МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ М. В. ЛОМОНОСОВА

На правах рукописи

**Козачинский Александр Николаевич**

# Сравнение коммуникационной, информационной и вопросной сложности

01.01.06 — математическая логика, алгебра и теория чисел

Автореферат
диссертации на соискание учёной степени
кандидата физико-математических наук

Москва — 2019

Работа выполнена на кафедре математической логики и теории алгоритмов механико-математического факультета ФГБОУ ВО «Московский государственный университет имени М. В. Ломоносова».

Научный руководитель: **Верещагин Николай Константинович,** доктор физико-математических наук, профессор.

Официальные оппоненты:

**Гирш Эдуард Алексеевич,** доктор физико-математических наук, доцент, профессор РАН, Санкт-Петербургское отделение Математического института им. В. А. Стеклова РАН, лаборатория математической логики, ведущий научный сотрудник, и.о. заведующего лабораторией.

**Аблаев Фарид Мансурович,** доктор физико-математических наук, профессор, член-корреспондент Академии Наук Республики Татарстан, Казанский (Приволжский) федеральный университет, институт вычислительной математики и информационных технологий, отделение фундаментальной информатики и информационных технологий, кафедра теоретической кибернетики, заведующий кафедрой.

**Вялый Михаил Николаевич,** кандидат физико-математических наук, доцент, Федеральный исследовательский центр «Информатика и управление» РАН, Вычислительный центр им. А.А. Дородницына РАН, отдел распознавания, защиты и анализа информации, старший научный сотрудник.

Защита диссертации состоится 6 декабря 2019 года в 16 часов 45 минут на заседании диссертационного совета МГУ.01.17 ФГБОУ ВО «Московский государственный университет имени М. В. Ломоносова» по адресу 119234, Москва, ГСП-1, Ленинские горы, д. 1., ФГБОУ ВО «Московский государственный университет имени М. В. Ломоносова», механико-математический факультат, аудитория 14-08.

E-mail: msu.01.17@mail.ru

С диссертацией можно ознакомиться в отделе диссертаций Фундаментальной библиотеки Московского государственного университета имени М. В. Ломоносова (Москва, Ломоносовский проспект, д. 27) и на сайте ИСА «ИСТИНА»: https://istina.msu.ru/dissertations/

Автореферат разослан 6 ноября 2019 года.

Ученый секретарь диссертационного совета МГУ.01.17 ФГБОУ ВО МГУ, член-корреспондент РАН — **Шафаревич А. И.**

# Общая характеристика работы

## Актуальность темы и степень ее разработанности

Диссертация посвящена различным вопросам в коммуникационной сложности. Исследуется как коммуникационная сложность конкретных функций, так и связь коммуникационной сложности с другими сложностными мерами — а именно, с информационной и вопросной сложностью.

Коммуникационная сложность была введена в работе Яо[1] в 1979 году. В модели коммуникационной сложности есть два игрока, Алиса и Боб. С каждым из игроков связано конечное множество, элемент которого игрок получает на вход. При этом Алиса не видит вход Боба, а Боб не видит входа Алисы. Игрокам нужно ответить на какой-то вопрос о своих входах, ответ на который зависит как от входа Алисы, так и от входа Боба, что делает невозможным ответить какому-то игроку на вопрос самостоятельно. Например, Алиса и Боб могут хотеть вычислить значение известной игрокам функции $f$, принимающей два аргумента, первый из которых — вход Алисы, а второй — вход Боба.

Для этого у Алисы и Боба есть канал коммуникации, по которому они могут общаться, посылая друг другу битовые сообщения. Алгоритмы их общения в этой науке называются коммуникационными протоколами. Для Алисы и Боба нужно придумать такой протокол, чтобы в конце общения, основываясь на полученной друг от друга информации, они могли ответить на вопрос, например, выдать значение $f$.

Алиса и Боб доверяют друг другу, при этом они стараются минимизировать количество бит, которое они друг другу посылают. Подчеркнем, что Алисе и Бобу даются неограниченные вычислительные ресурсы — можно представлять себе, что передача по каналу намного дороже затрат на локальные вычисления.

В простейшей модели, называемой детерминированной коммуникационной сложностью, Алиса и Боб должны всегда правильно выдавать значение $f$, а минимальное $d$, для которого найдется протокол, вычисляющий $f$, в котором на любой паре входов передается не более $d$ битов, называется коммуникационной сложностью $f$. Для детерминированной коммуникационной сложности $f$ используется обозначение $D(f)$. Рассматриваются и более сложные модели — недетерминированная, вероятностная сложность и т. д. (большинство моделей имеют аналогии в списке сложностных классов классической теории вычислений). Например, часто в этой диссертации мы будем рассматривать вероятностную коммуникационную сложность, в которой предполагается, что Алиса и Боб могут подбрасывать монетки, основывая на результатах бросаний дальнейшие действия. При этом, по аналогии с определением класса BPP, им разрешается на любой паре входов с небольшой вероятностью выдавать неправильный ответ. Можно требовать, чтобы ошибка была «односторонней» — тогда возникает аналогия с классом RP.

При определении различных моделей возникают и другие детали, связанные скорее с коммуникационной спецификой задачи. Например, одна и та же монетка у Алисы и Боба или у каждого своя? Рассматриваются оба варианта, причем первый называется моделью с общими случайными битами, а второй — с частными случайными битами. Взаимоотношение между общими и частными случайными битами также будет рассмотрено в диссертации. Подробный обзор этих двух и многих других моделей коммуникационной сложности можно найти в классической монографии Кушилевица и Нисана[2].

Коммуникационная сложность показала себя как очень успешный инструмент в получении нижних оценок в других разделах сложности вычислений. Среди такого рода результа-

[1] A. C.-C. Yao. Some Complexity Questions Related to Distributive Computing // Proceedings of the 11th annual ACM symposium on Theory of computing. — 1979. — P. 209-213.

[2] E. Kushilevitz, N. Nisan. Communication Complexity. — Cambridge University Press, 2006.

тов наибольшую известность, вероятно, имеет работа Вигдерсона и Карчмера[3], устанавливающая связь между коммуникационной и схемной сложностью. Помимо этого коммуникационная сложность использовалась для нижних оценок на конечные автоматы, в потоковых алгоритмах, в тестировании свойств, сложности доказательств и т. д. (см. например, монографию Ружгардена[4], целиком посвященную применениям коммуникационной сложности).

Далее мы чуть более подробно изложим те вопросы в коммуникационной сложности, в рамках которых получены основные результаты диссертации.

Примером конкретной функции, коммуникационная сложность которой изучается в диссертации, является функция Gap Hamming Distance. Соответствующую коммуникационную задачу можно сформулировать так. Алиса и Боб получают по $n$-битовой строке. Гарантируется, что расстояние Хемминга между их входами либо не больше $L$, либо не меньше $U$. Алиса и Боб должны выдать 0 в первом случае и 1 во втором. Здесь $L \leq U \leq n$ — некоторые натуральные числа. Эту задачу мы обозначим через $\mathrm{GHD}(n, L, U)$.

Формально говоря, задача Алисы и Боба состоит в вычислении следующей частично определенной функции:

$$\mathrm{GHD}(n, L, U) : \{0,1\}^n \times \{0,1\}^n \to \{0,1\},$$

$$\mathrm{GHD}(n, L, U)(x, y) = \begin{cases} 0 & \text{если } d(x,y) \leq L, \\ 1 & \text{если } d(x,y) \geq U, \\ \text{не определено} & \text{если } L < d(x,y) < U, \end{cases}$$

где через $d$ обозначено расстояние Хемминга.

Эта функция часто использовалась для получения нижних оценок в потоковых алгоритмах[5,6] и в тестировании свойств[7]. В серии работ[8,9,10,11,12,13] была полностью исследована вероятностная коммуникационная сложность этой функции для случая, когда $L$ и $U$ симметричны относительно $n/2$. Разные верхние оценки при других $L$ и $U$ были получены в

[3]M. Karchmer, A. Widgerson. Monotone Circuits for Connectivity Require Super-Logarithmic Depth // SIAM Journal of Discrete Mathematics. — 1990. — V. 3. №. 2. — P. 255-265.

[4]T. Roughgarden. Communication complexity (for algorithm designers) // Foundations and trends in Theoretical Comuter Science. — 2016. — v. 11. — №. 3–4. — P. 217-404.

