Майская проектная смена по математике и теоретической информатике

Сириус, 2024

МКН СПбГУ

Коммуникационные игры

Аннотация

Проект посвящён изучению коммуникационной сложности и её применений в различных областях компьютерных наук. Основной объект изучения — это игра двух игроков, Алисы и Боба, живущих в разных городах, в которой они должны вычислить значение некоторой функции $f(x,y)$, где x известен только Алисе, y — только Бобу. Игрокам разрешено общаться между собой, посылая друг другу битовые сообщения. Их задача — вычислить $f(x,y)$, передав как можно меньше сообщений. Коммуникационная сложность естественным образом возникает в потоковых и распределённых алгоритмах, схемной сложности и сложности доказательств, и в других областях компьютерных наук. Как это часто бывает в теоретической информатике, задачи, которые будут у нас возникать, имеют очень простые формулировки, но интересные и совсем нетривиальные доказательства, поэтому в течение смены нам предстоит освоить множество техник и трюков.

Мы начнем с классической коммуникационной сложности, далее рассмотрим ее различные модификации, такие как полудуплексная коммуникационная сложность, коммуникационная сложность с оракулом и универсальные коммуникационные протоколы, которые возникают в некоторых задачах теоретической информатики, и дойдем до множества открытых задач.

Белова Татьяна Сергеевна (ПОМИ РАН)
Аспирант и младший научный сотрудник ПОМИ РАН, выпускница МКН СПбГУ. Лектор курса по высокоточной сложности в СПбГУ 2024-2025, вела практические занятия по дискретной математике и алгоритмам в СПбГУ, ИТМО, ВШЭ. Победитель конкурса индивидуальных грантов «Молодая математика России». Финалист ACM ICPC.

Игнатьев Артур Андреевич (МКН СПбГУ, ВШЭ)
Студент магистратуры «Разработка программного обеспечения и науки о данных», выпускник бакалавриата МКН СПбГУ. Младший научный сотрудник лаборатории теории игр ВШЭ. На МКН ведет практики по курсу «Теоретическая информатика».

Дементьев Юрий Ильич (МКН СПбГУ, ВШЭ)
Студент магистратуры «Разработка программного обеспечения и науки о данных», выпускник бакалавриата МКН СПбГУ. Исследователь лаборатории теории игр ВШЭ, аналитик в MY.GAMES. На МКН ведет практики по курсу «Теоретическая информатика».

Содержание

1 Игра Алисы и Боба

Задача 1.0 (0 баллов). *Алиса и Боб играют в следующую игру. Они находятся в разных городах, Алисе сообщается число x, а Бобу — число y, причём x и y — это 0, 1, или 2. В их распоряжении есть устройство связи, которое позволяет передавать друг другу битовые сообщения (т.е. за одно сообщение можно послать «0» или «1»). Алиса и Боб могут заранее договориться о том, какие сообщения они будут посылать. Как им договориться, чтобы в результате оба игрока узнали значение $x + y$?*

Разбор задачи 1.0. Так как x и y принимают только значения 0, 1, или 2, то результат сложения $x + y$ принимает целые значения от 0 до 4. Алиса и Боб могут, например, использовать следующий подход: Алиса посылает Бобу двоичную запись x, Боб вычисляет $z = x + y$ и посылает Алисе двоичную запись z. Давайте посчитаем, сколько сообщений потребуется передать игрокам в худшем случае. Чем больше число, тем длиннее его двоичная запись, поэтому худший случай будет достигаться на входе $(2, 2)$. В этом случае Алиса передаст Бобу два сообщения «1» и «0», задающие двоичную запись числа 2, а Боб перешлёт Алисе три сообщения «1», «0», «0», задающие двоичную запись числа 4. Итого потребуется 5 сообщений (см. рис. 1).

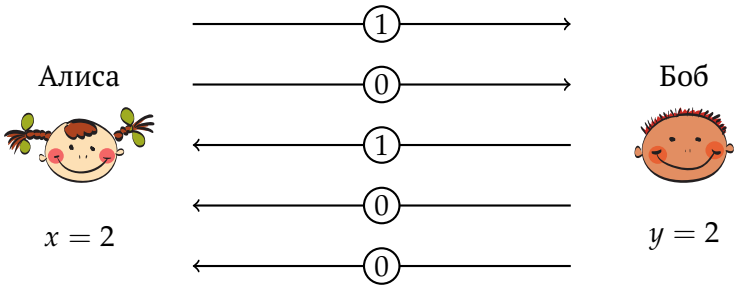


Рис. 1. Возможное взаимодействие Алисы и Боба на входе $(2, 2)$ в задаче 1.0.

