Летняя школа «Современная математика»
Дубна, июль 2009

А. А. Разборов

Коммуникационная сложность

Перевод с английского Ю. Л. Притыкина
под редакцией В. А. Клепцына и С. М. Львовского

Москва
Издательство МЦНМО
2012

УДК 510.52
ББК 22.12
Р17

Разборов А. А.

Р17 Коммуникационная сложность / Перев. с англ. Ю. Л. Притыкина под ред. В. А. Клепцына и С. М. Львовского. — М.: МЦНМО, 2012. — 24 с.

ISBN 978-5-4439-0202-9

Текст брошюры является переводом статьи «Communication complexity», опубликованной в сборнике «An Invitation to Mathematics: From Competitions to Research», D. Schleicher, M. Lackmann (eds.), Springer, 2011, при написании которой использовались материалы курса, прочитанного автором в 2009 году в Летней школе «Современная математика».

В брошюре рассказывается об основных понятиях теории коммуникационной сложности, и приводятся как начальные утверждения этой теории, так и формулировки открытых проблем.

Книга представляет интерес для широкого круга подготовленных читателей, интересующихся математикой.

ББК 22.12

Александр Александрович Разборов

Коммуникационная сложность

Издательство Московского центра
непрерывного математического образования
119002, Москва, Большой Власьевский пер., 11. Тел. (499) 241-74-83

Подписано в печать 23.05.2012 г. Формат $60\times90\,1/16$. Бумага офсетная.
Печать офсетная. Печ. л. 1,5. Тираж 1000. Заказ .

Отпечатано с готовых диапозитивов в ООО «Принт Сервис Групп».
105187, Москва, ул. Борисовская, д. 14.

Книги издательства МЦНМО можно приобрести в магазине
«Математическая книга», Большой Власьевский пер., д. 11.
Тел. (499) 241-72-85. E-mail: biblio@mccme.ru

ISBN 978-5-4439-0202-9

1. Введение

Как можно догадаться из названия, коммуникационная сложность изучает способы организовать *коммуникацию*, то есть общение между несколькими участниками, так, чтобы в конце концов они узнали то, что хотят узнать, причем сделали это как можно более эффективно, то есть как можно менее *сложно*. Теория коммуникационной сложности является небольшой, но красивой и важной частью *теории сложности* — области, лежащей на стыке математики и теоретической информатики (или theoretical computer science). Поэтому я хотел бы начать с нескольких слов о теории сложности в общем и о тех вопросах, которые в ней изучаются. Читатель, интересующийся непосредственно математическим содержанием, а не философией, может сразу перейти к разделу 2.

Теория сложности занимается задачами, которые грубо можно описать следующим образом. Предположим, что перед нами стоит задание T, которое мы хотим выполнить, или задача, которую мы хотим решить. В большинстве случаев (но не всегда) это подразумевает вычисления на одном или нескольких компьютерах. Способов выполнить задание T может быть много. Обозначим множество всех таких мыслимых способов $\mathscr{P}_T$. В зависимости от контекста элементы множества $\mathscr{P}_T$ могут называться *алгоритмами* или, как в нашем случае, *протоколами*. В большинстве случаев очевидно, что существует по крайней мере один алгоритм/протокол для решения T, так что множество $\mathscr{P}_T$ непусто.

Хотя всякий $P \in \mathscr{P}_T$ решает нашу задачу, не все они нам одинаково подходят. Какие-то из них могут быть лучше, чем остальные, — например, короче, проще, менее ресурсоемкими. Основная идея математической теории сложности в том, чтобы реализовать наши интуитивные предпочтения в виде такой действительнозначной функции $\mu(P)$ (где $P \in \mathscr{P}_T$), называемой *функцией сложности*, что чем меньше $\mu(P)$, тем лучше наше решение P. В идеале мы бы хотели найти наилучшее решение $P \in \mathscr{P}_T$, то есть то, которое минимизирует функцию $\mu(P)$. Обычно это довольно трудно сделать, и поэтому исследователи работают в двух направлениях.

• Постараться найти «разумное» решение $P \in \mathscr{P}_T$, для которого, возможно, $\mu(P)$ не минимально, но «достаточно мало». Результаты такого вида называются *верхними оценками*, потому что они соответствуют попыткам оценить сверху величину

$$\min_{P \in \mathscr{P}_T} \mu(P),$$

которая как раз и называется *сложностью* задачи T.

• Получать *нижние оценки*: для некоторого $a \in \mathbb{R}$ показать, что $\mu(P) \geqslant a$ для любого $P \in \mathscr{P}_T$, то есть что не существует решения сложности меньше a. Класс $\mathscr{P}_T$ обычно очень широк, и решения могут быть основаны на очень разнообразных и неожиданных идеях. Нам нужно учесть их все одновременно. Именно поэтому нахождение нижних оценок — одна из самых трудных задач в современной математике, и подавляющая часть естественных вопросов здесь остаются открытыми.

Теперь самое время для примеров. Многие олимпиадные математические задачи имеют отношение к теории сложности, даже если это не видно явно из их формулировок.

> Известно, что из 7 монет (или 100, или n, …) 3 монеты (или не более 100, или неизвестное количество, …) фальшивые: они тяжелее настоящих (или легче, или тяжелее на 1 грамм, …). У нас есть весы, на которых можно взвесить (или сравнить) сколько угодно монет (или не более десяти монет, …). Сколько взвешиваний понадобится, чтобы найти все (хотя бы одну, …) фальшивые монеты?

Это типичные задачи теории сложности, и они существенно связаны с так называемыми *сортирующими сетями* и *алгоритмами сортировки*. Задание T здесь в том, чтобы найти фальшивые монеты, а множество решений $\mathscr{P}_T$ состоит из всех позволяющих это сделать последовательностей взвешиваний. Мера сложности $\mu(P)$ — количество взвешиваний в решении P.

> Дано число (многочлен, выражение, …). Сколько сложений/умножений нужно, чтобы получить его из некоторого определенного набора простейших объектов?

Это не просто пример задачи теории сложности, но типичный пример такой задачи. Можете ли вы описать T, $\mathscr{P}_T$ и μ в этом случае? И кстати, если вы думаете, что «школьный» метод умножения чисел «в столбик» является оптимальным в смысле количества операций над цифрами, то вы ошибаетесь. Более эффективные способы последовательно находились в работах Карацубы и Офмана [14], Тоома [28] и Кука [10], Шенхаге и Штрассена [27] и Фюрера [12], и вопрос об оптимальности алгоритма Фюрера по-прежнему остается открытым. Правда, эти продвинутые алгоритмы становятся более эффективными, чем «школьный» алгоритм, только на довольно больших числах (обычно состоящих по крайней мере из нескольких тысяч цифр).

Знаменитая проблема равенства классов P и NP (если вы о ней не слышали, я рекомендую посмотреть, например, ее описание как одной

из «проблем тысячелетия»[1]) тоже относится к теории сложности. Здесь T состоит в решении любой конкретной NP-полной алгоритмической задачи, например, «выполнимость булевой формулы», и $\mathscr{P}_T$ — множество всех решающих эту задачу детерминированных алгоритмов.

В нашей брошюре мы обсуждаем сложностные задачи о *коммуникации*. Это простая для описания и понимания модель, но очень скоро мы дойдем до интересных задач, остающихся нерешенными уже в течение десятилетий... И хотя мы не обсудим этого во всех подробностях, идеи и методы коммуникационной сложности распространяются практически на все области теории сложности.

Почти все изложенное в этих записках (и даже гораздо больше) можно найти в классической книге [18]. Глава 13 недавнего учебника по вычислительной сложности [3] целиком посвящена коммуникационной сложности.