[5]D. Woodruff. Optimal Space Lower Bounds for All Frequency Moments. // Proceedings of the 15th annual ACM-SIAM symposium on Discrete algorithms. — 2004. — P. 167-175.

[6]J. Brody, D. P. Woodruff. Streaming Algorithms with One-Sided Estimation. // Proceedings of the 14th international conference on Approximation and the 15th International conference on Randomization, and combinatorial optimization: algorithms and techniques. — 2011. — P. 436-447.

[7]E. Blais, J. Brody, K. Matulef. Property Testing Lower Bounds via Communication Complexity. // Computational Complexity. — 2012. — V. 21. №. 2. — P. 311-358.

[8]T. S. Jayram, R. Kumar, D. Sivakumar. The One-Way Communication Complexity of Hamming Distance. // Theory of Computing. — 2008. — V. 4. №. 1. — P. 129-135.

[9]J. Brody, A. Chakrabarti. A Multi-Round Communication Lower Bound for Gap Hamming and Some Consequences. // Proceedings of the 24th Annual IEEE Conference on Computational Compleixty. — 2009. — P. 358-368.

[10]J. Brody, A. Chakrabarti, O. Regev, T. Vidick, R. De Wolf. Better Gap-Hamming Lower Bounds via Better Round Elimination. // Proceedings of the 13th international conference on Approximation and the 14th International conference on Randomization, and combinatorial optimization: algorithms and techniques. — 2010. — P. 476-489.

[11]A. Chakrabarti, O. Regev. An Optimal Lower Bound on the Communication Complexity of Gap-Hamming-Distance. // SIAM Journal on Computing. — 2012. — V. 41. №. 5. — P. 1299-1317.

[12]A. A. Sherstov. The Communication Complexity of Gap Hamming Distance. // Theory of Computing. — 2012. — V. 8. №. 1. — P. 197

[13]T. Vidick. A Concentration Inequality for the Overlap of a Vector on a Large Set. // Chicago Journal of Theoretical Computer Science. — 2012. — V. 1. — P. 1-12.

работах[14,15,16]. Эти верхние оценки интересны тем, что не зависят от $n$ (т. е. от размерности входа). Исследовалась также сложность Gap Hamming Distance с односторонней ошибкой[17,18]. Именно сложности с односторонней ошибкой и будет посвящен наш результат.

Второе направление в коммуникационной сложности, затронутое в диссертации, имеет отношение к теореме Раза — Маккинзи о связи коммуникационной сложности и сложности деревьев разрешения (вопросной сложности)[19]. Начнем с деревьев разрешения. Они вычисляют функции вида $f : \{0,1\}^n \to \{0,1\}$. На входе $x \in \{0,1\}^n$, чтобы вычислить $f(x)$, дерево может запрашивать значения $x$ в различных координатах. Номер очередной запрашиваемой координаты может зависеть от результатов предыдущих запросов. При этом нас не интересует время работы дерева. Единственное, что мы минимизируем, это суммарное число запросов (в худшем случае). Наименьшее $d$, для которого найдется дерево, вычисляющее $f$ и делающее не более $d$ запросов, называется вопросной сложностью $f$ и обозначается ниже через $D^{dt}(f)$.

Здесь мы рассматриваем только детерминированные деревья и, соответственно, только детерминированную вопросную сложность. О других видах вопросной сложности можно прочитать в обзоре Бурмана и де Вольфа[20].

Раз и Маккинзи предложили рассматривать композиции функций, чтобы связать коммуникационную и вопросную сложность. Точнее, для функции $f : \{0,1\}^n \to \{0,1\}$, у которой можно измерить вопросную сложность, и для булевой функции $g$, вход которой каким-то образом разбит на два аргумента, благодаря чему определена коммуникационную сложность $g$, можно естественным образом определить композицию $f \circ g$. А именно, надо рассмотреть $n$ пар входов для $g$, к каждому применить $g$ и к полученному $n$-битовому вектору применить $f$. Из такого определения вытекает неравенство $D(f \circ g) \leq D^{dt}(f) \cdot D(g)$ — дерево разрешения для $f$ легко преобразовать в протокол для $f \circ g$, в котором каждому запросу $f$ соответствует вычисление функции $g$ при помощи $D(g)$ битов.

Раз и Маккинзи исследовали вопрос: можно ли доказать обратное неравенство, т. е. неравенство вида $D(f \circ g) = \Omega(D^{dt}(f) \cdot D(g))$. Надежды на то, что оно выполнено для всех $f$ и $g$, нет — достаточно рассмотреть пример

$$f(x_1, x_2, \ldots, x_n) = x_1 \oplus x_2 \oplus \ldots \oplus x_n, \qquad g(x, y) = x \oplus y.$$

Тем не менее, Раз и Маккинзи доказали, что если взять в качестве $g$ «функцию адресации»:

$$\mathrm{IND}_k : \{0,1\}^k \times \{1, \ldots, k\} \to \{0,1\}, \qquad \mathrm{IND}_k(y, x) = y_x,$$

то неравенство $D(f \circ \mathrm{IND}_k) = \Omega(D^{dt}(f) \cdot D(\mathrm{IND}_k))$ будет выполнено для всех $f$ арности не более $k^{1/20}$ (арностью $f$ мы называем количество переменных $f$, выше это число обозначалось через $n$).

---

[14]E. Kushilevitz, R. Ostrovsky, Y. Rabani. Efficient Search for Approximate Nearest Neighbor in High Dimensional Spaces. // SIAM Journal on Computing. — 2000. — V. 30. №. 2. — P. 457-474.

[15]A. C.-C. Yao. On the Power of Quantum Fingerprinting. // Proceedings of 35th annual ACM symposium on Theory of computing. — 2003. — P. 77-81.

[16]W. Huang, Y. Shi, S. Zhang, Y. Zhu. The Communication Complexity of the Hamming Distance Problem. // Information Processing Letters. — 2006. — V. 99. №. 4. — P. 149-153.

[17]H. Buhrman, R. Cleve, A. Wigderson. Quantum vs Classical Communication and Computation. // Proceedings of the 30th annual ACM symposium on Theory of computing. — 1998. — P. 63-68.

[18]D. Gavinsky, J. Kempe, R. De Wolf. Quantum Communication Cannot Simulation a Public Coin. // arXiv preprint quant-ph/0411051. – 2004.

[19]R. Raz, P. McKenzie. Separation of the Monotone NC Hierarchy. // Combinatorica. — 1999. — V. 19. №. 3. — P. 403-435.

[20]H. Buhrman, R. De Wolf. Complexity Measures and Decision Tree Complexity: a Survey. // Theoretical Computer Science. — 2002. — V. 288. №. 1. — P. 21-43.

Примечательно в этом результате то, что коммуникационная сложность оценивается снизу через вопросную. Считается общепринятым, что нижние оценки на вопросную сложность зачастую намного легче получать, чем на коммуникационную сложность. При этом теорема Раза — Маккинзи автоматически преобразует нижние оценки на вопросную сложность в нижние оценки на коммуникационную сложность. В литературе такого рода результаты называются *лифтингом* (подъемом нижних оценок из более простой модели в более сложную). В данной области используется еще один специфический термин — функция $g$ называется гаджетом. Это отражает тот факт, что $g$ используется для «переноса» сложности «внешней» функции $f$.

Благодаря методу лифтинга, изобретенному Разом и Маккинзи, было получено много прорывных результатов в разных областях сложности вычислений. Например, сами Раз и Маккинзи при помощи своего метода (а также на основе упомянутой выше работы Вигдерсона и Карчмера) доказали неравенство сложностных классов $\mathrm{mNC}^i$ и $\mathrm{mNC}^{i+1}$ для всех $i \in \mathbb{N}$. В серии работ Ватсона, Гуса и Питасси при помощи лифтинга Раза – Маккинзи и его обобщений были выведены разделения между различными моделями в коммуникационной сложности из разделений соответствующих им моделей в вопросной сложности[21,22,23]. Техника лифтинга также использовалась в сложности доказательств и схем[24,25] и в нижних оценках для структур данных[26].