Обсудим, как Алиса и Боб будут вести себя на других входах. Пусть $x = 1$, а $y = 0$. По договорённости Алиса должна послать Бобу x. Она может попробовать сделать это, послав одно сообщение «1», но это приведёт к неопределённости — Боб не будет знать, следует ли ждать от Алисы ещё сообщения (например, если она собирается передать $x = 2$), или Алиса уже закончила и $x = 1$. Поэтому их общение должно быть устроено так, чтобы таких неоднозначностей не возникало. Например, Алиса и Боб могут договориться, что Алиса всегда посылает два бита: «0» и «0» при $x = 0$, «0» и «1» при $x = 1$, и «1» и «0» при $x = 2$. Боб в свою очередь всегда отвечает, посылая три бита, кодирующие числа от 0 до 4 аналогичным образом.

Задача 1.1 (1 балл). *Как решить задачу 1.0 так, чтобы Алиса и Боб в сумме послали не более четырёх сообщений?*

Задача 1.2 (1 балл). *Как решить задачу 1.0 так, чтобы Алиса и Боб всегда посылали не более четырёх сообщений, но при этом на некоторых входах посылали строго менее четырёх сообщений?*

Задача 1.3 (3 балла). *Докажите, что не существует способа решить задачу 1.0, при котором Алиса и Боб будут всегда посылать не более трёх сообщений.*

Последняя задача принципиально отличается от первых трёх, т.к. в ней нужно не придумать какой-то способ, а *доказать*, что такого способа не существует. Решением этой

задачи должно быть (математически строгое) доказательство. Давайте для примера разберём доказательство более простого утверждения «не существует способа решить задачу 1.0, посылая не более двух сообщений». Сначала рассмотрим пример *некорректного* рассуждения.

> За два сообщения Алиса сможет передать Бобу значение x, но ведь Бобу тоже нужно что-то послать в ответ Алисе, поэтому двух сообщений не хватит.

Это рассуждение не является корректным доказательством, т.к. мы рассуждаем про какой-то конкретный способ решения, который используют Алиса и Боб. Нам же нужно доказать, что *никакой* способ решения не сработает. Корректное доказательство могло бы выглядеть, например, так.

> Если при каких-то x и y все сообщения посылает один из игроков, то сам этот игрок не получает никаких сообщений, а, следовательно, он никак не может восстановить значение $x+y$ — этот игрок знает только одно из слагаемых, и не знает ничего про второе. Поэтому всегда сообщения посылают оба игрока. Рассмотрим поведение игроков на парах входов $(0,0)$, $(1,0)$ и $(2,0)$. Во всех трёх случаях Боб получает только одно битовое сообщение. Это значит, что на каких-то двух входах Боб получает одно и то же сообщение. Следовательно, две пары входов с разным x и одинаковым y не отличимы с точки зрения Боба, поэтому он не может знать $x+y$ — если бы он знал, то смог бы восстановить x.

Задача 1.4 (1 балл). *Пусть Алиса и Боб вместо суммы хотят вычислить произведение двух целых чисел от* 0 *до* $n = 2^k - 1$. *Как это сделать за* $2k$ *сообщений?*

Для продолжения нам нужно немного поговорить о множествах, функциях и деревьях.

2 Множества, функции и деревья

- *Множества* состоят из *элементов*. Запись $x \in M$ означает, что x является элементом множества M. Множество можно задать, перечислив его элементы в фигурных скобках, например, $M = \{0,1,2,3\}$, или при помощи записи с условием, $A = \{x \mid [\textit{условие}]\}$ (множество таких x, для которых верно [*условие*]). Например, $\{x \mid x \in \mathbb{Z}, x \bmod 2 = 0\}$ — множество чётных целых чисел.

- Множество *конечно*, если оно содержит конечное число элементов. *Мощность* конечного множества A — это количество элементов в нём, обозначается $|A|$.

- Множество A является *подмножеством* множества B (записывается как $A \subset B$), если все элементы A являются элементами B.

- *Декартово произведение* $A \times B$ состоит из всех возможных упорядоченных пар (a,b), где $a \in A$ и $b \in B$.

  $$A \times B = \{(x,y) \mid x \in A \text{ и } y \in B\}$$

  Декартово произведение множества A на само себя удобно записывать так:

  $$A \times A = A^2, \quad \underbrace{A \times A \times \cdots \times A}_{n} = A^n.$$

  Например, $\{0,1\}^5$ — множество всех битовых строк длины 5.

