\}.$$

Коммуникационная игра для универсального отношения является обобщением игры Карчмера — Вигдерсона: Алиса и Боб получают две битовые строки длины n и их задача — найти координату $i \in [n]$, такую что $x_i \neq y_i$. В отличие от игр Карчмера — Вигдерсона в игре для универсального отношения Алиса и Боб могут получить одинаковые строки. В таком случае они должны выдать специальный символ \perp , сообщающий о том, что такой координаты i не существует. Исследование универсальных

отношений тесно связано с гипотезой Карчмера — Раза — Вигдерсона. В частности, в работах [6; 10] авторы доказали аналог гипотезы Карчмера — Раза — Вигдерсона для блочной композиции универсальных отношений (понятие блочной композиции для функций можно естественным образом обобщить на случай отношений Карчмера — Вигдерсона и универсальных отношений). В последующих работах [7; 14] были доказаны нижние оценки на блочную композицию отношения Карчмера — Вигдерсона для произвольной булевой функции и универсального отношения.

В работе [6] авторы предлагают рассматривать *коммуникационную игру для отношения мультиплекса с общей функцией*.

Определение. В *коммуникационной игре для отношения мультиплекса с общей функцией* (игре для отношения мультиплекса) MUX_n Алиса получает функцию $f : \{0,1\}^n \rightarrow \{0,1\}$ и вход $x \in \{0,1\}^n$, такие что $f(x) = 0$, а Боб получает функцию $g : \{0,1\}^n \rightarrow \{0,1\}$ и вход $y \in \{0,1\}^n$, такие что $g(y) = 1$. Их общая цель — найти координату $i \in [n]$, такую что $x_i \neq y_i$, или вернуть специальный символ \perp , если $f \neq g$ (если $x \neq y$ и $f \neq g$, то оба варианта ответа возможны).

Игра для отношения мультиплекса может так же рассматриваться как обобщение игр Карчмера — Вигдерсона для булевых функций от n переменных. Действительно, игра Карчмера — Вигдерсона для произвольной функции $g : \{0,1\}^n \rightarrow \{0,1\}$ может быть сведена к игре для отношения мультиплекса: получив x и y Алиса и Боб используют протокол для отношения мультиплекса на входах (g,x) и (g,y) , соответственно, в результате находят координату $i \in [n]$, такую что $x_i \neq y_i$, и возвращают её в качестве ответа (игроки получили одну и ту же функцию, поэтому протокол не может вернуть \perp).

Вторая глава посвящена улучшению результата Меира и Вигдерсона из работы [15]. Они предложили изучить следующий вопрос: пусть случайная величина $X = (X_1, \dots, X_n)$ распределена на $\{0,1\}^n$ и имеет энтропию не менее $n - k$. Наш противник, который знает распределение X и некоторую (равномерно) случайно выбранную координату $i \in [n]$, хочет предсказать значение X_i . Ему разрешается запросить q координат X отличных от i . Насколько большим должно быть q , чтобы у противника было существенное преимущество? Меир и Вигдерсон дают ответ на этот вопрос: $q = \omega(n/k)$, причём это верно, даже если противнику разрешено делать недетерминированные запросы. Формально это определяется следующим образом.

Определение. *Свидетель* для координаты $i \in [n]$ — это пара (Q, a) , где $Q \subseteq [n] \setminus \{i\}$ и $a \in \{0,1\}^{|Q|}$. Свидетель *присутствует* в строке $x \in \{0,1\}^n$, если $x|_Q = a$. *Длина* свидетеля определяется как $|Q|$.

Определение. q -семейство свидетелей \mathcal{F} для координаты $i \in [n]$ — это множество свидетелей для i длины не более q . Мы будем говорить, что строка $x \in \{0,1\}^n$ удовлетворяет \mathcal{F} , и обозначать $x \models \mathcal{F}$, если хотя бы один свидетель из \mathcal{F} присутствует в x . Для случайной величины X , распределённой на $\{0,1\}^n$, бита $b \in \{0,1\}$ и $\epsilon \in [0,1]$ будем говорить, что \mathcal{F} ϵ -предсказывает $X_i = b$, если $\Pr[X_i = b \mid X \models \mathcal{F}] \geq (1 + \epsilon)/2$.