Помимо этого, работы[27,28] пытались ослабить ограничения на арность $f$ в теореме Раза — Маккинзи. Напомним, что неравенство $D(f \circ \mathrm{IND}_k) = \Omega(D^{dt}(f) \cdot D(\mathrm{IND}_k))$ было доказано лишь для $f$, арность которых не превосходит некоторой степени от длины входа гаджета $\mathrm{IND}_k$ (при чем эта степень даже меньше единицы). В упомянутых работах удалось для других гаджетов получить аналогичный результат для всех $f$, арность которых экспоненциальна по длине входа гаджета. Кроме того, в работе Чаттопадхая и др. был даже сформулирован признак того, что для гаджета выполнен аналог лифтинга Раза — Маккинзи. Признак заключается в наличии так называемых протыкающих распределений в коммуникационной матрице гаджета. Тем не менее, наличие протыкающих распределений с хорошими параметрами было доказано лишь для нескольких примеров гаджетов. В диссертации будет представлен новый метод получения таких примеров, а также будут исследованы ограничения этой техники.

Еще одна сложностная мера, про связь которой с коммуникационной сложностью будет идти речь в диссертации, называется информационной сложностью. Впервые информационная сложность была введена в работе[29]. В этой области предлагается измерять не только

[21] M. Göös, T. Pitassi, T. Watson. Deterministic Communication vs Partion Number. // Proceedings of the IEEE 56th Annual Symposium on Foundations of Computer Science. — 2015. — P. 1077-1088.

[22] M. Göös, T. Pitassi, T. Watson. Query-to-Communication Lifting for BPP. // Proceedings of the IEEE 58th Annual Symposium on Foundations of Computer Science. — 2017. — P. 132-143.

[23] M. Göös, P. Kamath, T. Pitassi, T. Watson. Query-to-Communication Lifting for $\mathrm{P}^{\mathrm{NP}}$. // Proceedings of the 32nd Computational Complexity Conference. — 2017. — Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik

[24] S.F. de Rezende, J. Nordström, M. Vinyals. How Limited Interaction Hinders Real Communication (and What It Means for Proof and Circuit Complexity). // Proceedings of the IEEE 57th Annual Symposium on Foundations of Computer Science. — 2016. — P. 295-304.

[25] A. Garg, M. Göös, P. Kamath, D. Sokolov. Monotone circuit lower bounds from resolution. // Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing. — 2018. — P. 902-911.

[26] A. Chattopadhyay, M. Koucký, B. Loff, S. Mukhopadhyay. Simulation Beats Richness: New Data-Structures Lower Bounds. // Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing. — 2018. — P. 1013-1020.

[27] X. Wu, P. Yao, H. S. Yuen. Raz-McKenzie Simulation with the Inner Product Gadget. // Electronic Colloquium on Computational Complexity (ECCC). — 2017. — https://eccc.weizmann.ac.il/report/2017/010.

[28] A. Chattopadhyay, M. Koucký, B. Loff, S. Mukhopadhyay. Simulation Theorems vis Pseudorandom Properties. // arXiv preprint arXiv:1704.06807. – 2017.

[29] Z. Bar-Yossef, T. S. Sayram, R. Kumar, D. Sivakumar. An Information Statistics Approach to Data Stream

коммуникационную длину, но и так называемое *информационное разглашение* коммуникационных протоколов. Грубо говоря, информационное разглашение протокола равно количеству информации, которое игроки (Алиса и Боб) узнали из протокола о входе противоположного игрока. Точное определение можно дать при помощи Шенновской теории информации.

В первую очередь здесь надо отметить то, что информационное разглашение не может превосходить коммуникационной длины (один бит, посланный по каналу, приносит максимум один бит информации принимающему и ничего — посылающему). Можно легко придумать пример, когда разглашение будет намного меньше — игроку посылают друг другу случайные биты, не зависящие от входа. Более содержательным примером является следующий протокол. Пусть Алиса и Боб пересылают другу другу биты своих входов по очереди, пока не будет найдено первое различие. Коммуникационная длина такого протокола будет порядка $n$, где $n$ — длина входа. В то же время его информационное разглашение не будет превосходить $O(\log n)$. Дело в том, что игроки, по сути, узнают только номер первого различия, которое может быть задано порядка $\log n$ битами.

Основным применением информационной сложности является так называемая проблема прямой суммы в коммуникационной сложности (см. обзор[30]). Ее суть в том, можно ли вычислить с точки зрения коммуникационной сложности $n$ копий функции в среднем быстрее, чем одну копию. Оказывается[31], что аналогичное утверждение неверно для информационной сложности. Таким образом подходом к проблеме прямой суммы в коммуникационной сложности может быть более подробное исследование связи коммуникационной сложности с информационной.

Такого рода результаты о связи этих двух сложностных мер известны в литературе как *сжатие* коммуникационных протоколов. Типичный результат о сжатии формулируется так. Показывается, что протокол с маленьким информационным разглашением можно преобразовать в протокол, делающий «то же самое» (например, вычисляющий ту же функцию), с маленькой коммуникационной длиной. В идеале мы хотим, чтобы коммуникационная длина результирующего протокола была ограничена с точностью до мультипликативной константы информационным разглашением исходного протокола. Для произвольных протоколов такого достичь не удается, известны лишь частичные результаты[32,33]. Но, например, для протоколов, использующих только общие случайные биты, доказаны почти что оптимальные результаты о сжатии[34,35,36]. Это обстоятельство мотивирует вопрос о роли частных случайных битов в информационной сложности. Точнее, всегда ли можно так сгенерировать частные случайные биты в общем источнике случайности, чтоб информационная сложность не сильно увеличилась? В литературе был дан положительный ответ на этот вопрос для однораундовых протоколов, то есть для протоколов, в которых передает всегда только один игрок[37,38].

---

and Communication Complexity. // Journal of Computer and System Sciences. — 2004. — V. 64 №. 4. — P. 702-732.

[30]O. Weinstein. Information Complexity and the Quest for Interactive Compression. // ACM SIGACT News. — 2015. — v. 46. №. 2.— P. 41-64.

[31]B. Barak, M. Braverman, X. Chen, A. Rao. How to Compress Interactive Communication. // SIAM Journal on Computing. — 2013. — V. 42. №. 3. — P. 1327-1363.

[32]B. Barak, M. Braverman, X. Chen, A. Rao. How to Compress...

[33]M. Braverman. Interactive Information Complexity. // SIAM Journal on Computing. — 2015. — V. 44. №. 6. — P. 1698.-1739.

[34]J. Brody, H. Buhrman, M. Koucky, B. Loff, F. Speelman, N. Vereshchagin. Towards a Reverse Newman's Theorem in Interactive Information Complexity. // Algorithmica. — 2016. — V. 76. №. 3. — P. 749-781.

[35]D. Pankratov. Direct Sum Questions in Classical Communication Complexity. — Master's thesis, University of Chicago. — 2012.

[36]B. Bauer, S. Moran, A. Yehudayoff. Internal Compression of Protocols to Entropy. // Proceedings of the 18th international conference on Approximation and the 19th International conference on Randomization, and combinatorial optimization: algorithms and techniques. — 2015. — P. 481-496.

[37]J. Brody, H. Buhrman, M. Koucky, B. Loff, F. Speelman, N. Vereshchagin. Towards a Reverse...

[38]M. Braverman, A. Garg. Public vs Private Coin in Bounded-Round Information. // Proceedings of the 41st Internationa Colloquium on Automata, Languages and Programming. — 2014. — P. 502-513.

В диссертации будет получена некая нетривиальная оценка для произвольных протоколов, которая однако позволяет лишь передоказать, а не усилить предыдущие результаты о сжатии.

Наконец, в диссертации будет рассмотрен еще один вопрос, берущий свое начало из теории информации. А именно, будут исследованы интерактивные аналоги теоремы Вольфа — Слепяна[39]. Также, как в этой теореме, мы будем предполагать, что имеется посылающий (Алиса) и принимающий (Боб), причем на входе у Алисы случайная величина $X$, а у Боба — случайная величина $Y$. Задача Алисы — передать $X$ Бобу. Случайные величины $X$ и $Y$ совместно распределены, поэтому $Y$ можно воспринимать как частичную информацию об $X$ у Боба (подчеркнем, что $Y$ не виден Алисе!)

Будет несколько отличий от исходной формулировки теоремы Вольфа — Слепяна. Во-первых случайные величины $X$ и $Y$ предполагаются произвольными; в частности не требуется, чтобы они были получены в результате большого числа независимых испытаний. Кроме того, Бобу будет разрешено посылать сообщения Алисе (раньше передавала только Алиса). Этим изменением исходной формулировки объясняется связь с коммуникационной сложностью. Кроме того, нас будет интересовать средняя длина коммуникации, а не длина в худшем случае.

