Введение в коммуникационная сложность[1].
Мехмат МГУ, весенний семестр, 2012.

В.В. Подольский, А.Е. Ромащенко.

Конспект лекций.

Содержание

[1] Для понимания лекций не требуется предварительных специальных знаний. Предполагается лишь знакомство с начальными курсами общей и линейной алгебры и базовые знания из теории вероятностей.

1 Лекция 1. 17 февраля.

1.1 Детерминированные коммуникационные протоколы и коммуникационная сложность – основные определения.

Мы будем говорить о задачах следующего вида. Пусть имеются два человека (или две машины, два компьютера) которые хотят совместно вычислить значение некоторой функции двух аргументов $f(x, y)$. По традиции мы будем называть первого участника игры Алисой, а второго Бобом. Значение первого аргумента функции (значение x)известно только Алисе, а значение второго аргумента (значение y) известно только Бобу. Алиса и Боб могут обмениваться сообщениями по каналу связи. Требуется вычислить значение $f(x, y)$, переслав по каналу связи минимальное количество информации.

Мы предполагаем, что Алиса и Боб заранее (до того, как им станут известны значения x и y) договариваются о коммуникационном "протоколе" — о наборе соглашений, какие именно данные и в каком порядке они будут пересылать друг другу при тех или иных значениях x, y.

Опишем понятие протокола более формально. Пусть задана некоторая функция $f : X \times Y \to Z$ (для конечных X и Y).

Определение. Коммуникационным протоколом для вычисления некоторой функции из $X \times Y$ в Z называется ориентированное двоичное дерево с корнем и со следующей разметкой на вершинах и рёбрах. Каждая внутренняя вершина дерева помечена буквой A или B. Каждой вершине с пометкой A приписана некоторая функция $g_i : X \to \{0, 1\}$, а каждой вершине с пометкой B приписана некоторая функция $h_j : Y \to \{0, 1\}$ (разным вершинам соответствуют, вообще говоря, разные функции g_i и h_j). Каждому листу дерева сопоставлен некоторый элемент из Z. Каждое ребро в графе помечено нулём или единицей; из каждой вершины, не являющейся листом, выходит по одному ребру с пометкой 0 и одному ребру с пометкой 1.

Данное определение самым общим образом формализует идею "протокола о намерениях", заранее подготовленного Алисой и Бобом. Выполнение протокола можно представлять себе так. Пусть Алисе задано некоторое значение $x \in X$, а Бобу некоторое значение $y \in Y$. Поместим в вершину дерева (протокола) фишку. Далее будем перемещать эту фишку вниз по дереву, последовательно удаляясь от корня, пока она не попадём в один из листьев. Перемещение фишки выполняется следующим образом. Пусть текущая вершина помечена буквой A. Это значит, что текущих ход делает Алиса. Она применяет функцию g_i для текущей вершины к своему значению x. Если $g_i(x) = 0$, то Алиса посылает Бобу по каналу связи бит 0, и фишка перемещается в соседнюю вершину по исходящему ребру с пометкой 0; если же $g_i(x) = 1$, то Алиса посылает Бобу бит 1, и фишка перемещается по исходящему ребру с пометкой 1. Аналогично, для вершин с пометкой B Боб вычисляет $h_j(y)$, посылает значение Алисе, и фишка перемещается в соответствующего сына текущей вершины. Когда фишка попадает в лист

дерева, записанное там значение $z \in Z$ объявляется результатом выполнения протокола.

Мы говорим, что протокол вычисляет $f : X \times Y \to Z$, если для любого $x \in X$ и любого $y \in Y$ при движении из корня по пути, соответствующему заданным x и y, мы попадаем в лист, помеченный $z = f(x, y)$.

Неформальное замечание: наше определение коммуникационного протокола соответствует тому, что ответ $f(x, y)$ узнают и Алиса, и Боб. Более, того, значение $f(x, y)$ может узнать наблюдатель, подслушивающий обмен сообщениями между Алисой и Бобом. Наблюдателю не нужно заранее знать значения x и y, достаточно знать лишь протокол — структуру дерева и разметку на его вершинах.

Определение. Сложностью коммуникационного протокола называется его глубина, т.е., максимальное расстояние от корня до листа. Коммуникационной сложностью функции f называется минимальная сложность протокола, вычисляющего f. Мы будем обозначать её $\mathsf{CC}(f)$.

Докажем несколько тривиальных оценок для коммуникационной сложности функции $f : X \times Y \to Z$.

Свойство 1: $\mathsf{CC}(f) \le \lceil \log |X| \rceil + \lceil \log |Y| \rceil$.

Доказательство: Алиса пересылает своё значение $x \in X$ Бобу, а Боб своё значение $y \in Y$ Алисе. Для этого им нужно отправить $\lceil \log |X| \rceil$ и $\lceil \log |Y| \rceil$ битов соответственно. В результате они оба могут вычислить $f(x, y)$.

Свойство 2: $\mathsf{CC}(f) \le \lceil \log |X| \rceil + \lceil \log |Z| \rceil$.

Доказательство: Алиса пересылает своё значение $x \in X$ Бобу, а Боб вычисляет значение $z = f(x, y)$ и сообщает z Алисе.

Свойство 3: Если функция $f \ X \times Y \to Z$ сюръективна, то $\mathsf{CC}(f) \ge \lceil \log |Z| \rceil$.

Доказательство: Поскольку каждый элемент множества Z может быть получен в качестве значения функции f, в дереве коммуникационного протокола для каждого элемента $z \in Z$ должен быть хотя бы один лист. (Для каждого значения $z \in Z$ в протоколе может быть несколько разных листьев, и мы не знаем, сколько именно. Но можно утверждать, что хотя бы один лист для каждого из z найдётся.) Протокол является двоичным деревом. Если в двоичном дереве имеется не менее $|Z|$ листьев, то его глубина не может быть меньше $\lceil \log |Z| \rceil$.

1.2 Примеры коммуникационных протоколов.

Пример 1: Пусть Алиса и Боб получили по целому числу из интервала $0, \ldots, 2^n - 1$ (числа могут быть стандартным образом представлены строчкой из n битов). Требуется вычислить функцию *максимума*

$$f(x, y) = \max\{x, y\}.$$

Другими словами, участники протокола хотят узнать, кто из них обладает большим числом, и узнать значение этого числа.

Легко увидеть, что коммуникационная сложность этой функции не превосходит $2n$. Первое решение: Алиса посылает своё число Бобу, а Боб посылает своё число Алисе; после этого они оба могут вычислить $\max\{x, y\}$. Второе решение: Алиса посылает своё число Бобу; Боб вычисляет максимум из двух чисел, и отправляет ответ Алисе. В обоих случаях протокола требует переслать по каналу связи $2n$ битов информации.

Упражнение (совсем простое). Постройте дерево для обоих описанных коммуникационных протоколов.

Таким образом, мы выяснили, что $\mathsf{CC}(\max\{x, y\}) \leq 2n$. С другой стороны, из Свойства 3 следует, что $\mathsf{CC}(\max\{x, y\}) \geq n$. Можно ли более точно оценить значение $\mathsf{CC}(\max\{x, y\})$?

Упражнение. Придумайте для функции $\max\{x, y\}$ протокол с как можно меньшей коммуникационной сложностью.

Пример 2: Пусть Алиса и Боб получили по набору чисел из интервала $1, \ldots, 2^n$, то есть $x, y \subset \{1, \ldots, 2^n\}$. Требуется вычислить среднее арифметическое (рациональное число) всех чисел Алисы и Боба. Можно переформулировать задачу так: требуется вычислить среднее арифметическое элементов *мультимножества* $x \cup y$, каждый элемент которого считается с кратностью один, если ровно один из участников получил это число, и с кратностью два, если оба участника получили это число в качестве элемента своего множества.

Коммуникационная сложность этой задачи не превосходит $O(\log n)$. Действительно, нетрудно построить коммуникационный протокол с указанной сложностью: Алис и Боб пересылают друг другу количество элементов, а также сумму всех чисел в x и y. С другой стороны, из Свойства 3 следует, что сложность задачи не меньше $\Omega(\log n)$ (как минимум все целые числа из интервала $1, \ldots, n$ могут появляться в качестве ответа).

Пример 3: Пусть Алиса и Боб получили по набору чисел из интервала $1, \ldots, 2^n$, то есть $x, y \subset \{1, \ldots, 2^n\}$. Требуется вычислить медиану[2] *мультимножества* $x \cup y$ (как и в примере 2, каждый элемент объединения считается с кратностью один, если один из участников имеет это число в своём множестве, или два, если это число было дано обоим участникам).

Отметим, что входные данные Алисы и Боба (в данном примере это подмножества $x, y \subset \{1, \ldots, 2^n\}$) можно представить в виде строчек их n нулей и единиц.

Первая попытка: Начнем с совсем простого протокола. Алиса посылает своё множество Бобу; Боб вычисляет медиану и сообщает ответ Алисе (см. Свойство 2). Коммуникационная сложность данного протокола не превосходит $n + \lceil \log n \rceil$.

[2]Медианой мультимножества целых чисел мы называем его "средний" элемент. Если мультимножество состоит из нечётного числа элементов, $a_1 \leq a_2 \leq \ldots \leq a_{2s+1}$, то его медианой называют число a_{s+1}. В мультимножестве из чётного числа элементов $a_1 \leq a_2 \leq \ldots \leq a_{2s}$ мы будем называть медианой элемент a_s.

Вторая попытка: Рассмотрим несколько более сложный протокол, имеющий гораздо меньшую коммуникационную сложность. Идея состоит в том, что Алиса и Боб совместными усилиями последовательно уточняют верхнюю и нижнюю оценку для медианы в объединении $x \cup y$, пока эти оценки не совпадут.

Для простоты рассмотрим сначала случай, когда $|x| = |y| = 2^k$ (и Алиса, и Боб получили множества одинакового размера, причем число элементов в этих множествах является степенью двойки: $x = \{a_1, \ldots, a_{2^k}\}$ и $y = \{b_1, \ldots, b_{2^k}\}$, $k > 1$). Будем считать для определённости, что $a_1 < a_1 < \ldots < a_{2^k}$ и $b_1 < b_1 < \ldots < b_{2^k}$.

Алиса и Боб находят медианы в своих множествах ($\mathsf{med}(x) = a_{2^{k-1}}$ и $\mathsf{med}(y) = b_{2^{k-1}}$) и сообщают их друг другу. Ясно, что медиана объединения $m = \mathsf{med}(x \cup y)$ лежит между $\mathsf{med}(x)$ и $\mathsf{med}(y)$. Можно сделать и более сильное утверждение: медиана мультимножества $x \cup y$ совпадает с медианой другого мультимножества — объединения

$$x' = \{a_{2^{k-1}}, \ldots, a_{2^k}\} \text{ и } y = \{b_1, \ldots, b_{2^{k-1}}\}$$

(мы можем отбросить половину самых маленьких элементов x и половину самых больших элементов y, и это не изменить медиану в объединении оставшихся элементов).

Таким образом, Алиса и Боб могут перейти к рассмотрению вдвое меньших множеств x' и y', сохранив значение медианы объединения. Через k итераций размеры множеств Алисы и Боба сократятся до 1 элемента, и медиану двухэлементного объединения можно будет узнать, обменявшись значениями оставшихся элементов x и y.

На каждом шаге протокола Алиса и Боб обмениваются $O(\log n)$ битами информации. Число итераций равно $k = \lceil \log n \rceil$. Таким образом, коммуникационная сложность получившегося протокола равна $O(\log^2 n)$.

Остаётся решить небольшую техническую проблему: что делать, если исходные множества x и y имеют неравные размеры, и число элементов в них не равно степени двойки. Мы сведем общую задачу к уже рассмотренному частному случаю. Для этого мы выберем наименьшую степень двойки $2^k \geq n$ (2^k менее, чем вдвое превосходит n) и добавим в x и y некоторые "лишние" элементы так, чтобы в результате размер обоих множеств стал равен 2^k. Мы хотим, чтобы после добавления новых элементов медиана объединения осталась бы прежней. Это можно гарантировать, если добавлять к x и y элементы 1 и n с соответствующей кратностью (в результате исходные множества x и y из множеств превратятся в *мультимножества*, но это нам не помешает).

Итак, опишем коммуникационный протокол для общего случая. Прежде всего Алиса и Боб сообщают друг другу размеры своих исходных x и y. Если оба множества состоят из четного числа элементов, то Алиса добавляет к своему x равное число копий чисел 1 и n (по $(2^k - |x|)/2$ штук) с тем, чтобы в итоге с учетом кратностей размер нового мультимножества стал равен 2^k. Аналогично, Боб добавляет к своему множеству y равное число копий 1 и n

(по $(2^k - |y|)/2$). Поскольку Алиса и Боб добавили к своим множество равное количество копий минимального элемента 1 и максимального элемента n, медиана объединения полученных расширений x и y совпадает с медианой объединения первоначальных множеств.

Если оба исходных множества x и y состоят из нечётного числа элементов, то Алиса добавляет к своему x на одну копию элемента 1 больше, чем копий n; а Боб, напротив, добавляет на одну копию n больше. В результате оба множества расширяются до 2^k элементов, и медиана их объединения не меняется. Если же чётность исходных множеств x и y различна, то к одному из них (чётного размера) добавляется равное число копий 1 и n, а к другому (нечётного размера) — на одну копию числа n больше.

Остаётся отметить, что "подготовительная" часть протокола (расширение x и y до мультимножеств размера 2^k) требует от Алисы и Боба обмена не более чем $O(\log n)$ битами. Таким образом, итоговая коммуникационная сложность протокола равна $O(\log^2 n)$.

Третья попытка: Далее мы улучшим описанный выше протокол и уменьшим коммуникационную сложность протокола до $O(\log n)$. Как мы уже объяснили выше, можно считать, что x и y оба имеют размер 2^k (для преобразования исходных множеств в мультимножества со свойством $|x| = |y| = 2^k$ Алисе и Бобу нужно обменяться $O(\log n)$ битами). Далее мы модифицируем протокол из 2-ой *попытки*.

На каждом шаге протокола Алиса и Боб будут оба знать некоторые приближения (m снизу и M сверху) к истинному значению медианы $x \cup y$. В начале эти приближения тривиальны: медиана заведомо лежит между 1 и 2^k. В конце протокола найденные приближения к значению медианы совпадут между собой; это будет означать, что истинное значение медианы найдено.

Мы пользуемся планом из 2-ой *попытки*: на каждом шаге Алиса и Боб находят медиану в своих текущих множествах (назовём эти медианы m_a и m_b) и пытаются их сравнить. Ранее мы предполагали, что Алиса и Боб полностью пересылают друг другу числа m_a и m_b. Теперь они будут действовать более аккуратно: сначала они обменяются старшими битами в двоичной записи m_a и m_b, затем вторыми по старшинству битами этих чисел, и т.д., пока не будет найден самый старший разряд, в котором числа m_a и m_b различаются. Этой информации уже достаточно, чтобы отбросить половину элементов x и половину элементов y и перейти к следующему шагу. Так что младшие биты m_a и m_b пересылать не нужно.

Кроме того, полученной информации достаточно, чтобы уточнить текущее приближение к медиане $x \cup y$ снизу и сверху. В самом деле, медиана $x \cup y$ должна лежать между m_a и m_b. Пусть, например, Алиса и Боб выяснили, что

$$m_a = 10110...$$

и

$$m_b = 10111...$$

(в пятом справа разряде найдено первое различие между m_a и m_b, и на

этом обмен информации на данном шаге заканчивается). Теперь Алиса и Боб знают, что медиана лежит между числам 1011000... и 10111111....

На следующем шаге при обмене новыми значениями m_a и m_b (для вдвое уменьшенных x и y) Алисе и Бобу не нужно начинать со старших разрядов: они заранее знаю, что новые m_a и m_b лежат между известными на данным момент приближениями сверху и снизу к значению медианы. В нашем примере m_a и m_b заведомо начинаются на 1011... Таким образом, Алиса и Боб могут начать обмен значениями m_a и m_b сразу с 5-го по старшинству разряда.

В результате, для выяснения каждого следующего разряда двоичной записи медианы Алиса и Боб обмениваются $O(1)$ битами информации. Следовательно, коммуникационная сложность получившегося протокола равна $O(\log n)$.

2 Лекция 2. 24 февраля.

На этой лекции мы изучим технику для доказательства нижних оценок для коммуникационной сложности функций.

2.1 Простейшие теоретико-информационные оценки.

Рассмотрим функцию побитового *исключающего или*

$$\mathsf{XOR}(x, y) : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$$

($\mathsf{XOR}(x_1, \ldots, x_n, y_1, \ldots, y_1) = x_1 \oplus y_1, \ldots, x_n \oplus y_n$, в каждом разряде биты Алисы и Боба складываются по модулю 2). Ясно, что $\mathsf{CC}(\mathsf{XOR}) \leq 2n$, для нахождения ответа Алисе и Бобу достаточно послать друг другу свои входы x и y. Интуитивно кажется, что это оптимальный протокол. В самом деле, если Алиса кроме своего входа x узнает после выполнения протокола ещё и значение $\mathsf{XOR}(x, y)$, она тем самым узнает y. Аналогично, Боб узнает значение x. Это значит, что так или иначе Алиса и Боб обязаны сообщить друг другу свои входы. А это значит, что в протоколе необходимо послать по n битов в каждом направлении, и сложность протокола невозможно сделать меньше $2n$.

Эта интуиция верна. Однако утверждение требует более строго доказательства. Формальная трудность состоит в том, что мы не можем гарантировать, что *при любых* входах x и y Алиса и Боб посылают друг другу по n битов. В самом деле, нетрудно придумать такой протокол, в котором *при некоторых* x и y Алиса или Боб (или даже одновременно оба участника) посылают значительно меньше битов. Мы должны доказать тем не менее, что для любого протокола, вычисляющего XOR, найдутся такие x и y, для которых и Алиса, и Боб обязаны послать своему визави не меньше n битов.

Зафиксируем некоторый коммуникационный протокол Π для вычисления XOR. Будем говорить, что пара $(x, y) \in \{0,1\}^n \times \{0,1\}^n$ *трудна для*

Алисы, если при выполнении протокола при данных входах Алиса посылает Бобу не менее n битов; аналогично, пара (x, y) *трудна для Боба*, если при выполнении протокола с данными входами Боб посылает Алисе не менее n битов. Нам нужно доказать, что есть хотя бы одна пара входов, которая трудна одновременно и для Алисы, и для Боба (это означает, что сложность протокола не меньше $2n$).

Лемма. Для любого входа Алисы x найдется строго больше 2^{n-1} входов Боба y таких: что пара (x, y) трудна для Алисы.

Доказательство леммы: При фиксированном x и различных y можно получить любое из 2^n значение $\mathsf{XOR}(x, y)$. Следовательно, при фиксированном x и разных y можно достичь 2^n разных листьев протокола. Некоторые из этих листьев могут находиться на расстоянии от корня меньше n. Однако таких листьев строго меньше 2^n. В самом деле, во всяком двоичном дереве число листьев на расстоянии менее n от корня не может быть больше 2^{n-1}, причём строгое равенство достигается только для полного двоичного дерева глубины $n-1$. Случай полного двоичного дерева мы можем отбросить — в нашем случае общее число листьев равно 2^n. Таким образом, больше половины листьев должны быть на расстоянии не менее n от корня, и лемма доказана.

Итак, более половины пар входов (x, y) трудны для Алисы. Аналогично, более половины пар входов трудны для Боба. Следовательно, найдётся пара, которая трудна сразу для обоих участников протокола. Это значит, что сложность протокола не меньше $2n$, что и требовалось доказать.

2.2 Одноцветные комбинаторные прямоугольники.

Теоретико-информационные оценки, подобные рассуждению из главы 2.1 работают лишь для очень специальных функций f. В этой главе мы изучим более мощный инструмент для доказательства нижних оценок коммуникационной сложности.

Определение 1. Множество $S \subset X \times Y$ называется *комбинаторным прямоугольником* (или просто *прямоугольным множеством*), если существуют такие $A \subset X$ и $B \subset Y$, что $S = A \times B$.

Определение 2. Множество $S \subset X \times Y$ называется *комбинаторным прямоугольником*, если для любых двух пар (x, y) и (x', y') из S пара (x, y') также принадлежит S.

Лемма. Определение 1 и Определение 2 эквивалентны.

Доказательство леммы: Определение 2 очевидно следует из определения 1. Для доказательства эквивалентности предположим, что некоторое множество S удовлетворяет определению 2. Обозначим через A и B проекции S на первую и вторую координаты. Нам нужно проверить, что S совпадает с декартовым произведением $A \times B$.

Пусть $x \in A$; это означает, что для некоторого v пара (x, v) принадлежит S. Далее, пусть $y \in B$; это означает, что некоторого w пара (w, y) принадлежит S. Согласно определению 2 мы можем заключить, что (x, y) ("гибридизация" (x, v) и (w, y)) также принадлежит S. Лемма доказана.

Пусть П – некоторый коммуникационный протокол для вычисления функции $f : X \times Y \to Z$, и l один из листьев данного протокола. Назовем S_l множество всех таких пар $(x, y) \in X \times Y$, что на входе (x, y) Алиса и Боб (следуя протоколу П) приходят в лист l.

Утверждение. Для всякого коммуникационного протокола П и для всякого листа l в этом протоколе множество S_l является комбинаторным прямоугольником.

Доказательство: Удобно воспользоваться вторым определением прямоугольного множества. Пусть на входах (x, y) и (x', y') Алиса и Боб попадают в один и тот же лист l. Тогда и на входе (x, y') они попадут в тот же самый лист. В самом деле, запустим протокол на входе (x, y'). Индукцией по номеру шага протокола можно показать следующее. На каждом шаге вся информация, доступная в данный момент Алисе (собственный вход x и сообщения, полученные ранее от Боба), не отличается от информации, известной Алисе при работе на входах (x, y). Это значит, что на каждом шаге Алиса будет вести себя также (посылать такие же сообщения), что в случае (x, y). Аналогично, информация известная Бобу неотличима от информации, известной ему при выполнении протокола на входе (x', y'). Следовательно, при работе с входами (x, y') Боб будет на каждом шаге посылать такие же сообщения, что и при работе с входами (x', y').

Итак, на паре входов (x, y') для Алисы ситуация оказывается неотличимой от входов (x, y), а для Боба ситуация неотличима от (x', y'). Следовательно, протокол приведёт их в тот же лист l.

Тоже рассуждение можно изложить другими словами. Рассмотрим путь в дерево протокола от корня к листу l. Известно, что на входах (x, y) и (x', y') Алиса и Боб проходят вдоль этого пути. В некоторых вершинах этого пути решение принимает Алиса; нам известно, что значение x согласовано с этими решениями (имея вход x Алиса не видит причин "свернуть" с этого пути). В других вершинах данного пути решение принимает Боб; нам известно, что значение y' согласовано с этими решениями Боба (имея вход y' Боб тоже не видит причин свернуть с пути к листу l). Таким образом, на паре входов (x, y') Алиса и Боб пройдет весь этот путь до листа l.