Теорема (Меир, Вигдерсон). Пусть X — случайная величина, распределённая на $\{0,1\}^n$, такая что $H(X) \geq n - k$, и пусть $q \leq n$. Для $\epsilon \in (0,1]$ и для всех $i \in [n]$ и $b \in \{0,1\}$ пусть \mathcal{F}_i^b является q -семейством свидетелей, которое ϵ -предсказывает $X_i = b$, и пусть σ_i обозначает вероятность того, что выполняется $X \models \mathcal{F}_i^0$ или $X \models \mathcal{F}_i^1$. Тогда $\mathbb{E}_i[\sigma_i] \leq \frac{300 \cdot k \cdot q}{\epsilon^3 \cdot n}$.

Из этой теоремы для случая $\epsilon = 1$ можно получить нижние оценки на схемы глубины три (подробнее см. [15]). В частности из анализа игры Карчмера — Вигдерсона для функции чётности можно показать, что любая схема глубины три, вычисляющая функцию чётности, имеет размер не менее $2^{\Omega(\sqrt{n})}$. При этом де-факто оценка получается на формулы Де Моргана специального вида, в которых на любом пути от корня к листьям происходит не более двух перемен типов логических связей. Такие формулы являются частным случаем схем глубины три. Схемы константной глубины можно преобразовать в формулы так, что их размер увеличится не более чем полиномиально, поэтому в контексте экспоненциальных оценок можно считать, что схемы глубины три являются формулами.

В разделе 2.2 описываются идеи, которые позволяют улучшить этот результат. На основе этих идей в разделе 2.3 теорема Меира — Вигдерсона улучшается для случая $\epsilon = 1$.

Определение. Для случайной величины X , распределённой на $\{0,1\}^n$, координаты $i \in [n]$ и бита $b \in \{0,1\}$, b -сертификат для i — это свидетель (Q, a) , такой что $\Pr[X_i = b \mid X|_Q = a] = 1$.

Теорема 2.5. Пусть X — случайная величина, распределённая на $\{0,1\}^n$, такая что $H(X) \geq n - k$, и пусть $q \leq n$. Для всех $i \in [n]$ и $b \in \{0,1\}$ пусть σ_i обозначает вероятность того, что X содержит какой-то сертификат для i . Тогда $\mathbb{E}_i[\sigma_i] \leq \frac{k \cdot (q+1)}{n}$.

Отметим, что полученная оценка является точной. Этот результат опубликован в работе [A4].

В разделе 2.4 теорема Меира — Вигдерсона улучшается для случая несовместных свидетелей. Будем говорить, что два свидетеля несовместны, если никакая строка не содержит сразу оба эти свидетеля.

Теорема 2.9. Пусть X — случайная величина, распределённая на $\{0,1\}^n$, такая что $H(X) \geq n - k$, и пусть $q < n$. Для $\epsilon \in (0,1]$ и для всех

$i \in [n]$ и $b \in \{0,1\}$ пусть \mathcal{F}_i^b является q -семейством попарно несовместных свидетелей, которые ϵ -предсказывают $X_i = b$, и пусть σ_i обозначает вероятность того, что выполняется $X \models \mathcal{F}_i^0$ или $X \models \mathcal{F}_i^1$. Тогда $\mathbb{E}_i[\sigma_i]$ не превосходит $\frac{k \cdot (q+1)}{(1-h(1/2+\epsilon)) \cdot n}$, где h обозначает бинарную функцию энтропии $h(p) = -p \log p - (1-p) \log(1-p)$.

Отметим, что оценка в этой теореме также является точной.