Поскольку в тексте встречается большое количество обозначений, некоторые из них собраны в конце вместе с коротким описанием.

2. Основная модель

Основная (детерминированная) модель была введена в основополагающей статье Яо [29]. В ней два участника Анна и Борис, два конечных множества X, Y и функция $f\colon X \times Y \to \{0, 1\}$. Задача T_f для Анны и Бориса заключается в том, чтобы посчитать значение функции $f(x, y)$ для заданных параметров x, y. Интрига в том, что изначально Анна знает только $x \in X$, а Борис — только $y \in Y$. В их распоряжении двусторонний канал связи, но только вроде трансатлантического телефона или радиосвязи с космическим аппаратом на марсианской орбите — очень дорогой. Поэтому Анна и Борис хотят минимизировать количество битов переданной информации при вычислении $f(x, y)$.

Таким образом, протокол связи $P \in \mathscr{P}_T$ устроен следующим образом (см. рис. 1): Анна посылает сообщение, которое для простоты будем считать закодированным *двоичным словом* a_1 (то есть конечной последовательностью нулей и единиц). Борис отвечает некоторым двоичным словом b_1, которое зависит только от y и полученного от Анны a_1. Так они продолжают до тех пор, пока один из них, допустим, Борис, не вычислит значение $f(x, y)$ и не отправит его Анне в последнем раунде t переговоров.

Замечание 1. Нужно отметить, что имена Анна и Борис здесь — это вольный перевод традиционных имен Алиса и Боб (Alice and Bob), при-

[1] `http://www.claymath.org/millenium/P_vs_NP`.

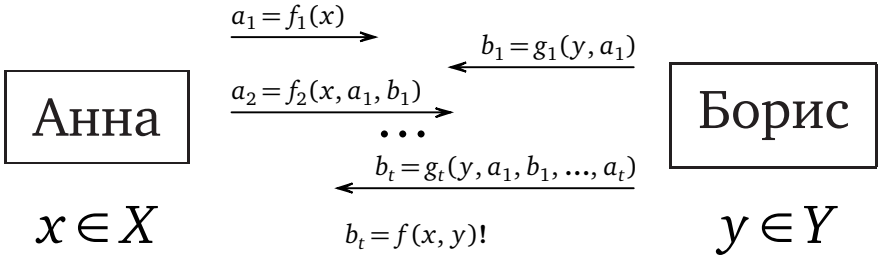

Рис. 1. Протокол P вычисления $f(x, y)$

надлежащих популярным персонажам, часто встречающимся в литературе по теории сложности и криптографии. Иногда цели этих героев совпадают лишь частично, и они ведут себя осторожно, чтобы не выдать нежелательную информацию, — такая ситуация относится к криптографии. Иногда их разговор по каналу связи подслушивают неприятели. Иногда они даже не могут доверять тому, что собеседник честно следует протоколу, — обычно в этом случае их называют Артур и Мерлин. Однако в рамках данного текста мы придерживаемся простейшего сценария: общая задача, полное взаимное доверие, никакого желания что-либо скрывать, безопасный и надежный канал связи.

В нашем определении мы специально оставили несколько неточностей. Например, фиксирована ли длина сообщения a_1 или она может зависеть от x? Может ли количество раундов t зависеть от x и y, и если да, как Анна узнает, что сообщение b_t, полученное от Бориса, на самом деле последнее? Оказывается, однако, что все эти детали не очень важны, и читатель может восполнить эти пробелы по своему усмотрению — они могут изменить сложность лишь на небольшую аддитивную константу.

Как измерить сложность $\mu(P)$ протокола P? Есть несколько разумных способов, но мы остановимся на наиболее важном и популярном — модели *сложности в худшем случае*. Для любых входных параметров $(x, y) \in X \times Y$ можно определить стоимость протокола на этом входе как общее количество переданных битов $|a_1| + |b_1| + \ldots + |b_t|$ при применении протокола к этому входу (здесь $|a|$ обозначает длину двоичного слова a; см. также рис. 1). Далее сложность (по историческим причинам иногда называемая *стоимостью*) $\mathrm{cost}(P)$ протокола P определяется как максимальная стоимость P по всем входам $(x, y) \in X \times Y$. Наконец, *коммуникационная сложность* $C(f)$ (вычисления) функции $f : X \times Y \to \{0, 1\}$ определяется как $\min_{P \in \mathscr{P}_f} \mathrm{cost}(P)$ по всем корректным

протоколам P, то есть таким, которые корректно вычисляют $f(x, y)$ на всех возможных входах. Мы хотели бы вычислить сложность $C(f)$ для «интересных» функций f или хотя бы получать на нее хорошие оценки.

Первое очевидное наблюдение заключается в том, что

$$C(f) \leqslant \lceil \log_2 |X| \rceil + 1 \tag{1}$$

для любой функции f (через $\lceil x \rceil$ обозначается наименьшее целое число, большее или равное x). Действительно, протокол с такой стоимостью легко получается следующим образом: Анна кодирует свою часть входа x, превращая ее в двоичное слово длины $\lceil \log_2 |X| \rceil$, с помощью какого-нибудь однозначного кодирования $f_1 : X \to \{0,1\}^{\lceil \log_2 |X| \rceil}$, и посылает $a_1 = f_1(x)$ Борису. Затем Борис расшифровывает сообщение (мы считаем, что f_1 известно обоим участникам заранее) и отправляет ответ $f(f_1^{-1}(a_1), y)$ Анне.

Удивительно, что лишь для небольшого количества интересных функций f можно существенно улучшить оценку (1) в рамках основной модели. Один более или менее тривиальный пример такой. Пусть $X = Y = \{1, 2, \ldots, N\}$. Анна и Борис хотят посчитать функцию $f_N(x, y)$ со значениями в $\{0, 1\}$, которая равна 1 тогда и только тогда, когда $x + y$ делится на 2011. Гораздо более экономичным тогда для Анны будет послать Борису не x целиком, а только остаток от деления x на 2011. Ясно, что этой информации по-прежнему достаточно для Бориса, чтобы выяснить, делится ли $x + y$ на 2011 (и тем самым найти $f_N(x, y)$), и стоимость этого протокола всего лишь $\lceil \log_2 2011 \rceil + 1 = 12$. Таким образом,

$$C(f_N) \leqslant 12. \tag{2}$$

Специалисты по теории сложности обычно довольно ленивые люди и, кроме того, не очень хорошо владеют элементарной арифметикой. Самое замечательное в неравенстве (2) — это что его правая часть представляет собой абсолютную константу, которая чудесным образом вообще не зависит от входных параметров! Поэтому вместо вычисления конкретного значения мы предпочитаем сконцентрироваться на этом факте, используя специальное обозначение, с помощью которого (2) переписывается как

$$C(f_N) \leqslant O(1).$$

Оно означает, что существует такая положительная универсальная константа $K > 0$ (которую каждый интересующийся обычно может извлечь из доказательства) такая, что для всех N имеем $C(f_N) \leqslant K \cdot 1 = K$. Анало-

гично, $C(f_N) \leqslant O(\log_2 N)$ значит, что $C(f_N) \leqslant K \log_2 N$, и т. д. Мы будем использовать это стандартное обозначение и далее[1].

Рассмотрим теперь следующую, очевидно очень важную, задачу. Пусть $X = Y$ — равные множества из N элементов (можно считать, что это опять $\{1, 2, \ldots, N\}$, хотя в данном случае это уже неважно). *Функция равенства* EQ_N определяется следующим образом: $\mathrm{EQ}_N(x, y) = 1$, если и только если $x = y$. Другими словами, Анна и Борис хотят проверить, идентичны ли их файлы, базы данных, и т. д. — важная задача во многих приложениях.