В подобной постановке за последние годы в литературе было получено несколько верхних оценок[40,41,42]. В диссертации будут усилены эти верхние оценки, а также будут получены нижние.

## Цели и задачи исследования

Целью данной работы является получение новых результатов о связи коммуникационной сложности с другими сложностными мерами, а именно с информационной сложностью и с вопросной сложностью, а также получение новых оценок на коммуникационную сложность конкретных функций.

## Объект и предмет исследования

Основным объектом и предметом исследования данной работы является коммуникационная сложность. Исследуются также и другие сложностные меры, такие как информационная сложность и вопросная сложность, их взаимосвязь с коммуникационной сложностью.

## Научная новизна

Полученные в диссертации результаты являются новыми.

## Теоретическая и практическая значимость

Работа имеет теоретический характер. Полученные результаты представляют интерес для специалистов в области коммниукационной сложности, схемной сложности, вопросной сложности, интерактивного кодирования из Московского Государственного Университета имени

[39]D. Slepian, J. Wolf. Noiseless Coding of Correlated Information Sources. // IEEE Transactions on Information Theory. — 1973. — V. 19. №. 4. — P. 471-480.

[40]M. Braverman, A. Rao. Information Equals Amortized Communication. // IEEE Transactions on Information Theory. — 2014. — V. 60. №. 10. — P. 6058-6069.

[41]J. Brody, H. Buhrman, M. Koucky, B. Loff, F. Speelman, N. Vereshchagin. Towards a Reverse...

[42]M. Braverman, A. Rao, O. Weinstein, A. Yehudayoff. Direct Product via Round-Preserving Compression. // Proceedings of the 40th International Colloquium on Automata, Languages and Programming. — 2013. — P. 502-513.

М. В. Ломоносова, Санкт-Петербургского Государственного Университета, математического института имени В. А. Стеклова Российской Академии наук и других академических институтов и университетов.

## Основные методы исследования

В работе используются комбинаторные и вероятностные методы. Применены различные технические инструменты из теории информации (цепное правило, неравенство Пинскера) и из теории псевдослучайности (хеш-функции, экспандеры).

## Основные положения, выносимые на защиту

На защиту выносятся: обоснование актуальности, научная значимость работы, а также следующие положения, которые подтверждаются результатами исследования, представленными в заключении диссертации.

1. Нижняя оценка $\Omega(L^2/U+1)$ и верхняя оценка $O((L^2/U+1)\log L)$ на сложность функции $\mathrm{GHD}(n, L, U)$ с односторонней ошибкой (когда нельзя ошибаться на входах на расстоянии не больше $L$), а также SMP-протокол, доказывающий верхнюю оценку.

2. Способ, как из экспандеров получать гаджеты с протыкающими распределениями. Новый гаджет с рекордным взаимоотношением между арностью внешней функции и длиной входа гаджета, полученный при помощи этого способа. Невозможность улучшить это взаимоотношение при помощи текущей техники.

3. Способ безошибочно моделировать протоколы с частными случайными битами протоколами с общими случайными битами так, что информационное разглашение моделирующего протокола не превосходит $O(\sqrt{Id})$, где $I$ и $d$ — информационное разглашение и коммуникационная длина исходного протокола.

4. Протокол, решающий задачу Вольфа – Слепяна для пары случайных величин $X, Y$ с вероятностью ошибки $\varepsilon$, со средней длиной не более $(1 + 1/r)H + r + O(\log(1/\varepsilon))$ и со средним количеством раундов не более $2H/r+2$, где $H = H(X|Y)$ — условная энтропия $X$ при известном $Y$, а $r$ — произвольное натуральное число. Пример случайных величин $X, Y$, показывающий, что от члена порядка $O(\log(1/\varepsilon))$ в верхней оценке избавиться нельзя.

## Достоверность

Достоверность результатов исследования подтверждается теоретическими выкладками, а также сравнением с результатами других исследователей.

## Апробация работы

Основные результаты, полученные в диссертации, докладывались на следующих научных семинарах и конференциях:

- Колмогоровский семинар по сложности вычислений и сложности определений, механико-математический факультет МГУ им. М. В. Ломоносова, 2014–2018 гг.

- Научно-исследовательский семинар кафедры математической логики и теории алгоритмов, механико-математический факультет МГУ им. М. В. Ломоносова, 2018 год.

- Конференция “10th International Computer Science Symposium in Russia” в Листвянке в 2015 году.
- Конференция “Проблемы теоретической информатики” в Москве в 2015 году.
- Воркшоп “Algorithms in Communication Complexity, Property Testing and Combinatorics” в Москве в 2016 году.
- Конференция “11th International Computer Science Symposium in Russia” в Санкт-Петербурге в 2016 году.
- Конференция “Проблемы теоретической информатики” в Москве в 2016 году.
- Конференция “43rd International Symposium on Mathematical Foundations of Computer Science” в Ливерпуле в 2018 году.

На конференции “International Computer Science Symposium in Russia” в Санкт-Петербурге в 2016 году работа автора получила награду Yandex Best Student Paper Award.

### Публикации автора

Работа автора, посвященная роли частных случайных битов в информационной сложности, опубликована в сборнике трудов конференции “10th International Computer Science Symposium in Russia” ([1], Серия Lecture Notes in Computer Science, входит в систему Scopus). Работа автора, посвященная интерактивному аналогу теоремы Вольфа — Слепяна, опубликована в специальном выпуске журнала Theory of Computing Systems ([2], входит в систему Web of Science). Работа, посвященная задаче Gap Hamming Distance (совместная с Е. Клениным) и работа о теореме Раза — Маккинзи опубликованы в сборнике трудов конференции “43rd International Symposium on Mathematical Foundations of Computer Science” ([4,5], серия Leibniz International Proceedings in Informatics, входит в систему Scopus).

### Структура и объем диссертационной работы диссертации

Диссертация состоит из введения, обзора основных понятий, четырех глав, излагающих основные результаты диссертации, заключения и списка литературы из 49 наименований. Общий объем диссертации составляет 81 страниц, включая 74 страницы основного текста.

## Основное содержание работы

Во **введении** описывается актуальность темы, цели работы, список основных результатов, список используемых обозначений, сведения о публикациях автора и об апробации работы.

**Глава 1** является обзором основных понятий и определений. В начале в ней перечислены используемые в дальнейшем в доказательствах технические факты из комбинаторики, теории вероятностей, теории информации и теории псевдослучайности. Затем в ней даются все необходимые определения и вспомогательные утверждения, касающиеся коммуникационной, информационной и вопросной сложности.

В **главе 2** проводится исследование коммуникационной сложности задачи Gap Hamming Distance с односторонней ошибкой. Сначала доказывается нижняя оценка $R^0(\mathrm{GHD}(n, L, U)) = \Omega(L^2/U + 1)$.Благодаря серии очевидных сведений

$$R^0(\mathrm{GHD}(n, L, U)) \geq R^0(\mathrm{GHD}(U, L, U)) = R^1(\mathrm{GHD}(U, 0, U - L),$$

легко видеть, что достаточно исследовать только величину $R^1(\mathrm{GHD}(p,0,q))$. В соответствующей коммуникационной задаче Алиса и Боб получают по $p$-битовой строке, причем их строки либо равны, либо расстояние Хемминга между ними не меньше $q$. Надо определить, какой из случаев имеет место, причем ошибаться нельзя во втором случае. Для этой задачи, используя теорему Клейста из экстремальной комбинаторики, мы доказываем нижнюю оценку $\Omega((p-q)^2/p+1)$. Подставляя $p=U$, $q=U-L$, мы получаем требуемую оценку $\Omega(L^2/U+1)$.