Третья глава посвящена исследованию *полудуплексной коммуникационной сложности*. Важное свойство классической коммуникационной модели заключается в том, что на каждом раунде общения один из игроков посылает некоторое битовое сообщение, а другой игрок его принимает. В **разделе 3.2** подробно описывается мотивация для изучения подобных моделей. В **разделе 3.3** определяются три новые модели коммуникационной сложности, которые обобщают классическую модель и описывают общение по так называемому *полудуплексному каналу*. Предполагается, что у игроков есть некоторый механизм синхронизации (например, синхронизированные часы), позволяющий им определять границы раундов. На каждом раунде каждый игрок выбирает одно из трёх действий: отправить 0, отправить 1 или принимать. Могут быть три типа раундов.

- Один из игроков посылает, а другой игрок принимает. Это *обычный* или *классический* раунд. Гарантируется, что принимающий игрок получит именно то сообщение, которое было передано.
- Оба игрока посылают сообщения. Такой раунд называется *потерянным*, т.к. в этом случае сообщения теряются, но игроки об этом не знают (в точно такой же ситуации оказываются два человека, которые передают сообщение по радию одновременно).
- Оба игрока принимают. Такой раунд называется *тихим*.

Предлагается три вариации этой модели.

- Если в тихих раундах оба игрока понимают, что никакого сообщения не было передано, т.е. они отличают «тишину» от 0 и 1, то такая модель называется *полудуплексной коммуникационной моделью с тишиной*.
- Если в тихих раундах оба игрока получают 0, т.е. они не могут отличить тихий раунд от раунда, в котором их собеседник послал 0, то такая модель называется *полудуплексной коммуникационной моделью с нулём*.
- Если в тихих раундах оба игрока получают какие-то произвольные биты (например, случайные или заданные противником), такая модель называется *полудуплексной коммуникационной моделью с противником*.

Для каждой модели минимальное количество раундов, необходимое для решения некоторой коммуникационной задачи на всех возможных входах,

определяет её *полудуплексную коммуникационную сложность с тишиной*, с нулём и с противником, которые, соответственно, обозначаются CC_s^{hd} , CC_0^{hd} и CC_a^{hd} .

В **разделе 3.4** доказываются общие оценки, устанавливающие взаимосвязь между сложностью одной и той же коммуникационной задачи в разных моделях коммуникации. **Раздел 3.5** посвящён доказательству верхних оценок на функции из подраздела 1.3.3. В **разделе 3.6** предлагаются два метода для получения нижних оценок на полудуплексную сложность: метод прямоугольников и метод элиминации раундов. С их помощью доказывается серия нижних оценок на те же функции. **Раздел 3.7** содержит обзор известных оценок на полудуплексную коммуникационную сложность функций, представленные в табл. 1. Звёздочкой отмечены результаты, полученные соискателем лично или при его активном участии.

Таблица 1 — Известные оценки на полудуплексную коммуникационную сложность функций.

	EQ_n		IP_n		$DISJ_n$
CC_s^{hd}	$\geq n/\log 5$	*	$\geq n/2$	*	$\geq n/\log 5$
	$\leq n/\log 5 + o(n)$	*	$\leq n/2 + 2$		$\leq n/2 + 2$
CC_0^{hd}	$\geq n/\log 3$	*	$\geq n/\log \frac{2}{3-\sqrt{5}}$	*	$\geq n/\log 3$
	$\leq n/\log 3 + o(n)$	*	$\leq 7n/8 + O(1)$		$\leq 3n/4 + o(n)$
CC_a^{hd}	$\geq n/\log 2.5$	*	$\geq n/\log(7/3)$	*	$\geq n/\log 2.5$

В **разделе 3.8** с использованием теоретико-информационных методов доказываются нижние оценки на полудуплексную коммуникационную сложность отношения Карчмера — Вигдерсона для функции подсчёта по модулю $\text{MOD}p_n(x) = \sum_{i=1}^n x_i \bmod p$. Для этого доказываются верхние оценки на количество информации, которым игроки могут обменяться за один раунд полудуплексной коммуникации: 2 бита в модели с тишиной и 1.389 бита в модели с нулём. Для случая, когда частные распределения на входах игроков являются независимыми, доказываются более сильные оценки: 1.67 бита в модели с тишиной и 1.234 бита в модели с нулём. Для полудуплексной коммуникации с противником аналогичная верхняя оценка доказана соавтором: игроки не могут обменяться более чем одним битом информации за раунд. В результате доказывается следующая теорема.