Конечно, мы можем применить очевидную оценку (1), то есть Анна может просто передать x целиком Борису. Но можно ли сэкономить хоть чуть-чуть по сравнению с этим тривиальным протоколом? Здесь я хотел бы предложить читателю отложить этот текст и попробовать несколько идей решения этой задачи самостоятельно. Это очень поможет пониманию дальнейшего изложения.

3. Нижние оценки

Ну что, не удалось? Не расстраивайтесь, оказывается, оценку (1) нельзя улучшить: любой протокол для EQ_N имеет стоимость как минимум $\log_2 N$. Это было доказано в той же основополагающей статье Яо [29]. Вообще, идеи из этой статьи определили развитие теории сложности на несколько десятилетий вперед. Посмотрим теперь на несложное, но поучительное доказательство этой нижней оценки.

Итак, у нас есть протокол P, такой, как на рис. 1, и мы знаем, что после его исполнения Борис знает $\mathrm{EQ}_N(x, y)$. Нам надо доказать, что $\mathrm{cost}(P) \geqslant \log_2 N$.

Очень распространенная ошибка, которую совершают начинающие игроки в «нижние оценки», происходит, когда они говорят, что́ именно P «должен делать», то есть осознанно или неосознанно из каких-то общих соображений предполагают что-то о наилучшем протоколе P. Например, типичное рассуждение может начинаться так: «Пусть i — первый бит в двоичном представлении x и y, который сравнивается в протоколе P». «Рассуждения» такого типа принципиально ошибочны, так как непонятно, почему наилучший протокол должен вести себя именно так, а не иначе, и вообще должен следовать какому-то «самому разумному» поведению. В теории сложности постоянно встречаются

[1] Обычно обозначение $O(\cdot)$ используется с равенством, а не с неравенством; например, пишут $C(f_N) = O(\log_2 N)$. Однако нам представляется, что использование неравенства более информативно и позволяет избежать недоразумений, особенно в более сложных ситуациях.

хитроумные алгоритмы и протоколы, которые в течение длительного времени делают что-то странное и, кажется, не относящееся к делу, и только в конце — как кролика из шляпы — предъявляют правильный ответ. Мы увидим подобный пример ниже. Теория сложности именно потому так прекрасна и трудна, что необходимо учесть все, в том числе и сколь угодно странные, протоколы, и мы не можем предполагать о протоколе P ничего кроме того, что сказано в определении.

После такого лирического отступления разберем рассуждение Яо и посмотрим, какую информацию мы можем извлечь исключительно из определения (рис. 1). Заметьте, что хотя сейчас мы и остановились на случае $f = \mathrm{EQ}_N$, рассуждение Яо гораздо более общее и применимо к любой функции f. Так что пока предположим, что f — произвольная функция, для которой мы хотим оценить коммуникационную сложность. Мы вернемся к EQ_N в следствии 2.

Принципиальная идея здесь в том, чтобы рассмотреть всю *историю* сообщений $(a_1, b_1, \ldots, a_t, b_t)$, переданных при реализации Анной и Борисом протокола P на определенном входе. Эта идея в разных формах оказывается очень продуктивной в разных ситуациях, и не только в коммуникационной сложности.

Заметим, что существует не более $2^{\mathrm{cost}(P)}$ возможных историй, поскольку этим числом ограничивается[1] количество вообще всех возможных строк длины $\mathrm{cost}(P)$. Для каждой истории h можно определить множество R_h всех тех входов (x, y), которые при выполнении протокола P в итоге приводят к истории h. А что можно сказать об этих множествах?

Прежде всего, каждый вход (x, y) может привести ровно к одной возможной истории. Это означает, что семейство множеств $\{R_h\}$ представляет собой *разбиение* множества всех входов $X \times Y$:

$$X \times Y = \bigcup_{h \in \mathcal{H}} R_h, \tag{3}$$

где $\mathcal{H}$ обозначает множество всех возможных историй и $R_h \cap R_{h'} = \varnothing$ для любых двух различных историй $h, h' \in \mathcal{H}$.

Далее, любая история h содержит в качестве последнего сообщения Бориса b_t значение функции $f(x, y)$. Это означает, что любое множество R_h является *f-одноцветным*, то есть либо $f(x, y) = 0$ для всех $(x, y) \in R_h$, либо $f(x, y) = 1$ для всех таких (x, y).

[1] В зависимости от конкретных деталей модели истории могут иметь разную длину, может быть важно расположение запятых и т. д., так что общее количество может быть немного больше. Но мы не будем обращать внимания на небольшие аддитивные и даже мультипликативные константы.

Наконец, и это очень важно, каждое множество R_h является *комбинаторным прямоугольником* (или просто прямоугольником), то есть имеет вид $R_h = X_h \times Y_h$ для некоторых $X_h \subseteq X, Y_h \subseteq Y$. Чтобы понять, почему это так, попытаемся развернуть определение «(x, y) приводит к истории $(a_1, b_1, \ldots, a_t, b_t)$». Оно эквивалентно набору условий (см. рис. 1):

$$f_1(x) = a_1, \quad g_1(y, a_1) = b_1, \quad f_2(x, a_1, b_1) = a_2, \quad \ldots, \quad g_t(y, a_1, \ldots, a_t) = b_t.$$

Заметим, что первое, третье, пятое и т. д. условия в этой последовательности зависят только от x (история h фиксирована!). Обозначим множество тех x, которые удовлетворяют всем этим условиям, через X_h. Аналогично, обозначим через Y_h множество всех тех y, которые удовлетворяют второму, четвертому, шестому и т. д. условиям. Теперь несложно заметить, что $R_h = X_h \times Y_h$!

Итак, для каждого протокола P, решающего нашу задачу $f : X \times Y \to \to \{0, 1\}$, мы построили разбиение множества $X \times Y$ не более чем на $2^{\mathrm{cost}(P)}$ частей, так что каждая часть является f-одноцветным прямоугольником. Перефразируя немного, обозначим через $\chi(f)$ (да, специалисты по теории сложности любят вводить побольше всяких мер сложности!) минимальное количество f-одноцветных прямоугольников, на которые можно разбить $X \times Y$. Таким образом, мы доказали (с точностью до небольшой мультипликативной константы, которая может зависеть от технических тонкостей в определении модели) следующее утверждение:

Теорема 1 (Яо). $C(f) \geqslant \log_2 \chi(f)$.

Вернемся теперь к нашему конкретному случаю $f = \mathrm{EQ}_N$. Все f-одноцветные прямоугольники — это либо 0-прямоугольники, либо 1-прямоугольники. Функции EQ_N соответствует много больших 0-прямоугольников. (Можете найти хотя бы один?) Но все соответствующие ей 1-прямоугольники устроены тривиально и состоят просто из одного элемента (x, x). Следовательно, чтобы покрыть даже все «диагональные» прямоугольники $\{(x, x) \mid x \in X\}$, необходимо хотя бы N различных прямоугольников, что доказывает оценку $\chi(\mathrm{EQ}_N) \geqslant N$. Объединив это с теоремой 1, мы получаем то, к чему стремились:

Следствие 2. $C(\mathrm{EQ}_N) \geqslant \log_2 N$.

Упражнение 1. Пусть функция LE_N («меньше либо равно») определена на множестве $\{1, 2, \ldots, N\} \times \{1, 2, \ldots, N\}$ следующим образом:

$$\mathrm{LE}_N(x, y) = 1, \text{ если и только если } x \leqslant y.$$

Докажите, что $C(\mathrm{LE}_N) \geqslant \log_2 N$.