Основное содержание второй главы относится к верхней оценке. А именно, строится SMP-протокол с общими случайными битами длины не более $O((L^2/U+1)\log L)$ для задачи $\mathrm{GHD}(n,L,U)$, не ошибающийся на входах на расстоянии не больше $L$. Построение этого протокола происходит в несколько этапов. На первом этапе строится так называемый HT-протокол (HT расшифровывается как неравенство треугольника). Этот протокол основан на четырех идеях. Первая идея заключается в *использовании неравенства треугольника* для получения односторонней ошибки. Более подробно, пусть Алиса и Боб получают по $n$-битовой строке, $x$ и $y$. Алиса и Боб в общем источнике случайности генерируют с равномерным распределением строку $r$ и пересылают Чарли расстояния от $x$ и $y$ до $r$. После этого Чарли в состоянии вычислить величину $|d(x,r)-d(y,r)|$. Предположим Чарли выдает 0, если эта величина не превосходит $L$. Поскольку по неравенству треугольника $|d(x,r)-d(y,r)|\le d(x,y)$, то при вычислении $\mathrm{GHD}(n,L,U)$ Чарли никогда не ошибается на $(x,y)$ таких, что $d(x,y)\le L$. Но что если $d(x,y)\ge U$? Здесь вступает в игру вторая идея, а именно *идея использования случайного блуждания* для оценки $|d(x,r)-d(y,r)|$ снизу. Показывается, что с отделенной от нуля вероятностью (по выбору $r$) величина $|d(x,r)-d(y,r)|$ не меньше $\sqrt{d(x,y)}$. Легко понять, что эти соображения дают протокол с длиной $O(\log n)$ для вычисления $\mathrm{GHD}(n,L,U)$ с односторонней ошибкой при $U>L^2$. Это почти что соотносится с заявленной верхней оценкой, которая для таких $L$ и $U$ имеет вид $O(\log L)$. Что же делать, когда $U$ существенно меньше $L^2$? Для этого случая используется *идея разбиения на блоки*, заключающаяся в следующей модификации описанного выше протокола. Разобьем строки $x$ и $y$ на $k$ блоков, $x_1$ и $y_1$, $x_2$ и $y_2$ и так далее, и для каждого блока $i$ в общем источнике случайности выберем случайную строку $r_i$ той же длины. Тогда выражение

$$\sum_{i=1}^{k}|d(x_i,r_i)-d(y_i,r_i)|, \tag{1}$$

как и раньше, согласно неравенству треугольника, будет нижней оценкой для $d(x,y)$. На вычисление этого выражения уйдет $O(k\log n)$ битов коммуникации. Если Чарли всегда будет выдать 0, когда это выражение не превосходит $L$, то ошибка при вычислении $\mathrm{GHD}(n,L,U)$ будет односторонняя. Это опять же оставляет вопрос, что делать, когда на входе строки на расстоянии хотя бы $U$. Для этого у нас еще остается свобода в выборе способа разбиения на блоки. Последняя, четвертая идея заключается в *случайном разбиении на блоки*. Более точно, каждая координата входа попадает в $i$-й блок с вероятностью $1/k$, выбор для разных координат делается независимо. Тогда с отделенной от нуля вероятностью для константной доли блоков величина $d(x_i,y_i)$ будет не меньше $\Omega(d(x,y)/k)$ (именно столько, $d(x,y)/k$, будет в среднем отличий у строк $x_i$ и $y_i$). С другой стороны, по тем же соображениям со случайным блужданием, константная доля слагаемых в сумме (1) будет давать вклад не меньше $\Omega(\sqrt{d(x,y)/k})$. Значит с отделенной от нуля вероятностью сумма (1) будет не меньше $\Omega(k\sqrt{d(x,y)/k})=\Omega(\sqrt{k\cdot d(x,y)})$, что при $k=O(L^2/U)$ больше $L$ (для $(x,y)$ таких, что $d(x,y)\ge U$).

HT-протокол передает не более $O((L^2/U+1)\log n)$ бит и решает задачу $\mathrm{GHD}(n,L,U)$ с односторонней ошибкой для всех $L,U$ таких, что $U/L>C$, где $C$ — некоторая положительная абсолютная константа. Последнее ограничение техническое и возникает на этапе случайного разбиения на блоки. Тем не менее, это препятствие легко преодолеть при

помощи протокола из работы Гавинского и др.[43] Этот протокол является простой модификацией известного в литературе SMP-протокола для функции EQ. Он решает задачу $\mathrm{GHD}(n, L, L{+}1)$ с односторонней ошибкой, передавая $O(L \log n)$ бит. Поскольку при $U/L \le C$ выражение $O(L \log n)$ есть $O((L^2/U) \cdot \log n)$, то мы для всех $L, U$ и $n$ получаем оценку $R^0(\mathrm{GHD}(n, L, U)) = O((L^2/U + 1) \log n)$.

Нам еще требуется сделать эту оценку не зависящей от $n$, улучшив ее до $O((L^2/U + 1) \log L)$. Для этого мы сначала используем технику понижения размерности из работы Хуанга и др.[44] А именно, мы разбиваем $x, y$ случайно (как при построении HT-протокола) на $O(L^8)$ блоков. Каждый блок Алиса и Боб заменяют на сумму битов в блоке по модулю 2. В результате получаются строки $u$ и $v$ длины $O(L^8)$. Заметим, что всегда выполнено неравенство $d(u, v) \le d(x, y)$. С другой стороны, легко показать, что если $d(x, y) \le L^4$, то с большой вероятностью $d(u, v) = d(x, y)$. Поэтому можно запустить протокол, описанный в предыдущих параграфах, не на $(x, y)$, а на $(u, v)$. Ошибка, как и раньше, будет односторонняя, а длина протокола станет $O((L^2/U + 1) \log L)$ (поскольку запуск происходит на строках длины не $n$, а $O(L^8)$).

Остается рассмотреть случай $d(x, y) \ge L^4$. В этом режиме заявленная верхняя оценка имеет вид просто $O(\log L)$. Здесь мы применяем ту же идею, что и в HT-протоколе, но без разбиения на блоки. Алиса и Боб просто генерируют одну случайную $n$-битовую строку $r$. Алиса вычисляет $a = d(x, r)$, а Боб вычисляет $b = d(y, r)$. Разница между $a$ и $b$ по модулю либо не превосходит $L$ (если $d(x, y) \le L$), либо с большой вероятностью не меньше $L^2$ (если $d(x, y) \ge L^4$). Алисе и Бобу нужно отличить эти два случая. Тривиальный протокол для этой задачи передает $O(\log n)$ битов (Алиса и Боб просто обмениваются $a$ и $b$). Несложно, основываясь на простом хешировании, получить 1-раундовый протокол для этой задачи с коммуникацией $O(\log L)$. Для этого Алиса перешлет Бобу $O(\log L)$ хеш-значений $a$, после чего Боб определит, есть ли в $L$-окрестности $b$ числа с теми же, что и у $a$, хеш-значениями. Эта конструкция, однако, не переносится в SMP-модель. Дело в том, что третьему участнику, Чарли, который не знает $b$, хеш-значения Алисы ничего не скажут. В конце третьей главы мы устраняем этот недостаток, строя для той же задачи SMP-протокол длины $O(\log L)$. Проблема в том, что $a, b$ пробегают числа от 0 до $n$. Чтобы решить эту проблему, Алиса и Боб будут рассматривать все числа по модулю $4L + 2$. При этом числа $a$ и $b$, даже если они были очень далеки друг от друга, могут стать близки. Чтобы этого не допустить, Алиса и Боб заменят $a$ и $b$ на $Z_0 + \ldots + Z_a$ и $Z_0 + \ldots + Z_b$, где $Z_0, \ldots, Z_n$ — независимые стандартные бернуллиевские случайные величины. Основной технический результат здесь заключается в том, что если $|a - b| > L^2$, то разница между $Z_0 + \ldots + Z_a$ и $Z_0 + \ldots + Z_b$ будет почти что равномерно распределена по модулю $4L + 2$. Это означает, что далекие друг от друга $a$ и $b$ с большой вероятностью так и останутся далеки.

В **главе 3** излагаются результаты, связанные с теоремой Раза-Маккинзи. Сначала нам нужно определить протыкающие распределения. Пусть $M$ — некоторая матрица размера $a \times b$, состоящая из нулей, единиц, а также из специальных символов неопределенности $\perp$. Ее подматрицу назовем *$i$-одноцветной*, если все элементы подматрицы равны $i$ (здесь $i \in \{0, 1\}$). Далее, рассмотрим распределение вероятностей $\mu$ на подматрицах матрицы $M$. Распределение $\mu$ назовем *$(\delta, h)$-протыкающим*, если для любой подматрицы $M'$ матрицы $M$ с хотя бы $2^{-h}a$ строками и хотя бы $2^{-h} \cdot b$ столбцами выполнено следующее: случайно выбранная по распределению $\mu$ подматрица с вероятностью не меньше $1 - \delta$ имеет с $M'$ общий элемент.