Теорема 3.37. *Для любых натуральных n и $p \geq 2$ верны следующие оценки: $CC_s^{hd}(\text{KW}_{\text{MOD}p_n}) \geq \log n - O(1)$, $CC_0^{hd}(\text{KW}_{\text{MOD}p_n}) \geq 1.439 \log n$ и $CC_a^{hd}(\text{KW}_{\text{MOD}p_n}) \geq 2 \log n - O(1)$.*

Результаты третьей главы опубликованы в работах [A1; A2].

В **четвертой главе** формулируется гипотеза XOR-KRW и доказывается нетривиальная нижняя оценка на композицию универсального

отношения и отношения Карчмера — Вигдерсона для некоторой функции. В разделе 4.1 определяется понятие XOR-композиции функций и формулируется гипотеза XOR-KRW, которую можно рассматривать как некоторую альтернативу гипотезы Карчмера — Раза — Вигдерсона, из которой тоже следует $\mathbf{P} \not\subseteq \mathbf{NC}^1$. В этом разделе также рассматриваются различные варианты ослабления этой гипотезы, которых уже недостаточно для разделения \mathbf{P} и \mathbf{NC}^1 , но из их доказательства будет следовать суперкубическая нижняя оценка на формульную сложность явной булевой функции. Для того, чтобы продвинуться в этом направлении, предлагается доказывать нижнюю оценку на XOR-композицию универсального отношения и отношения Карчмера — Вигдерсона для некоторой функции.

В разделе 4.2 представлен обзор методов и полученных результатов. В этой главе для доказательства используются два основных технических приёма: доказательство нижних оценок на коммуникационную сложность с помощью сведения недетерминированной коммуникационной задачи для функции неравенства и метод преобразования нижних оценок на отношение мультиплексера в нижние оценки на функции через полудуплексную коммуникационную сложность. С помощью этих методов получается доказать нижнюю оценку на коммуникационную сложность следующей задачи, которую можно рассматривать как XOR-композицию U_n и KW_g .

Определение. В коммуникационной игре $U_n \boxplus KW_g$ для функции $g : \{0,1\}^n \rightarrow \{0,1\}^n$ Алиса получает $x_a, y_a \in \{0,1\}^n$, Боб получает $x_b, y_b \in \{0,1\}^n$, и их задача найти $i \in [2n]$, такой что $(x_a \circ y_a)_i \neq (x_b \circ y_b)_i$. Если $g(x_a) \oplus g(y_a) = g(x_b) \oplus g(y_b)$, то игрокам разрешается ответить \perp .

Теорема 4.12. Для любого $n \in \mathbb{N}$ существует функция $g : \{0,1\}^n \rightarrow \{0,1\}^n$, такая что $CC(U_n \boxplus KW_g) \geq 1.5n - O(\log n)$.

Эта теорема частично отвечает на открытый вопрос из работы [7], устанавливая нижнюю оценку на XOR-композицию универсального отношения и функции. Ответ является частичным, т.к. открытый вопрос в оригинальной формулировке касается нижней оценки на композицию $U_n \diamond KW_g$ для любой функции g , в то время как теорема выше гарантирует оценку лишь для некоторой сложной функции g . К тому же, в нашем случае размеры входа для U_n и для g совпадают, а в оригинальной постановке предполагается, что размеры входов могут быть различными. Кроме того, в этой теореме используется XOR-композиция вместо блочной композиции, но в разделе 4.6 показывается, что соответствующий результат для блочной композиции является следствием из доказательства этой теоремы.