Доказанное утверждение показывает, что коммуникационный протокол для вычисления функции f задаёт разбиение $X \times Y$-таблицы значений f на прямоугольные множества, соответствующие листьям. Поскольку каждому листу протокола приписано одно значение функции f, эти прямоугольные множества являются *одноцветными*, т.е., во всех точках такого прямоугольного множества функция f принимает одно и то же значение.

Подведём итог: всякий протокол с l листьями (вычисляющий функцию f) задаёт разбиение таблицы значений f на l одноцветных прямоугольных множеств. Чтобы доказать, что коммуникационная сложность функции f больше n, достаточно показать, что таблицу значений n невозможно разбить на $\leq 2^n$ одноцветных множеств.

Пример. Рассмотрим предикат равенства $\mathsf{EQ} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$.

$$\mathsf{EQ}(x,y) = \begin{cases} 1, \text{ если } x = y \\ 0, \text{ если } x \neq y \end{cases}$$

Очевидно, что $\mathsf{CC}(\mathsf{EQ}) \leq n+1$. Сейчас мы докажем, что коммуникационная сложность этой функции в точности равна $n+1$.

Таблица значений EQ устроена очень просто: на диагонали стоят единицы, вне диагонали – нули. Покажем, что эту таблицу нельзя разрезать на $\leq 2^n$ одноцветных прямоугольников.

Достаточно доказать, что разбиении данной таблицы должно быть ровно 2^n прямоугольных множеств для значения 1 (и ещё некоторое ненулевое число прямоугольных множеств для значения 0). Мы утверждаем, что каждое прямоугольное множество для значения 1 будет тривиальным, оно будет содержать ровно одну пару (u,u). В самом деле, если в прямоугольное множество входить две разные пары (u,u) и (v,v), то в это же множество должна входить "гибридная" пара (u,v). Но это невозможно, поскольку $\mathsf{EQ}(u,u) = \mathsf{EQ}(v,v) = 1$, а $\mathsf{EQ}(u,v) = 0$.

Упражнение. Рассмотрим функцию $\mathsf{GT} : \{1,\ldots,2^n\} \times \{1,\ldots,2^n\} \to \{0,1\}$

$$\mathsf{GT}(x,y) = \begin{cases} 1, \text{ если } x > y, \\ 0, \text{ если } x \leq y. \end{cases}$$

Докажите, что $\mathsf{CC}(\mathsf{GT}) = n+1$.

2.3 Метод трудного множества.

В этой главе мы изучим другой метод получения оценок, также связанный с одноцветными прямоугольными множествами.

Определение. Для функции $f : X \times Y \to Z$ будем называть множество $S \subset X \times Y$ *трудным* (в англоязычной литературе *a fooling set*), если найдется такое $z \in Z$, что

(1) для всякой пары $(x,y) \in S$ имеем $f(x,y) = z$, и

(2) для любых двух (несовпадающих) пар $(x,y), (x',y') \in S$ имеем $f(x,y') \neq z$ или $f(x',y) \neq z$.

Теорема. Если для функции $f : X \times Y \to Z$ имеется трудное множество размера K, то $\mathsf{CC}(f) > \log K$.

Доказательство: Пусть S является трудным множество для f, и для всякой пары $(x,y) \in S$ значение f равно z. Тогда во всяком протоколе для

вычисления f должно быть не менее K листьев соответствующих данному значению z. (Отсюда мы можем заключить, что $\mathsf{CC}(f)$ *строго* больше $\log K$, поскольку в протоколе должны быть ещё и листья с другими пометками z'.)

Предположим противное: пусть есть коммуникационный протокол, в котором число листьев с пометкой z меньше K. Тогда найдется хотя бы один лист, в который Алиса и Боб попадают для двух разных пар входов из S. Обозначим эти пары (x, y) и (x', y'). Мы знаем, что множество пар входов для каждого листа протокола является комбинаторным прямоугольником. Это значит, что следуя протоколу на "гибридных" входах (x, y') и (x', y) Алиса и Боб приходят в тот же самый лист. Но по определению трудного множества хотя бы одно из значений $f(x', y)$, $f(x, y')$ отлично от z. Это противоречит тому, что протокол вычисляет данную функцию f.

Пример 1. Рассмотрим ещё раз уже известный нам предикат равенства EQ. В качестве трудного множества можно взять

$$S = \{(u, u,) \mid u \in \{0,1\}^n\}$$

(на всех парах (u, u) из S предикат равенства равен единице, а на всех "гибридных" парах (u, u') предикат равен нулю). Из доказанной теоремы следует, что $\mathsf{CC}(\mathsf{EQ}) \geq n + 1$.

Упражнение. Докажите с помощью метода трудных множеств, что $\mathsf{CC}(\mathsf{GT}) \geq n + 1$.

Пример 2. Рассмотрим предикат дизъюнктности: x и y являются подмножествами $\{1, \ldots, n\}$, и

$$\mathsf{DISJ}(x, y) = \begin{cases} 1, \text{ если } x \cap y = \emptyset, \\ 0, \text{ иначе .} \end{cases}$$

Как обычно, очевидна оценка $\mathsf{CC}(\mathsf{DISJ}) \leq n + 1$. Покажем, что $\mathsf{CC}(\mathsf{DISJ})$ в точности равно $n + 1$.

В качестве трудного множества возьмём

$$S = \{(u, \{1, \ldots, n\} \setminus u) \mid u \subset \{1, \ldots, n\}\}.$$

Действительно, с одной стороны, для каждой пары $(u, \bar{u}) \in S$ значение $\mathsf{DISJ}(u, \bar{u}) = 1$. С другой стороны, для любых двух пар $(u, \bar{u})$ и $(v, \bar{v})$ из S имеем две возможности:

(1) либо u не лежит внутри v, а значит u пересекается с $\bar{v}$,

(2) либо u лежит внутри v, а значит $\bar{u}$ пересекается с v.

Таким образом, мы имеем трудное множество из 2^n элементов. Следовательно, $\mathsf{CC}(\mathsf{DISJ}) > n$.

3 Лекция 3. 2 марта.

3.1 Получение нижних оценок с помощью ранга матрицы

Пусть Алиса и Боб хотят вычислить значение некоторого функции

$$f : X \times Y \to \{0, 1\}.$$

Как обычно, считаем, что Алисе известно значение $x \in X$, а Бобу известно $y \in Y$. Мы покажем, что коммуникационную сложность f можно оценить с помощью ранга матрицы, соответствующей этой функции.

Обозначим M_f матрицу размера $|X| \times |Y|$, представляющую функцию f. Будем считать, что строки матрицы соответствуют элементам X (входы Алисы), а столбцы соответствуют элементам Y (входы Боба). На пересечении x-ой строки и y-ого столбца будет стоять соответствующее значение функции $f(x, y)$. Таким образом, матрица заполнена нулями и единицами.

Мы будем рассматривать M_f как числовую матрицу над полем вещественных чисел; ранг её будем обозначать $\mathsf{rk}(M_f)$.

Утверждение 1. Для любой функции $f : X \times Y \to \{0, 1\}$

$$\mathsf{CC}(f) \geq \log \mathsf{rk}(M_f)$$

Доказательство: Рассмотрим произвольный коммуникационный протокол Π для вычисления f. Этот протокол есть двоичное дерево с листьями, помеченными нулями и единицами. Мы покажем, что число листьев Π с пометкой 1 не меньше $\mathsf{rk}(M_f)$. Отсюда немедленно следует доказываемое Утверждение.

Для каждого листа l_i в протоколе Π мы рассмотрим множество пар $(x, y) \in X \times Y$, согласованных с данным листом (точнее, множество всех таких пар, которые при выполнении протокола приводят Алису и Боба в данный лист). Из прошлой лекции мы уже знаем, что множество всех таких пар является комбинаторным прямоугольником. Это значит, что существуют такие $A_i \subset X$ и $B_i \subset Y$, что пара (x, y) приводит Алису и Боба в лист l_i, если и только если $x \in A_i$ и $y \in B_i$.

Обозначим M_i матрицу размера $|X| \times |Y|$, у которой единицы стоят на пересечении строк $x \in A_i$ и столбцов $y \in B_i$, а в остальных местах стоят нули. Нетрудно видеть, что для протокола Π, вычисляющего функцию f, выполнено

$$M_f = \sum_{\text{все листья } l_i \text{ с пометкой } 1} M_i$$

Отметим, что для разных листьев протокола множества единиц в матрицах M_i попарно не пересекаются.

Каждая матрица M_i содержит строки двух видов: строки из одних нулей и столбцы с единицами в позициях B_i. Ранг такой M_i равен единице.

Ранг суммы нескольких матриц не превосходит суммы рангов слагаемых. Следовательно,

$$\mathsf{rk}(M_f) \leq \text{число всех листьев протокола с пометкой 1.}$$

Утверждение доказано.

В доказательстве Утверждения 1 мы учитывали только листья с пометкой единица. Понятно, что аналогичное рассуждение можно провести и для листьев с пометкой ноль. Формально мы должны перейти от функции f к её отрицанию $\bar{f}(x,y) = 1 - f(x,y)$. При этом в матрице функции все нули заменятся на единицы и наоборот:

$$M_{\bar{f}} = \begin{pmatrix} 1111\ldots1 \\ 1111\ldots1 \\ \ldots\ldots\ldots \\ 1111\ldots1 \end{pmatrix} - M_f$$

Поскольку матрица $|X| \times |Y|$, состоящая из одних единиц, имеет ранг 1, разница рангов M_f и $M_{\bar{f}}$ не превышает единицы.

Далее мы можем повторить рассуждение из Утверждения 1 для листьев, соответствующих нулевому значению функции f. Получаем

$$\mathsf{rk}(M_{\bar{f}}) \leq \text{число всех листьев протокола с пометкой 0.}$$

Следовательно, общее число всех листьев в протоколе для вычисления f не может быть меньше

$$\mathsf{rk}(M_f) + \mathsf{rk}(M_{\bar{f}}) \geq 2\mathsf{rk}(M_f) - 1.$$

Таким образом, мы получаем усиление Утверждения 1:

Утверждение 1'. Для любой функции $f : X \times Y \to \{0,1\}$

$$\mathsf{CC}(f) \geq \log(2\mathsf{rk}(M_f) - 1).$$

Пример 1. Для предиката равенства $\mathsf{EQ}(x,y)$ матрица M_{EQ} устроена совсем просто — это диагональная матрица $2^n \times 2^n$. Ранг этой матрицы равен 2^n. Получаем

$$\mathsf{CC}(\mathsf{EQ}_n) \geq \log(2 \cdot 2^n - 1) \geq n.$$

Таким образом, мы ещё раз доказали, что коммуникационная сложность предиката равенства равна $(n+1)$.

Пример 2. Рассмотрим функцию скалярного произведения по модулю 2: для $x, y \in \{0,1\}^n$

$$\mathsf{IP}(x,y) = \sum x_i y_i \pmod 2.$$

Мы используем обозначение IP, принятое в англоязычной литературы (сокращение слов *inner product*).

Мы покажем, что функция $\mathsf{IP}(x, y)$ имеет коммуникационную сложность $n + 1$. Существование протокола с такой сложностью очевидно (например, Алиса сообщает Бобу своё значение x, а Боб возвращает Алисе значение $\mathsf{IP}(x, y)$). Для доказательства нижней оценки на $\mathsf{CC}(\mathsf{IP})$ мы воспользуемся методом ранга матрицы.

Матрица M_{IP} устроена довольно непросто. Удобно перейти к рассмотрению её квадрата: обозначим $N = (M_{\mathsf{IP}})^2$ (обычное возведение в квадрат матрицы над полем вещественных чисел).

Матрица N имеет размер $2^n \times 2^n$, и её строки и столбцы удобно нумеровать строчками из n нулей и единиц. По определению матрицы N, её элементы можно записать следующим образом:

$$(N)_{x,y} = \sum_{z \in \{0,1\}^n} \mathsf{IP}(x, z) \cdot \mathsf{IP}(z, y).$$

Если x или y состоит из одних нулей, то и данная сумма равна нулю. Это значит, что вся первая строка и весь первый столбец N равен нулю.

Если $x = y \neq 00\ldots0$, то $(N)_{x,x}$ есть число всех таких z, скалярное произведение которых с x дает единицу (по модулю 2). Иначе говоря, нас интересует число решений $z = (z_1, \ldots, z_n)$ линейного уравнения

$$x_1 z_1 + x_2 z_2 + \ldots + x_n z_n = 1$$

над полем из двух элементов. Поскольку уравнение невырождено (x не тождественный нуль), то размерность пространства решений (над полем из двух элементов) равна $n - 1$, а число таких решений равно 2^{n-1}.

Если же $x \neq y$ и обе строки x, y ненулевые, то $(N)_{x,y}$ есть число всех таких z, скалярное произведение которых одновременно и с x, и с y дает единицу по модулю 2. Это значит, что нас интересует число решений невырожденной системы из двух линейных уравнений с n неизвестными (снова над полем из двух элементов). Размерность пространства решений такой системы равна $n - 2$, и число решений есть 2^{n-2}.

Теперь у нас есть полное описание матрицы N: первая строка и первый столбец заполнены нулями; все диагональные элементы кроме первого равны 2^{n-1}; все остальные элементы равны 2^{n-2}:

$$N = \begin{pmatrix} 0 & 0 & 0 & 0 & \ldots & 0 \\ 0 & 2^{n-1} & 2^{n-2} & 2^{n-2} & \ldots & 2^{n-2} \\ 0 & 2^{n-2} & 2^{n-1} & 2^{n-2} & \ldots & 2^{n-2} \\ 0 & 2^{n-2} & 2^{n-2} & 2^{n-1} & \ldots & 2^{n-2} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 2^{n-2} & 2^{n-2} & 2^{n-2} & \ldots & 2^{n-1} \end{pmatrix}.$$

Нетрудно проверить, что ранг этой матрицы равен $2^n - 1$.

Теперь мы можем определить $\mathsf{rk}(M_{\mathsf{IP}})$. С одной стороны, ранг должен быть меньше 2^n (если бы матрица имела полный ранг, то и её квадрат тоже

имел бы полный ранг и не мог бы иметь нулевую строки и нулевой столбец). С другой стороны, при возведении в квадрат ранг матрицы не мог возрасти. Следовательно, $\mathsf{rk}(M_{\mathsf{IP}})$ тоже равен $2^n - 1$.

Теперь мы можем применить Утверждение 1' и заключить, что $\mathsf{CC}(\mathsf{IP}) \geq n + 1$.

3.2 Минимальное число листьев vs минимальная глубина для коммуникационных протоколов

Для всякой функции $f : X \times Y \to Z$ можно рассмотреть три параметра: (1) коммуникационная сложность $\mathsf{CC}(f)$ (минимальная глубина дерева коммуникационного протокола для f), (2) минимальное число листьев в протоколе, вычисляющем f, и (3) минимальное число одноцветных прямоугольников, на которые можно разбить матрицу M_f. Между этими тремя значениями есть очевидные соотношения:

минимальное число одноцветных прямоугольников в разбиении $M_f \leq$

$\leq$ минимальное число листьев в протоколе для вычисления $f \leq 2^{\mathsf{CC}(f)}$.

Данные неравенства нельзя заменить на равенства — не всякое разбиение M_f на одноцветные прямоугольные множества соответствует некоторому протоколу. Интересно было бы установить, насколько велика может быть разница между $\mathsf{CC}(f)$ и логарифмом минимального число одноцветных прямоугольников в разбиении матрицы M_f (скажем, являются ли эти величины полиномиально связанными). Этот вопрос остаётся открытым и, по-видимому, очень сложен.

А вот разницу между $\mathsf{CC}(f)$ и *минимальным число листьев* в протоколе для вычисления f оценить нетрудно. Эти две величины не могут отличаться больше, чем в константу раз. Нужно иметь в виду, что бывают коммуникационные протоколы, в которых глубина значительно больше логарифма числа листьев (это означает, что дерево протокола очень несбалансировано). Но такие патологические коммуникационные протоколы можно переделать в другие, более сбалансированные:

Утверждение 2. Для всякой функции $f : X \times Y \to Z$

$\mathsf{CC}(f) \leq 3 \log_2$[минимальное число листьев в протоколе для вычисления f].

Более точно, всякий протокол Π с l листьями для вычисления f можно переделать в другой протокол Π', глубина которого не будет превосходить $3\lceil \log_2 l \rceil$.

Доказательство: Мы воспользуемся несложной комбинаторной леммой:

Лемма. В двоичном дереве с l листьями можно найти внутреннюю вершину u, которая разбивает граф на три части, каждая из которых содержит не более $l/2$ листьев. (Одна из трёх частей может быть пустой – в некоторых случаях корень разбивает дерево на две части с ровно $l/2$ листьями в каждой.)

Доказательство леммы: Каждой внутренней вершине u дерева соответствует поддерево с некоторым числом листьев (обозначим его l_u). Выберем самую низкую (самую далекую от корня) вершину u, для которой $l_u > l/2$. Назовём v и w сыновей u. Тогда, во-первых, поддеревья для v и w содержат не более $l/2$ листьев. И, во-вторых, число листьев, не лежащих ниже u, будет меньше $l - l_u < l/2$. Лемма доказана.

Теперь опишем новый протокол Π' для вычисления f. Прежде всего, зафиксируем вершину u, которая делит исходный протокол на три части, в каждой из которых $\leq l/2$ листьев. Для определённости будем считать, что u соответствует ходу Алисы.

В новом протоколе Алиса и Боб сначала сообщают друг другу, согласованы ли их входы x и y с путём из корня в вершину u в исходном протоколе. Если оказывается, что согласованы, то Алиса сообщает Бобу, следует ли при заданном (известном ей) значении x перейти к левому или к правому сыну u.

Таким образом, обменявшись 3 битами, Алиса и Боб уменьшают вдвое (по крайней мере до $l/2$) число потенциально возможных листьев в протоколе Π — потенциально достижимыми остаются либо все потомки левого сына u, либо потомки правого сына u, либо листья вне поддерева u.

Удалив из Π все заведомо недостижимые листья, мы получаем новый протокол Π_1, в котором остаётся $l_1 \leq l/2$ листьев. Далее можно снова повторить тот же приём: находим в Π_1 вершину, которая разбивает протокол на три части с не более чем $l_1/2$ листьями, Алиса и Боб обмениваются 3 битами и выбирают из этих трёх частей одну, и т.д.

На каждой итерации данной конструкции Алиса и Боб обмениваются не более чем тремя битами, и число остающихся листьев сокращается минимум вдвое. В итоге мы получаем новый протокол, сложность которого не больше $3\lceil \log_2 l \rceil$.

4 Лекция 4, 11 марта.

4.1 Недетерминированная коммуникационная сложность.

Как и раньше, мы изучаем коммуникационные протоколы для вычисления некоторой функции $f : X \times Y \to Z$ в ситуации, когда Алисе известно значение $x \in X$, а Бобу $y \in Y$. Мы по-прежнему считаем, что Алиса и Боб заранее (ещё не зная свои значения x и y) договариваются о *коммуникационном протоколе*, т.е., о правилах, по которым они будут обмениваться информацией по каналу связи. Однако теперь мы допускаем *недетерминированные* протоколы – протоколы, в которых каждое очередное действие

Алисы (или Боба) не определяется однозначно значением x (или, соответственно, y).

В недетерминированных коммуникационных протоколах мы предполагаем, что Алиса и Боб *угадывают* некоторые полезные "подсказки" n_a и n_b соответственно. Эти подсказки позволяют им более эффективно вычислить значение функции f. Для любой пары входов (x, y) при удачно угаданных подсказках протокол приводит игроков к верному ответу $f(x, y)$. При этом для любых (x, y), каковы бы ни были подсказки n_a и n_b, они не могут привести к неправильному ответу. Однако, если "подсказки" оказались неудачными, то Алиса и Боб могут не получить никакого ответа. Далее мы дадим более формальное определение.

Определение. Недетерминированным коммуникационным протоколом для вычисления функции из $X \times Y$ в Z называется двоичное дерево с выделенным корнем, со следующей разметкой. Каждая внутренняя вершина дерева помечена буквой A или B. Каждой вершине с пометкой A приписана некоторая функция $g_i : X \times Adv_a \to \{0, 1\}$, а каждой вершине с пометкой B приписана некоторая функция $h_j : Y \times Adv_b \to \{0, 1\}$ (разным вершинам соответствуют, вообще говоря, разные функции g_i и h_j). Каждому листу дерева сопоставлен либо некоторый элемент из Z, либо знак **?** (неопределённость).

Мы считаем, что недетерминированный коммуникационный протокол вычисляет некоторую функцию $f : X \times Y \to Z$, если выполнены следующие условия:

1. для любых $x \in X$ и $y \in Y$ найдутся такие "советы" $n_a \in Adv_a$ и $n_b \in Adv_b$, что следуя ветви дерева (протокола), соответствующего данной четвёрке (x, n_a, y, n_b) Алиса и Боб попадают в лист, помеченный значением $f(x, y)$;

2. для любых $x \in X$ и $y \in Y$ и для любых "советов" $n_a \in Adv_a$ и $n_b \in Adv_b$, следуя ветви протокола для данной четвёрки (x, n_a, y, n_b), Алиса и Боб могут попасть либо в некоторый лист, помеченный значением $f(x, y)$, либо в некоторый лист с пометкой неопределённость (но не могут попасть в лист, помеченный значением $z \in Z$ отличным от $f(x, y)$).

   Сложностью недетерминированного протокола называется глубина его дерева (максимальное расстояние от корня до листа). Недетерминированной коммуникационной сложностью функции f называется минимальная сложность недетерминированного протокола для вычисления f. Мы обозначаем недетерминированную сложность функции $\mathsf{NCC}(f)$.

   Утверждение. Всякий недетерминированный протокол сложности k можно переделать в недетерминированный "двухраундовый" протокол сложности $k + 1$ (вычисляющий ту же функцию). Двухраундовость означает, что в новом протоколе сначала Алиса посылает Бобу k битов, а затем Боб посылает один бит Алисе.

Доказательство: Пусть n_a и n_b обозначают подсказки Алисы и Бобы в исходном протоколе. В новом протоколе Боб получает старую подсказку n_b, а Алиса новую подсказку n'_a, которая в "удачном" случае понимается следующим образом:

$$n'_a = (n_a, y, n_b)$$

(Алиса пытается угадать свою "старую" подсказку, а также подсказку Боба и слово Боба y). Далее Алиса восстанавливает обмен сообщениями в старом протоколе (для данных (x, n_a, y, n_b)) и посылает эту последовательность из k битов Бобу. Боб проверяет, что соответствующий пусть в дереве исходного протокола действительно согласован с его входом y и со значением подсказки n_b. В случае согласованности он посылает Алисе бит 1; в противном случае он посылает бит 0.

Нетрудно проверить (*проверьте!*), что в новый недетерминированный протокол вычисляет ту же функцию, что и исходный.

5 Лекция 5, 16 марта.

5.1 Недетерминированные протоколы (продолжение).

Напомним, что функцию $f : X \times Y \to Z$ нам удобно представлять в виде матрицы размера $|X| \times |Y|$, заполненную элементами из Z (на пересечении x-ой строки и y-ого столбца в этой матрице стоит значение $f(x, y)$). Эту матрицу мы обозначаем M_f.