С произвольной функцией вида $g\colon \mathcal{X} \times \mathcal{Y} \to \{0, 1\}$, где $\mathcal{X}, \mathcal{Y}$ — некоторые конечные множества, можно связать матрицу $M_g$ с множеством столбцов $\mathcal{X}$, множеством строк $\mathcal{Y}$, у которой

[43] D. Gavinsky, J. Kempe, R. De Wolf. Quantum Communication...

[44] W. Huang, Y. Shi, S. Zhang, Y. Zhu. The Communication Complexity...

на пересечении строки $x \in \mathcal{X}$ и столбца $y \in \mathcal{Y}$ стоит $g(x, y)$. Чаттопадхай и др.[45] формулируют следующий результат, являющийся обобщением теоремы Раза — Маккинзи. Пусть $g : \mathcal{X} \times \mathcal{Y} \to \{0, 1\}$ —некоторая функция, у которой для любого $i \in \{0, 1\}$ в матрице $M_g$ есть $(1/1000, h)$-протыкающее распределение, сосредоточенное на $i$-одноцветных подматрицах $M_g$. Тогда для любого $\varepsilon \geq 6/h$ и любой булевой функции $f$ арности не более $2^{(1-\varepsilon)h}$ выполнено следующее неравенство:

$$D(f \circ g) \geq \frac{\varepsilon h}{4} \cdot D^{dt}(f).$$

Первым результатом четвертой главы является способ получения функций $g$ с хорошими протыкающими распределениями из *спектральных экспандеров*. Сначала опишем этот способ. Пусть $G = (V, E)$ — $d$-регулярный граф, в котором любые две различные вершины имеют не более одного общего соседа. Функции вида $c : V \to \{0, 1\}$ будем называть раскрасками $G$. Тогда корректно определена следующая частично-определенная функция:

$$g(G, c) : V \times V \to \{0, 1\},$$
$$g(G, c)(u, v) = \begin{cases} 1 & \text{если } u \neq v \text{ и } \exists w \in \Gamma(u) \cap \Gamma(v) \text{ т.ч. } c(w) = 1, \\ 0 & \text{если } u \neq v \text{ и } \exists w \in \Gamma(u) \cap \Gamma(v) \text{ т.ч. } c(w) = 0, \\ \perp & \text{иначе,} \end{cases}$$

где $\perp$ означает неопределенность, а через $\Gamma(s)$ обозначено множество соседей вершины $s$ в графе $G$. Назовем раскраску $c$ сбалансированной, если размер $c^{-1}(0)$ не меньше $|V|/3$ и не больше $2|V|/3$. Оказывается, что если $G$ является спектральным экспандером и $c$ сбалансирована, то $g(G, c)$ обладает хорошими протыкающими распределениями. А именно, выполнена следующая теорема:

**Теорема 1.** *Существует* ***полиномиальный*** *алгоритм со следующим свойством. Пусть граф $G = (V, E)$ — спектральный $(m, d, \gamma)$-экспандер, в котором у любых двух различных вершин есть не более одного общего соседа, а функция $c : V \to \{0, 1\}$ является его сбалансированной раскраской. Пусть также $m \geq 1/\gamma^2$. Тогда, получив на вход матрицу смежности $G$, таблицу истинности $c$ и бит $i \in \{0, 1\}$, алгоритм выдает последовательность пар*

$$(R_1, q_1), \ldots, (R_l, q_l)$$

*где $R_1, \ldots, R_l$ — различные $i$-одноцветные подматрицы $M_{g(G,c)}$, а $q_1, \ldots, q_l$ — неотрицательные рациональные числа, в сумме дающие единицу. Кроме того, распределение вероятностей $\mu_i$ на множестве $\{R_1, \ldots, R_l\}$, определенное следующим образом:*

$$\mu_i(R_1) = q_1, \ldots, \mu_i(R_l) = q_l,$$

*является $\left(\frac{1}{1000}, \lfloor 2 \log_2(1/\gamma) \rfloor - 100\right)$-протыкающим для матрицы $M_{g(G,c)}$.*

Заметим, что из явных конструкций экспандеров в последней теореме получаются явные протыкающие распределения (которые можно, грубо говоря, «выписать» за полиномиальное от размера матрицы время).

Мы применяем этот результат к следующему явному семейству экспандеров. Через $AP_q$ обозначим граф, вершинами которого являются пары элементов поля $\mathbb{F}_q$. Две вершины $(a, b), (x, y) \in \mathbb{F}_q$ соединяются ребром тогда и только тогда, когда в $\mathbb{F}_q$ выполнено равенство: $ax = b + y$. Хорошо известно, что граф $AP_q$ является спектральным $(q^2, q, 1/\sqrt{q})$-экспандером. Несложно убедиться в том, что в $AP_q$ у любых двух различных вершин не более одного общего соседа.

[45] A. Chattopadhyay, M. Koucký, B. Loff, S. Mukhopadhyay. Simulation Theorems...

Таким образом, варьируя сбалансированные раскраски графа $AP_q$, мы можем получать различные гаджеты с хорошими протыкающими распределениями. В частности, мы рассматриваем следующий, выглядящий относительно естественно, гаджет:

$$\mathrm{SQR}^q : \mathbb{F}_{q^2} \times \mathbb{F}_{q^2} \to \{0,1\},$$
$$\mathrm{SQR}^q(a,b) = \begin{cases} 1 & a-b \text{ является квадратом какого-то элемента } \mathbb{F}_{q^2}, \\ 0 & \text{иначе.} \end{cases}$$

Входы у функций $\mathrm{SQR}^q$ и $g(AP_q, c)$ можно естественным образом отождествить. Кроме того, можно показать, что найдется сбалансированная раскраска $c$ такая, что $g(AP_q, c)$ является подфункцией $\mathrm{SQR}^q$.

**Теорема 2.** *Для всех достаточно больших натуральных $q$, являющихся степенью нечетного простого числа, у графа $AP_q$ найдется сбалансированная раскраска $c$, таблица истинности которой вычислима за полиномиальное от $q$ время, такая, что везде, где функция $g(AP_q, c)$ определена, она равна функции $\mathrm{SQR}^q$.*

Благодаря последней теореме можно сказать следующее о гаджете $\mathrm{SQR}^q$. Во-первых, длина входа у этого гаджета равна $k = 2\log_2 q$. Из теоремы 1 вытекает, что у $\mathrm{SQR}^q$ есть два $\left(\frac{1}{10}, k/2 - O(1)\right)$-протыкающих распределения, одно сосредоточенное на 0-одноцветных, а другое на 1-одноцветных подматрицах. Благодаря тому, что матрица смежности $AP_q$, а также таблица истинности раскраски $c$ из теоремы 2 вычислимы за полиномиальное от $q$ время, соответствующие протыкающие распределения являются явными. Согласно работе Чаттопадхая и др.[46] это означает, что для гаджета $\mathrm{SQR}^q$ неравенство $D(f \circ \mathrm{SQR}^q) = \Omega(D^{dt}(f) \cdot k)$ выполнено для всех внешних функций $f$ арности $2^{(1/2-\Omega(1))k}$.

Протыкающие распределения с теми же параметрами известны и для гаджета $\mathrm{IP}_k$ (Чаттопадхай и др.) Значит в теореме Раза-Маккинзи для этого гаджета выполнено такое же соотношение между длиной входа гаджета и арностью внешней функции. Однако для $\mathrm{IP}_k$, в отличии от $\mathrm{SQR}^q$, явных протыкающих распределений неизвестно.

Можно ли вообще построить протыкающие распределения с лучшими, чем у $\mathrm{SQR}^q$ и $\mathrm{IP}_k$ параметрами? Мы отвечаем отрицательно в следующей

**Теорема 3.** *Для любого гаджета $g : \{0,1\}^k \times \{0,1\}^k \to \{0,1\}$ и любого целого $h \geq 1$ выполнено следующее. Существует $b \in \{0,1\}$ такое, что для любого распределения вероятностей $\mu$ на $b$-одноцветных подматрицах $M_g$ найдутся $X, Y \subset \{0,1\}^k$ размера хотя бы $2^{k-h}$ т. ч.*

$$\Pr_{R \sim \mu}[R \cap X \times Y \neq \varnothing] \leq 2^{k-2h+1}.$$

В частности эта теорема говорит, что для гаджета с длиной входа $k$ невозможно построить $(1-\Omega(1), (1/2+\Omega(1))k)$-протыкающих распределений над одноцветными подматрицами обоих типов.