Упражнение 2 (сложное). Функция DISJ_n определена на множестве $\{0,1\}^n \times \{0,1\}^n$ следующим образом:

$$\mathrm{DISJ}(x,y)=1, \text{ если и только если } \forall i \leqslant n\colon x_i=0 \vee y_i=0,$$

то есть множество позиций, в которых в строках x и y стоит 1, не пересекаются. Докажите, что $C(\mathrm{DISJ}_n) \geqslant \Omega(n)$.

(Здесь $\Omega(\cdot)$ — это еще одно обозначение, которое любят специалисты по теории сложности. Оно имеет смысл, противоположный смыслу обозначения $O(\cdot)$, и означает, что существует такая константа $\varepsilon > 0$, что $C(\mathrm{DISJ}_n) \geqslant \varepsilon n$ для всех n.)

Указание. Сколько есть входов (x,y), для которых $\mathrm{DISJ}_n(x,y)=1$? И каков максимальный размер 1-прямоугольника?

4. Точны ли эти оценки?

Следующий интересный вопрос — это насколько точна теорема 1. Может ли так оказаться, что $\chi(f)$ мало, то есть существует хорошее разбиение на f-одноцветные прямоугольники, и при этом все равно $C(f)$ велико, то есть, в частности, мы не можем перевести наше разбиение в хороший протокол? Рис. 2 показывает, что это как минимум нетривиальный вопрос: на нем изображено разбиение на пять прямоугольников, которое не соответствует никакому протоколу. (В самом деле, первое сообщение Алисы должно провести разрез по всей длине квадрата на два нетривиальных множества прямоугольников, что, очевидно, невозможно.)

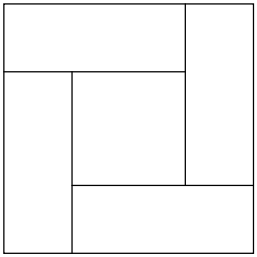

Рис. 2. Что делать Анне?

Как и во многих подобных ситуациях, ответ зависит от того, насколько точным он должен быть. В оказавшей большое влияние статье [1], посвященной коммуникационной сложности, была доказана, среди прочего, такая оценка.

Теорема 3 (Ахо, Ульман, Яннакакис). $C(f) \leqslant O(\log_2 \chi(f))^2$.

Доказательство не очень сложно, но все-таки нетривиально. Читатель может попытаться найти его самостоятельно или обратиться, например, к книге [18].

Можно ли избавиться от квадрата в теореме 3? За почти 30 лет, прошедших с момента публикации статьи [1], множество людей пыталось ответить на этот вопрос тем или иным способом, но он не поддается и по сей день...

Нерешенная проблема 1. *Верно ли, что* $C(f) \leqslant O(\log_2 \chi(f))$*?*

Помимо теоремы 3, работа [1] содержит много других результатов, относящихся к так называемой *недетерминированной коммуникационной сложности*. В этой модели у Анны и Бориса также есть доступ к слову z, не определенному протоколом, но данному всесильным третьим участником, который пытается убедить Анну и Бориса, что $f(x, y) = 1$. Требуется, чтобы «убеждающее» слово z существовало тогда и только тогда, когда $f(x, y)$ *на самом деле* равно 1; отметим, что в данном определении мы отказываемся от равноправия ответов 0 и 1. Мы обсудим это понятие очень кратко; соответствующие меры сложности не будут использоваться в дальнейшем тексте.

Определим $t(f)$ так же, как и $\chi(f)$, только теперь разрешим одноцветным прямоугольникам в покрытии перекрываться. Очевидно, $t(f) \leqslant \chi(f)$, но оказывается, что оценка теоремы 3 по-прежнему верна: $C(f) \leqslant O(\log_2 t(f))^2$. С другой стороны, существуют примеры, в которых $C(f)$ примерно равно $(\log_2 t(f))^2$. Это значит, что на вопрос, аналогичный проблеме 1, для прямоугольников, которые могут пересекаться, ответ (отрицательный) известен.

Пусть $\chi_0(f)$ и $\chi_1(f)$ определяются так же, как $\chi(f)$, но отдельно для непересекающегося покрытия всех тех входов, на которых значение функции равно 0 (для $\chi_0(f)$), или, соответственно, всех входов, где значение функции равно 1 (для $\chi_1(f)$). Заметим при этом, что $\chi(f) = \chi_0(f) + \chi_1(f)$. Оказывается, по-прежнему $C(f) \leqslant O(\log_2 \chi_1(f))^2$ и, симметрично, $C(f) \leqslant O(\log_2 \chi_0(f))^2$. Аналогично, можно определить величины $t_0(f)$ и $t_1(f)$. Тогда недетерминированная коммуникационная сложность, определенная выше, оказывается равной $\log_2 t_1(f)$. Заметим, что невозможно получить какую-то разумную (скажем, лучше, чем экспоненциальную) оценку на $C(f)$ в терминах только $\log_2 t_1(f)$ или $\log_2 t_0(f)$: например, $t_0(\mathrm{EQ}_N) \leqslant O(\log_2 N)$ (почему?), но при этом, как мы уже знаем, $C(\mathrm{EQ}_N) \geqslant \log_2 N$.

Подытожим: для детерминированной коммуникационной сложности не существует никакой хорошей оценки в терминах недетерминированной, но такая оценка становится возможной, если дополнитель-

но известно, что недетерминированная коммуникационная сложность *отрицания* рассматриваемой функции также мала.

В еще одной важной статье [20] были введены в обиход *алгебраические методы*. До этого все наши методы оценивания снизу $\chi(f)$ (следствие 2 и упражнения 1 и 2) были основаны на одной и той же несложной идее: выбрать «много» входов $D \subseteq X \times Y$, так что любой f-одноцветный прямоугольник R может покрыть лишь «немного» из них, и затем воспользоваться принципом Дирихле. Этот подход никак не использует, что прямоугольники в покрытии (3) не пересекаются, или, другими словами, может быть применен к оценке $t(f)$ точно так же, как и к оценке $\chi(f)$. Хорошо это или плохо? Как посмотреть. Всегда хорошо иметь возможность доказать больше утверждений за раз, например, как в случае с нижней оценкой на недетерминированную коммуникационную сложность $\log_2 t_1(f)$. Но иногда оказывается, что величина, аналогичная $t(f)$, всегда мала, и если мы хотим оценить снизу $\chi(f)$, мы должны использовать метод, который «чувствует» разницу между двумя этими понятиями. «Ранговая нижная оценка» Мелхорна и Шмидта [20] была первым таким методом.

Нам понадобятся самые базовые понятия из линейной алгебры, такие как *матрица* M и ее *ранг* $\mathrm{rk}(M)$, и их простейшие свойства. Если читатель до сих пор с ними не знаком, сейчас самое время взять какой-нибудь учебник по линейной алгебре и прочесть оттуда несколько глав. Такие знания пригодятся в жизни в любом случае, но здесь еще и сразу будет видно неожиданное и интересное применение этих на первый взгляд абстрактных понятий.

Для любой функции $f\colon X \times Y \to \{0,1\}$ ее значения можно записать в виде *коммуникационной матрицы* M_f. Строки этой матрицы занумерованы элементами множества X, а столбцы — элементами множества Y (каким именно способом мы занумеруем строки и столбцы, несущественно). На пересечении строки x и столбца y мы пишем $f(x,y)$. Следующий результат связывает довольно различные миры комбинаторики и алгебры.

Теорема 4. $\chi(f) \geqslant \mathrm{rk}(M_f)$.