Детерминированный коммуникационный протокол для вычисления f задаёт разбиение M_f на "одноцветные" комбинаторные прямоугольники: каждому листу детерминированного протокола соответствует прямоугольное множество пар $(x, y) \in X \times Y$, которые приводят Алису и Боба в данный лист; во всех точках этого прямоугольного множества функция f принимает одно и то же значение (именно это значение приписано листу протокола).

В недетерминированных протоколах ситуация немного другая. Как и в случае детерминированных протоколов, каждому листу соответствует одноцветный комбинаторный прямоугольник. Однако теперь эти прямоугольники могут пересекаться (на некоторой паре входов (x, y) Алиса и Боб могут попадать в разные листья протокола, в зависимости от "советов", которые они получают). Таким образом, в недетерминированном случае вместо *разбиений* матрицы M_f на прямоугольные множества следует изучать *покрытия* M_f одноцветными прямоугольными множествами.

Обозначение: Назовём $cov_z(f)$ минимальное число комбинаторных прямоугольников, покрывающих все элементы матрицы M_f со значением z (и не задевающих никаких элементов $z' \neq z$). Обозначаем $cov(f)$ минимальное число одноцветных комбинаторных прямоугольников, покрывающих всю матрицу M_f (по определению $cov(f) = \sum_{z \in Z} cov_z(f)$).

Следующее утверждение показывает, что $cov_z(f)$ и $\mathsf{NCC}(f)$ по существу задают одну и ту же меру "сложности" функции f.

Утверждение. Для любой $f : X \times Y \to Z$ (а) $\mathsf{NCC}(f) \le \lceil \log(cov(f)) \rceil + 1$ и (б) $cov(f) \le 2^{\mathsf{CC}(f)}$.

Доказательство: (а) Зафиксируем покрытие M_f минимальным числом одноцветных комбинаторных прямоугольников (если минимальных покрытий несколько, произвольным образом выберем одно из них). Протокол устроен следующим образом: Алиса угадывает номер одного из прямоугольников в покрытии (пересекающий строку, соответствующую известному ей x) и посылает этот номер Бобу. Для этого требуется переслать $\lceil \log(cov(f)) \rceil$ битов информации. Затем Боб проверяет, что указанный комбинаторный прямоугольник пересекает столбец, соответствующий его значению y и сообщает о результатах проверки Алисе (пересылка ещё одного бита). Если Алиса правильно угадала прямоугольное множество, покрывающее пару (x, y), то в результате Алиса и Боб знают значение $f(x, y)$ (это "цвет" данного прямоугольника). В противном случае (если результат проверки Боб отрицателен) значение функции остаётся неизвестным.

(б) Зафиксируем недетерминированный коммуникационный протокол для вычисления f. Листья этого протокола задают покрытие M_f одноцветными комбинаторными прямоугольниками. Число этих прямоугольников не больше $2^{\mathsf{CC}(f)}$. Утверждение доказано.

Пример. В этом примере мы рассмотрим коммуникационную задачу, для которой недетерминированная сложность существенно меньше детерминированной. Обозначим $k = \lfloor \sqrt{n} \rfloor$. Будем рассматривать $x, y \in \{0,1\}^n$ как квадратные матрицы $k \times k$ из нулей и единицы. Мы рассматриваем задачу о равенстве столбцов (Matrix Column Equality): найдётся ли номер i от 1 до k такой, что i-ые столбцы в матрицах x и y совпадают.

$$\mathsf{MCE}(x,y) = \begin{cases} 1, & \text{если } \exists i = 1..k \text{ такое, что } i\text{-ые столбцы в } x \text{ и } y \text{ совпадают,} \\ 0, & \text{иначе.} \end{cases}$$

Упражнение. Докажите, что $\mathsf{CC}(\mathsf{MCE}) = \Omega(n)$.

Покажем, что недетерминированная сложность данной задачи почти квадратично меньше детерминированной. Наш недетерминированный протокол будет устроен следующим образом. Сначала Алиса угадывает ответ: есть ли номер столбца i такой, что i-ые столбцы в x и y совпадают. Она сообщает Бобу о своей догадке (пересылается один бит). Если Алиса полагает, что равные столбцы есть, то она пересылает Бобу угаданный номер этого столбца i и его содержимое ($\lceil \log k \rceil + k$ битов). Если же Алиса полагает, что равных столбцов нет, то для каждого $i = 1..k$ она угадывает позицию m_i (тоже от 1 до k), в которой i-ые столбцы у Алисы и Боба отличаются, а также бит из своей матрицы x в данной позиции (i, m_i). В этом случае Алиса пересылает Бобу $k(1 + \lceil \log k \rceil)$ битов информации. Боб проверяет, что догадки Алисы согласованы с содержимым его матрицы y, и сообщает

о результатах проверки Алисе (пересылка ещё одного бита). Таким образом, коммуникационная сложность протокола равна $O(\sqrt{n}\log n)$.

В рассмотренном выше примере зазор между детерминированной и недетерминированной коммуникационной сложностью функции MCE оказывался почти квадратичным. Далее мы покажем, что для предикатов (функций со значениями 0 и 1) разрыв не может быть *более* чем квадратичным.

Теорема. Для любой функции $f : X \times Y \to \{0,1\}$

$$\mathsf{CC}(f) = O(\mathsf{NCC}(f)^2).$$

Доказательство: Мы докажем несколько более точную оценку:

$$\mathsf{CC}(f) = O(\log(cov_0(f)) \cdot (\log(cov_1(f)) + 2).$$

Прежде всего, зафиксируем минимальное покрытие M_f одноцветными прямоугольными множествами.

Лемма. Пусть R_0 и R_1 два комбинаторных прямоугольника "цвета" 0 и 1 соответственно из покрытия матрицы M_f. Тогда эти комбинаторные прямоугольники либо не имеют общих столбцов, либо не имеют общих строк.

Доказательство леммы: Немедленно следует из определения комбинаторного прямоугольника: если бы R_0 и R_1 имели общую строку и общий столбец, то они должны были бы пересекаться, что противоречит одноцветности этих прямоугольников.

Следствие леммы: Пусть R_1 один из прямоугольников цвета 1 из покрытия M_f, а $R_0^1, \ldots, R_0^s$ — некоторый набор прямоугольников цвета 0 из того же покрытия. Тогда R_1 либо не имеет общих строк с $\geq 50\%$ прямоугольников R_0^j, либо не имеет общих столбцов с $\geq 50\%$ прямоугольников R_0^j.

Теперь мы готовы описать детерминированный коммуникационный протокол. Протокол будет состоять из нескольких однотипных шагов. В начале протокола мы имеем $cov_0(f)$ прямоугольников цвета 0, которые покрывают все нули в M_f. На каждом шаге Алиса и Боб будут исключать из рассмотрения не менее половины имеющихся прямоугольников цвета 0.

Очередной шаг устроен следующим образом. Алиса пытается найти такой прямоугольник цвета 1, который пересекает строку x и при этом не имеет общих столбцов с $\geq 50\%$ (не исключенных из рассмотрения ранее) прямоугольников цвета 0 из покрытия. Если ей это удаётся, она сообщает номер этого прямоугольника Бобу. После этого Алиса и Боб исключают из дальнейшего рассмотрения прямоугольники цвета 0, не пересекающиеся по столбцам с указанным 1-прямоугольником. Если же Алисе не удалось найти такой 1-прямоугольник, то Боб пытается в свою очередь найти такой прямоугольник цвета 1, который пересекает столбец y и при этом не имеет общих строк с $\geq 50\%$ (ещё не исключённых) прямоугольников цвета 0.

Если Бобу это удаётся, они с Алисой исключают из дальнейшего рассмотрения прямоугольники цвета 0, не пересекающиеся по строкам с указанным 1-прямоугольником. Далее Алиса и Боб переходят к следующем шагу.

Если в итоге *все* прямоугольники цвета 0 из покрытия оказываются исключены, то Алиса и Боб считают, что $f(x, y) = 1$. Если же на некотором шаге ни Алиса, ни Боб не могут найти нужный 1-прямоугольник, то протокол завершается, и участники считают, что $f(x, y) = 0$.

Оценка коммуникационной сложности: Число итераций не превосходит $\lceil \log cov_0(f) \rceil$, так как на каждой итерации исключает не менее половины из остающихся прямоугольников цвета 0. Одна итерация требует передачи номера одного прямоугольника цвета 1 и ещё двух битов служебной информации (сообщения об успехе или неудаче Алисы и Боба в поиске нужного прямоугольника цвета 1). В итоге мы имеем протокол сложности $O(\log(cov_0(f)) \cdot (\log(cov_1(f)) + 2) = O((\log cov(f))^2)$.

Корректность протокола: Если $f(x, y) = 0$, то пара (x, y) покрыта каким-то (хотя бы одним) прямоугольником цвета 0. Нетрудно видеть, что этот прямоугольник никогда не будет удалён. Следовательно, если протокол завершился с результатом 1, ошибки быть не может. Если же $f(x, y) = 1$, то пара (x, y) покрыта каким-то прямоугольником цвета 1. Этот прямоугольник согласован и с x, и с y, так что на каждой итерации он позволяет или Алисе, или Бобу отсечь не менее половины не исключённых ранее 0-прямоугольников, см. Следствие из леммы. (Возможно, найдутся и другие 1-прямоугольники, позволяющие произвести такое отсечение; но мы знаем, что хотя бы один такой прямоугольник есть наверняка.) Таким образом, если протокол завершился с результатом 0, то ошибки также быть не может.

Теорема. $\mathsf{NCC}(\mathsf{EQ}) = n + 1$.

Доказательство: Достаточно заметить, что рассуждение с трудным множеством (которые мы применяли для доказательства $\mathsf{CC}(\mathsf{EQ}) = n + 1$) применимо и для недетерминированных протоколов.

5.2 Вероятностные протоколы.

В этой главе вы будем рассматривать вероятностные протоколы вычисления $f : X \times Y \to Z$. В вероятностных коммуникационных протоколах Алисе и Бобу разрешается использовать случайность. Формально это означает, что Алиса и Боб независимо выбирают случайные (по равномерной мере) последовательности битов $r_a \in \{0, 1\}^{l_a}$ и $r_b \in \{0, 1\}^{l_b}$ соответственно. Далее на каждом шаге протокола действия Алисы зависят от её входа x и от r_a, а действия Бобы зависят от его входа y и r_b. Для каждой пары (x, y) возникает распределение вероятностей на множестве листьев, в которые (при заданных x, y) Алиса и Боб могут попасть.

Вероятностные коммуникационные протоколы отчасти похожи на недетерминированные: ходы игроков определяются не только входными данными, а зависят ещё от выбора дополнительных значений r_a, r_b. Есть техническое отличие: в вероятностных протоколах каждому листу приписано

некоторое значение $z \in Z$ (в недетерминированных протоколах возможно безрезультатное завершение общения между Алисой и Бобом; в вероятностных протоколах для любых x, y и для любых значений случайных битов Алиса и Боб заканчивают протокол получением некоторого ответа). Существенная разница состоит также и в том, что для некоторых x, y и некоторых r_a, r_b Алиса и Боб могут, вообще говоря, получить неправильное значение $f(x, y)$. И, разумеется, важнейшим новшеством по сравнению с недетерминированными протоколами является появление вероятностной меры на "подсказках" r_a, r_b.

Для каждого вероятностного протокола и для каждой пары входов x, y мы имеем вероятность $\varepsilon(x, y)$ ошибки — вероятность того, что Алиса и Боб придут в лист протокола с пометкой z' отличной от $z = f(x, y)$. Коммуникационной сложностью вероятностного протокола (в худшем случае) мы, как обычно, называем глубину этого протокола – максимальное расстояние от корня до листа (т.е., максимум числа пересылаемых битов среди всех пар входов x, y и всех значений случайных битов r_a, r_b).

Определение 1. Для $\varepsilon > 0$ вероятностной коммуникационной сложностью $\mathsf{RCC}_\varepsilon(f)$ назовём минимальную глубину вероятностного протокола, который для любой пары входов x, y имеет вероятность ошибки не больше ε.

Средней коммуникационной сложностью заданного вероятностного протокола для данных входов x, y мы называем математическое ожидание числа пересылаемых битов (при фиксированных x, y). Средней коммуникационной сложностью данного протокола в худшем случае мы называем максимум средней коммуникационной сложности по всем парам входов x, y.

Определение 2. Вероятностной коммуникационной сложностью *с нулевой ошибкой* $\mathsf{RCC}_0(f)$ называется наилучшая (минимальная) средняя коммуникационная сложность вероятностных протоколов с нулевой ошибкой.

Утверждение. Для любой функции f

$$\mathsf{NCC}(f) \leq \mathsf{RCC}_0$$

Доказательство: Протокол с нулевой ошибкой и средней сложностью h легко превратить в недетерминированный протокол сложности h. Достаточно отсечь все листья на расстоянии больше h от корня (на месте отсекаемых вершин можно поместить неопределённый ответ "?"). В полученном недетерминированном протоколе "подсказки" для Алисы и Боба – это соответствующие значения случайных битов, которые в исходном (вероятностном) протоколе приводили участников к ответу за $\leq h$ шагов.

Следствие. $\mathsf{RCC}_0(\mathsf{EQ}) = n + 1$.

5.3 Приложение коммуникационной сложности: распознавание языка палиндромов на 1-ленточных машинах Тьюринга

Палиндромами называются слова, которые одинаково читаются слева направо и справа налево. Рассмотрим множество всех палиндромов, составленных из нулей и единиц. Понятно, что свойство слова "быть палиндромом" можно проверить алгоритмически. Более того, нетрудно построить одноленточную машину Тьюринга, которая будет распознавать язык двоичных палиндромов за квадратичное время — входы из n битов будут обрабатываться машиной за время $O(n^2)$. Далее мы покажем, что указанную оценку невозможно существенно улучшить. Более точно, язык палиндромов нельзя распознавать быстрее, чем за квадратичное время.

Теорема. Сложность распознавания языка палиндромов на одноленточных машинах Тьюринга есть $\Omega(n^2)$ (существует такая константа c, что при всех достаточно больших n на некоторых словах длины n машина работает не менее cn^2 шагов).

Набросок доказательства: Машину Тьюринга, распознающую язык палиндромов, можно преобразовать в вероятностный коммуникационный протокол для вычисления предиката равенства $\mathsf{EQ}(u,v)$. В самом деле, для слов u, v длины n рассмотрим работу машины на входе $u0^{2n}v^{-1}$ (длины $4n$). Алиса и Боб проводят границу в случайно выбранном месте ленты в позициях между n-ой и $(3n)$-ой. Затем Алиса и Боб моделируют работу машины. Алиса ответственная за хранение информации на ленте левее границы и за моделирование работы в то время, когда головка машины находится левее границы. Боб же отвечает за хранение содержимого на ленте правее проведённой границы и за моделирование работы машины в то время, когда головка находится правее границы. В те моменты, когда головка пересекает границу, происходит передача управления от Алисы к Бобу или наоборот. Каждая такая передача управления требует пересылки $O(1)$ битов информации (точнее, $\log Q$ битов, где Q есть число внутренних состояний моделируемой машины).

Обозначим $t_i(u,v)$ число пересечений машиной границы i на входе $u0^{2n}v^{-1}$. Заметим, что средняя коммуникационная сложность описанного протокола (на данной паре входов u, v) равна математическому ожиданию по i величины $t_i(u,v)$, то есть

$$\frac{t_0(u,v) + t_1(u,v) + t_{2n}(u,v)}{2n+1} \cdot \log Q.$$

Это число заведомо не больше $O(T(u,v)/(2n+1))$, где $T(u,v)$ обозначает общее время работы машины на входе $u0^{2n}v^{-1}$.

Поскольку средняя коммуникационная сложность протокола не может быть меньше $2n+1$ (см. Следствие выше), мы заключаем, что для некоторых u, v время работы машины $T(u,v) = \Omega(n^2)$. Теорема доказана.

6 Лекция 6, 23 марта.

6.1 Детерминированная сложность функции MCE.

На прошлой лекции мы сформулировали упражнение, в котором требовалось доказать нижнюю оценку на детерминированную сложность функции MCE. На этой лекции мы начнем с разбора этого упражнения.

Лемма. $\mathsf{CC}(\mathsf{MCE}) = \Omega(n)$.

Стоит задуматься о том, какие методы доказательства подобных оценок нам известны. У нас было два метода доказательства нижних оценок детерминированной коммуникационной сложности: трудные множества и ранг матриц. Однако мы уже отмечали, что размер трудного множества дает оценку не только на детерминированную сложность, но и также и на недетерминированную. Поскольку мы знаем, что недетерминированная сложность задачи MCE меньше чем нужная нам оценка, метод трудных множеств нам не подходит. Поэтому остается только метод ранга.

Доказательство: Для простоты предположим, что n — полный квадрат, а значит $\sqrt{n}$ — целое. Ясно, что достаточно доказать оценку только для таких n (если n не является полным квадратом достаточно рассмотреть наибольший полный квадрат n' меньший n, тогда функция MCE на $2n$ переменных содержит как подфункцию функцию MCE на $2n'$ переменных).

Обозначим $k = \sqrt{n}$ и для всякого $l = 1, \ldots, k$ определим вспомогательную функцию $\mathsf{MCE}_l(x, y)$, где $x, y \in \{0,1\}^{k \times l}$ рассматриваются как матрицы размера $k \times l$. Функция $\mathsf{MCE}_l(x, y)$ равна 1 тогда и только тогда, когда существует $i = 1, \ldots, l$ такое что i-ый столбец x совпадает с i-ым столбцом y. Нетрудно видеть, что функция MCE_k совпадает с функцией MCE на $2n$ переменных, а функция MCE_1 есть функция EQ на k переменных.

Для функции MCE_l обозначим через A_l матрицу, представляющую эту функцию. Матрица A_l имеет размер $2^{kl} \times 2^{kl}$. Для доказательства леммы нам достаточно показать, что $\mathsf{rk}(A_k) \geq 2^{k^2}$. Для этого мы покажем, что для всякого $l = 2, \ldots, k$ верно

$$\mathsf{rk}(A_l) \geq 2^k \mathsf{rk}(A_{l-1})/4.$$

Заметив также, что $\mathsf{rk}(A_1) = 2^k$, отсюда мы легко получаем требуемую оценку.

Для доказательства нужного нам неравенства рассмотрим подробнее матрицу A_l. Ее строки и столбцы соответствуют входам Алисы $x \in \{0,1\}^{k \times l}$ и входам Боба $y \in \{0,1\}^{k \times l}$ соответственно. Упорядочим строки и столбцы в лексикографическом порядке, причем x и y будем проходить "по столбцам". То есть, самым старшим битом в x (и в y) будет ячейка $(1,1)$, следующей по старшинству будет ячейка $(2,1)$, далее $(3,1)$, и так далее до $(k,1)$. Дальше идут $(1,2), (2,2), (3,2), \ldots, (k,2)$, и так далее. Самыми младшими будут биты $(1,l), (2,l), (3,l), \ldots, (k,l)$.

Далее разобьем строки матрицы A_l на равные блоки последовательных строк, всего блоков 2^k, в каждом блоке, таким образом, по $2^{(k-1)l}$ строк.

То же самое сделаем со столбцами. Заметим, что в каждом блоке строк у соответствующих входов Алисы $x \in \{0,1\}^{k\times l}$ первые столбцы одинаковы. То же самое верно и для столбцов.

При таком разбиении строк и столбцов на блоки матрица A_l приобретает блочную структуру, которую нетрудно описать. А именно, легко видеть, что

$$A_l = \left(\begin{array}{c|c|c|c|c} I & A_{l-1} & A_{l-1} & A_{l-1} & A_{l-1} \\ \hline A_{l-1} & I & A_{l-1} & A_{l-1} & A_{l-1} \\ \hline A_{l-1} & A_{l-1} & I & A_{l-1} & A_{l-1} \\ \hline A_{l-1} & A_{l-1} & A_{l-1} & I & A_{l-1} \\ \hline A_{l-1} & A_{l-1} & A_{l-1} & A_{l-1} & I \end{array}\right).$$

Вычитая последнюю блок-строку из всех остальных строк матрицы получаем

$$\left(\begin{array}{c|c|c|c|c} I-A_{l-1} & 0 & 0 & 0 & A_{l-1}-I \\ \hline 0 & I-A_{l-1} & 0 & 0 & A_{l-1}-I \\ \hline 0 & 0 & I-A_{l-1} & 0 & A_{l-1}-I \\ \hline 0 & 0 & 0 & I-A_{l-1} & A_{l-1}-I \\ \hline A_{l-1} & A_{l-1} & A_{l-1} & A_{l-1} & I \end{array}\right).$$

Заметим, что если от полученной матрицы отбросить последнюю блок-строку и последний блок-столбец, то мы получим диагональную блочную матрицу, ранг которой не меньше $(2^k-1)\mathsf{rk}(I-A_{l-1}) \geq (2^k-1)(\mathsf{rk}A_{l-1}-1) \geq 2^k\mathsf{rk}(A_{l-1})/4$ для всех достаточно больших k.

6.2 Вероятностные протоколы. Продолжение.

На прошлой лекции мы определили вероятностные протоколы и вероятностную коммуникационную сложность функций. Сейчас мы продолжим изучение этого вида сложности. Начнем с примера эффективного протокола.

Лемма. $\mathsf{RCC}_\varepsilon(\mathsf{EQ}) = O(\log n/\varepsilon)$.

Доказательство: Положим $k = n/\varepsilon$. Для достаточно больших k существует такое простое число p такое что $k < p < 2k$. (Это утверждение называется постулат Бертрана. Доказал его П.Л. Чебышёв, получивший для количества простых чисел не больших x оценки $c_1\frac{x}{\ln x} < \pi(x) < c_2\frac{x}{\ln x}$ для некоторых $c_1, c_2 > 0$. В настоящее время известны более точные оценки, например, $\frac{x}{\ln x+2} < \pi(x) < \frac{x}{\ln x-4}$ для $x \geq 55$, см. English Wikipedia). Алиса и Боб заранее выбирают такое простое число p (то есть, p фиксировано в протоколе). Будем обозначать вход Алисы через $a = (a_0, a_1, \ldots, a_{n-1})$, а вход Боба через $b = (b_0, b_1, \ldots, b_{n-1})$. Алиса рассматривает свой вход как многочлен

$$A(x) = \sum_i a_i x^i (\mod p),$$

а Боб рассматривает свой вход как многочлен

$$B(x) = \sum_i b_i x^i (\mod p).$$

Протокол устроен следующим образом. Алиса выбирает равномерно и случайно точку $t \in \mathbb{Z}_p$ и посылает Бобу значения t и $A(t)$. Боб вычисляет $B(t)$ и сравнивает с $A(t)$. Если значения оказались равны, то Боб выдает 1, если не равны, то 0.

Заметим, что общее число переданных битов не превышает $2\log(2k)+1 = O(\log(n/\varepsilon))$. Действительно, Алисе нужно передать два числа не больше $2k$, а Бобы нужно передать один бит.

Теперь оценим вероятность ошибки. Если $a = b$, то многочлены Алисы и Боба совпадают и участники протокола всегда выдают правильный ответ. Если же $a \neq b$, то многочлены $A(x)$ и $B(x)$ не совпадают. Два разных многочлена степени меньше n могут совпасть не более чем в $n-1$ точке. Поскольку всего элементов поля k, вероятность ошибки не превышает $n/k = \varepsilon$.