Таким образом улучшить взаимоотношение между длиной входа гаджета и арностью внешней функции, просто улучшив протыкающие распределения, нельзя. Но откуда вообще берется ограничение на арность внешней функции в теореме Раза-Маккинзи для различных гаджетов? Можно убедиться, что единственным местом в доказательстве, в котором фигурирует эта арность, является так называема лемма о толщине. Сформулируем эту лемму.

Пусть $A$ — некоторое конечное множество, а $X$ — подмножество $A^n$ (здесь $n$ соответствует арности внешней функции). Через $X_{[n]/\{i\}}$ обозначим проекцию множества $X$ вдоль $i$-й координаты. Иными словами, множество $X_{[n]/\{i\}}$ получается из $X$ удалением $i$-й координаты. Определим вспомогательный двудольный граф $G_i(X)$. В левой доле этого графа находятся

[46] A. Chattopadhyay, M. Koucky, B. Loff, S. Mukhopadhyay. Simulation Theorems...

элементы множества $A$, а в правой — элементы $X_{[n]/\{i\}}$. Мы соединяем вершину $a$ из левой доли с вершиной $(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)$ из правой доли тогда и только тогда, когда

$$(x_1, \ldots, x_{i-1}, a, x_{i+1}, \ldots, x_n) \in X.$$

Минимальную степень вершины из правой доли графа $G_i(X)$ обозначим через $MinDeg_i(X)$, а среднюю степень вершин из правой доли (то есть $|X|/|X_{[n]/\{i\}}|$, количество ребер поделить на количество правых вершин) — через $AvgDeg_i(X)$.

Лемма о толщине связывает эти две величины. А именно, в ней показывается, что если $AvgDeg_i(X)$ велико для всех $i$, то существует подмножество $Y \subset X$, занимающее достаточно большую долю $X$ такое, что $MinDeg_i(Y)$ велико для всех $i$. Более точно:

**Лемма 1** (о толщине, Раз и Маккинзи). *Рассмотрим произвольные $\delta > 0$ и $X \subset A^n$. Предположим для любого $i \in \{1, 2, \ldots, n\}$ выполнено $AvgDeg_i(X) \geq d$. Тогда найдется $Y \subset X$ размера хотя бы $(1-\delta)|X|$ такое, что для любого $i \in \{1, 2, \ldots, n\}$ выполнено $MinDeg_i(Y) \geq \frac{\delta d}{n}$.*

Можно было бы улучшить взаимоотношение между длиной входа гаджета и арностью внешней функции в теореме Раза-Маккинзи, улучшив лемму о толщине. Например, если бы в этой лемме $\frac{\delta d}{n}$ можно было бы заменить на $\frac{\delta d}{\sqrt{n}}$, то для $g \in \{\mathrm{IP}_k, \mathrm{SQR}^q\}$ теорема Раза-Маккинзи выполнялась бы для всех внешних функций арности $2^{(1-\Omega(1))k}$, а не $2^{(1/2-\Omega(1))k}$.

Мы показываем, что лемма о толщине неулучшаема. Заметим, что в этой лемме ничего не говорится о том, существует ли вообще непустое $Y$ такое, что $MinDeg_i(Y) > \frac{d}{n}$ для всех $i \in \{1, 2, \ldots, n\}$. Мы приводим пример, когда такого $Y$ не существует. Более точно,

**Теорема 4.** *Для любого $\varepsilon > 0$ и для всех целых $n \geq 2, s \geq 1$ существует целое $m$ и множество $X \subset \{0, 1, \ldots, m\}^n$ такое, что*

- *для всех $i \in \{1, 2, \ldots, n\}$ выполнено $AvgDeg_i(X) \geq s(n - \varepsilon)$;*
- *не существует непустого $Y \subset X$ такого, что для всех $i \in \{1, 2, \ldots, n\}$ выполнено $MinDeg_i(Y) \geq s + 1$.*

В конце 3-й главы мы исследуем вопрос, насколько обременительно для нашей конструкции гаджетов из экспандеров ограничение, что у любых двух различных вершин есть не более одного общего соседа. Во-первых, мы показываем, что все экспандеры с такими же параметрами, как у $AP_q$, автоматически удовлетворяют этому ограничению.

**Теорема 5.** *Пусть граф $G$ является спектральным $(m, d, \gamma)$-экспандером и выполнено следующее:*

$$2d + 4 \geq d^2 \left(2\gamma^2 + \frac{4(1-\gamma^2)}{m}\right).$$

*Тогда любые две различные вершины $G$ имеют не более одного общего соседа.*

Из последней теоремы вытекает, что этому ограничению удовлетворяют все спектральные $(m^2, m, 1/\sqrt{m})$-экспандеры. Эта теорема является достаточными, но не необходимых условием, как показывает знаменитая конструкция графов Раманджана, принадлежащая Любоцкому, Филлипсу и Сарнаку[47]. На основе этой конструкции строятся хорошие спектральные экспандеры с рядом интересных комбинаторных свойств, из которых, в частности, вытекает, что любые две различные вершины в них имеют не более одного общего соседа. Однако для них условие из теоремы 5 не выполнено.

[47] A. Lubotzky, R. Phillips, P, Sarnak. Ramanujan Graphs. // Combinatorica. — 1988. — V. 8. №. 3. — P. 261-277.

**Глава 4** посвящена роли частных случайных битов в информационной сложности. Напомним, что основным результатом здесь является теорема о том, что любой вероятностный протокол с информационным разглашением $I$ и длиной $d$ можно безошибочно моделировать протоколом, не использующим частных случайных битов, информационное разглашение которого не превосходит $O(\sqrt{Id})$. Для доказательства этого утверждения мы сначала рассматриваем случай $d = 1$, то есть случай протоколов, в которых передается всего 1 бит. В этом случае информационное разглашение моделирующего протокола не должно превосходит $O(\sqrt{I})$, где $I$ — разглашение исходного однобитового протокола. Затем мы применяем этот результат побитово к исходному $d$-битовому протоколу. Информационное разглашение получающегося таким образом протокола, $I'$, мы оцениваем по неравенству Коши-Буняковского:

$$I' = O(\sqrt{I_1} + \ldots + \sqrt{I_d}) = O(\sqrt{(I_1 + \ldots + I_d)d}) = O(\sqrt{Id}).$$

Здесь через $I_i$, грубо говоря, обозначено информационное разглашение $i$-го бита исходного протокола.

Основным содержанием главы является случай однобитовых протоколов. Здесь мы применяем технику *совместного семплирования*, появившуюся еще в работе Барака и др.[48] Предположим для простоты, что исходный однобитовый протокол использует только частные случайные биты. Тогда на входе $x$ Алиса с какой-то вероятностью $p(x)$ посылает Бобу 0, а с оставшейся вероятностью — 1. Выбор, что послать, Алиса делает при помощи своих частных случайных бит. Мы будем моделировать этот протокол при помощи общих случайных битов так. В общем источнике будет сгенерировано случайное вещественное число $R \in [0, 1]$. Если оно меньше $p(x)$, Алиса пошлет 0, иначе 1. Как видно, вероятностью посылки нуля на любом входе $x$ у такого протокола та же самая — $p(x)$. Остается показать лишь оценку $O(\sqrt{I})$ на информационное разглашение этого протокола. Основным техническим инструментом здесь является неравенство Пинскера.

**Глава 5** посвящена интерактивному аналогу теоремы Вольфа — Слепяна. Пусть есть две совместно распределенные случайные величины, $X$ и $Y$. Алиса получает на вход значение $X$, а Боб — значение $Y$. Задача в том, чтобы Боб узнал $X$.

Если Алиса просто перешлет $X$ Бобу, то мы получим протокол с информационным разглашением $H(X|Y)$. Можно ли придумать протокол с примерно такой же коммуникационной длиной?

Впервые подобная задача была поставлена в статье Вольфа и Слепяна[49]. Их теорема посвящена случаю, когда $(X, Y)$ получены в результате $n$ независимых испытаний одной и той же пары совместно распределенных случайных величин. Тогда Алиса может послать одно сообщение фиксированной длины, а именно длины $H(X|Y)+O(\sqrt{n})$, прочитав которое, Боб с большой вероятностью сможет восстановить $X$. Наша задача отличается от теоремы Слепяна-Вольфа в трех отношениях: (а) распределение $X, Y$ может быть произвольным, (б) протокол передачи может быть многораундовым, (в) мы интересуемся средней длиной коммуникации, а не длиной в худшем случае.