Доказательство на удивление просто. Пусть $R_1, \ldots, R_\chi$ — непересекающиеся 1-прямоугольники, покрывающие все клетки (x,y), для которых $f(x,y)=1$, так что $\chi \leqslant \chi(f)$. Пусть $f_i\colon X \times Y \to \{0,1\}$ — *характеристическая* функция прямоугольника R_i, то есть $f_i(x,y)=1$, если и только если $(x,y) \in R_i$. Пусть $M_i = M_{f_i}$ — коммуникационная матрица функции f_i. Тогда $\mathrm{rk}(M_i)=1$ (почему?) и $M_f = \sum\limits_{i=1}^{\chi} M_i$. Следовательно, $\mathrm{rk}(M_f) \leqslant \sum\limits_{i=1}^{\chi} \mathrm{rk}(M_i) \leqslant \chi \leqslant \chi(f)$. □

Чтобы вполне осознать, насколько полезна теорема 4, заметим, что M_{EQ_N} — это единичная матрица (мы благоразумно предполагаем, что в случае $X = Y$ порядок на строках и столбцах согласован), и значит, $\mathrm{rk}(M_{\mathrm{EQ}_N}) = N$. Так мы сразу получаем следствие 2. Матрица M_{LE_N} — верхнетреугольная, и следовательно, опять $\mathrm{rk}(M_{\mathrm{LE}_N}) = N$. Так получается упражнение 1. Немного подумав, можно заметить также, что матрица M_{DISJ_n} невырожденная, так что $\mathrm{rk}(M_{\mathrm{DISJ}_n}) = 2^n$. Так мы получаем оценку $C(\mathrm{DISJ}_n) \geqslant n$, которая точна согласно (1) и, более того, сильнее той, что получается в упражнении 2 (потому что мы избавляемся от Ω).

Насколько точна оценка теоремы 4? В течение какого-то времени продержалась гипотеза о том, что $\chi(f) \leqslant (\mathrm{rk}(M_f))^{O(1)}$ или даже $\chi(f) \leqslant \leqslant O(\mathrm{rk}(M_f))$. В таком виде гипотеза была опровергнута в серии публикаций [2, 24, 22]. Однако по-прежнему возможно и даже правдоподобно, что

$$\chi(f) \leqslant 2^{O(\log_2 \mathrm{rk}(M_f))^2}.$$

В совокупности с теоремой 3 это могло бы дать крайне нетривиальную оценку $C(f) \leqslant O(\log_2 \mathrm{rk}(M_f))^4$.

После многолетних попыток мы по-прежнему не знаем ответ и на самом деле даже не знаем, как подступиться к проблеме, которая стала известна под названием log-rk *гипотезы*[1]:

Нерешенная проблема 2 (log-rk **гипотеза).** *Верно ли, что*

$$\chi(f) \leqslant 2^{(\log_2 \mathrm{rk}(M_f))^{O(1)}}?$$

Или (что эквивалентно в силу теорем 1 и 3) верно ли, что $C(f) \leqslant \leqslant (\log_2 \mathrm{rk}(M_f))^{O(1)}$*?*

Это всё, что мы хотели рассказать про базовую модель коммуникационной сложности.

5. Вероятностные модели

Еще более увлекательные и трудные задачи возникают, когда мы переходим к рассмотрению разных вариантов основного определения. Наиболее важный из них и единственный, который мы рассмотрим здесь достаточно подробно, — это модель *вероятностной коммуникационной сложности*.

[1] После того как английский вариант этого текста был напечатан, довольно неожиданный подход к этой проблеме, основанный на идеях из *аддитивной комбинаторики*, был предложен в недавней работе [6].

Предположим, что Анна и Борис теперь не так требовательны и могут позволить себе ошибиться при вычислении $f(x,y) \in \{0,1\}$ с небольшой вероятностью. Им предоставляется честная монета (выражаясь академическим языком, *генератор случайных битов*), они могут подбрасывать монету во время исполнения протокола и согласовывать посылаемые друг другу сообщения с результатами подбрасываний. Все остальное остается таким же, как на рис. 1, но теперь необходимо специально объяснить, что значит, что протокол P корректно вычисляет функцию f.

Зафиксируем вход (x,y) и предположим, что Анна и Борис в процессе исполнения протокола вместе подбросили монету r раз[1], что дает 2^r возможных исходов подбрасываний. Назовем *хорошими* те исходы, при которых в конце Борису удается правильно посчитать $f(x,y)$, а остальные, в которых он ошибается, *плохими*. Обозначим множество всех хороших исходов подбрасываний монет через $\mathrm{Good}(x,y)$. Тогда величина

$$p_{x,y} = \frac{|\mathrm{Good}(x,y)|}{2^r}, \tag{4}$$

как и следовало ожидать, называется *вероятностью успеха* на входе (x,y).

Чего мы от нее хотим? Существует очень простой протокол стоимости 1, для которого $p_{x,y} = 1/2$. Борис просто-напросто подбрасывает монету один раз и выдает в качестве ответа результат подбрасывания. Таким образом, мы заведомо хотим потребовать выполнения неравенства

$$p_{x,y} > 1/2. \tag{5}$$

Но насколько сильно вероятность успеха должна быть отделена от $1/2$?

Оказывается, что по существу есть только три различные возможности (если мы по-прежнему не заботимся о конкретных значениях констант). В наиболее популярном и важном варианте требуют, чтобы для любого входа (x,y) было выполнено неравенство $p_{x,y} \geqslant 2/3$. Минимальная стоимость вероятностного протокола, удовлетворяющего этому условию, называется *вероятностной коммуникационной сложностью функции f в модели с ограниченной ошибкой* (bounded-error probabilistic communication complexity) и обозначается через $R(f)$. Если для любого входа (x,y) мы требуем только выполнения неравенства (5), то получаем модель *с неограниченной ошибкой* (unbounded-error), и соответствующая мера сложности обозначается через $U(f)$.

[1] Без ограничения общности можно считать, что суммарное число подбрасываний всегда одно и то же и не зависит от результатов подбрасываний (почему?).

В третьей модели (менее популярной и не рассматриваемой нами далее) по-прежнему требуется неравенство (5), но, кроме того, подбрасывания монеты уже не бесплатные для Анны и Бориса и учитываются в стоимости протокола. Из этого, например, следует, что для протокола стоимости $O(\log_2 n)$ из оценки (5) автоматически вытекает и более сильная оценка $p_{x,y} \geqslant \frac{1}{2} + \frac{1}{p(n)}$ для некоторого многочлена $p(n)$.

Почему в определении $R(f)$ мы потребовали лишь $p_{x,y} \geqslant 2/3$, а не, скажем, $p_{x,y} \geqslant 0{,}9999$? Используя так называемую *амплификацию*, можно показать, что разница здесь не очень важна. Именно, предположим, что в распоряжении Анны и Бориса имеется протокол стоимостью $R(f)$, для которого $p_{x,y} \geqslant 2/3$. Они выполняют его независимо 1000 раз и в конце выдают наиболее часто встретившийся в этих испытаниях конечный ответ. Вероятность ошибки такого протокола стоимостью всего лишь $1000R(f)$ не превысит 10^{-10}. (Чтобы это доказать, необходимо определенное знание элементарной теории вероятностей, например, неравенства Чернова (Chernoff bound).)

Действительно ли подбрасывание монеты может в чем-то помочь? Существуют ли интересные задачи, которые можно решить более эффективно в вероятностной модели? Ответ на этот вопрос дает следующая красивая конструкция, обычно приписываемая Рабину и Яо. Ее полезно сравнить со следствием 2.

Теорема 5. $R(\mathrm{EQ}_N) \leqslant O(\log_2 \log_2 N)$.