Теперь мы исследуем вопрос о том, как меняется сложность, если уменьшать желаемую вероятность ошибки.

Утверждение Пусть $0 < \varepsilon < \varepsilon' < 1/2$. Тогда $\mathsf{RCC}_\varepsilon(f) = O(\mathsf{RCC}_{\varepsilon'}(f))$.

Для доказательства этого утверждения мы воспользуемся неравенством Чернова.

Лемма (неравенство Чернова) Пусть $x_1, \ldots, x_n$ — независимые случайные величины такие что

$$x_i = \begin{cases} 1, & \text{с вероятностью p,} \\ 0, & \text{с вероятностью 1-p.} \end{cases}$$

Положим $X = x_1 + \ldots + x_n$. Тогда для всяких θ и δ таких, что $0 \leq \theta \leq 1$ и $0 \leq \delta \leq p$, верно

$$\Pr[X/n \geq (1+\theta)p] \leq e^{-\frac{\theta^2}{3}pn},$$

$$\Pr[X/n \geq p + \delta] \leq e^{-\frac{\delta^2}{3}n}.$$

Доказательство утверждения: По протоколу с ошибкой ε' мы построим протокол с ошибкой ε. Новый протокол устроен следующим образом: мы повторяем старый протокол k раз (где k – параметр, который мы определим позднее), каждый раз с новыми случайными битами, и на выход выдаем наиболее часто встречающийся ответ.

Чтобы оценить вероятность ошибки нового протокола определим случайную величину x_i: x_i равна 1, если i-ый повтор протокола допустил ошибку. Заметим, что $x_1, \ldots, x_k$ – независимые одинаково распределенные случайные величины и вероятность того, что они равны 1 не превышает ε'.

Тогда вероятность того, что новый протокол допускает ошибку не превышает

$$\Pr[\frac{\sum_i x_i}{k} \geq \frac{1}{2}] \leq e^{-\frac{\delta^2}{3}k}$$

для некоторой константы δ. Нетрудно видеть, что для того чтобы сделать ошибку меньше ε достаточно взять в качестве k достаточно большую константу.

7 Лекция 7, 30 марта.

7.1 Вероятностные протоколы, продолжение.

Начнем с доказательства неравенства Чернова, которым мы воспользовались в прошлый раз. Напомним формулировку.

Лемма (неравенство Чернова) Пусть $x_1, \ldots, x_n$ — независимые случайные величины такие что

$$x_i = \begin{cases} 1, & \text{с вероятностью p,} \\ 0, & \text{с вероятностью 1-p.} \end{cases}$$

Положим $X = x_1 + \ldots + x_n$. Тогда для всяких θ и δ таких что $0 \leq \theta \leq 1$ и $0 \leq \delta \leq p$ верно

$$\Pr[X/n \geq (1+\theta)p] \leq e^{-\frac{\theta^2}{3}pn},$$

$$\Pr[X/n \geq p + \delta] \leq e^{-\frac{\delta^2}{3}n}.$$

Доказательство: Второе неравенство вытекает из первого, если положить $\theta = \frac{\delta}{p}$, следовательно достаточно доказать первое неравенство. Преобразуем левую часть.

$$\begin{aligned} \Pr[X \geq (1+\theta)p] = \Pr[e^{tX} \geq e^{t(1+\theta)pn}] \leq \frac{E(e^{tX})}{e^{t(1+\theta)pn}} = \\ e^{-t(1+\theta)pn}(1-p+pe^t)^n \leq e^{-t(1+\theta)pn}e^{np(e^t-1)} = \\ e^{pn(e^t-1-t(1+\theta))}, \end{aligned}$$

где t — действительный параметр, первое неравенство частный случай неравенства Маркова, во втором равенстве используется независимость переменных x_i и явно вычисляется математическое ожидание случайной величины e^{tx_i}, третье неравенство опирается на неравенство $(1+x) \leq e^x$. В получившейся оценке положим $t = \log(\theta+1)$. Тогда раскладывая в ряд Тейлора нетрудно видеть, что

$$e^t - 1 - t(1+\theta)) = \theta - (1+\theta)\log(\theta+1) \leq -\frac{\theta^2}{2} + \frac{\theta^3}{6} \leq -\frac{\theta^2}{3},$$

Откуда получается нужное неравенство.

На прошлой лекции на примере функции EQ мы видели, что вероятностная сложность может быть сильно меньше детерминированной, а именно, экспоненциально меньше. Сейчас мы докажем, что это максимально возможный разрыв.

Лемма $\mathsf{RCC}_\varepsilon(f) = \Omega(\log CC(f))$.

Доказательство: Мы докажем более сильное неравенство

$$CC(f) \leq 2^{\mathsf{RCC}_\varepsilon(f)}(\mathsf{RCC}_\varepsilon(f) + \log^{-1}(\frac{1}{2} - \varepsilon)),$$

для чего построим детерминированный протокол на базе вероятностного. Введем обозначение $k = \mathsf{RCC}_\varepsilon(f)$ и зафиксируем вероятностный протокол сложности k.

Для начала рассмотрим совсем простой детерминированный протокол. Для каждого листа протокола l Алиса посылает p_l^A — вероятность того, что ее сообщения согласованы с путем в дереве протокола, ведущим в этот лист. (Число листьев в протоколе не превосходит 2^k.) После этого Боб вычисляет p_l^B — вероятности того, что его сообщения согласованы с путем в дереве протокола, ведущим в l, вычисляет произведения $p_l^A \cdot p_l^B$, и суммирует эти произведения по всем листам, выдающим ноль. Нетрудно заметить, что получившееся число есть вероятность того, что протокол выдает ноль на заданных входах. Если это число меньше $1/2$, то Боб выдает 1, а если больше $1/2$, то выдает 0 (в действительности эта вероятность либо не больше ε, либо не меньше $1 - \varepsilon$).

Однако, в приведенном выше решении есть трудность. А именно, вероятности p_l^A – это некоторые рациональные числа, возможно с большим знаменателем, так что для их пересылки может потребоваться передать слишком много битов. Но на самом деле нам достаточно передать приближенное значение вероятности. Действительно, если мы передадим значения p_l^A с ошибками не более $\frac{\frac{1}{2}-\varepsilon}{2^k}$, то значение вероятности выдать ноль, вычисленное Бобом, отличается от правильного на не более чем $\frac{1}{2} - \varepsilon$, и протокол по прежнему выдает правильный ответ. Осталось заметить, что для пересылки действительного числа из отрезка $[0, 1]$ с точностью $\frac{\frac{1}{2}-\varepsilon}{2^k}$ достаточно передать $k + \log^{-1}(\frac{1}{2} - \varepsilon)$ знаков после запятой.

Заметим, что из доказанной леммы следует, что вероятностный протокол для функции равенства, построенный нами на прошлой лекции, оптимален (с точностью до умножения на некоторую константу).

Следствие. Для всякого $\varepsilon > 0$ $\mathsf{RCC}_\varepsilon(\mathsf{EQ}) = \Omega(\log n)$.

7.2 Вероятностные протоколы с общими случайными битами.

До настоящего момента в рассматриваемых нами вероятностных протоколах и у Алисы, и у Боба имеются свои случайные биты, причем случайные

биты одного не известны другому. Но разумна (и важна для теории и приложений) также и постановка задачи, в которой Алиса и Боб используют один общий источник случайности. Интуитивно понятно, что это может только облегчить Алисе и Бобу вычисление функции.

Формально мы требуем, чтобы что в начале работы протокола случайно выбиралась строка $r \in \{0,1\}^l$ фиксированной длины l, и далее на каждом шаге протокола действия Алисы зависят от x и r, а действия Боба зависят от y и r. Более того, мы будем считать, что от значения случайных битов r может зависеть, кто из участников (Алиса или Боб) посылает сообщение на очередном шаге.

Вероятностный протокол с общими случайными битами можно рассматривать как распределение вероятностей на детерминированных протоколах: Алиса и Боб сначала выбирают случайную строку r, а затем следуют детерминированному протоколу соответствующему этой строке r.

Меры вероятностной коммуникационной сложности с общими случайными битами определяются аналогично коммуникационной сложности с частными битами. Чтобы отличать меры сложности с общими битами от мер сложности с частными битами, к первым мы будем добавлять верхний индекс *pub*. Так, например, вероятностная коммуникационная сложность функции f с ошибкой ε и с общими случайными битами обозначается через $\mathsf{RCC}_\varepsilon^{pub}(f)$ и есть глубина минимального вероятностного протокола с общими случайными битами, вычисляющего функцию f с ошибкой не более ε на каждом входе.

Всякий протокол π с раздельными источниками случайности можно тривиально превратить в протокол с общими случайными битами. Можно считать, например, что в Алиса использует из общей последовательности случайных битов только те, которые стоят на чётных местах, а Боб использует случайные биты на нечётных местах. Таким образом, протокол π преобразуется в протокол с общим источником случайности с *такой же* вероятностью ошибки и *такой же* коммуникационной сложностью, как и у исходного протокола. Это несложное рассуждение доказывает следующее утверждение:

Утверждение 1 *Для всякой функции f и для всякого ε верно*

$$\mathsf{RCC}_\varepsilon^{pub}(f) \le \mathsf{RCC}_\varepsilon(f),\ \mathsf{RCC}_0^{pub}(f) \le \mathsf{RCC}_0(f).$$

Доказательство: Достаточно рассмотреть произвольный коммуникационный протокол с частными битами и по нему построить протокол с общими битами следующим образом: общие биты будут состоять из конкатенации частных битов Алисы и Боба, и протокол просто повторяет протокол с частными битами.

Рассмотрим важный пример – сложность предиката равенства для вероятностных протоколов с общим источником случайности.

Утверждение 2 $\mathsf{RCC}_\varepsilon^{pub}(\mathsf{EQ}) = O(\log \frac{1}{\varepsilon})$

Доказательство: Протокол устроен следующим образом. На входах $x, y \in \{0,1\}^n$ Алиса и Боб выбирают случайную строку $r \in \{0,1\}^n$. Алиса вычисляет скалярное произведение $\langle x, r\rangle$ над полем из двух элементов и передает вычисленный бит Бобу. Боб вычисляет скалярное произведение $\langle y, r\rangle$, сравнивает со скалярным произведением Алисы и, если произведения равны, выдает 1, иначе выдает 0.

Заметим, что если $x = y$, то протокол всегда выдает правильный ответ. Если же $x \neq y$, то протокол выдает 1 (то есть, ошибается), если $\langle x-y, r\rangle = 0$. Это линейное уравнение на r и его решения образуют линейное пространство размерности $n-1$ над полем из двух элементов. Легко понять, что число векторов в таком пространстве равно 2^{n-1}, а значит ошибка происходит ровно на половине случайных наборов, то есть ошибка происходит с вероятностью $1/2$.

Если мы теперь повторим описанный протокол k раз с независимыми случайными битами и будем выдавать 0, если хотя бы один раз скалярные произведения оказались не равны, то в случае равных x и y ошибки по прежнему быть не может, а в случае различных входов ошибка происходит с вероятностью $1/2^k$. Таким образом, чтобы добиться ошибки ε, достаточно повторить протокол $\log \frac{1}{\varepsilon}$ раз.

Когда мы изучали недетерминированную коммуникационную сложность, мы рассматривали функцию MCE, которая служила примером того, что недетерминированная сложность бывает меньше детерминированной. Докажем, что вероятностная сложность этой функции с нулевой ошибкой тоже довольно мала.

Утверждение $\mathsf{RCC}_0^{pub}(\mathsf{MCE}) = O(\sqrt{n})$.

Доказательство: Протокол будет состоять из последовательного сравнения соответствующих столбцов во входах Алисы и Боба слева направо. Сравнение будет происходить путем применения протокола для функции равенства, описанного выше. Более конкретно, сначала Алиса и Боб сравнивают первые столбцы с ошибкой $1/2$. Если обнаружилось, что столбцы не равны, то Алиса и Боб переходят к следующим столбцам и повторяют процесс. Если же такого не обнаружилось, то Алиса и Боб повторяют процедуру для первого столбца, и так далее. Всего мы сделаем $4\sqrt{n}$ сравнений. Если при этом мы успели обнаружить, что все столбцы различные, то мы готовы выдать ответ. Если же такого не обнаружилось, то Алиса передает целиком свой текущий столбец Бобу, на это нужно $\sqrt{n}$ битов. Если обнаружилось, что эти столбцы совпали, то мы снова готовы дать ответ. Если же столбцы не совпали, то Алиса передает Бобу весь x, после чего Боб вычисляет ответ. Это требует пересылки n битов, но можно доказать, что до этого случая мы доходим с очень маленькой вероятностью. Окончание доказательства мы оставляем в качестве упражнения.

Упражнение. Докажите, что построенный протокол действительно имеет среднюю сложность $O(\sqrt{n})$. *Указание:* Воспользуйтесь неравенством Чернова.

8 Лекция 8, 6 апреля.

8.1 Общий и частные источники случайности в вероятностных протоколах.

Мы рассматривали два разных подхода к определению вероятностного коммуникационного протокола с ограниченной вероятностью ошибки. В первом из них предполагалось, что каждый из участников протокола (Алиса и Боб) раздельные источники случайности; при этом участники не могут видеть случайные друг друга. Во втором варианте определения предполагалось, что Алиса и Боб видят общую последовательность случайных битов. Соответствующие коммуникационные сложности функции f обозначались $\mathsf{RCC}_\varepsilon(f)$ и $\mathsf{RCC}^{pub}_\varepsilon(f)$ соответственно.

Всякий протокол π с раздельными источниками случайности можно считать частным случаем протокола с общими случайными битами. При этом $\mathsf{RCC}^{pub}_\varepsilon(f)$ может быть несколько меньше, чем $\mathsf{RCC}_\varepsilon(f)$. Например, мы уже видели, что для предиката равенства $\mathsf{RCC}_{1/4}(\mathsf{EQ}) = 2$, а $\mathsf{RCC}^{pub}_{1/4}(\mathsf{EQ}) = \Theta(\log n)$. Сейчас мы докажем, что разница между двумя вариантами вероятностной коммуникационной сложности не может быть больше $O(\log n)$.

Теорема 1 *Для любой функции $f : \{0,1\}^n \times \{0,1\}^n \to Z$ и для любых $\varepsilon > 0$, $\delta > 0$*

$$\mathsf{RCC}_{\varepsilon+\delta}(f) \le \mathsf{RCC}^{pub}_\varepsilon(f) + O(\log n + \log 1/\delta).$$

Доказательство: Мы покажем, что любой коммуникационный протокол с общим источником случайности можно переделать в протокол с раздельными источниками случайных битов; при этом коммуникационная сложность возрастет не более чем на $O(\log n + \log 1/\delta)$.

Пусть дан некоторый вероятностный протокол π для общей случайности. Конструкция нового протокола (с раздельными источниками случайности) основана на двух идеях.

Идея 1: В новом протоколе случайные биты будет порождать Алиса. Она подбросит нужное число раз монету и сообщит результаты бросания Бобу. Далее они могут использовать эти случайные биты (ставшие "общими") для выполнения коммуникационного протокола с общей случайностью. В этой конструкции Бобу вовсе не нужно использовать свой собственный источник случайности. Коммуникационная сложность при этом будет включать число случайных битов (Алиса пересылает их Бобу по каналу связи).

На первый взгляд этот план кажется безнадежным. Исходный протокол π может требовать очень большого числа случайных битов, так что пересылка битов от Алисы Бобу катастрофически увеличит коммуникационную сложность. Однако оказывается, что в любом коммуникационном протоколе можно уменьшить число используемых случайных битов до $O(\log n)$, заплатив за это лишь небольшим увеличение вероятности ошибки. В этом и состоит вторая (основная) идея доказательства.

Идея 2: Протокол π, использующий N общих для Алисы и Боба случайных битов и имеющий вероятность ошибки ε, можно переделать в про-

токол π' с $k = O(\log n + \log 1/\delta)$ общими случайными битами и вероятностью ошибки не более $\varepsilon + \delta$.

Поясним, как будет устроен протокол π'. Мы подберём $K = 2^k$ наборов "псевдослучайных" битов

$$\mathbf{b}_1, \ldots, \mathbf{b}_K$$

(каждое $\mathbf{b}_i \in \{0,1\}^N$). Эти K наборов будут частью нового протокола π'. В этом новом протоколе Алиса и Боб будут брать из общего источника случайности k битов. Эти биты они интерпретируют как номер $i = 1, \ldots, K$. Далее они берут соответствующий $\mathbf{b}_i = (b_i^1, \ldots, b_i^N)$ и следуют исходному протоколу π как если бы $b_i^1, \ldots, b_i^N$ были получены из настоящего источника случайности.

Мы должны доказать, что при некотором выборе "псевдослучайных" наборов $\mathbf{b}_1, \ldots, \mathbf{b}_K$ вероятность ошибки нового протокола не будет превышать $\varepsilon + \delta$. Будем говорить, что набор $\mathbf{b}_1, \ldots, \mathbf{b}_K$ *плох* для некоторой пары входов $x, y \in \{0,1\}^n$, если новый протокол протокол π' с этим набором "псевдослучайных" битов ошибается на входах x, y с вероятностью больше $\varepsilon + \delta$. Другими словами, данный набор считается плохим для x, y, если

$$\mathrm{Prob}_{i \in_r \{1,\ldots,K\}}[\pi \text{ для данных } x,\ y,\ \mathbf{b}_i \text{ ошибается}] > \varepsilon + \delta.$$

(Здесь вероятность берется по случайному выбору i.) Нам нужно найти такой набор $\mathbf{b}_1, \ldots, \mathbf{b}_K$, который не является плохим ни для какой пары входов.

Обозначим

$$e(x, y, \mathbf{b}) = \begin{cases} 1, & \text{если протокол } \pi \text{ для аргументов } x, y \\ & \text{и случайных битов } \mathbf{b} \text{ ошибается,} \\ 0, & \text{если протокол } \pi \text{ для аргументов } x, y \text{ и случайных} \\ & \text{битов } \mathbf{b} \text{ находит правильный ответ.} \end{cases}$$

Поскольку протокол π ошибается с вероятностью не более ε, мы имеем

$$\mathrm{Prob}_{\mathbf{b}}[e(x, y, \mathbf{b}) = 1] < \varepsilon$$

для любых $x, y \in \{0,1\}^n$. Применяя неравенство Чернова, получаем

$$\mathrm{Prob}_{\mathbf{b}_1,\ldots,\mathbf{b}_K}[e(x, y, \mathbf{b}_1) + \ldots + e(x, y, \mathbf{b}_K) > (\varepsilon + \delta)K] < 2^{-c\delta^2 K}$$

(для некоторой константы $c > 0$). Если взять $K > 2n/(c\delta^2)$, то данная вероятность станет меньше 2^{-2n}. Тогда сумма вероятностей "плохости" по всем парам x, y (таких пар 2^{2n}) будет меньше единицы. Это и означает, что некоторый набор $\mathbf{b}_1, \ldots, \mathbf{b}_K$ не будет плохим ни для каких x, y.

Таким образом, необходимое семейство псевдослучайных последовательностей битов можно подобрать для протокола π' при $k = \log(2n/(c\delta^2)) = O(\log n + \log 1/\delta)$. Теорема доказана.

8.2 Вероятностная коммуникационная сложность GT

Оценим вероятностную коммуникационную сложность предиката GT. Для начала рассмотрим самый очевидный протокол. Чтобы выяснить, какое из чисел $x, y \in 1, 2, \ldots, 2^n$ больше, Алисе и Бобу необходимо найти самый старший бит (самую левую позицию), в котором двоичные записи этих чисел различаются. Когда эта позиция найдена, Алисе и Бобу остается обменяться битами, которые стоят в их словах на этом месте.

Будем искать нужную позицию двоичным поиском, применяя *тест на равенство* к блокам двоичных слов всё меньшего и меньшего размера. Поскольку на каждой итерации мы можем сужать область поиска вдвое, нам потребуется $\lceil \log n \rceil$ применений теста на равенство. Чтобы итоговая вероятность ошибки не превосходила ε, каждый такой тест на равенство должен ошибаться с вероятностью не более $\delta = \varepsilon / \lceil \log n \rceil$.

Напомним, что известный нам коммуникационный протокол с раздельными случайными битами для проверки равенства двух слов длины $\leq n$ с вероятностью ошибки δ имеет коммуникационную сложность $O(\log(n/\delta))$. Подставляя сюда $\delta = \varepsilon / \log n$ и суммируя по $\log n$ итерациям, получаем $\mathsf{RCC}_\varepsilon(\mathsf{GT}) = O(\log^2 n)$ (для любого фиксированного $\varepsilon > 0$).

Теперь рассмотрим аналогичную стратегию для вероятностного протокола с общим источником случайности. Коммуникационная сложность одного *тест на равенство* с вероятностью ошибки δ не превосходит $O(\log \frac{1}{\delta})$. Суммируя число переданных битов в $\log n$ итерациях, получаем

$$\mathsf{RCC}^{pub}_\varepsilon(\mathsf{GT}) = O(\log n \log\log n).$$

Применяя Теорему 1, мы получаем

$$\mathsf{RCC}_\varepsilon(\mathsf{GT}) = \mathsf{RCC}^{pub}_\varepsilon(\mathsf{GT}) + O(\log n) = O(\log n \log\log n)$$

(также для любого фиксированного $\varepsilon > 0$). Таким образом, с помощью Теоремы 1 нам удалось почти квадратично уменьшить коммуникационную сложность по сравнению с "очевидным" протоколом.

Упражнение. Покажите, что $\mathsf{RCC}_\varepsilon(\mathsf{GT}) = O(\log n)$ для любого $\varepsilon > 0$. *Указание:* Сначала рассмотрите протоколы с общим источником случайности. Как и в изученных выше протоколах, примените двоичный поиск самого старшего бит, в котором двоичные записи чисел x и y различаются. В процессе двоичного поиска размер интервала, предположительно содержащего нужную нам позицию, будет постепенно сокращаться. Используйте тест на равенство с вероятностью ошибки $1/4$, который имеет коммуникационную сложность $O(1)$; периодически тестируйте корректность текущего интервала. При каждом обнаружении ошибки возвращайтесь к предыдущему значению левого края интервала поиска.

9 Лекция 9, 13 апреля.

В этой главе мы изучим технику доказательства нижних оценок для вероятностной коммуникационной сложности. Для этого мы введём два новых понятия – *(детерминированная) коммуникационная сложность функции для распределения на входах* (distributional complexity) и *неоднородность функции при заданном распределении (discrepancy)*.