В качестве промежуточного шага к доказательству этой теоремы предлагается рассмотреть вспомогательную задачу и доказать для неё нижнюю оценку. Следующую задачу можно рассматривать как XOR-композицию U_n и отношения мультиплексера.

Определение. В коммуникационной задаче $U_n \boxplus \text{MUX}_n$ Алиса получает $x_a, y_a \in \{0,1\}^n$ и функцию $g_a : \{0,1\}^n \rightarrow \{0,1\}^n$, Боб получает $x_b, y_b \in \{0,1\}^n$ и функцию $g_b : \{0,1\}^n \rightarrow \{0,1\}^n$. Задача игроков — найти число $i \in [2n]$, такое что $(x_a \circ y_a)_i \neq (x_b \circ y_b)_i$. Если $g_a(x_a) \oplus g_a(y_a) = g_b(x_b) \oplus g_b(y_b)$ или $g_a \neq g_b$, то игрокам разрешается ответить \perp .

Теорема 4.14. Для любого $n \in \mathbb{N}$ верно $CC(U_n \boxplus \text{MUX}_n) \geq 1.5n - o(n)$.

В разделе 4.3 описывается дополнительный инструментарий: определяется понятие *частичной полудуплексной коммуникационной задачи* и демонстрируется, как нижние оценки на полудуплексную сложность отношения мультиплексера помогают доказать существование функции большой сложности. Потом этот приём будет использоваться для преобразования нижней оценки для задачи $U_n \boxplus \text{MUX}_n$ в нижнюю оценку для задачи $U_n \boxplus \text{KW}_g$.

Раздел 4.4 посвящён доказательству нижней оценки для задачи $U_n \boxplus \text{MUX}_n$. В подразделе 4.4.1 даётся общий план доказательства и вводятся необходимые определения. Подразделы 4.4.2 и 4.4.3 описывают две стадии доказательства. В подразделе 4.4.4 доказывается основная техническая лемма, позволяющая провести сведение недетерминированной коммуникационной задачи неравенства к задаче $U_n \boxplus \text{MUX}_n$.

В разделе 4.5 нижняя оценка для задачи $U_n \boxplus \text{MUX}_n$ постепенно преобразуется в нижнюю оценку для задачи $U_n \boxplus \text{KW}_g$ с некоторой функцией g . Задача $U_n \boxplus \text{KW}_g$ является частным случаем задачи $U_n \boxplus \text{MUX}_n$ для конкретного g . Интуиция подсказывает, что если задача $U_n \boxplus \text{MUX}_n$ является сложной, то и для какой-то функции g задача $U_n \boxplus \text{KW}_g$ тоже является сложной. Поэтому для получения нижней оценки для задачи $U_n \boxplus \text{KW}_g$ для некоторой функции g из нижней оценки для задачи $U_n \boxplus \text{MUX}_n$ нам нужно показать, что задача $U_n \boxplus \text{MUX}_n$ является не менее сложной чем задача $U_n \boxplus \text{KW}_g$ для «самой сложной» функции, которую мы можем дать игрокам, и поэтому мы можем подставить эту «самую сложную» функцию в задачу $U_n \boxplus \text{MUX}_n$ и получить задачу $U_n \boxplus \text{KW}_g$. Для того, чтобы этот план сработал, нужно преодолеть ряд препятствий и применить весь запасённый к этому моменту инструментарий.

В разделе 4.6 показано, что из полученной нижней оценки на XOR-композицию универсального отношения и отношения Карчмера — Вигдерсона для некоторой функции следует нижняя оценка для блочной композиции таких отношений.

Теорема 4.33. Для любого $n \in \mathbb{N}$ существует функция $f : \{0,1\}^n \rightarrow \{0,1\}$, такая что $CC(U_n \diamond f) \geq 1.5n - O(\log n)$.