- Подмножество R множества $A \times B$ называют *отношением* между множествами A и B.
- Отношение $f \subset A \times B$ называют *функцией из A в B*, если оно не содержит пар с одинаковым первым членом и разными вторыми. Это означает, что для каждого $a \in A$ существует не более одного $b \in B$, при котором $(a, b) \in f$. Множество всех $a \in A$, для которых существует такое $b \in B$, что $(a, b) \in f$, называется *областью определения* f. Для всех a из области определения f можно определить *значение* f на аргументе a как тот единственный элемент $b \in B$, при котором $(a, b) \in f$ (обозначается $f(a)$). Если область определения f совпадает с A, то пишут: $f\colon A \to B$ (т.е. f сопоставляет каждому элементу A элемент B).

В соответствии с этими определениями мы можем рассматривать сложение двух целых чисел 0 до 2 как функцию из множества $\{0,1,2\} \times \{0,1,2\}$ в множество $\{0,\dots,4\}$. Таким образом, в задаче 1.0 мы рассматривали функцию от двух аргументов

$$f\colon \{0,1,2\} \times \{0,1,2\} \to \{0,1,2,3,4\}$$

такую, что $f(x,y) = x + y$. Подробнее о множествах и функциях можно прочитать здесь.

Упорядоченное корневое двоичное дерево состоит из *вершин*, соединённых *рёбрами* следующим образом (см. рис. 2, вершины обозначаются кружочками, а рёбра — отрезками):

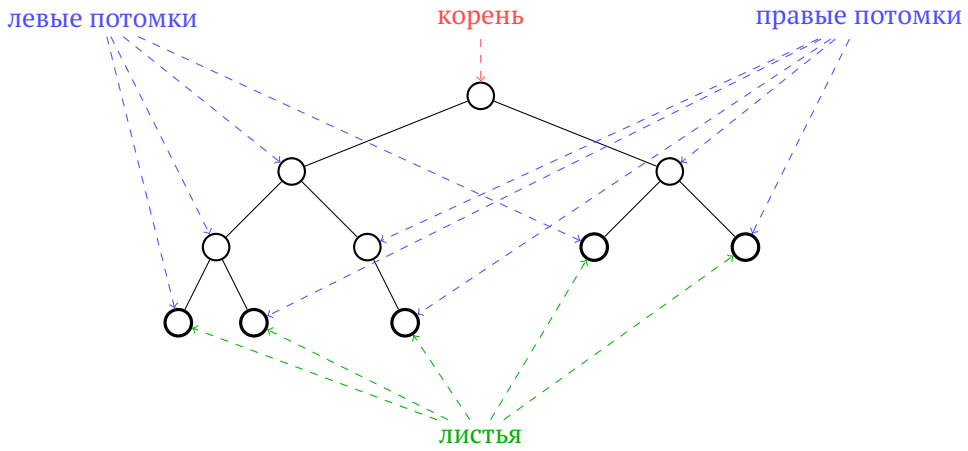


Рис. 2. Упорядоченное корневое двоичное дерево.

- есть выделенная вершина — *корень*,
- у каждой вершины не более двух *потомков*, с которыми она соединена рёбрами,
- корень — это единственная вершина, которая не является является чьим-то потомком,
- каждый потомок является либо *левым*, либо *правым*, если потомка два, то один из них левый, а второй — правый,
- вершины без потомков называются *листьями*, остальные вершины называются *внутренними вершинами*.

3 Игра для произвольной функции

Обобщим игру Алисы и Боба на случай произвольной функции от двух аргументов. Пусть X, Y и Z — непустые конечные множества. Цель Алисы и Боба в игре для функции $f\colon X \times Y \to Z$ заключается в вычислении значения f на входах $x \in X$ и $y \in Y$.

Задача 3.1 (1 балл). *Как вычислить $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^k$ за $2n$ сообщений?*

Задача 3.2 (1 балл). *Как вычислить $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^k$ за $n + k$ сообщений?*

Задача 3.3 (2 балла). *Пусть $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ и $f(x,y) = x$. Докажите, что всегда будет пара (x,y), на которой Алиса и Боб пошлют не менее n сообщений.*

В последней задаче по сути требуется доказать, что не существует более эффективного способа решить эту задачу, чем способ, при котором Алиса посылает Бобу весь x целиком. Для доказательства более сложных утверждения такого рода, нам нужно формально определить, что значит, что Алиса и Боб договорились о некотором способе решить задачу. Будем говорить, что Алиса и Боб договорились, если они определили *протокол общения*.

Определение 3.1 (Протокол общения)

Пусть X, Y и Z — это три произвольных непустых конечных множества, а $f\colon X \times Y \to Z$ — некоторая функция. *Протокол общения* Π для функции f — это упорядоченное корневое двоичное дерево со следующими пометками:

- каждая внутренняя вершина помечена буквой «А» или «Б»,
- каждое ребро к левому потомку помечено нулём, к правому — единицей,
- каждый лист помечен элементом множества Z.