Доказательство. Представим элементы множеств X и Y в виде двоичных строк длины n, где $n = \lceil \log_2 N \rceil$. Далее, будем отождествлять двоичное слово $x_1 x_2 \ldots x_n$ с многочленом $x_1 + x_2\xi + \ldots + x_n\xi^{n-1}$ от одной переменной ξ. Таким образом, у Анны и Бориса вначале есть многочлены вышеуказанного вида $g(\xi)$ и $h(\xi)$, и они хотят определить, равны ли эти многочлены. Для этого они заранее выбирают простое число $p \in [3n, 6n]$ (оно всегда существует по знаменитой теореме Чебышева, известной также как постулат Бертрана). Анна подбрасывает монету несколько раз и в итоге выбирает случайное число $\xi \in \{0, 1, \ldots, p-1\}$. Затем она вычисляет остаток $g(\xi) \bmod p$ и отправляет пару $(\xi, g(\xi) \bmod p)$ Борису. Борис вычисляет $h(\xi) \bmod p$ и выдает 1, если и только если его значение $h(\xi) \bmod p$ оказалось равно полученному от Анны значению $g(\xi) \bmod p$.

Чтобы передать пару чисел $(\xi, g(\xi) \bmod p)$, каждое из которых не больше $p \leqslant O(n)$, необходимо передать не более $O(\log_2 n)$ битов, то есть оценка на стоимость протокола получается $O(\log_2 n)$, как и требовалось. Какова вероятность успеха? Если $\mathrm{EQ}(g, h) = 1$, то $g = h$, и, очевид-

но, Борис всегда выдаст 1, без всякой ошибки. Но что, если $g \neq h$? Тогда $(g-h)$ — это ненулевой многочлен степени не более n. Любой такой многочлен имеет не более n корней в конечном поле $\mathbb{F}_p$. Если вы не понимаете последнее предложение, то просто поверьте мне, что количество плохих $\xi \in \{0, 1, \ldots, p-1\}$, для которых Борис введен в заблуждение тем, что $g(\xi) = h(\xi)$, не превосходит $n \leqslant \frac{p}{3}$. И поскольку ξ было выбрано случайно из множества $\{0, 1, \ldots, p-1\}$, это в точности означает, что вероятность успеха не менее $2/3$. □

Рассмотрим теперь и другие ранее встречавшиеся задачи в контексте вероятностной коммуникационной сложности. Функция «меньше либо равно» из упражнения 1 также становится несложной: $R(\mathrm{LE}_N) \leqslant \leqslant O(\log_2 \log_2 N)$, хотя доказательство уже гораздо труднее, чем для равенства (см. [18, упражнение 3.18]). С другой стороны, подбрасывание монеты не помогает вычислять функцию DISJ (см. [13, 25]):

Теорема 6. $R(\mathrm{DISJ}_n) \geqslant \Omega(n)$.

Доказательство достаточно трудное и поэтому мы его здесь обсуждать не будем. Оно немного проще для другой важной функции, *скалярного произведения по модулю* 2, и сейчас мы его разберем.

Для слов $x, y \in \{0,1\}^n$ рассмотрим, так же как и для DISJ, множество таких i, что $x_i = y_i$. Тогда $\mathrm{IP}_n(x, y) = 1$, если количество таких индексов i нечетно, и $\mathrm{IP}_n(x, y) = 0$, если это количество четно. Хор и Голдрайх [9] доказали следующую теорему.

Теорема 7. $R(\mathrm{IP}_n) \geqslant \Omega(n)$.

Полное доказательство по-прежнему слишком сложно, чтобы привести его здесь полностью; мы рассмотрим только его основную идею.

До сих пор мы рассматривали исключительно f-одноцветные прямоугольники, то есть состоящие только из нулей или только из единиц. Обычно мы хотели доказать, что каждый такой прямоугольник в каком-нибудь смысле мал. В вероятностной модели нам необходимо рассматривать уже произвольные прямоугольники R. Пусть $N_0(f, R)$ обозначает количество таких точек в прямоугольнике, для которых $f(x, y) = 0$, а $N_1(f, R)$ — количество точек, для которых $f(x, y) = 1$. Нам нужно доказать, что даже если R «большой», то он все-таки достаточно «сбалансированный», то есть что величины $N_0(f, R)$ и $N_1(f, R)$ достаточно близки друг к другу. Более строго, *отклонением* (discrepancy) от равномерного распределения[1] функции $f : X \times Y \to \{0, 1\}$ назовем

$$\mathrm{Disc}_u(f) = \max_R \frac{|N_0(f, R) - N_1(f, R)|}{|X| \times |Y|},$$

[1] Это понятие может быть также обобщено и на другие распределения.

где максимум берется по всем возможным комбинаторным прямоугольникам $R \subseteq X \times Y$.

Оказывается, можно показать, что

$$R(f) \geqslant \Omega(\log_2(1/\operatorname{Disc}_u(f))), \tag{6}$$

то есть из верхних оценок на отклонение можно получать нижние оценки для вероятностных протоколов. Далее для доказательства теоремы 7 остается доказать оценку $\operatorname{Disc}_u(\mathrm{IP}_n) \leqslant 2^{-n/2}$ (что довольно нетривиально).

Что произойдет, если мы пойдем дальше и отменим ограничение на вероятность ошибки, то есть потребуем только, чтобы вероятность успеха (4) была строго больше $1/2$? Функция равенства становится совсем простой [21]:

Теорема 8. $U(\mathrm{EQ}_N) \leqslant 2$.

Функция DISJ тоже становится проще:

Упражнение 3. Докажите неравенство $U(\mathrm{DISJ}_n) \leqslant O(\log_2 n)$.

Однако скалярное произведение держит оборону:

Теорема 9. $U(\mathrm{IP}_n) \geqslant \Omega(n)$.

Этот очень красивый и неожиданный результат Фостера [11], один из моих любимых во всей теории сложности.

6. Другие варианты

В заключение мы кратко остановимся на нескольких современных направлениях в теории коммуникационной сложности, которые сейчас развиваются особенно активно.

6.1. Квантовая коммуникационная сложность

Я даже не буду пытаться определять, что такое *квантовые компьютеры* или что они имеют общего с «Квантом милосердия»[1] — вероятно, большинство читателей хоть что-то слышали об этих по-прежнему лишь воображаемых устройствах. Скажем только, что квантовые компьютеры тоже могут использоваться для решения задач по обмену информацией [30], и обозначим соответствующую меру сложности $Q(f)$. У квантовых компьютеров имеется доступ к случайным битам (которые до этого нам встречались как результат подбрасывания монеты), поэтому $Q(f) \leqslant R(f)$. С другой стороны, нижняя оценка на отклонение (6) для квантовых протоколов по-прежнему выполняется [17], что

[1] Фильм из серии про Джеймса Бонда, последний на момент написания данного текста.

дает для них ту же оценку, что и в теореме 7. Более интересная ситуация с функцией DISJ: ее сложность падает со значения n до $\sqrt{n}$ [7, 26]. Могут ли квантовые протоколы дать еще более существенный выигрыш по сравнению с вероятностными? Это одна из наиболее принципиальных и трудных задач в этой области:

Нерешенная проблема 3. *Верно ли, что сложность $R(f)$ ограничена сверху полиномом от $Q(f)$ для функций $f: X \times Y \to \{0,1\}$?*

6.2. Коммуникационная сложность для нескольких участников

Теперь у нас не два, а больше участников: Анна, Борис, Валентина, Григорий, Дарья, Евгений... и они совместно хотят вычислять значения некоторой функции f. Тут можно рассматривать разные модели в зависимости от того, как вход функции f распределен среди участников. В простейшем случае у каждого участника есть своя часть входа, не известная никому из остальных. Однако наиболее важная и имеющая больше всего приложений — другая модель: «число на лбу». В ней по-прежнему k участников хотят вычислить значение функции $f(x^1, \ldots, x^k)$, $x^i \in \{0,1\}^n$. Но отличие от предыдущей ситуации в том, что теперь вход x^i написан «на лбу» i-го участника, или, другими словами, он видит все x^j для $j \neq i$, но не видит x^i. Пусть $C^k(f)$ обозначает, как всегда, минимальное количество битов, которые участники должны передать, чтобы вычислить $f(x^1, \ldots, x^k)$. Для простоты будем считать, что каждое сообщение любого участника мгновенно доставляется всем остальным.