В разделе 4.7 доказывается нижняя оценка на композицию произвольной функции и отношения Карчмера — Вигдерсона для функции мультиплексера. Эта оценка является следствием результата из работ [7; 14]. Аналогичная оценка для отношения мультиплексера неизвестна.

Теорема 1.53. Для любых $m, n \in \mathbb{N}$, таких что $n \geq 6 \log m$, и любой непостоянной функции $f : \{0,1\}^m \rightarrow \{0,1\}$ выполняется

$$CC(KW_f \diamond KW_{M_n}) \geq \log L(f) + n - O(\log n).$$

Результаты четвёртой главы опубликованы в работе [A3].

В **заключении** приведены основные результаты работы:

1. Получены результаты о предсказании семействами сертификатов и семействами несовместных свидетелей, улучшающие известные оценки до точных.
2. Сформулированы и изучены полудуплексные модели коммуникационной сложности. В частности был доказан ряд верхних и нижних оценок на полудуплексную коммуникационную сложность функций и игр Карчмера — Вигдерсона. Для получения нижних оценок был разработан набор методов, специфичный для полудуплексных моделей.
3. Доказана нижняя оценка $1.5n - o(n)$ на коммуникационную сложность композиции универсального отношения и некоторой функции для случаев XOR-композиции и блочной композиции. Доказательство использует новые методы, специально разработанные для этих целей: сведение задач недетерминированной коммуникационной сложности для получения нижних оценок на композицию с отношением мультиплекса и метод преобразования нижних оценок на отношение мультиплекса в нижние оценки на сложность некоторой функции через полудуплексную коммуникационную сложность.

Публикации автора по теме диссертации

- A1. *Dementiev, Y., Ignatiev, A., Sidelnik, V., Smal, A., Ushakov, M.* New Bounds on the Half-Duplex Communication Complexity // SOFSEM 2021. Т. 12607. — Springer, 2021. — С. 233–248. — (LNCS). — URL: https://doi.org/10.1007/978-3-030-67731-2%5C_17.
- A2. *Hoover, K., Impagliazzo, R., Mihajlin, I., Smal, A. V.* Half-Duplex Communication Complexity // ISAAC 2018. Т. 123. — Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2018. — 10:1–10:12. — (LIPIcs). — URL: <https://doi.org/10.4230/LIPIcs.ISAAC.2018.10>.
- A3. *Mihajlin, I., Smal, A.* Toward Better Depth Lower Bounds: The XOR-KRW Conjecture // CCC 2021. Т. 200. — Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2021. — 38:1–38:24. — (LIPIcs). — URL: <https://drops.dagstuhl.de/opus/volltexte/2021/14312>.

- A4. *Smal, A. V., Talebanfard, N.* Prediction from partial information and hindsight, an alternative proof // *Inf. Process. Lett.* — 2018. — Т. 136. — С. 102–104. — URL: <https://doi.org/10.1016/j.ipl.2018.04.011>.