9.1 Коммуникационная сложность функции с распределением на аргументах

Определение. Пусть дана функция $f : X \times Y \to Z$ и распределение вероятностей μ на множестве $X \times Y$. Коммуникационной сложностью f для распределения μ с ошибкой ε называется минимум глубины среди всех детерминированных протоколов π, которые правильно вычисляет значение f для пар $(x, y) \in X \times Y$ общей μ-меры не менее $(1 - \varepsilon)$, т.е.,

$$\mathrm{Prob}_\mu[\pi(x, y) = f(x, y)] \geq 1 - \varepsilon.$$

Мы будем обозначать эту сложность $\mathsf{CC}^\mu_\varepsilon(f)$

Пример 1. Рассмотрим предикат равенства EQ, определенный на парах n-битных строк. Введем равномерное распределение μ на $\{0,1\}^n \times \{0,1\}^n$. Пусть n достаточно велико; для определённости положим $n \geq 7$. Тогда $\mathsf{CC}^\mu_{1/100}(\mathsf{EQ}) = 0$. Чтобы получить правильный ответ с вероятностью $> 99/100$ Алисе и Бобу вовсе не нужно обмениваться сообщениям! Они могут на любых входах объявлять, что ответ равен 0, т.е., заданные x и y не равны. Этот тривиальный протокол ошибается на всех парах равных слов. Понятно, что вероятность ошибки равна $1/2^n$, что меньше $\varepsilon = 1/100$.

Пример 2. Рассмотрим предикат GT, определенный на парах слов $x, y \in \{0, \ldots, 2^n - 1\}$. Напомним, что

$$\mathsf{GT}(x, y) = \begin{cases} 1, & \text{если } x > y, \\ 0, & \text{если } x \leq y. \end{cases}$$

Как и в первом примере, введем равномерное распределение μ на всех парах входов. Тогда $\mathsf{CC}^\mu_{1/4}(\mathsf{GT}) \leq 2$. Достаточно рассмотреть протокол, в котором Алиса и Боб обмениваются старшими битами из двоичных записей x и y. Если один из этих битов равен нулю, другой единице, то Алиса и Боб смогут достоверно узнать, какое из двух чисел больше. Если же старшие биты оказываются равны, то Алиса и Боб полагают, что значение предиката равно 0 (x не больше y). В этом случае протокол может дать неверный ответ. Однако более чем для половины x и y равными старшими битами ответ 0 будет правильным. Таким образом, более чем для $3/4$ пар (x, y) описанный коммуникационный протокол находит правильное значение $\mathsf{GT}(x, y)$. Это доказывает, что $\mathsf{CC}^\mu_{1/4}(\mathsf{GT}) \leq 2$.

Упражнение. Покажите, что протокол из примера 2 невозможно сделать ещё проще: $\mathsf{CC}^{\mu}_{1/4}(\mathsf{GT})$ в точности равна 2.

Следующая теорема показывает связь между привычной нам вероятностной коммуникационной сложностью $\mathsf{RCC}^{pub}_{\varepsilon}(f)$ и новым понятием $\mathsf{CC}^{\mu}_{\varepsilon}(f)$.

Теорема 2 *Для любой функции* $f : X \times Y \to Z$

$$\mathsf{RCC}^{pub}_{\varepsilon}(f) = \max_{\mu} \mathsf{CC}^{\mu}_{\varepsilon}(f).$$

Доказательство: Сначала докажем более важное для нас неравенство:

$$\mathsf{RCC}^{pub}_{\varepsilon}(f) \geq \max_{\mu} \mathsf{CC}^{\mu}_{\varepsilon}(f).$$

Пусть имеется вероятностный коммуникационный протокол π с общими для Алисы и Боба источником случайных битов, длина максимального пути в протоколе равна h, и для любых x, y

$$\mathrm{Prob}_r[\pi(x, y, r) = f(x, y)] \geq 1 - \varepsilon$$

(вероятность берется по источнику случайных битов r данного протокола). Далее, пусть дана произвольная мера μ на множестве пар $X \times Y$. Тогда

$$\mathrm{Prob}_{r,(x,y)}[\pi(x, y, r) = f(x, y)] \geq 1 - \varepsilon$$

(теперь случайно выбираются и биты r, и пара входов x, y). Следовательно, можно так зафиксировать значение случайных битов $r = r_0$ таким образом, что

$$\mathrm{Prob}_{(x,y)}[\pi(x, y, r_0) = f(x, y)] \geq 1 - \varepsilon$$

Подставим выбранные биты r_0 в протокол $\pi(x, y, r)$. При этом мы получаем детерминированный протокол $\pi'(x, y) = \pi(x, y, r_0)$, который возвращает правильное значение $f(x, y)$ с вероятностью не менее $1-\varepsilon$ по мере μ. Глубина полученного протокола не превосходит h (коммуникационной сложности исходного вероятностного протокола π). Таким образом, первая половина теоремы доказана.

Вторая часть теоремы – неравенство

$$\mathsf{RCC}^{pub}_{\varepsilon}(f) \leq \max_{\mu} \mathsf{CC}^{\mu}_{\varepsilon}(f)$$

нам в курсе нигде не потребуется. Однако доказательство этого результат использует красивую идею, и мы кратко обсудим это рассуждение. Доказательство этого неравенства использует метод из теории игр. Пусть $h = \max_{\mu} \mathsf{CC}^{\mu}_{\varepsilon}(f)$. Рассмотрим следующую игру с двумя участниками.

Оба игрока одновременно делают свои ходы. Первый игрок своим ходом объявляет некоторый детерминированный коммуникационный протокол π глубины не более h; второй игрок называет некоторую пару входов (x, y) из $X \times Y$.

Первый игрок побеждает, если $\pi(x,y) = f(x,y)$; в противном случае побеждает второй игрок. В случае победы первого игрока второй игрок выплачивает ему 1 рубль; в случае победы второго игрока никто не получает и не теряет денег. Это пример игры с нулевой суммой – выигрыш первого игрока равен проигрышу второго. По предположению, h не меньше $\mathsf{CC}^{\mu}_{\varepsilon}(f)$ для любой меры μ. Это значит, что для любой *вероятностной* стратегии второго игрока (если второй игрок выбирает свой ход (x,y) случайно по распределению μ) имеется некоторая *детерминированная* стратегия π для второго игрока, позволяющего выигрывать рубль с вероятностью не меньше $1-\varepsilon$. Вообще говоря, эта стратегия π может зависеть от стратегии второго игрока μ. Тогда по теореме фон Неймана о минимаксе (она же *теорема о седловой точке*, она же *теорема о цене игры с нулевой суммой*) у первого игрока есть вероятностная стратегия ρ (вероятностная стратегия первого игрока есть некоторое распределение вероятностей на детерминированных протоколах глубины не более h), которая для любой (детерминированной или вероятностной) стратегии второго игрока ρ обеспечивает получение выигрыша с вероятностью не менее $1-\varepsilon$. В частности, это означает, что если второй игрок всегда делает ход (x,y), то вероятностная стратегия ρ будет выигрывать против этого хода с вероятностью не менее $1-\varepsilon$.

Таким образом, вероятностную стратегию первого игрока ρ можно рассматривать как вероятностный коммуникационный протокол (с общим источником случайности), который с вероятностью не менее $(1-\varepsilon)$ дает правильный ответ на любой паре входов. Это и означает, что $\mathsf{RCC}^{pub}_{\varepsilon}(f) \le h$. Теорема доказана.

9.2 Мера неоднородности распределения.

Теорема 2 дает нам способ доказывать нижние оценки для вероятностной коммуникационной сложности $\mathsf{RCC}^{pub}_{\varepsilon}(f)$. Чтобы показать, что $\mathsf{RCC}^{pub}_{\varepsilon}(f) \ge h$, достаточно подобрать некоторое распределение вероятностей μ на $X \times Y$ и доказать, что $\mathsf{CC}^{\mu}_{\varepsilon}(f) \ge h$. Остается подготовить технику для получения нижних оценок для детерминированной коммуникационной сложности с заданным распределением $\mathsf{CC}^{\mu}_{\varepsilon}(f)$. Для этого мы введем меру "неоднородности" функции при заданном распределении.

Определение. Пусть дана функция $f : X \times Y \to \{0,1\}$ и распределение вероятностей μ на $X \times Y$. Для комбинаторного прямоугольника $R \subset X \times Y$ будем называть *неоднородностью* f на R разницу между μ-мерами таких пар $(x,y) \in R$, на которых функция f равна единице, и таких пар $(x,y) \in R$, на которых функция f равна нулю. Будем обозначать неоднородность на заданном комбинаторном прямоугольнике $Disc_{\mu}(R,f)$:

$$Disc_{\mu}(R,f) := |\mathrm{Prob}_{\mu}[(x,y) \in R \text{ и } f(x,y)=1] - \mathrm{Prob}_{\mu}[(x,y) \in R \text{ и } f(x,y)=0]|.$$

Далее, возьмем максимум неоднородности по всем комбинаторным прямоугольникам $R \subset X \times Y$:

$$Disc_{\mu}(f) := \max_{R} Disc_{\mu}(R,f).$$

Эту величину будем называть *неоднородностью* f по мере μ.

Теорема 3 *Для всякой функции $f : X \times Y \to \{0,1\}$, для любой вероятностной меры μ на $X \times Y$ и любого вещественного $\varepsilon > 0$ выполнено*

$$\mathsf{CC}^{\mu}_{\frac{1}{2}-\varepsilon}(f) \geq \log_2 \frac{2\varepsilon}{Disc_{\mu}(f)}.$$

Доказательство. Пусть детерминированный протокол π правильно вычисляет f на множестве пар (x,y) μ-меры $> 1-\varepsilon$. Это означает, что

$$\mathrm{Prob}_{\mu}[\pi(x,y) = f(x,y)] - \mathrm{Prob}_{\mu}[\pi(x,y) \neq f(x,y)] \geq (\frac{1}{2}+\varepsilon) - (\frac{1}{2}-\varepsilon) = 2\varepsilon.$$

Если глубина протокола π равна h, то он имеет не более 2^h листьев. Каждому листу l сопоставим комбинаторный прямоугольник $R_l = A_l \times B_l$, состоящий из всех пар аргументов (x,y), согласованных с путем в лист l в коммуникационном протоколе π. Теперь ещё раз подсчитаем разность вероятностей между правильными и неправильными ответами в каждом комбинаторном прямоугольнике R_l:

$$\sum_l \mathrm{Prob}_{\mu}[(x,y) \in R_l \;\&\; \pi(x,y) = f(x,y)] - \mathrm{Prob}_{\mu}[(x,y) \in R_l \;\&\; \pi(x,y) \neq f(x,y)].$$

Поскольку для всех точках комбинаторного прямоугольника R_l протокол π возвращает одно и то же значение (приписанное листу l), полученная сумма не превосходит

$$\sum_l \left|\mathrm{Prob}_{\mu}[(x,y) \in R_l \;\&\; f(x,y) = 1] - \mathrm{Prob}_{\mu}[(x,y) \in R_l \;\&\; f(x,y) = 0]\right|.$$

Каждое слагаемое в этой сумме есть $Disc_{\mu}(R,f)$. Таким образом, мы получаем

$$2\varepsilon \leq 2^h Disc_{\mu}(f),$$

и теорема доказана.

Теперь рассмотрим конкретный пример применения данной теоремы. Мы получим линейную нижнюю оценку на вероятностную коммуникационную сложность функции скалярного произведения.

Утверждение 3 *Для равномерного распределения μ на $\{0,1\}^n \times \{0,1\}^n$*

$$Disc_{\mu}(\mathsf{IP}) \leq 2^{-n/2}.$$

Доказательство: Предикат $\mathsf{IP}(x,y)$ (скалярное произведение x и y по модулю 2) удобно представить следующей матрицей H размера $2^n \times 2^n$; строки и столбцы этой матрицы занумерованы битовыми строками длины n, и

$$\begin{array}{ll} H(x,y) = +1, & \text{если } \langle x,y\rangle = 0 \ mod\ 2, \\ H(x,y) = -1, & \text{если } \langle x,y\rangle = 1 \ mod\ 2. \end{array}$$

(Напоминание для знатоков: такая матрица H называется матрицей Адамара.)

Эта матрица H удобна для вычисления неоднородности предиката IP по равномерной мере. В самом деле, для любого комбинаторного прямоугольника $A \times B \subset \{0,1\}^n \times \{0,1\}^n$

$$(*) \qquad Disc_{uniform}(A \times B, \mathsf{IP}) = \frac{\sum\limits_{x \in A, y \in B} H(x,y)}{2^{2n}} = \frac{\vec{1}_A \cdot H \cdot \vec{1}_B^t}{2^{2n}},$$

где $\vec{1}_A$ обозначает характеристический вектор-строку для множества A (на позициях, соответствующих элементам A стоят единицы, на всех других позициях стоят нули), а $\vec{1}_B^t$ аналогично обозначает характеристический вектор-столбец для множества B. Чтобы оценить сумму (*), нам нужно вычислить нормы векторов $\vec{1}_A$ и $\vec{1}_B$, а также норму матрицы H. Первое совсем просто: $\|\vec{1}_A\| = \sqrt{|A|}$ и $\|\vec{1}_B\| = \sqrt{|B|}$.

Остаётся подсчитать норму H. Для этого удобно возвести матрицу в квадрат. Элемент матрицы H^2 на пересечении x-ой строки и y-ого столбца есть

$$(H^2)|_{(x,y)} = \sum_z H(x,z) \cdot H(z,y) = \begin{cases} 2^n, & \text{если } x = y, \\ 0, & \text{если } x \neq y \end{cases}$$

(если $x = y$, то сумма состоит из 2^n квадратов плюс или минус единиц; если же $x \neq y$, то сумма состоит из равного числа плюс и минус единиц и равна нулю). Таким образом, $H^2 = 2^n \cdot E$, где E единичная матрица $2^n \times 2^n$. Следовательно, $\|H\| = \sqrt{2^n}$.

Возвращаясь к (*), получаем

$$Disc_{uniform}(A \times B, \mathsf{IP}) \leq \frac{\sqrt{|A|} \cdot \sqrt{2^n} \cdot \sqrt{|B|}}{2^{2n}} \leq \frac{\sqrt{2^{3n}}}{2^{2n}} = 2^{-n/2}.$$

Теорема доказано.

Из Теоремы 3 и Утверждения 3 немедленно получаем следствие:

Следствие 1 $\mathsf{CC}^{uniform}_{\frac{1}{2}-\varepsilon}(\mathsf{IP}) \geq n/2 - O(\log \frac{1}{\varepsilon})$.

Вместе с Теоремой 2 этот результат даёт нижнюю оценку для вероятностной сложности функции скалярного произведения:

Следствие 2 $\mathsf{RCC}^{pub}_{\frac{1}{2}-\varepsilon}(\mathsf{IP}) \geq n/2 - O(\log \frac{1}{\varepsilon})$.

10 Лекция 10, 20 апреля.

10.1 Вероятностная коммуникационная сложность для случайных функций.

В этой главе мы покажем, что большинство функций имеют довольно большую вероятностную коммуникационную сложность. Точнее, подавляющее большинство предикатов $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ имеют сложность $\Omega(n)$.

Теорема 4 *Для любого $\varepsilon > 0$ и всех достаточно больших n для значительного большинства функций $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ (для определённости скажем, что для 99% таких функций)*

$$\mathsf{RCC}^{pub}_{\frac{1}{2}-\varepsilon}(f) \geq 0.1n.$$

Замечание: Константу 0.1 в формулировке теоремы можно заменить на любое $c < 1$. Мы выбрали число 0.1 для упрощения доказательства.

Доказательство: Согласно Теореме 3 и Теореме 2 достаточно показать, что для 99% функций f

$$Disc_\mu(f) \leq 2^{-0.1n}$$

для некоторой вероятностной меры μ на $\{0,1\}^n \to \{0,1\}$. Мы докажем эту оценку для равномерного распределения вероятностей на всех парах входов.

Каждый комбинаторный прямоугольник $R \subset \{0,1\}^n \to \{0,1\}$ содержит не менее 1 и не более 2^{2n} элементов. Нам нужно показать, что для "типичной" функции f для всех комбинаторных прямоугольников R

$$(**) \qquad Disc_{uniform}(R, f) \leq 2^{-0.1n}.$$

По определению неоднородности функции,

$$Disc_\mu(R, f) = |\mathrm{Prob}_\mu[(x,y) \in R \text{ и } f(x,y) = 1] - \mathrm{Prob}_\mu[(x,y) \in R \text{ и } f(x,y) = 0]|.$$

Заметим, что для прямоугольников R, содержащих менее $2^{1.9n}$ пар для равномерного распределения μ

$$Disc_\mu(R, f) \leq 2^{1.9n}/2^{2n} = 2^{-0.1n}.$$

Таким образом, нам остается оценить неоднородность f в прямоугольниках R достаточно большого размера (состоящих не менее, чем из $2^{1.9n}$ пар).

Пусть комбинаторный прямоугольник R состоит из N пар, и $N \geq 2^{1.9n}$. Применим неравенство Чернова. Если выбирать функцию $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ случайно (значения функции на всех парах $\{0,1\}^n \to \{0,1\}$ выбирается равномерно и независимо), то

$$\mathrm{Prob}_f[\ \left|[\text{число единиц функции } f \text{ в } R] - \frac{N}{2}\right| \geq \delta N\ ] \leq 2^{-\frac{\delta^2}{3}N} \leq 2^{-\frac{\delta^2}{3}2^{1.9N}}$$

Нас интересует δ такое, что $\delta N = 2^{1.9n}$. В этом случае $\delta \geq \frac{2^{1.9n}}{2^{2n}} = 2^{-0.1n}$. Следовательно, вероятность того, что в неоднородность случайной f в прямоугольнике R превысит $2^{-0.1n}$, можно оценить как

$$\mathrm{Prob}_f[|[\text{число единиц функции } f \text{ в } R] - \frac{N}{2}| \geq \delta N] \leq 2^{-\frac{\delta^2}{3}N} \leq 2^{-\frac{1}{3}2^{1.7N}}.$$

Если просуммировать эту вероятность по всем комбинаторным прямоугольникам R достаточно большого размера (таких прямоугольников заведомо не больше $(2^{2^n}) \times (2^{2^n})$), то получится величина

$$2^{-\frac{1}{3}2^{1.7N}+2\cdot 2^n} \ll 1/100.$$

Отрицательный член в показателе степени растет быстрее положительного члена. Это значит, что при достаточно больших n вероятность того, что на *хотя бы одном* прямоугольнике R неоднородность больше $2^{-0.1n}$, не превосходит $1/100$. (Более того, эта вероятность суперэкспоненциально стремится к нулю с ростом n.) Таким образом, для 99% функций f выполнено (**), и теорема доказана.

Упражнение (простое). Докажите Теорему 4, заменив в формулировке константу 0.1 на 0.3.

Упражнение (более сложное). Докажите Теорему 4, заменив в формулировке константу 0.1 на 0.99.

10.2 Уточнение оценки вероятностной коммуникационной сложности IP.

В главе 9.2 мы уже доказали, что $\mathsf{RCC}_\varepsilon(\mathsf{IP}) = \Omega(n)$. Сейчас мы уточним эту оценку и покажем, что вероятностная коммуникационная сложность скалярного произведения не просто равна $\Omega(n)$, а достаточно близка к n.

Теорема 5 *Для любого $\varepsilon > 0$*

$$\mathsf{RCC}^{pub}_{\frac{1}{2}-\varepsilon}(\mathsf{IP}_n) \geq n - O(\log \frac{1}{\varepsilon}).$$

Доказательство: Согласно Теореме 2 достаточно доказать, что

$$\mathsf{CC}^{\mu}_{\frac{1}{2}-\varepsilon}(\mathsf{IP}) \geq n - O(\log \frac{1}{\varepsilon}).$$

Мы докажем требуемую оценку для равномерного распределения на $\{0,1\}^n \times \{0,1\}^n$:

$$\mathsf{CC}^{uniform}_{\frac{1}{2}-\varepsilon}(\mathsf{IP}) \geq n - 3\log \frac{1}{\varepsilon} - O(1).$$

Пусть некоторый детерминированный протокол π имеет глубину h и правильно вычисляет предикат IP на долее $(\frac{1}{2} + \varepsilon)$ пар из $\{0,1\}^n \times \{0,1\}^n$. Покажем, что в этом случае глубина h не может быть слишком мала.

Каждому листу l протокола h соответствует некоторый комбинаторный прямоугольник $R_l = A_l \times B_l$, состоящий из всех пар (x, y), согласованных с путём в данный лист. Поскольку протокол детерминированный, эти прямоугольники попарно не пересекаются. Кроме того, каждому листу в дереве прокола соответствует бит — тот ответ, который π возвращает при попадании в данный лист.

Будем говорить, что R_l покрывает некоторую пару (x, y), если $(x, y) \in R_l$ и протокол π возвращает на данной паре входов правильное значение $\mathsf{IP}(x, y)$. Поскольку данный протокол ошибается на доле входов не более $(\frac{1}{2} - \varepsilon)$, все комбинаторные прямоугольники R_l в совокупности покрывают не менее $(\frac{1}{2} + \varepsilon)2^{2n}$ пар (x, y).

Исключим из рассмотрения все листья l, для которых $|R_l| < \frac{\varepsilon}{2} \cdot 2^{2n}/2^h$. Поскольку общее число всех листьев в протоколе не превосходит 2^h, все исключаемые нами прямоугольники R_l в вместе покрывают не больше $\frac{\varepsilon}{2} \cdot 2^{2n}$ разных пар. Следовательно, оставшиеся (не исключенные из рассмотрения) комбинаторные прямоугольники должны покрывать не меньше $(\frac{1}{2} + \frac{\varepsilon}{2})2^{2n}$ пар (x, y).

Каждый комбинаторный прямоугольник R_l состоит из $|A_l \times B_l|$ точек. Среди не исключенных из рассмотрения комбинаторных прямоугольников средняя "плотность" (доля) правильных ответов не меньше $(\frac{1}{2} + \frac{\varepsilon}{2})$. Таким образом, найдется хотя бы один такой не исключенный прямоугольник $R_l = A_l \times B_l$, в котором

(а) $|A_l \times B_l| \geq \frac{\varepsilon}{2} \cdot 2^{2n}/2^h$ (поскольку прямоугольник не был исключен из рассмотрения), и

(б) R_l покрывает не меньше $(\frac{1}{2} + \frac{\varepsilon}{2})|A_l \times B_l|$ точек.

Зафиксируем номер l такого комбинаторного прямоугольника и исследуем его более детально.

Обозначим $|A_l| = 2^a$ и $|B_l| = 2^b$. Рассмотрим равномерную вероятностную меру ν на элементах данного комбинаторного прямоугольника R_l (каждая пара $(x, y) \in R_l$ имеет вероятность $1/2^{a+b}$). По условию (б)

$$\mathrm{Prob}_\nu[\pi(x, y) = f(x, y)] \geq \frac{1}{2} + \frac{\varepsilon}{2}.$$

Далее, рассмотрим такую же как в доказательстве утверждения 3 матрицу H (элемент $H(x, y)$ равен $(-1)^{\mathsf{IP}(x,y)}$) и такие же векторы 1_{A_l} и 1_{B_l} (характеристические векторы множеств A_l и B_l). Как в доказательстве утверждения 3,

$$\mathrm{Prob}_\nu[\pi(x, y) = f(x, y)] - \mathrm{Prob}_\nu[\pi(x, y) \neq f(x, y)] = 1_{A_l} \cdot H \cdot 1^t_{B_l}.$$

Это значит, что

$$\varepsilon \leq \|1_{A_l}\| \cdot \|H\| \cdot \|1_{B_l}\| = \sqrt{2^{n-a-b}}.$$

После логарифмирования получаем

$$2 \log \varepsilon \leq n - a - b.$$

С другой стороны, из условия (а) для данного комбинаторного прямоугольника $|A_l \times B_l| = 2^{a+b} \geq \frac{\varepsilon}{2} \cdot 2^{2n-h}$. Логарифмируя это неравенство, имеем

$$a + b \leq 2n - h + \log \frac{\varepsilon}{2}.$$

Складывая эти неравенства, получаем $h \geq n + 3 \log \varepsilon - 1$, и теорема доказана.