Во-первых, мы усиливаем предыдущие верхние оценки для этой задачи. Наше усиление достигается более аккуратным анализом вероятности ошибки в протоколах из предыдущих работ.

Во-вторых, мы получаем первую нижнюю оценку на среднюю длину коммуникации, превышающую $H(X|Y)$. Доказательство представляет собой комбинацию достаточно стандартных техник коммуникационной сложности и теории информации: комбинаторные прямоугольники, выпуклость энтропии, энтропийная оценку на среднюю длину префиксного кода и т. д.

[48] B. Barak, M. Braverman, X. Chen, A. Rao. How to Compress...

[49] D. Slepian, J. Wolf. Noiseless Coding of Correlated Information Sources. // IEEE Transactions on Information Theory. — 1973. — V. 19. №. 4. — P. 471-480.

В **заключении** перечисляются основные результаты диссертации.

# Заключение

Работа содержит четыре основных результата, один совместный и три полученных без соавторов.

Первый результат (полученный совместно с Е. Клениным) относится к коммуникационной сложности задачи Gap Hamming Distance с односторонней ошибкой. А именно, доказывается нижняя оценка $\Omega(L^2/U+1)$ и верхняя оценка $O((L^2/U+1)\log L)$ на сложность функции $\mathrm{GHD}(n, L, U)$ с односторонней ошибкой (когда нельзя ошибаться на входах на расстоянии не больше $L$). Таким образом указанная величина вычислена с точностью до множителя порядка $O(\log L)$. Показывается, что верхняя оценка выполнена также для SMP-протоколов (в которых Алиса и Боб не общаются между собой, а посылают по сообщению третьему игроку, Чарли, который, не видя входов Алисы и Боба, вычисляет ответ).

Второй результат связан с теоремой Раза — Маккинзи. Во-первых, предложен способ, как из экспандеров получать гаджеты с хорошими протыкающими распределениями. Из экспандера, основанного на аффинной плоскости над конечным полем, получено новое семейство гаджетов, для которого верен аналог теоремы Раза — Маккинзи. При этом взаимотношение между арностью внешней функции и длиной входа гаджета у этого семества такое же, как у гаджета из работы Чаттопадхая и др.[50] (у других гаджетов, изучавшихся в литературе, оно хуже). Кроме того, получен ряд результатов, показывающих, что улучшить это взаимотношение с текущей техникой нельзя. А именно, показано, что не существует гаджетов с лучшими, чем у нашего нового семейства гаджетов, протыкающими распределениями. Также доказана неулучшаемость леммы о толщине (Thickness Lemma) — технического утверждения из доказательства теоремы Раза — Маккинзи. Наконец, мы показываем, что наша конструкция протыкающих распределений явная в том смысле, что носитель протыкающего распределения может быть выписан за полиномиальное от размера матрицы гаджета время (для упомянутого выше гаджета из работы Чаттопадхая и др.[51] это неизвестно). Интерес к явным протыкающим распределениям мотивируется как шаг к эффективному варианту теоремы Раза — Маккинзи.

Третий результат исследует роль частных случайных битов в информационной сложности. Доказывается, что любой протокол с частными случайными битами можно безошибочно моделировать протоколом, не использующим частных случайных битов, так, что информационное разглашение моделирующего протокола не превосходит $O(\sqrt{Id})$, где $I$ и $d$ — информационное разглашение и коммуникационная длина исходного протокола. Под безошибочным моделированием мы понимаем следующее: на любой паре входов коммуникация у исходного и у моделирующего протокола имеет одно и то же распределение. Из этого результата можно вывести новое доказательство сжатия из работы Барака и др.[52]

Четвертый результат относится к интерактивному аналогу теоремы Вольфа — Слепяна. Показано, что для любого натурального $r$ и любого $\varepsilon$ задачу Вольфа — Слепяна для пары случайных величин $X, Y$ можно решить с вероятностью ошибки $\varepsilon$ при помощи протокола со средней длиной не более $(1+1/r)H + r + O(\log(1/\varepsilon))$ и со средним количеством раундов не более $2H/r + 2$, где $H = H(X|Y)$ — условная энтропия $X$ при известном $Y$. Отсюда для любого $\alpha \in [1/2, 1]$, подобрав нужное $r$, легко получить протокол со средней длиной $H + O(H^\alpha)$ и со средним числом раундов $O(H^{1-\alpha})$. Ранее такая оценка была известна лишь

[50] A. Chattopadhyay, M. Koucký, B. Loff, S. Mukhopadhyay. Simulation Theorems...

[51] A. Chattopadhyay, M. Koucký, B. Loff, S. Mukhopadhyay. Simulation Theorems...

[52] B. Barak, M. Braverman, X. Chen, A. Rao. How to Compress...

для $\alpha = 1/2$[53] и для $\alpha = 1$[54,55]. Кроме того, если минимизировать лишь среднюю длину и забыть о числе раундов, то, положив, $r = \sqrt{H}$, мы получаем оценку $H + 2\sqrt{H} + O(\log(1/\varepsilon))$, что немного улучшает оценку $H + 5\sqrt{H} + O(\log(1/\varepsilon))$ из работы Бравермана и Рао[56]. Кроме того, в этой главе мы исследуем вопрос о возможности дальнейших улучшений этих оценок. Мы показывем, грубо говоря, что в общем случае от члена порядка $O(\log(1/\varepsilon))$ избавиться нельзя. Более точно, для любого натурального $n$ мы приводим пример случайных величин $X$ и $Y$, принимающих $n$ возможных значений, для которых выполнена следующая нижняя оценка. Любой протокол, решающий для них задачу Вольфа — Слепяна с ошибкой $\varepsilon$ при $\log_2 n \leq 1/\varepsilon \leq n$, передает в среднем не меньше $H(X|Y) + \Omega(\log(1/\varepsilon))$ бит. Константа в $\Omega(\cdot)$ может быть сделана сколь угодно близкой к единице.


## Благодарности

Автор глубоко признателен своему научному руководителю Николаю Константиновичу Верещагину за неоценимую помощь при работе над диссертацией и постоянную поддержку.


# Список публикаций автора по теме диссертации

## Статьи в рецензируемых научных изданиях, рекомендуемых для защиты в диссертационном совете МГУ по специальности

[1] Alexander Kozachinskiy. Making randomness public in unbounded-round information complexity // Proceedings of the 10th International Computer Science Symposium in Russia. – 2015. – Lecture Note in Computer Science, Springer, V. 9139. – P. 296-309.
DOI: 10.1007/978-3-319-20297-6_19. Импакт-фактор: Scopus — 1,174.

[2] Alexander Kozachinskiy. On Slepian-Wolf theorem with interaction // Theory of Computing Systems. – 2018. – V. 62, №3. – P. 583-599. DOI: 10.1007/s00224-016-9741-x. Импакт-фактор: Scopus — 0,950; Web of Science — 0.604.

[3] Egor Klenin, Alexander Kozachinsiy. One-sided error communication complexity of Gap Hamming Distance // Proceedings of the 43rd International Symposium on Mathematical Foundations of Computer Science. – 2018. – Leibniz International Proceedings in Informatics, V. 117. – P. 7:1-7:15. DOI: 10.4230/LIPIcs.MFCS.2018.7. Импакт-фактор: Scopus — 0,940.

*Автору принадлежит доказательство следствия 4 (нижняя оценка). В доказательстве теоремы 2 (верхняя оценка) Е. Кленину принадлежит конструкция HT-протокола, а автору принадлежит анализ HT-протокола (Лемма 15), а также следующие за HT-протоколом шаги доказалъства.*

[4] Alexander Kozachinsiy. From expanders to hitting distributions and simulation theorems // Proceedings of the 43rd International Symposium on Mathematical Foundations of Computer Science. – 2018. – Leibniz International Proceedings in Informatics, V. 117. – P. 4:1-4:15.
DOI:10.4230/LIPIcs.MFCS.2018.4. Импакт-фактор: Scopus — 0,940.

[53] M. Braverman, A. Rao. Information Equals...
[54] J. Brody, H. Buhrman, M. Koucky, B. Loff, F. Speelman, N. Vereshchagin. Towards a Reverse...
[55] M. Braverman, A. Rao, O. Weinstein, A. Yehudayoff. Direct Product...
[56] M. Braverman, A. Rao. Information Equals...