Список литературы

1. *Андреев, А. Е.* Об одном методе получения более чем квадратичных эффективных нижних оценок сложности π -схем // *Вестн. Моск. ун-та. Сер. 1. Матем., мех.* — 1987. — Вып. 1. — С. 70–73.
2. *Нечипорук, Э. И.* Об одной булевой функции // *Докл. АН СССР.* — 1966. — Т. 169, вып. 4. — С. 765–766.
3. *Субботовская, Б. А.* О реализации линейных функций формулами в базисе $\vee, \&, -$ // *Докл. АН СССР.* — 1961. — Т. 136–3. — С. 553–555.
4. *Храпченко, В. М.* О сложности реализации линейной функции в классе Π -схем // *Матем. заметки.* — 1971. — Т. 9, № 1. — С. 35–40.
5. *Dinur, I., Meir, O.* Toward the KRW Composition Conjecture: Cubic Formula Lower Bounds via Communication Complexity // *Comput. Complex.* — 2018. — Т. 27, № 3. — С. 375–462. — URL: <https://doi.org/10.1007/s00037-017-0159-x>.
6. *Edmonds, J., Impagliazzo, R., Rudich, S., Sgall, J.* Communication complexity towards lower bounds on circuit depth // *Computational Complexity.* — 2001. — Т. 10, № 3. — С. 210–246. — URL: <https://doi.org/10.1007/s00037-001-8195-x>.
7. *Gavinsky, D., Meir, O., Weinstein, O., Wigderson, A.* Toward better formula lower bounds: an information complexity approach to the KRW composition conjecture // *STOC 2014.* — ACM, 2014. — С. 213–222. — URL: <https://doi.org/10.1145/2591796.2591856>.
8. *Gavinsky, D., Meir, O., Weinstein, O., Wigderson, A.* Toward Better Formula Lower Bounds: The Composition of a Function and a Universal Relation // *SIAM J. Comput.* — 2017. — Т. 46, № 1. — С. 114–131. — URL: <https://doi.org/10.1137/15M1018319>.
9. *Håstad, J.* The Shrinkage Exponent of de Morgan Formulas is 2 // *SIAM J. Comput.* — 1998. — Т. 27, № 1. — С. 48–64. — URL: <https://doi.org/10.1137/S0097539794261556>.
10. *Håstad, J., Wigderson, A.* Composition of the Universal Relation // *DIMACS 1990.* Т. 13. — DIMACS/AMS, 1990. — С. 119–134. — URL: <http://dimacs.rutgers.edu/Volumes/Vol13.html>.

11. *Jukna, S.* Boolean Function Complexity - Advances and Frontiers. T. 27. — Springer, 2012. — (Algorithms and combinatorics). — URL: <https://doi.org/10.1007/978-3-642-24508-4>.
12. *Karchmer, M., Raz, R., Wigderson, A.* Super-Logarithmic Depth Lower Bounds Via the Direct Sum in Communication Complexity // Computational Complexity. — 1995. — T. 5, № 3/4. — C. 191–204. — URL: <https://doi.org/10.1007/BF01206317>.
13. *Karchmer, M., Wigderson, A.* Monotone Circuits for Connectivity Require Super-logarithmic Depth // STOC 1988. — ACM, 1988. — C. 539–550. — URL: <http://doi.acm.org/10.1145/62212.62265>.
14. *Koroth, S., Meir, O.* Improved Composition Theorems for Functions and Relations // APPROX/RANDOM 2018. T. 116. — Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2018. — 48:1–48:18. — (LIPIcs). — URL: <http://drops.dagstuhl.de/opus/volltexte/2018/9452>.
15. *Meir, O., Wigderson, A.* Prediction from Partial Information and Hindsight, with Application to Circuit Lower Bounds // ECCC. — 2017. — T. 24. — C. 149. — URL: <https://eccc.weizmann.ac.il/report/2017/149>.
16. *Razborov, A. A., Rudich, S.* Natural proofs // Journal of Computer and System Sciences. — 1997. — T. 55, № 1. — C. 24–35.
17. *Riordan, J., Shannon, C. E.* The Number of Two-Terminal Series-Parallel Networks // Journal of Mathematics and Physics. — 1942. — T. 21, № 1–4. — C. 83–93. — URL: <https://onlinelibrary.wiley.com/doi/abs/10.1002/sapm194221183>.
18. *Tal, A.* Shrinkage of De Morgan Formulae by Spectral Techniques // FOCS 2014. — IEEE Computer Society, 2014. — C. 551–560. — URL: <https://doi.org/10.1109/FOCS.2014.65>.
19. *Yao, A. C.-C.* Some Complexity Questions Related to Distributive Computing (Preliminary Report) // STOC 1979. — ACM, 1979. — C. 209–213. — URL: <http://doi.acm.org/10.1145/800135.804414>.