10.3 Вероятностная коммуникационная сложность дизъюнктности для множеств ограниченного размера.

На следующей лекции мы докажем, что $\mathsf{RCC}_\varepsilon(\mathsf{DISJ}) = \Omega(n)$ для достаточно малого $\varepsilon > 0$. А сейчас мы покажем, что проверка дизьюнктности множеств ограниченного размера может быть меньше n. Более точно, имеет место следующее утверждение.

Утверждение 4 *Обозначим DISJ_n^k предикат дизъюнктности, который определен на таких парах множеств $x, y \subset \{1, \ldots, n\}$, для которых $|x| \leq k$ и $|y| \leq k$. Тогда*

$$\mathsf{RCC}_\varepsilon^{pub}(\mathsf{DISJ}_n^k) = O(k).$$

Набросок доказательства: Мы должны построить вероятностный коммуникационный протокол с общим для Алисы и Боба источником случайности. Нам будет удобно разбить последовательность случайных битов из этого источника на блоки по n битов $S_1, S_2, \ldots$. Эти блоки можно рассматривать как случайные подмножества $S_i \subset \{1, \ldots, n\}$ (каждое число от 1 до n с равными вероятностями входит или не не входит в выбираемое подмножество S_i, для разных чисел выбор производится независимо.)

Протокол для вычисления DISJ_n^k будет состоять из последовательности этапов следующего вида:

Этап 1. Алиса дожидается первого множества S_i, которое содержит внутри себя множество x, и сообщает номер i Бобу. Боб заменяет своё множество y на $y' = y \cap S_i$.

Этап 2. Боб дожидается первого множества S_j (для $j > i$), которое содержит y', и сообщает разницу $j - i$ Алисе. Алиса заменяет своё множество x на $x' = x \cap S_j$.

Этап 3. Боб дожидается первого множества S_k для $k > j$, которое содержит x', и сообщает Бобу разницу $k - j$. Боб заменяет своё текущее множество x' на $x'' = x \cap S_k$.

И так далее... Процесс останавливается, либо если одно из двух текущих множеств становится пустым, либо если число переданных битов превышает порог ck (для некоторой константы c, выбор которой мы обсудим ниже.)

Заметим, что в описанном процессе текущие множества Алисы и Боба либо всегда остаются дизъюнктными, либо всегда имеют непустое пересечение. Так что если на некотором шаге текущее множество Алисы или текущее множество Боба становится пустым, то можно заключить, что исходные x и y не пересекались. Следовательно, если исходные x и y имели непустое пересечение, то протокол обязательно выдаст правильный ответ. Далее, коммуникационная сложность данного протокола по построению не превосходит $O(k)$. Осталось объяснить, почему для непересекающихся x и y протокол с большой вероятностью (для правильно подобранной константы c) это обнаружит.

Доказательство корректности протокола основано на двух следующих наблюдениях.

Наблюдение первое: Если текущее множество Алисы x состоит из m элементов, то в среднем нужно перебрать 2^m случайных S_i, прежде чем появится множество, содержащее x в качестве подмножества. Таким образом, на данном этапе Алисе потребуется передать Бобу в среднем $O(m)$ битов. (Будьте осторожны: нельзя утверждать, что среднее число битов, передаваемых Алисой на данном этапе, равно в точности m.)

Наблюдение второе: Если множества x и y не пересекаются, то для случайно выбранного $S \subset x$ размер пересечения $y \cap S$ будет в среднем в двое меньше текущего размера y.

Итак, если исходные множества x и y не пересекались, то на каждом шаге протокола размер одного из множеств будет уменьшаться в среднем вдвое. При этом среднее число битов, передаваемых на очередном шаге, будет равно $O([\text{текущий размер множества}])$. Можно заключить, что в среднем после передачи $O(k)$ битов одно из текущих множеств (у Алисы или у Боба) станет пустым.

Таким образом, если прервать протокол после передачи ck битов, то вероятность ошибки будет ограничена $O(1/c)$.

Упражнение. Завершите доказательство утверждения 4.

11 Лекции 11–12, 27 апреля и 4 мая.

11.1 Вероятностная коммуникационная сложность предиката дизъюнктности.

В этой главе мы получим линейную нижнюю оценку для вероятностной коммуникационной сложности предиката дизъюнктности. Мы изложим доказательство, предложенное А.А. Разборовым.

Напомним, что предикат дизъюнктности DISJ действует на парах подмножеств универсума $\{1, \ldots, n\}$

$$\mathsf{DISJ} : \mathcal{P}(\{1, \ldots, n\}) \times \mathcal{P}(\{1, \ldots, n\}) \to \{0, 1\}.$$

Предикат определяется следующим образом:

$$\mathsf{DISJ}(x, y) = \begin{cases} 1, & \text{если } x \cap y = \emptyset, \\ 0, & \text{иначе,} \end{cases}$$

где x и y подмножества $\{1, \ldots, n\}$.

Теорема 6 *Существует такая вероятностная мера μ на $\mathcal{P}(\{1, \ldots, n\}) \times \mathcal{P}(\{1, \ldots, n\})$, что для всех достаточно малых $\varepsilon > 0$*

$$\mathsf{CC}^{\mu}_{\varepsilon}(\mathsf{DISJ}) = \Omega(n).$$

Из этой теоремы и теоремы 2 немедленно следует, что $\mathsf{CC}^{pub}_{\varepsilon}(\mathsf{DISJ}) = \Omega(n)$ для всех достаточно малых ε.

Приступим к доказательству теоремы 6. Будем считать, что $n = 4m - 1$. Далее мы определим распределение вероятностей на парах подмножеств $U = \{1, \ldots, n\}$. Точнее, нам будет полезно ввести не оно распределение вероятностей на таких парах, а три разных распределения, которые мы будем обозначать μ, μ_0 и μ_1. Для одного из этих распределений мы и докажем оценку $\mathsf{CC}^{\mu}_{\varepsilon}(\mathsf{DISJ}) = \Omega(n)$. Два других распределения вводятся по техническим причинам — их будет удобно использоваться в доказательстве.

Мы опишем нужные нам распределения как случайный процесс порождения пары подмножеств. Этот процесс начинается с того, что мы разбиваем универсум $U = \{1, \ldots, n\}$ на три попарно не пересекающиеся части – два множества их $2m - 1$ элементов и одно одноэлементное множество. Более точно, мы выбираем некоторые множества z_A и z_B по $2m - 1$ элементов и число i такие, что

$$U = z_A \cup z_B \cup \{i\}.$$

Все разбиения такого вида мы считаем равновероятными.

Далее мы выбираем m-элементное подмножество x в $Z_A \cup \{i\}$ и m-элементное подмножество y в $Z_B \cup \{i\}$ (все способы выбрать x и y равновероятны). Получившееся распределение мы и будем обозначать μ. Отметим, что в этом распределении случайные x и y с вероятностью $1/4$ пересекаются по одному элементу и с вероятностью $3/4$ не пересекаются вовсе.

Далее, случайно выберем пару m-элементных подмножеств из z_A и z_B соответственно. Это распределение мы обозначим μ_0. В этом распределении вероятностей выбираемые множества всегда имеют пустое пересечение. Отметим, что полученное распределение вероятностей инвариантно относительно перестановок элементов универсума (все m-элементные пары подмножеств с пустым пересечением получаются с равными вероятностями). Будем обозначать (x_0, y_0) получаемые случайные пары подмножеств.

Наконец, выберем по $(m-1)$-элементному подмножеству в z_A и z_B и добавим к обоим полученным подмножествам элемент i. В результате мы получим пару m-элементных подмножеств, имеющих в пересечении ровно один элемент. Это распределение вероятностей мы будем обозначать μ_1. Это распределение вероятностей также инвариантно относительно перестановок элементов универсума (все m-элементные пары подмножеств с одноэлементным пересечением получаются с одной и той же вероятностью). Будем обозначать (x_1, y_1) получаемые случайные пары подмножеств.

Основное распределение μ можно представить как смесь распределений μ_0 и μ_1 (если с вероятностью $3/4$ использовать распределение μ_0, а с веротяностью $1/4$ распределение μ_1, то в сумме мы получим в точности распределение μ).

Отметим, что x_0 и y_0 (соответственно, x_1 и y_1) независимы при фиксированном значении разбиения $t = (z_A, z_B, i)$. Это простое соображение является ключевым для всего доказательства.

Зафиксируем некоторые $A, B \subset \{1, \ldots, n\}$. Нас будет интересовать комбинаторный прямоугольник $A \times B$. Пусть $t = (z_A, z_B, i)$ есть разбиение универсума на подмножества размера $2m - 1$, $2m - 1$ и 1 соответствен-

но. Введём несколько обозначений для определённых нами распределений вероятностей:

$$\begin{array}{rcl} p_x(t) & := & \mathrm{Prob}_\mu[x \in A|t], \\ p_y(t) & := & \mathrm{Prob}_\mu[y \in B|t], \\ p_{x_0}(t) & := & \mathrm{Prob}_{\mu_0}[x_0 \in A|t], \\ p_{x_1}(t) & := & \mathrm{Prob}_{\mu_1}[x_1 \in A|t], \\ p_{y_0}(t) & := & \mathrm{Prob}_{\mu_0}[y_0 \in B|t], \\ p_{y_1}(t) & := & \mathrm{Prob}_{\mu_1}[y_1 \in B|t]. \end{array}$$

Отметим, что

$$\mathrm{Prob}_{\mu_0}[(x_0, y_0) \in A{\times}B] = E_{\mu_0}[p_{x_0}(t){\cdot}p_{y_0}(t)] \text{ и } \mathrm{Prob}_{\mu_1}[(x_1, y_1) \in A{\times}B] = E_{\mu_1}[p_{x_1}(t){\cdot}p_{y_1}(t)].$$

Лемма 1.

$$p_x(t) = \frac{1}{2}(p_{x_0}(t) + p_{x_1}(t))$$

и

$$p_y(t) = \frac{1}{2}(p_{y_0}(t) + p_{y_1}(t)).$$

Доказательство леммы 1: Достаточно заметить, что

$$\mathrm{Prob}_\mu[i \in x|t] = \mathrm{Prob}_\mu[i \in y|t] = 1/2.$$

Лемма 2. Хотя формально $p_x(t)$ и $p_{y_0}(t)$ определяются как функции тройки $t = (z_A, z_B, i)$, они существенно зависят лишь от z_B. Аналогично, $p_y(t)$ и $p_{x_0}(t)$ существенно зависят лишь от z_A.

Доказательство леммы 2: Утверждение леммы немедленно следует из определения: x случайно и равновероятно выбирается в дополнении z_B, а y_0 случайно и равновероятно выбирается внутри z_B. Рассуждение для y, x_0 и z_A симметрично.

Далее нам нужно выбрать некоторое достаточно маленькое (положительное) значение δ. Для определённости можно положить $\delta = 0.01$.

Определение. Разбиение $t = (z_A, z_B, i)$ называется

- *плохим для* A, если $p_{x_1}(t) < \frac{1}{3}p_{x_0}(t) - 2^{-\delta n}$,
- *плохим для* B, если $p_{y_1}(t) < \frac{1}{3}p_{y_0}(t) - 2^{-\delta n}$,
- просто *плохим*, если оно плохое для A или плохое для B.

Лемма 3 (техническая). Для любых $(2m-1)$-элементных множеств z_A, z_B

$$\begin{array}{l} \mathrm{Prob}[t = (z_A, z_B, i) \text{ плохо для } A|z_B] < 1/5, \\ \mathrm{Prob}[t = (z_A, z_B, i) \text{ плохо для } B|z_A] < 1/5. \end{array}$$

Вероятность в технической лемме берется по случайному выбору разбиения t. Мы отложим доказательство "технической леммы" – оно самое громоздкое в этой главе. Сначала мы покажем, как и для чего эта техническая лемма применяется.

Обозначим $\chi(t)$, $\chi_A(t)$, $\chi_B(t)$ индикаторы событий "t плохое", "t плохое для A" и "t плохое для B".

Лемма 4. $E_{\mu_0}[p_{x_0}(t) \cdot p_{y_0}(t) \cdot \chi(t)] \le \frac{4}{5}E_{\mu_0}[p_{x_0}(t) \cdot p_{y_0}(t)]$.

Доказательство леммы 4: Достаточно проверить, что $E_{\mu_0}[p_{x_0}(t)\cdot p_{y_0}(t)\chi_A(t)] \le \frac{2}{5}E_{\mu_0}[p_{x_0}(t)\cdot p_{y_0}(t)]$. Докажем это неравенство для каждого фиксированного значения z_B.

$E_{\mu_0}[p_{x_0}(t)\cdot p_{x_1}(t)\chi_A(t)|z_B] \le$
[*по лемме 2 вероятность* $p_{y_0}(t)$ *есть константа при фиксированном* z_B]
$\le p_{y_0}\cdot E_{\mu_0}[p_{x_0}(t)\chi_A(t)|z_B] \le$
[*по лемме 1*]
$\le 2p_{y_0}\cdot p_x\cdot E_{\mu_0}[\chi_A(t)|z_B] \le$
[*по лемме 3*]
$\le \frac{2}{5}p_{y_0}p_x = \frac{2}{5}p_{y_0}E_{z_A,z_B,i}[p_{x_0}(z,z_B,i)|z_B] =$
[*снова по лемме 2*]
$= \frac{2}{5}E_{\mu_0}[p_{x_0}(t)p_{y_0}(t)|z_B]$

Главная Лемма. Существуют такие положительные α и β, что для любых $A, B \subset \{1,\dots,n\}$

$$\mathrm{Prob}[(x_1,y_1)\in A\times B] \ge \alpha\mathrm{Prob}[(x_0,y_0)\in A\times B] - 2^{-\beta n}.$$

Доказательство главной леммы:

$\mathrm{Prob}_{\mu_1}[(x_1,y_1)\in A\times B] = E_{\mu_1}[p_{x_1}(t)]\cdot p_{y_1}(t)] \ge$
$\ge E_{\mu_1}[p_{x_1}(t)]\cdot p_{y_1}(t)(1-\chi(1))] \ge$
[*по определению "плохого" t*]
$\ge E_{\mu_1}[(\frac{1}{3}p_{x_0}(t) - 2^{-\delta n})(\frac{1}{3}p_{y_0}(t) - 2^{-\beta n})(1-\chi(1))] \ge$
$\Omega(E_{\mu_1}[p_{x_0}(t)]\cdot p_{y_0}(t)(1-\chi(1))]) - 2^{-\beta n} \ge$
[*по лемме 4*]
$\ge \Omega(E_{\mu_1}[p_{x_0}(t)]\cdot p_{y_0}(t))]) - 2^{-\beta n} = \Omega(\mathrm{Prob}_{\mu_0}[(x_0,y_0)\in A\times B]) - 2^{-\beta n}.$

Теперь мы готовы доказать Теорему 6. Пусть $c = \mathsf{CC}^{\varepsilon}_{\mu}(\mathsf{DISJ})$. Это значит, что имеется коммуникационный протокол глубины c, который находит правильный ответ для всех пар (x,y) кроме доли ε по мере μ. Пусть в этом протоколе r листьев (при этом $r \le 2^c$). Обозначим $R_1,\dots R_r$ комбинаторные прямоугольники, соответствующие листьям протокола с ответом 1. Тогда

$\varepsilon \ge \mathrm{Prob}_{\mu}[(x,y)\in \cup R_i$ и правильный ответ $0] =$
$= \sum_i \mathrm{Prob}_{\mu}[(x,y)\in \cup R_i$ и правильный ответ $0] =$
[*в распределении* μ *множества* x *и* y *пересекаются с вероятностью* $1/4$]
$= \frac{1}{4}\sum_i \mathrm{Prob}_{\mu_1}[(x_1,y_1)\in \cup R_i] \ge$
[*по Главной лемме*]
$\ge \frac{1}{4}\sum \alpha\mathrm{Prob}_{\mu_0}[(x_0,y_0)\in R_i] - 2^{-\beta n} \ge$
$\ge \alpha(\frac{3}{4} - \varepsilon) - 2^{-\beta n}\cdot r.$

При достаточно малых ε получаем, что $r \ge 2^{Const\cdot n}$, и теорема доказана.

Нам остается лишь *доказать "техническую" лемму.* Поскольку два утверждения технической леммы симметричны друг другу, достаточно доказать одно неравенство: нам нужно проверить, что

$$\mathrm{Prob}[t \text{ плохо для } A|z_B] < 1/5.$$

Напомним, что подмножество z_B однозначно определяет величину $p_x(t)$.

Первый случай, простой: Если $p_x < 2^{-\delta n}$, то по лемме 1 $p_{x_0} \le 2p_x$, а значит

$$\text{Prob}[t \text{ плохо для } A|z_B] = 0,$$

и лемма доказана.

Второй случай, основной: Предположим, что $p_x \ge 2^{-\delta n}$. Обозначим S семейство таких m-элементных подмножеств $s \subset \{1,\dots,n\}$, все элементы которых лежат вне z_B, причём $s \in A$. По определению p_x имеем

$$p_x(t) = \frac{|S|}{C_{2m}^m}.$$

Нетрудно проверить, что

- $p_{x_0}(z_A, z_B, i) = 2p_x \cdot \text{Prob}_s \in S[s \text{ не содержит } i]$,
- $p_{x_1}(z_A, z_B, i) = 2p_x \cdot \text{Prob}_s \in S[s \text{ содержит } i]$.

В самом деле, если $t = (z_A, z_B, i)$, то по формуле Байеса

$$p_{x_0}(t) = \text{Prob}[x \in A|t, i \notin x] = \frac{\text{Prob}[x \in A|t]}{1/2} = 2\text{Prob}[i \notin x | x \in A, t] \cdot \text{Prob}[x \in A|t].$$

Вычисление для $p_{x_1}(t)$ аналогично. Следовательно, если t плохо для A, то

$$\text{Prob}_{s\in S}[i \in s] \le \frac{1}{3}\text{Prob}_{s\in S}[i \notin S].$$

Другими словами,

$$(*) \qquad \text{Prob}_{s\in S}[i \in s] \le 1/4.$$

Множество $s \in S$ есть m-элементное подмножество в $2m$ множестве (в $\{1,\dots,n\}\setminus z_B$). При фиксированном z_B нам будет удобно представлять это множество в виде строки из $2m$ битов $s = (s_1,\dots,s_{2m})$ (в этой строке должно быть по m нулей и m единиц; каждый бит s_i показывает, входит ли соответствующий элемент дополнения z_B в s).

Пусть $\text{Prob}[t \text{ плохое для } A|t] \ge 1/5$. Тогда неравенство (*) выполнено для не менее, чем $\frac{2}{5}m$ различных i. Теперь мы можем оценить энтропию Шеннона для случайной величины s. С одной стороны, она не может быть меньше $m(2 - 4\delta - o(1))$ (s равномерно распределена на множестве размера не менее $2^{m(2-4\delta-o(1))}$). С другой стороны, в строке $(s_1,\dots,s_{2m})$ многие биты s_i распределены очень неравномерно. Получаем

$$m(2-4\delta-o(1)) \le H(s) = H(s_1,\dots,s_{2m}) \le \sum H(s_i) \le \frac{8m}{5} + \frac{2m}{5}\cdot h(1/4) \le 1.93m,$$

где

$$h(1/4) = \frac{1}{4}\cdot\log\frac{1}{1/4} + \frac{3}{4}\cdot\log\frac{1}{3/4}$$

обозначает энтропию случайной величины, которая принимает значения 0 и 1 с вероятностями 1/4 и 3/4. При достаточно больших m мы получаем противоречие.

Таким образом, мы доказали техническую лемму и закончили доказательство оценки $\mathsf{CC}_\varepsilon^{pub}(\mathsf{DISJ}) = \Omega(n)$.

12 Лекция 13, 11 мая.

12.1 Коммуникационные протоколы без диалога.

В этой главе мы рассмотрим новую модель коммуникационного протокола. Удобно считать, что в протоколе участвуют не два, а три игрока: Алиса, Боб и Чарли (A, B и C). Как и в предыдущих лекциях, целью протокола является вычисление значения некоторой функции $f : X \times Y \to Z$. Как и раньше, Алиса получает первый аргумент функции $x \in X$, а Боб второй аргумент функции $y \in Y$. В нашей новой модели значение $f(x, y)$ должен узнать Чарли. Для этого Алиса и Боб посылают Чарли некоторую информацию. При этом информация передаются только в одну сторону: Алиса и Боб посылают сообщения Чарли, но не получают ничего в ответ; между собой Алиса и Боб информацией не обмениваются. Такие протоколы называют *протоколами с одновременными сообщениями*, поскольку Алиса и Боб могут отправлять Чарли свои сообщения одновременно (или в произвольном порядке), не согласовывая их друг с другом.

Можно рассматривать несколько вариантов данной модели – детерминированную (все участники пользуются детерминированными алгоритмами), вероятностную с общим источником случайности (Алиса, Боб и Чарли имеют доступ к общему источнику случайных битов) и вероятностную с индивидуальными источниками случайности (каждый из трёх участников подбрасывает свою собственную монету и использует полученные случайные биты). Коммуникационной сложность протокола мы будем называть максимальное количество битов, которые могут послать в сумме Алиса и Боб (как обычно, мы берём максимум по всем парам $(x, y) \in X \times Y$). Далее, коммуникационной сложностью функции f мы называем минимальную коммуникационную сложность протокола, вычисляющего эту функцию.

Коммуникационную сложность функции f для модели с одновременными сообщениями мы будем обозначать $\mathsf{CC}^{||}(f)$ для детерминированных протоколов, $\mathsf{RCC}_\varepsilon^{||,pub}(f)$ для вероятностных протоколов с общим источником случайности и $\mathsf{RCC}_\varepsilon^{||}(f)$ для вероятностных протоколов с раздельными источниками случайности. Как обычно, ε обозначает максимальную вероятность ошибки протокола (максимум среди всех пар $(x, y) \in X \times Y$).

Пример. Пусть $X = \{0,1\}^n$ и $Y = \{1, \ldots, n\}$. Обозначим $index : X \times Y \to \{0,1\}$ функцию

$$index(x, i) = x_i$$

(значение функции $index$ на паре $(x, i) \in X \times Y$ равно i-ому биту слова x). Для обычной коммуникационной модели $\mathsf{CC}(index) = O(\log n)$. Действительно, Боб должен сообщить Алисе значение индекса $i \in Y$, а Алиса в ответ пришлет Бобу искомый бит x_i.

Нетрудно заметить, что в модели с параллельными сообщениями коммуникационная сложность данной функции оказывается намного больше. А именно, $\mathsf{CC}^{||}(index) = n + \lceil \log n \rceil$ (это означает, Алиса и Боб обязаны сообщить Чарли всю известную им информацию).

Упражнение. Докажите, что $\mathsf{CC}^{||}(index) = n + \lceil \log n \rceil$.