Наши основные функции DISJ_n и IP_n можно естественным образом обобщить на эту модель как DISJ_n^k и IP_n^k. (Можете ли вы восстановить подробности? Ответ можно проверить на стр. 22.) В классической статье [4] была доказана следующая оценка:

Теорема 10. *$C^k(\mathrm{IP}_n^k) \geqslant \Omega(n)$ при $k \leqslant \varepsilon \log_2 n$ для достаточно малой константы $\varepsilon > 0$.*

Если бы мы могли распространить этот результат на большее количество участников (пусть даже и для какой-нибудь другой «хорошей» функции f), мы получили бы совершенно сказочные следствия в теории сложности — некоторые из них перечислены в [4]. Однако пока такой результат для наших методов совершенно недоступен.

Нерешенная проблема 4. *Доказать оценку $C^k(\mathrm{IP}_n^k) \geqslant n^\varepsilon$ для, скажем, $k = \lceil (\log_2 n)^2 \rceil$ и некоторой константы $\varepsilon > 0$.*

Коммуникационная сложность для нескольких участников функции DISJ_n^k оставалась неизвестной до самого последнего времени, даже для $k = 3$. Совсем недавний прорыв [8, 19, 5] позволил получить

нижнюю оценку на $C^k(\mathrm{DISJ}_n^k)$, которая нетривиальна вплоть до $k = \varepsilon(\log_2 n)^{1/3}$.

6.3. Коммуникационная сложность задач поиска

До сих пор мы рассматривали функции только с двумя значениями 0 и 1. В теории сложности такие функции часто ассоциируют с *задачами разрешения* или *языками*. Но мы можем рассмотреть и функции более общего вида $f: X \times Y \to Z$, где Z — некоторое конечное множество. Мы можем даже пойти дальше и предположить, что f — *многозначная* функция или, другими словами, такое отношение $R \subseteq X \times Y \times Z$, что для каждой пары (x, y) существует хотя бы один $z \in Z$ («значение» многозначной функции f), для которого $(x, y, z) \in R$. Получив на вход (x, y), протокол P должен выдать на выход любой $z \in Z$, удовлетворяющий условию $(x, y, z) \in R$. Такого типа задачи называются *задачами поиска*.

Изучать сложность для задач поиска еще труднее, чем для задач разрешения. Рассмотрим только один пример, навеянный функцией равенства.

Пусть $X, Y \subseteq \{0,1\}^n$ — непересекающиеся множества строк: $X \cap Y = \varnothing$. Тогда $\mathrm{EQ}(x, y) = 0$ для любых $x \in X$, $y \in Y$, и всегда существует позиция i, в которой эти строки различаются: $x_i \neq y_i$. Пусть задача Анны и Бориса — найти хотя бы одну такую позицию расхождения.

Оказывается, что эта на первый взгляд невинная задача эквивалентна второй по значимости нерешенной проблеме теории сложности [16, 23] (первое место занято знаменитой проблемой равенства классов P и NP). У нас нет никаких идей, как можно доказывать здесь какие-то нижние оценки. Более простая задача получается аналогичным образом из функции DISJ. Вместо $X \cap Y = \varnothing$ мы предполагаем, что для любого входа $(x, y) \in X \times Y$ существует такое i, что $x_i = y_i = 1$. Задача Анны и Бориса — найти какое-нибудь из этих i. Нижние оценки для этой задачи были доказаны в [16, 23, 15]. Из них получаются интересные следствия о глубине *монотонных* схем вычисления булевых функций.

7. Заключение

Мы постарались показать, как быстро, казалось бы, простые и элементарные вопросы переходят в проблемы, не поддающиеся решению в течение десятилетий. В теории вычислительной сложности таких вопросов гораздо больше, и они ожидают новых исследователей. Если этот текст вдохновит по крайней мере кого-то из читателей на то, чтобы заинтересоваться этой областью более основательно, автор сочтет свою задачу полностью выполненной.

8. Обозначения

Поскольку в тексте используется довольно много обозначений, некоторые наиболее важные из них собраны здесь с короткими описаниями и страницей, на которой они впервые появляются.

Меры сложности

$\mathrm{cost}(P)$ *стоимость протокола* P — наибольшее количество битов, которые приходится передать для вычисления значения функции на аргументах (x, y) с помощью протокола P (с. 6)

$C(f)$ *коммуникационная сложность функции* f — минимальная возможная стоимость протокола, вычисляющего f (с. 6)

$\chi(f)$ минимальное количество попарно непересекающихся f-одноцветных прямоугольников, покрывающих область определения функции f (с. 10)

$t(f)$ минимальное количество f-одноцветных прямоугольников, покрывающих область определения функции f (с. 12)

$\chi_0(f)$ минимальное количество попарно непересекающихся f-одноцветных прямоугольников, покрывающих $f^{-1}(\{0\})$ (с. 12)

$\chi_1(f)$ минимальное количество попарно непересекающихся f-одноцветных прямоугольников, покрывающих $f^{-1}(\{1\})$ (с. 12)

$t_0(f)$ минимальное количество f-одноцветных прямоугольников, покрывающих $f^{-1}(\{0\})$ (с. 12)

$t_1(f)$ минимальное количество f-одноцветных прямоугольников, покрывающих $f^{-1}(\{1\})$ (с. 12)

$R(f)$ *вероятностная коммуникационная сложность функции* f *в модели с ограниченной ошибкой* — минимальная стоимость вероятностного протокола, гарантирующего, что на любом входе результат будет правильным с вероятностью не менее $\frac{2}{3}$ (с. 15)

$U(f)$ *вероятностная коммуникационная сложность функции* f *в модели с неограниченной ошибкой* — минимальная стоимость вероятностного протокола, гарантирующего, что на любом входе результат будет правильным с вероятностью более $\frac{1}{2}$ (с. 15)

$\mathrm{Disc}_u(f)$ *отклонение* от равномерного распределения функции f — максимум по всем прямоугольникам разницы количества входов, на которых значение равно 0 и 1 (деленный на $|X \times Y|$, где $X \times Y$ — область определения f) (с. 17)

$Q(f)$ *квантовая коммуникационная сложность* — минимальная возможная стоимость протокола, использующего квантовый компьютер для вычисления f (с. 18)

$C^k(f)$ *коммуникационная сложность для нескольких участников* функции f — минимальное количество битов, которыми должны обменяться k участников для вычисления значения функции f (с. 19)

Двоичные функции

EQ_N *функция равенства* — отображает $\{1, 2, \ldots, N\} \times \{1, 2, \ldots, N\}$ в $\{0, 1\}$; $\mathrm{EQ}_N(x, y) = 1$, если и только если $x = y$ (с. 8)

LE_N *функция «меньше либо равно»* — отображает $\{1, 2, \ldots, N\} \times \{1, 2, \ldots, N\}$ в $\{0, 1\}$; $\mathrm{LE}_N(x, y) = 1$, если и только если $x \leqslant y$ (с. 10)