В этой главе нас в основном будет интересовать вероятностная коммуникационная сложность для одновременных сообщений $\mathsf{RCC}_\varepsilon^{||}(f)$. Заметим прежде всего, что в определении вероятностных коммуникационных протоколов с раздельными источниками случайности можно было бы потребовать, чтобы алгоритм действий

Чарли был детерминированным. Переход от вероятностного алгоритма Чарли к детерминированному не требует увеличения коммуникационной сложности и лишь в два раза увеличивает вероятность ошибки. Более точно, можно доказать следующее утверждение:

Утверждение 5 *Пусть для некоторой функции $f : X \times Y \to Z$ имеется вероятностный коммуникационный протокол π с одновременными сообщениями с раздельными источниками случайности, коммуникационная сложность этого протокола равна h, а вероятность ошибки ограничена некоторым числом ε.*

Тогда для вычисления f найдётся коммуникационный протокол π' с одновременными сообщениями, в котором Алиса и Боб пользуются раздельными источниками случайности, алгоритм действий Чарли детерминированный, и вероятность ошибки не превосходит 2ε.

Доказательство: В протоколе π' Алиса и Боб будут действовать также, как в исходном протоколе π, изменятся лишь действия Чарли. Получив от Алисы и Боба сообщения a и b, Чарли вычисляет условные вероятности для каждого возможного ответа $z \in Z$ в исходном протоколе π (напомним, что условные вероятности получения каждого ответа z при фиксированных сообщения Алисы и Боба зависят только от случайных битов Чарли). Далее Чарли возвращает тот ответ z, который имеет наибольшую вероятность.

Коммуникационная сложность нового протокола совпадает с коммуникационной сложностью исходного протокола π, поскольку сообщения Алисы и Боба не изменились. Остаётся оценить вероятность ошибки.

Будем называть пару сообщений (a, b), отправленных Алисой и Бобом, *плохими* для данных $(x, y) \in X \times Y$, если в протоколе π условная вероятность ошибки Чарли при данных a и b оказывается больше или равна $1/2$, т.е.,

$$\text{Prob}[\text{Чарли получил неверный ответ } z \mid \text{Алиса и Боб отправили сообщения } a \text{ и } b] \geq 1/2.$$

Лемма. Для любых $(x, y) \in X \times Y$ вероятность того, что Алиса и Боб отправят плохие сообщения (a, b), не превосходит 2ε.

Доказательство леммы: Вероятность того, что в протоколе π Чарли ошибется, не меньше

$$\frac{1}{2} \cdot \text{Prob}[\text{Алиса и Боб отправили плохие сообщения } a \text{ и } b].$$

Поскольку вероятность ошибки в протоколе π ограничена ε, вероятность отправки плохих сообщений не может превосходить 2ε. Лемма доказана.

Для доказательства утверждения остаётся заметить, что в новом протоколе π' Чарли мог ошибиться, только если полученная им пара сообщений (a, b) была плохой.

В дальнейшем при изучении вероятностных коммуникационных протоколов мы всегда будем предполагать, что алгоритм Чарли детерминированный.

Далее мы рассмотрим простейший пример, который демонстрирует, что три варианта коммуникационной сложности $\mathsf{CC}^{||}(f), \mathsf{RCC}^{||}_{\varepsilon}(f), \mathsf{RCC}^{||,pub}_{\varepsilon}(f)$ могут иметь существенно разные значения. Мы рассмотрим предикат равенства n-битных строк EQ и докажем, что $\mathsf{CC}^{||}(\mathsf{EQ}) = 2n$, $\mathsf{RCC}^{||,pub}_{\varepsilon}(f) = O(1)$ для любого $\varepsilon > 0$ и $\mathsf{RCC}^{||}_{\varepsilon}(\mathsf{EQ}) = \Theta(\sqrt{n})$ для всех достаточно малых ε.

Первое из этих утверждений совсем простое, и мы оставляем его в качестве упражнения:

Упражнение: Докажите, что $\mathsf{CC}^{||}(\mathsf{EQ}) = 2n$. *Указание:* Если Алиса посылает одно и то же сообщение на разных входах x, то на некоторых парах входов (x, y) Чарли неизбежно будет ошибаться.

Для модели с общим источником случайности в случае параллельных сообщений можно использовать вероятностный коммуникационный протокол, аналогичный протоколу из Утверждения 1.

Утверждение 6 *Для любого* $\varepsilon > 0$ $\mathsf{RCC}_{\varepsilon}^{||,pub}(f) = O(1)$.

Доказательство: Алиса и Боб берут из общего источника случайности n битов $r \in \{0,1\}^n$ и вычисляют скалярные произведения $\langle x, r, \rangle$ и $\langle y, r, \rangle$ по модулю 2. Полученные значения скалярных произведений они отсылают Чарли. Если $x = y$, то полученные скалярные произведения всегда будут одинаковыми. Если же $x \neq y$, то с вероятностью $1/2$ вычисленные скалярные произведения будут отличаться. Чтобы сделать вероятность ошибки протокола меньше заданного ε, достаточно повторить описанную процедуру $\log(1/\varepsilon)$ раз. Утверждение доказано.

Для оценки коммуникационной сложности $\mathsf{RCC}_{\varepsilon}^{||}(\mathsf{EQ})$ нам потребуется нетривиальное рассуждение. Разделим его на две части – оценку сверху и оценку снизу.

Теорема 7 *Для любого* $\varepsilon > 0$ $\mathsf{RCC}_{\varepsilon}^{||}(\mathsf{EQ}_n) = O(\sqrt{n})$.

Доказательство: Мы начнём доказательство с несложной комбинаторной леммы.

Лемма. Для всякого чётного числа m в линейном пространстве $\mathbb{F}_2^m$ найдется не менее $2^{\Omega(m^2)}$ подпространств размерности $m/2$.

Доказательство леммы: Подсчитаем число интересующих нас линейных подпространств. Всякое подпространство размерности $k = m/2$ можно однозначно задать базисом, состоящим из k векторов $e_1, \ldots, e_k$ из $\mathbb{F}_2^m$. Подсчитаем число таких базисов. Для выбора первого вектора имеется $2^m - 1$ вариант (можно взять любой вектор кроме нулевого). Когда e_1 уже выбран, остаётся $2^m - 2$ варианта для выбора второго базисного вектора (он должен быть линейно независим с e_1, т.е., не должен совпадать ни с нулевым вектором, ни с e_1). Далее, для выбора третьего базисного вектора остаётся $2^m - 4$ варианта (e_3 не должен совпадать ни с одной из линейных комбинацией уже выбранных векторов e_1 и e_2). Продолжая рассуждение по индукции, мы получаем, что k линейно независимых векторов можно выбрать в $\mathbb{F}_2^m$

$$(2^m - 1)(2^m - 2)(2^m - 4) \cdots (2^m - 2^{k-1})$$

разными способами.

Соответствие между линейными подпространствами размерности k и наборами из k линейно независимых векторов не является взаимно однозначным. Действительно, базис в каждом таком подпространстве можно выбирать многими разными способами. Мы можем точно вычислить количество базисов в каждом подпространстве размерности k. В самом деле, для выбора первого вектора в фиксированном подпространстве имеется $2^k - 1$ вариант (можно взять любой вектор

подпространства кроме нулевого). Когда e_1 зафиксирован, остаётся $2^k - 2$ способа для выбора второго базисного вектора, затем $2^k - 4$ способа для выбора третьего базисного вектора, и т.д. Всего в подпространстве размерности k над полем из двух элементов можно найти

$$(2^k - 1)(2^k - 2)(2^k - 4) \cdots (2^k - 2^{k-1})$$

базисов. Следовательно, общее число k-мерных подпространств в m-мерном пространстве над полем из двух элементов равно

$$\frac{(2^m - 1)(2^m - 2) \cdots (2^m - 2^{k-1})}{(2^k - 1)(2^k - 2) \cdots (2^k - 2^{k-1})}.$$

Для каждого $i = 0, 1, \ldots, k-1$ отношение $\frac{2^m - 2^i}{2^k - 2^i}$ больше, чем $\frac{2^m}{2^k}$. Следовательно, для $k = m/2$ интересующее нас число k-мерных подпространств оказывается не меньше, чем

$$\frac{(2^m)^k}{(2^k)^k} = 2^{m^2/4},$$

и лемма доказана.

Возьмём минимальное четное число $m = m(n)$ такое, чтобы число $m/2$-мерных подпространств в $\mathbb{F}_2^m$ было не меньше n. Из доказанной леммы следует, что такое будет не больше $O(\sqrt{n})$. Поставим в соответствие каждому двоичному слову $z \in \{0,1\}^n$ своё уникальное подпространство L_z размерности $m/2$ в $\mathbb{F}_2^m$.

Теперь мы готовы описать коммуникационный протокол. Алиса находит для своего слова x соответствующее подпространство L_x, выбирает случайный вектор $v \in L_x$ и посылает его Чарли. Боб также находит линейное подпространство L_y, соответствующее его слову y. Далее Боб переходит к ортогональному дополнению этого подпространства $L_y^\perp$ ($L_y^\perp$ состоит из всех векторов $\mathbb{F}_2^m$, которые при скалярном умножении на каждый вектор $L_y^\perp$ дают ноль по модулю 2). Заметим, что размерность $L_y^\perp$ равна $m - \frac{m}{2} = \frac{m}{2}$. Затем Боб выбирает случайный вектор $w \in L_y^\perp$ и посылает его Чарли.

Если векторы v и w оказываются ортогональны (их скалярное произведение по модулю 2 равно нулю), то Чарли полагает, что x и y равны. В противном случае он считает, что x и y не равны.

Описание протокола закончено. Остаётся оценить коммуникационную сложность и найти вероятность ошибки. Начнём с коммуникационной сложности. Протокол состоит в том, что Алиса и Боб посылают Чарли по одному вектору из линейного пространства $\mathbb{F}_2^m$. Мы уже показали, что $m = O(\sqrt{n})$, так что коммуникационная сложность протокола не превосходит $O(\sqrt{n})$.

Теперь оценим вероятность ошибки протокола. В случае $x = y$ подпространства L_x и L_y будут совпадать. Таким образом, подпространство $L_y^\perp$ будет в точности ортогональным дополнением L_x. Это значит, что векторы v и w будут непременно ортогональными, и Чарли не ошибется. Если же $x \neq y$, то пространства L_x и L_y будет различными. Следовательно, подпространства $L_x^\perp$ и $L_y^\perp$ также не будут совпадать. Пересечение двух линейных подпространств $L_x^\perp$ и $L_y^\perp$ само является линейным подпространством, и его размерность заведомо не больше $\frac{m}{2} - 1$. Другими словами, векторы из данного пересечения составляют не более половины линейного подпространства $L_y^\perp$. Следовательно, вероятность того, что случайный вектор из $w \in L_y^\perp$ попадёт одновременно и в ортогональное дополнение к L_x, не превосходит $1/2$. Таким образом, Чарли ошибается с вероятностью не более $1/2$.

Итак, мы проверили, что описанный протокол не ошибается в случае $x = y$, и вероятность ошибки ограничена $1/2$ в случае $x \neq y$. Повторяя протокол $\log 1/\varepsilon$ раз, можно сделать вероятность ошибки меньше любого наперед заданного $\varepsilon > 0$. При ограниченном числе повторений коммуникационная сложность протокола остается равной $O(\sqrt{n})$. Теорема доказана.

Теорема 8 $\mathsf{RCC}^{||}_{\varepsilon}(\mathsf{EQ}_n) = \Omega(\sqrt{n})$ *для любого* $\varepsilon < 1/2$.

Доказательство: Пусть имеется некоторый коммуникационный протокол π с параллельной отправкой сообщений для вычисления предиката EQ. Мы считаем, что Алиса и Боб пользуются раздельными источниками случайности, а Чарли использует детерминированный алгоритм для получения ответа.

Обозначим множество всех возможных сообщений Алисы через $\mathcal{A}$, а множество всех возможных сообщений Боба через $\mathcal{B}$. Таким образом, можно считать, что Алиса отправляет Чарли сообщение длиной $l_a = \log|\mathcal{A}|$ битов, а Боб – сообщение длиной $l_b = \log|\mathcal{B}|$ битов. Мы хотим доказать, что максимум из этих двух чисел $\max\{l_a, l_b\}$ не меньше $\Omega(\sqrt{n})$. Без ограничения общности можно считать, что для любой пары (x, y) вероятность ошибки протокола π не больше $1/100$ (вероятность ошибки всегда можно уменьшить в константу раз, последовательно повторяя коммуникационный протокол несколько раз).

Поскольку Алиса и Боб пользуются источниками случайности, для каждой пары входов $x, y \in \{0,1\}^n$, имеются распределение вероятностей на возможных сообщениях Алисы и Боба (при данных входах). Будем обозначать эти распределения μ_x (распределение на $\mathcal{A}$) и ν_y (распределение на $\mathcal{B}$) соответственно. Поскольку Чарли пользуется детерминированным алгоритмом, его решение можно обозначит функцией $\rho : \mathcal{A} \times \mathcal{B} \to \{0,1\}$. Значение $\rho(a,b)$ есть ответ, который выдает Чарли, получив от Алисы сообщение a и от Боба сообщение b.

Обозначим

$$F(x,b) := \sum_{a \in \mathcal{A}} \mu_x(a)\rho(a,b)$$

Определение. Сообщение $b \in \mathcal{B}$ называется *c-сильным* для x, если $F(x,b) \geq c$. В противном случае b называется *c-слабым*.

Будем обозначать

$$\begin{aligned} S_x &= \{b \ : \ b \text{ является 0.9-сильным для } x\}, \\ W_x &= \{b \ : \ b \text{ является 0.9-слабым для } x\}. \end{aligned}$$

Поскольку на любой паре входов протокол π ошибается с вероятностью не более 0.01,

$$\begin{aligned} &\text{если } f(x,y) = 0, \text{ то } \quad \sum_{a \in \mathcal{A}, b \in \mathcal{B}} \mu_x(a)\nu_y(b)\rho(a,b) \leq 0.01, \\ &\text{если } f(x,y) = 1, \text{ то } \quad \sum_{a \in \mathcal{A}, b \in \mathcal{B}} \mu_x(a)\nu_y(b)\rho(a,b) \geq 0.99 \end{aligned}$$

Лемма 1. (а) Если $f(x,y) = 0$, то $\nu_y(W_x) \geq 0.9$.
(б) Если $f(x,y) = 1$, то $\nu_y(S_x) \geq 0.9$.

Доказательство леммы 1: (а) Поскольку вероятность ошибки протокола на паре входов (x, y) не превосходит 0.01, мы имеем

$$\begin{aligned} 0.01 &\geq \sum_{a,b} \mu_x(a)\nu_y(b)\rho(a,b) \\ &\geq \sum_{b \not\in W_x} \nu_y(a) \cdot [\sum_a \mu_x(a)\rho(a,b)] \\ &\geq 0.1 \cdot \sum_{b \not\in W_x} \nu_y(a) \\ &= 0.1(1 - \nu_y(W_x)). \end{aligned}$$

Таким образом, $\nu_y(W_x) \geq 0.9$. Доказательство пункта (б) симметрично.

Для каждого x мы определим некоторое мультимножество $T_x = \{a_1, \ldots, a_t\}$, состоящее из элементов из $\mathcal{A}$ (мы говорим, что T_x *мультимножество*, поскольку некоторые элементы могут учитываться с кратностью больше единицы). Параметр t (число элементов в T_x с учетом кратности) мы выберем позднее. При этом окажется, что разным x соответствуют разные T_x. Так что слово $x \in \{0,1\}^n$ будет однозначно определяться соответствующим T_x.

Для фиксированного T_x обозначим

$$\xi_i(b) = \begin{cases} 1, & \text{если Чарли выдает ответ 1, получив пару сообщений } (a_i, b), \\ 0, & \text{иначе.} \end{cases}$$

Лемма 2. Для некоторого $t = O(\log |\mathcal{B}|)$ для каждого x можно таким образом выбрать мультимножество $T_x = \{a_1, \ldots, a_t\}$, состоящее из элементов $\mathcal{A}$, что для всякого $b \in \mathcal{B}$

$$|\sum_{i=1}^{t} \xi_i(a) - t \cdot F(x,a)| \leq 0.1 \cdot t.$$

Доказательство леммы: Зафиксируем $b \in \mathcal{B}$ и будем выбирать T случайно: каждый элемент a_i выбирается из $\mathcal{A}$ случайно по распределению μ_x; для разных i выбор делается независимо. Тогда среднее значение

$$E_T \sum \xi_i(a) = t \cdot F(x,a).$$

Применяя неравенство Чернова, получаем (для некоторой константы $c > 0$)

$$\mathrm{Prob}_T[|\sum_{i=1}^{t} \xi_i(a) - t \cdot F(x,a)| > 0.1 \cdot t] < e^{-c \cdot t} < \frac{1}{2|\mathcal{B}|}$$

(последнее неравенство гарантируется выбором t). Лемма доказана.

Зафиксируем для каждого $x \in \{0,1\}^n$ мультимножество T_x, существование которого гарантируется Леммой 2. Покажем, что разным x соответствуют обязательно разные T_x.

Лемма 3. Для любых $z, z' \in \{0,1\}^n$ $(z \neq z')$ мультимножества T_z и $T_{z'}$ не совпадают.

Доказательство леммы: Предположим, что $z \neq z'$ и $T_z = T_{z'}$. Тогда

$$0 = \mathsf{EQ}(z, z') \neq \mathsf{EQ}(z', z') = 1.$$

Из Леммы 1 получаем

- $\nu_{x'}(S_x) \geq 0.9$,
- $\nu_{x'}(W_{x'}) \geq 0.9$.

Из этой пары неравенств заключаем, что S_z и $W_{z'}$ с необходимостью пересекаются. Выберем некоторый элемент $z_0 \in S_z \cap W_{z'}$.

Далее, из Леммы 2 следует, что

- $|\sum_{i=1}^{t} \xi_i(z_0) - t \cdot F(z, z_0)| \leq 0.1 \cdot t$,
- $|\sum_{i=1}^{t} \xi_i(z_0) - t \cdot F(z', z_0)| \leq 0.1 \cdot t$.

При этом $F(z, z_0) \geq 0.9$ (поскольку $z_0 \in S_z$), а $F(z', z_0) \leq 0.1$ (поскольку $z_0 \in W_{z'}$). Получаем противоречие, и лемма доказана.

Лемма 3 говорит, что мультимножество T_z однозначно определяет $z \in \{0,1\}^n$. Это означает, что разных T_z должно быть не менее 2^n. Вспоминаем, что T_z состоит из $t = O(\log |\mathcal{B}|)$ элементов (с учетом кратностей). Следовательно,

$$2^n \leq |\mathcal{A}|^t \leq |\mathcal{A}|^{O(\log |\mathcal{B}|)} = 2^{O(\log |\mathcal{A}| \cdot \log |\mathcal{B}|)}.$$

Мы получаем оценку $n \leq O(\log |\mathcal{A}| \cdot \log |\mathcal{B}|)$, которая и означает, что либо сообщения Алисы, либо сообщения Боба должны иметь длину не менее $\Omega(\sqrt{n})$. Теорема доказана.

Упражнение. Докажите, что $\mathsf{RCC}^{||}_{\varepsilon}(\mathsf{GT}_n) = \Omega(\sqrt{n})$ для любого $\varepsilon < 1/2$.

13 Лекция 14, 18 мая.

13.1 Приложения коммуникационной сложности: время и память для вычисления на машине Тьюринга.

В этой главе мы воспользуемся коммуникационной сложностью, чтобы доказать нижние оценки на сложность вычисления на машинах Тьюринга. Напомним, что ранее (в лекции 5) мы уже доказали для одноленточных машин следующее утверждение:

Утверждение 1. Пусть $f_n : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ некоторая функция на парах двоичных строк, и одноленточная машина Тьюринга $\mathcal{M}$ вычисляет отображение $\hat{f}_n : \{0,1\}^{3n} \to \{0,1\}$ такое, что

$$\hat{f}_n(x0^n y) = f(x, y).$$

Обозначим $T(n)$ максимальное время работы данной машины на входах длины n. Тогда

$$\mathsf{CC}_0^{pub}(f_n) = O(T(3n)/n).$$

Следствие: Одноленточная машина не может распознавать язык палиндромов быстрее, чем за $\Omega(n^2)$ шагов.

Далее мы применим похожую технику, чтобы получить нижнюю оценку для сложности распознавания палиндромов на *многоленточных* машинах Тьюринга.

Утверждение 2. Пусть $f_n : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ некоторая функция на парах двоичных строк, и многоленточная машина Тьюринга $\mathcal{M}$ вычисляет отображение $\hat{f}_n : \{0,1\}^{3n} \to \{0,1\}$ такое, что

$$\hat{f}_n(x0^n y) = f(x,y).$$

Обозначим $T(3n)$ максимальное время работы данной машины на входах длины $3n$, и $S(3n)$ максимальное количество используемых ячеек памяти. Тогда

$$\mathsf{CC}(f_n) = O(T(3n)S(3n)/n).$$

Замечание: При работе с многоленточными машинами Тьюринга обычно предполагают, что одна из лент выделена для хранения входных данных. Эта лента доступна для чтения, но не для записи. Другие ленты машины называются "рабочими", они доступны и для чтения, и для записи. Используемая память S есть число ячеек рабочих лент, которые посещает машина до момента остановки; ячейки входной *read only* ленты при этом не учитываются.

Доказательство утверждения 2: Пусть машина $\mathcal{M}$ вычисляет функцию $\hat{f}_n$ за время не более $T(3n)$ и использует при этом не более $S(3n)$ ячеек памяти на рабочих лентах. Мы преобразуем эту машину в детерминированный коммуникационный протокол для вычисления функции $f(x,y)$.

Как обычно, мы считаем, что Алисе доступен вход x, а Бобу вход y. Алиса и Боб будут совместными усилиями моделировать шаг за шагом работу машины $\mathcal{M}$ на входе $x0^n y$. В каждый момент один из участников протокола будет "ответственным" за моделирование работы машины. Иногда один из них будет "передавать управление" другому. Когда Алиса "передает управление" Бобу, она пересылает ему текущую конфигурацию машины Тьюринга (записи на всех рабочих лентах и положение всех головок машины); аналогично поступает Боб, "передавая управление" Алисе.

Остаётся уточнить, когда именно управление моделированием передаётся от одного участника протокола другому. Это определяется положением читающей головки на входной ленте. Напомним, что на входной ленте записано двоичное слово $x0^n y$ (длины $3n$). Для определённости будем считать, что в начале работы читающая головка указывает на первый символ слова x, и управление находится в руках Алисы. Алиса будет отдавать управление Бобу каждый раз, когда читающая головка машины на входной ленте достигает первого (самого левого) символа слова y. После этого управление находится в руках Боба до тех пор, пока головка не достигнет самого правого символа слова x.

Между моментами передачи управления от Алисы к Бобу и обратно проходит не менее n шагов моделирования машины $\mathcal{M}$, поскольку за это время головка на входной ленте должна преодолеть дистанцию в n ячеек, разделяющих самый правый символ x и самый левый символ y. Следовательно, общее число передач управления между Алисой и Бобом за всё время моделирования не может быть больше $T(3n)/n$.

Поскольку при каждой передаче управления нужно переслать текущее содержимое памяти машины Тьюринга, это требует пересылки между Алисой и Бобом $O(S(3n))$ битов информации.

Таким образом, коммуникационный протокол вычисления функции $f_n(x,y)$ требует передачи не более, чем $(T(3n)/n) \cdot O(S(3n))$ битов информации. Утверждение доказано.

Пример применения утверждения 2: Пусть машина Тьюринга $\mathcal{M}$ распознаёт язык палиндромов — множество (двоичных) слов, которые одинаково читаются слева направо и справа налево. Обозначим $T(n)$ и $S(n)$ максимальное время и память (число использованных ячеек), которые требуются этой машине для обработки входов длины n. Покажем, что $T(n)$ и $S(n)$ не могут быть слишком маленькими. Более точно, мы покажем, что имеет место следующий баланс между затратами времени и памяти:

$$T(n) \cdot S(n) = \Omega(n^2).$$

(В англоязычной литературе в таких случаях пишут, что имеет место trade-off: можно "продать" время за память или наоборот; но "обменный курс" ограничен).

Чтобы доказать указанную оценку, рассмотрим функцию $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$

$$f(x,y) = \begin{cases} 1, & x = y^{-1}, \\ 0, & \text{иначе.} \end{cases}$$

Понятно, что $f(x,y) = 1$, если и только если слово $x0^n y$ является палиндромом. Поскольку машина $\mathcal{M}$ распознаёт язык палиндромов, мы можем применить Утверждение 2:

$$\mathsf{CC}(f_n) = O(T(3n)S(3n)/n).$$

Коммуникационная сложность $\mathsf{CC}(f_n) = n + 1$, поскольку функция f_n — это хорошо знакомый нам предикат равенства. Получаем

$$n + 1 = O(T(3n)S(3n)/n),$$

то есть

$$T(n)S(n) \geq cn^2$$

для некоторой константы $c > 0$.

Упражнение. (а) Докажите, что существует многоленточная машина Тьюринга $\mathcal{M}_1$, распознающая язык палиндромов, для которой $T(n) = O(n)$ и $S(n) = O(n)$. (б) Докажите, что существует многоленточная машина Тьюринга $\mathcal{M}_2$, распознающая язык палиндромов, для которой $T(n) = O(n^2)$ и $S(n) = O(\log n)$. (в) Докажите, что для любой машины Тьюринга, распознающей язык палиндромов, размер используемой памяти не может быть меньше $c \log n$, т.е., $S(n) = \Omega(\log n)$.

13.2 Приложения коммуникационной сложности: сложность булевых формул.

В этой главе мы будем изучать сложность описания функций булевыми формулами. Мы рассматриваем формулы, составленные из пропозициональных переменных с помощью связок $\&, \vee, \neg$ (конъюнкция, дизъюнкция и отрицания).

Чтобы было удобнее говорить о структуре формулы, мы будем их описывать не как последовательность символов (переменных, связок, скобок), а как двоичное дерево. В каждой внутренней вершине такого дерево помещается двухместная связка — конъюнкция или дизъюнкция; в каждом листе дерева помещается пропозициональная переменная или отрицание пропозициональной переменной. Каждому такому дереву естественным образом сопоставляется булева функция.

Ясно, что всякую булеву функцию (n переменных) можно записать такого рода формулой.

У булевой формулы есть две естественные меры сложности — глубина (глубина дерева) и размер (число связок, т.е., число внутренних вершин дерева). Минимальную глубину/сложность формулы, реализующей функцию f, мы обозначаем $d(f)$ и $L(f)$ соответственно. Величина $L(f)$ соответствует (с точностью до умножения на некоторую константу) числу символов в обычной записи булевой формулы; величина $d(f)$ соответствует "глубине вложенности" скобок в стандартной линейной записи формулы.

Утверждение 3. $d(f) = \Theta(\log L(f))$.

Доказательство утверждения: В одну сторону оценка очевидна — двоичное дерево глубины d содержит не более 2^d внутренних вершин, так что

$$L(f) \leq 2^{d(f)}.$$

С другой стороны, формула сложности L может иметь глубину намного больше $\log L$. Поэтому для доказательства утверждения мы должны проверить, что всякую формулу сложности L можно переделать в *быть может другую* формулу глубины $C \log L$ (для некоторой константы C). Это можно доказать индукцией по L, используя лемму, аналогичную лемме на странице 17:

Лемма. В двоичном дереве с L вершинами можно найти внутреннюю вершину u, которая разбивает дерево на три компоненты связности, каждая из которых содержит не более $L/2$ листьев.

Упражнение. Докажите эту лемму.

Построим формулы минимальной глубины для каждого из трёх полученных поддеревьев. По предположению индукции, глубина каждого из этих деревьев ограничена $C \log(L/2)$. Теперь формулу для исходной функции можно представить в виде булевой комбинации формул для этих трёх поддеревьев. При этом нам может потребоваться несколько копий указанных формул, но это не существенно — нам важно контролировать глубину итоговой формулы, а не её размер. Таким образом получаем для f формулу, глубина которой не превосходит

$$C \log(L/2) + O(1) \leq C \log L,$$

что завершает шаг индукции.

Далее мы докажем оценки на формульную сложность некоторых функций. Для этого нам будет удобно рассмотреть новый тип задач коммуникационной сложности.

Задача Вигдерсона–Карчмера (Karchmer–Wigderson). Пусть задана булева функция (предикат) $f : \{0,1\}^n \to \{0,1\}$. Рассмотрим следующую коммуникационную задачу. Пусть Алисе дано слово $x \in \{0,1\}^n$ такое, что $f(x) = 1$, а Бобу дано слово $y \in \{0,1\}^n$ такое, что $f(y) = 0$. Алиса и Боб должны найти такое целое число i (из интервала $1..n$), что i-ые биты слов x и y различаются. Мы обозначаем эту задачу KW_f.

Коммуникационный протокол для данной задачи должны работать корректно лишь для пар входов (x, y) с указанным свойством ($f(x) = 1$ и $f(y) = 0$); для других пар входов протокол может выдавать произвольный ответ. Отметим, что для пар слов (x, y), которые различаются в нескольких позициях, корректным

ответами будут сразу несколько чисел i; каждое из них допускается в виде ответа протокола.

Как обычно, коммуникационной сложностью этой задачи мы называем минимальное число битов, которыми должны обменяться Алиса и Боб для нахождения требуемого i. Мы обозначаем коммуникационную сложность этой задачи $\mathsf{CC}(KW_f)$.

Теорема 1. Для любой функции $f : \{0,1\}^n \to \{0,1\}$

$$\mathsf{CC}(KW_f) \leq d(f).$$

Доказательство теоремы: Пусть имеется некоторая формула глубины d для вычисления функции f. Мы переделаем эту формулу в коммуникационный протокол для решения задачи KW_f, причём коммуникационная сложность протокола будет совпадать с глубиной формулы d.

Итак, мы предполагаем, что Алисе дан такой набор битов $x = (x_1 \dots x_n)$, что $f(x) = 1$, а Бобу такой набор битов $y = (y_1 \dots y_n)$, что $f(y) = 0$. Будущий коммуникационный протокол можно неформально описать следующим образом. Мы будем двигаться по дереву формулы от корня к листьям вдоль такого пути, каждой вершине которого на входах x и y сопоставляются разные булевы значения.

В начале мы находимся в корне дерева, которому (по условию) на входах x и y соответствуют значения 1 и 0. Предположим для определённости, что корень дерева помечен дизъюнкцией. Тогда на входе x хотя бы одно из двух поддеревьев корня должно возвращать значение 1, а на входе y оба поддерева должны возвращать значение 0. Следовательно, Алиса может (зная x) выбрать одно из двух поддеревьев, в котором вычисленное значение на входах x и y заведомо различаются. Алиса сообщает о выбранном поддереве Бобу, и они переходят к рассмотрению этого поддерева. Аналогично Алиса действует во всех вершинах, помеченных дизъюнкцией. Если же вершина помечена конъюнкцией, то на входе x оба потомка этой вершины возвращают значение 1, а на входе y хотя бы один из двух потомков возвращает значение 0. В данном случае Боб (зная y) выбирает того из двух потомков текущей вершины, для которого вычисленное значение на входе x и на входе y различаются.

Когда Алиса и Боб попадают в лист дерева, они тем самым узнают литерал, значение которого для x и для y различны, что и требовалось. Ясно, что коммуникационная сложность совпадает с глубиной формулы.

Упражнение. Докажите, что для любой функции $f : \{0,1\}^n \to \{0,1\}$

$$\mathsf{CC}(KW_f) \geq d(f)$$

(вместе с теоремой 1 получаем, что $\mathsf{CC}(KW_f) = d(f)$). *Указание:* Рассмотрите дерево коммуникационного протокола для задачи KW_f и замените в нём ходы Алисы на дизъюнкцию, а ходы Боба на конъюнкцию. Листья пометьте литералами (пропозициональными переменными или их отрицаниями), в зависимости от значения, вычисленного протоколом.

Лемма. (Храпченко) Пусть дана функция $f : \{0,1\}^n \to \{0,1\}$ и пара множеств $X, Y \subset \{0,1\}^n$ таких что, $f(x) = 1$ для любого $x \in X$ и $f(y) = 0$ для любого $y \in Y$. Обозначим

$$C = \{(x,y) \in X \times Y \ : \ dist(x,y) = 1\}.$$

Тогда $\mathsf{CC}(KW_f) \geq \log \frac{|C|^2}{|X|\cdot|Y|}$.

(Здесь $dist(x,y)$ обозначает хэмминговское расстояние: слова x и y должны отличаться ровно в одной позиции.)

Доказательство леммы: Зафиксируем коммуникационный протокол для решения задачи KW_f. Нас интересуют только такие x и y, которые лежат в X и Y соответственно. Поэтому мы можем исключить из рассмотрения все (x,y), лежащие вне $X \times Y$. Обозначим $R_1, \ldots, R_t$ прямоугольные множества в $X \times Y$, соответствующие листьям заданного коммуникационного протокола. Множество $X \times Y$ оказывается разбитым на непересекающиеся комбинаторные прямоугольники:

$$(*) \qquad |X| \cdot |Y| = \sum_{i=1}^{t} |R_i|$$

Каждому из этих комбинаторных прямоугольников R_j сопоставляется значение $j = j(i)$ из интервала $1..n$, которое объявляется ответом, если в заданном протоколе Алиса и Боб приходят в i-ый лист. Обозначим $m_i = |R_i \cap C|$. Поскольку протокол детерминированный (а значит, прямоугольные множества R_j не пересекаются между собой), имеем

$$|C| = \sum_{i=1}^{t} m_i.$$

Теперь мы сделаем ключевое для всего доказательства наблюдение. Рассмотрим какой-либо из прямоугольников R_i. Пусть i-му листу дерева протокола соответствует ответ j (Алиса и Боб приходят к выводу, что их слова x и y отличаются в j-ой позиции). Зафиксируем какую-нибудь строку x, пересекающую данный комбинаторный прямоугольник и посмотрим, какие пары (x,y) из множества C могут лежать на пересечении x-ой строки и комбинаторного прямоугольника R_i. С одной стороны, все такие элементы y обязаны отличаться от x хотя бы в позиции j (это верно для всех пар (x,y) в R_i). С другой стороны, все такие y должны отличаться от x ровно в одной позиции (это верно для всех пар (x,y) в C). Следовательно, на пересечении строки x и прямоугольника R_i может лежать не более одной пары (x,y) из множества C. Поскольку мы обозначили $m_i = |R_i \cap C|$, получаем, что в R_i должно быть не менее m_i строк. Аналогично доказывается, что в R_i должно быть не менее m_i столбцов. Следовательно, для каждого из рассматриваемых прямоугольных множеств

$$(**) \qquad |R_i| \geq m_i^2.$$

Таким образом, мы получаем

$$|C|^2 = \Big(\sum m_i\Big)^2 \leq t \cdot \sum m_i^2 \leq t \cdot \sum |R_i| = t \cdot |X| \cdot |Y|$$

(первое неравенство есть применение неравенства Коши–Буняковского, второе следует из (**), и последнее равенство получается из (*)). Лемма доказана.

Пример применения леммы Храпченко. Рассмотрим функцию чётности:

$$\oplus(x_1, \ldots, x_n) = x_1 + \ldots + x_n \ mod\ 2.$$

Обозначим X и Y множество n-ок битов с нечётным и чётным числом единиц соответственно (т.е., $\oplus(x) = 1$ для всех $x \in X$ и $\oplus(y) = 0$ для всех $y \in Y$). В

данном примере $|X| = |Y| = 2^{n-1}$, а $|C| = n \cdot 2^{n-1}$ (для каждого $x \in X$ имеется n соседних $y \in Y$, которые отличаются от x ровно в одном бите).

Из леммы Храпченко получаем оценку $\mathsf{CC}(KW_{\oplus}) \geq \log(n^2) = 2\log n$. Применяя Теорему 1 и Утверждение 3, получаем

$$d(\oplus) \geq 2\log n$$

и $L(\oplus) \geq n^2$. Таким образом, функция чётности требует булевой формулы не менее чем квадратичного размера.

Упражнение. Докажите, что полученная оценка для функции чётности является точной, т.е., $L(\oplus) = \Theta(n^2)$. *Указание:* Индукцией по k докажите, что функцию чётности на $n = 2^k$ входах можно описать формулой глубины $2k$.

13.3 Приложения коммуникационной сложности: сложность монотонных булевых формул.

В этой главе[3] мы докажем очень сильную (экспоненциальную) нижнюю оценку на монотонную формульную сложность некоторой естественной булевой функции.

Прежде всего, напомним определения. Булева функция $f(x_1, \ldots, x_n)$ называется *монотонной*, если при изменении одного из аргументов с 0 на 1 значение функции либо не меняется, либо меняется тоже с 0 на 1.

Монотонной формулой мы будем называть булеву формулу в базисе $\{\&, \vee\}$. Отличие от общего определения формулы (из предыдущей главы) состоит в том, что в формуле не используется отрицание (все литералы в листьях дерева формулы являются пропозициональными переменными, а не их отрицаниями).

Упражнение. Докажите, что всякая монотонная булева функция может быть представлена некоторой монотонной булевой формулой.

Паросочетание. Рассмотрим неориентированные графы на n вершинах, без кратных рёбер и петель. Каждая пара вершин в графе либо соединена ребром, либо не соединена. Таким образом, что описать граф, нам нужно $m = C_n^2 = \frac{n(n-1)}{2}$ битов.

Говорят, что в графе имеется совершенное паросочетание, если можно выбрать среди всех рёбер графа $m/2$ рёбер так им образом, чтобы каждая из вершин была инцидентна ровно одному ребру.

Рассмотрим функцию $Match_n(x_1, \ldots, x_m)$, которая зависит от m булевых переменных: рассматриваем набор из m битов как описание графа на n вершинах; i-ая переменная равна единице, если соответствующее ребро входит в граф. Полагаем функцию $Match_n$ на некотором булевом наборе равной 1, если в соответствующем графе есть совершенное паросочетание. Данная функция монотонна (если к некоторому графу с совершенным паросочетанием добавить новые рёбра, то совершенное паросочетание сохранится).

Упражнение. Докажите, что для функции $Match_n$ есть монотонная булева схема размера $2^{O(m)} = 2^{O(n^2)}$.

Упражнение. Разрешим использовать в дереве формулы конъюнкции и дизъюнкции не с двумя, а с неограниченным числом входов. Докажите, что по таким

[3] Материал этой главы не был подробно рассказан не лекции.

правилам для функции $Match_n$ можно построить монотонную булеву схему размера $2^{O(n)}$.

Основной результат этой главы: для монотонной функции $Match_n$ нельзя построить монотонную формулу размера меньше 2^{cn}.

Теорема 2. Всякая монотонная формула для функции $Match_n$ имеет сложность $2^{\Omega(n)}$.

Доказательство: основано на уже известной нам оценке коммуникационной сложности задачи DISJ. Сведение коммуникационной задачи DISJ к задаче о монотонной булевой формуле для задачи $Match_n$ будет состоять из нескольких шагов. Сначала мы сведём DISJ к некоторой коммуникационной задаче о покрытии рёбер в графе, а затем сведём задачу о покрытии к задаче о паросочетании.

Рассмотрим следующую коммуникационную задачу о покрытии рёбер в графе (Covering). Алисе дан некоторый неориентированный граф без петель $G = (V, E)$ на $3n$ вершинах и с n рёбрами, а Бобу дано некоторое множество вершин $W \subset V$ размера n. Требуется узнать, покрывают ли вершины W все ребра графа G.

Предложение 1. Если существует вероятностный коммуникационный протокол сложности $o(n)$ для задачи $Covering$, то существует вероятностный коммуникационный протокол сложности $o(n)$ для предиката DISJ.

Доказательство предложения 4: В исходной задаче DISJ Алисе и Бобу даны множества $X, Y \subset \{1, \ldots, n\}$ соответственно, и требуется узнать, пересекаются ли эти множества. Построим соответствующую задачу о покрытии.

Граф Алисы $G = (V, E)$ будет состоять из $3n$ вершин. Мы обозначим их a_i, b_i, c_i для $i = 1, \ldots, n$. Рёбра в графе проводятся следующим образом. Если $i \in X$, то ребром соединяются вершины a_i и b_i. Если же $i \notin X$, то ребром соединяются вершины b_i и c_i. Таким образом, всего в графе будет n рёбер.

Теперь определим множество вершин W (вход Боба). Если $i \in Y$, то W содержит вершину c_i, а если $i \notin Y$, то W содержит вершину b_i. По построению W состоит из n вершин.

Упражнение. Докажите, что исходные множества X и Y дизъюнктны, если и только если W покрывает все рёбра построенного графа G.

Упражнение показывает, что вместо решения задачи о дизъюнктности множеств Алиса и Боб могут решать соответствующую задачу о покрытии. Предложение 1 доказано.

Далее нам будет удобно рассмотреть следующую задачу о (несовершенном) паросочетании. Пусть задан граф на $3n$ вершинах; требуется узнать, есть ли в нём паросочетание из n рёбер (можно ли выбрать n рёбер, покрывающих $2n$ вершин). Обозначим $Match(n, 3n)$ булеву функцию, которая описанию графа (на $3n$ вершинах) сопоставляет единицу, если в этом графе есть паросочетание размера n, и ноль в противном случае.

Мы введём для монотонных функций $f : \{0,1\}^n \to \{0,1\}$ "монотонный" аналог коммуникационной задачи Вигдерсона–Карчмера KW_f^m (индекс m в обозначении KW_f^m означает *монотонность*). В задаче KW_f^m Алисе дано такое x, что $f(x) = 1$, а Бобу такое y, что $f(y) = 0$. Требуется найти такое i, что i-ый бит слова x равен 1, а i-ый бит слова y равен нулю (это всегда возможно, если f монотонная).

В частности, задача $KW_{Match_n}^m$ означает, что Алисе дан граф на n вершинах, в котором есть совершенное паросочетание, а Бобу дан граф на тех же n вершинах,

в котором совершенного паросочетания нет. Требуется найти такую пару вершин (i, j), которые в графе Алисы соединены ребром, а в графе Боба не соединены.

Нас также будет интересовать аналогичная коммуникационная задача Вигдерсона–Карчмера $KW^m_{Match(n,3n)}$. Содержательно её можно сформулировать следующим образом. Алисе дан некоторый граф на $3n$ вершинах, и известно, что в этом графе есть паросочетание размера n. Бобу дан другой граф на $3n$ вершинах, и в этом графе нет паросочетания размера n. Требуется найти такую пару вершин (i, j), которые в графе Алисы соединены ребром, а в графе Боба не соединены.

Предложение 2. Если существует *детерминированный* коммуникационный протокол сложности $o(n)$ для задачи $KW^m_{Match(n,3n)}$, то для задачи $Covering$ существует *вероятностный* коммуникационный протокол с коммуникационной сложностью $o(n)$.

Доказательство предложения 2: Доказательство состоит в вероятностном сведении задачи $Covering$ к задаче $KW^m_{Match(n,3n)}$. Прежде всего мы опишем вероятностную процедуру, которая преобразует условия задачи $Covering$ в условия задачи $KW^m_{Match(n,3n)}$.

Напомним, что в задаче $Covering$ Алисе дан граф $G = (V, E)$, состоящий из $3n$ вершин и n рёбер, а Бобу дано множество из n вершин $W \subset V$. Боб применяет следующее вероятностное преобразование, которое превращает множество W в некоторый граф $G' = (V, E')$ на $3n$ вершинах. Прежде всего, Боб случайно выбирает вершину $v \in W$. Обозначим $W' = W \setminus \{v\}$. В качестве G' Боб берёт двудольный граф, в котором соединены ребрами каждая вершина из W' с каждой вершиной из $V \setminus W'$.

Далее Алиса и Боб используют общий источник случайности и применяют к $3n$ вершинам своих графов одну и ту же случайно выбранную перестановку π. В результате каждый из них получает некоторый граф на $3n$ вершинах. Данная пара графов и берётся в качестве пары входов задачи $KW^m_{Match(n,3n)}$.

Далее Алиса и Боб применяют к построенным графам коммуникационный протокол задачи $KW^m_{Match(n,3n)}$ и находят ребро (i, j), которое имеется в (новом) графе Алисы, но не в графе Боба. Если один из концов этого ребра совпадает с $\pi(v)$, то Боб объявляет, что множество W в исходной задаче покрывало все рёбра графа Алисы. В противном случае Боб объявляет, что множество W не было покрытием в графе.

Упражнение. Докажите, что если множество W является покрытием для исходного графа G, то описанный протокол никогда не ошибается. Если же W не является покрытием, то вероятность ошибки в описанном протоколе не превосходит $1/2$.

Предложение 3. Если задача $KW^m_{Match_n}$ имеет коммуникационную сложность $o(n)$, то и задача $KW^m_{Match(n,3n)}$ тоже имеет коммуникационную сложность $o(n)$.

Упражнение. Докажите Предложение 3.

Предложение 4. Если для функции $Match_n$ существует монотонная булева формула сложности $2^{o(n)}$, то коммуникационная сложность задачи $KW^m_{Match_n}$ равна $o(n)$.

Доказательство: аналогично доказательству Теоремы 1 и Утверждения 3 из главы 13.2.

В главе 11 мы доказали, что $\mathsf{CC}_\varepsilon(\mathsf{DISJ}) = \Omega(n)$. Из этого факта и Предложений 1–4 получаем Теорему 2.

Список литературы

[1] Eyal Kushilevitz and Noam Nisan. Communication Complexity. Cambridge University Press. 1998.

[2] Alexander Razborov. Communication Complexity. In: An Invitation to Mathematics: from Competitions to Research. Springer, 2011.

[3] Александр Александрович Разборов. Коммуникационная сложность. Серия Летняя школа “Современная математика”. МЦНМО, 2012.

[4] Sanjeev Arora and Boaz Barak. Computational Complexity: A Modern Approach. Cambridge University Press. 2009.

[5] László Babai and Peter G. Kimmel. Randomized Simultaneous Messages: Solution of a Problem of Yao in Communication Complexity. IEEE Conference on Computational Complexity, 1997, 239–246.