DISJ_n отображает $\{0, 1\}^n \times \{0, 1\}^n$ в $\{0, 1\}$; $\mathrm{DISJ}_n(x, y) = 1$, если и только если для любого $i \leqslant n$ выполнено хотя бы одно из двух равенств $x_i = 0$ и $y_i = 0$ (с. 11)

IP_n *скалярное произведение по модулю* 2 — отображает $\{0, 1\}^n \times \{0, 1\}^n$ в $\{0, 1\}$; $\mathrm{IP}_n(x, y) = 1$, если и только если количество таких i, что $x_i = y_i = 1$, нечетно (с. 17)

DISJ_n^k отображает $(\{0, 1\}^n)^k$ в $\{0, 1\}$; $\mathrm{DISJ}_n^k(x^1, \ldots, x^k) = 1$, если и только если для любого $i \leqslant n$ найдется такое $v \in \{1, \ldots, k\}$, что $x_i^v = 0$ (с. 19)

IP_n^k *обобщенное скалярное произведение по модулю* 2 — отображает $(\{0, 1\}^n)^k$ в $\{0, 1\}$; $\mathrm{IP}_n^k(x^1, \ldots, x^k) = 1$, если и только если количество таких i, что $x_i^1 = \ldots = x_i^k = 1$, нечетно (с. 19)

Скорость роста функций и др.

$O(f(n))$ $g(n) \leqslant O(f(n)))$ тогда и только тогда, когда существует $C > 0$, такое что $g(n) \leqslant Cf(n)$ для любого n (с. 7)

$\Omega(f(n))$ $g(n) \geqslant \Omega(f(n)))$ тогда и только тогда, когда существует $\varepsilon > 0$, такое что $g(n) \geqslant \varepsilon f(n)$ для любого n (с. 11)

$\lceil x \rceil$ наименьшее целое число $n \geqslant x$ для $x \in \mathbb{R}$ (с. 7)

Список литературы

[1] *A. V. Aho*, *J. D. Ullman*, *M. Yannakakis*. On notions of information transfer in VLSI circuits // Proceedings of the 15th ACM Symposium on the Theory of Computing. New York: ACM Press, 1983. P. 133—139.

[2] *N. Alon*, *P. D. Seymour*. A counterexample to the rank-coloring conjecture // J. Graph Theory 1989. V. 13, № 4. P. 523—525.

[3] *S. Arora*, *B. Barak*. Computational complexity. A modern approach. Cambridge: Cambridge University Press, 2009.

[4] *L. Babai*, *N. Nisan*, *M. Szegedy*. Multiparty protocols, pseudorandom generators for logspace, and time-space trade-offs // J. Comput. System Sci. 1992. V. 45, № 2. P. 204—232.

[5] *P. Beame*, *D.-T. Huynh-Ngoc*. Multiparty communication complexity and threshold circuit size of AC^0. Technical Report TR08-082, Electronic Colloquium on Computational Complexity, 2008.

[6] *E. Ben-Sasson*, *S. Lovett*, *N. Zewi*. An additive combinatorics approach to the log-rank conjecture in communication complexity. ECCC 2011, TR11-157, `http://eccc.hpi-web.de/report/2011/157/`

[7] *H. Buhrman*, *R. Cleve*, *A. Wigderson*. Quantum vs. classical communication and computation // Proceedings of the 30th ACM Symposium on the Theory of Computing (Dallas, TX). New York: ACM Press, 1998. P. 63—86. Препринт: arXiv:quant-ph/9802040v2.

[8] *A. Chattopadhyay*, *A. Ada*. Multiparty communication complexity of disjointness. Technical Report TR08-002, Electronic Colloquium on Computational Complexity, 2008.

[9] *B. Chor*, *O. Goldreich*. Unbiased bits from sources of weak randomness and probabilistic communication complexity // SIAM J. Comput. 1988. V. 17, № 2. P. 230—261.

[10] *S. A. Cook*. On the minimum computation time of functions. Ph. D. thesis, Dept. of Mathematics, Harvard University, 1966.

[11] *J. Forster*. A linear lower bound on the unbounded error probabilistic communication complexity // J. Comput. System Sci. 2002. V. 65, № 4. P. 612—625.

[12] *M. Fürer*. Faster integer multiplication // SIAM J. Comput. 2009. V. 39, № 3. P. 979—1005.

[13] *B. Kalyanasundaram*, *G. Schnitger*. The probabilistic communication complexity of set intersection. SIAM J. Discrete Math. 1992. V. 5, № 4. P. 545—557.

[14] *А. А. Карацуба*, *Ю. П. Офман*. Умножение многозначных чисел на автоматах // ДАН СССР. 1962. Т. 145, № 2. С. 293—294.

[15] *M. Karchmer*, *R. Raz*, *A. Wigderson*. Super-logarithmic depth lower bounds via direct sum in communication complexity // Comput. Complexity. 1995. V. 5, № 3—4. P. 191—204.

[16] *M. Karchmer*, *A. Wigderson*. Monotone circuits for connectivity require super-logarithmic depth // SIAM J. Discrete Math. 1990. V. 3, № 2. P. 255—265.

[17] *I. Kremer*. Quantum communication. Master's thesis, Hebrew University, Jerusalem, 1995.

[18] *E. Kushilevitz, N. Nisan*. Communication complexity. Cambridge: Cambridge University Press, 1997.
[19] *T. Lee, A. Shraibman*. Disjointness is hard in the multiparty number-on-theforehead model // Comput. Complexity. 2009. V. 18, № 2. P. 309—336.
[20] *K. Mehlhorn, E. M. Schmidt*. Las Vegas is better than determinism in VLSI and distributive computing // Proceedings of the 14th ACM Symposium on Theory of Computing. New York: ACM Press, 1982. P. 330—337.
[21] *R. Paturi, J. Simon*. Probabilistic communication complexity // J. Comput. System Sci. 1986. V. 33, № 1. P. 106—123.
[22] *R. Raz, B. Spieker*. On the "log-rank"-conjecture in communication complexity // Combinatorica. 1995. V. 15, № 4. P. 567—588.
[23] *A. Razborov*. Applications of matrix methods to the theory of lower bounds in computational complexity // Combinatorica. 1990. V. 10, № 1. P. 81—93.
[24] *A. Razborov*. The gap between the chromatic number of a graph and the rank of its adjacency matrix is superlinear // Discrete Math. 1992. V. 108, № 1—3. P. 393—396.
[25] *A. Razborov*. On the distributional complexity of disjointness // Theoret. Comput. Sci. 1992. V. 106, № 2. P. 385—390.
[26] *А. А. Разборов*. О квантовой коммуникационной сложности симметричных предикатов // Изв РАН. Сер. мат. 2003. Т. 67 № 1. С. 159—176.
[27] *A. Schönhage, V. Strassen*. Schnelle Multiplikation großer Zahlen // Computing (Arch. Elektron. Rechnen). 1971. Bd. 7. S. 281—292.
[28] *А. Л. Тоом*. О сложности схем из функциональных элементов, реализующих умножение целых чисел // ДАН СССР. 1963. Т. 150, № 3. С. 496—498.
[29] *A. Yao*. Some complexity questions related to distributive computing // Proceedings of the 11th ACM Symposium on the Theory of Computing. New York: ACM Press, 1979. P. 209—213.
[30] *A. Yao*. Quantum circuit complexity // 34th Annual Symposium on Foundations of Computer Science (Palo Alto, CA, 1993). Los Alamitos, CA: IEEE Comput. Soc. Press, 1993. P. 352—361.