Для каждой внутренней вершины v с пометкой «А» определена функция $A_v\colon X \to \{0,1\}$, а для каждой внутренней вершины u с пометкой «Б» определена функция $B_u\colon Y \to \{0,1\}$.
Результат протокола Π на входе (x,y) обозначается $\Pi(x,y)$, и определяется, как пометка конечной вершины пути $\pi(x,y)$, построенного по следующим правилам:

- первая вершина пути $\pi(x,y)$ — это корень,
- каждая следующая вершина пути является потомком предыдущей, причём
  - каждая вершина пути v с пометкой «А» соединена с потомком ребром с пометкой $A_v(x)$
  - каждая вершина u с пометкой «Б» соединена с потомком ребром с пометкой $B_u(y)$
- последняя вершина пути $\pi(x,y)$ — лист.

Протокол Π называется *корректным* протоколом для функции f, если для каждой пары входов (x,y) выполняется $\Pi(x,y) = f(x,y)$.

Протокол описывает общение игроков на всех возможных входах. Пометки во внутренних вершинах — это указание на игрока, который посылает сообщение, пометки на рёбрах — это посылаемые сообщения, пометки в листьях — это результат вычисления $f(x,y)$, а функции в вершинах — это правила, по которым игроки выбирают сообщение, которое нужно послать в данный момент. Каждой паре входов (x,y) соответствует путь

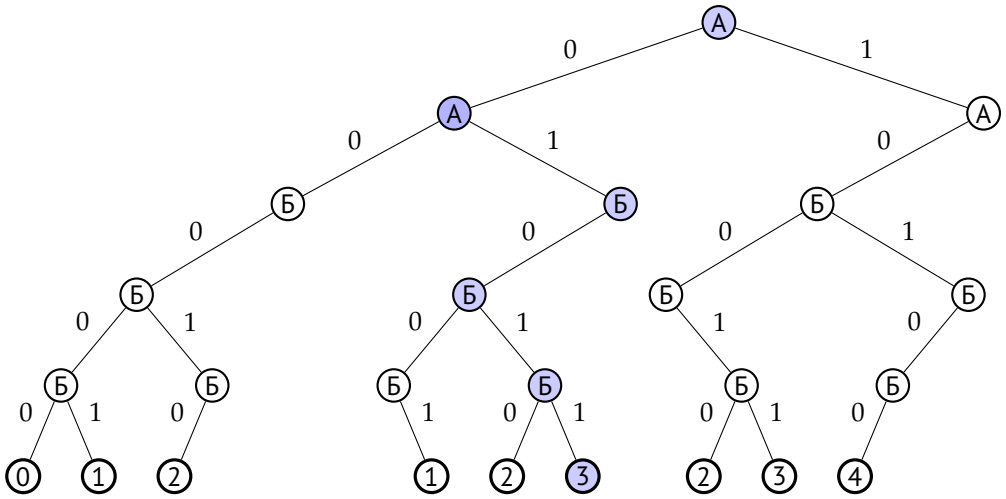


Рис. 3. Дерево протокола для решения задачи 1.0 описанного в разборе. Синим цветом выделены вершины пути $\pi(1,2)$.

$\pi(x,y)$ от корня к некоторому листу, который задаётся описанными выше правилами. Если протокол корректный, то для каждой пары входов (x,y) путь $\pi(x,y)$ заканчивается в листе с пометкой $f(x,y)$.

Задача 3.4 (2 балла). *Пусть* Π *— некоторый протокол для функции* $f\colon X \times Y \to Z$*, и пусть на входах* (x_1,y_1) *и* (x_2,y_2) *пути* $\pi(x_1,y_1)$ *и* $\pi(x_2,y_2)$ *заканчиваются в одном и том же листе. Докажите, что* $\pi(x_1,y_2)$ *и* $\pi(x_2,y_1)$ *заканчиваются в том же листе.*

Задача 3.5 (1 балл). *Докажите, что если Ева, подслушивающая общение Алисы и Боба, знает протокол общения, то она может восстановить* $f(x,y)$ *не зная* x *и* y*.*

Определение 3.2

Сложностью функции f называется наименьшая глубина протокола, вычисляющего функцию f (обозначается $C(f)$). (Глубина дерева — это максимальная рёберная длина пути от корня до листа.)

Функция $\mathrm{EQ}_n\colon \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ проверяет две битовые строки длины n на равенство: $\mathrm{EQ}_n(x,y) = 1$ тогда и только тогда, когда $x = y$.

Задача 3.6 (4 балла). *Докажите, что* $C(\mathrm{EQ}_n) = n+1$.
(В этой задаче нужно показать, что любой протокол для EQ_n *будет глубины не меньше* $n+1$*. Попробуйте оценить минимальное число листьев в таком протоколе.)*

Функция РАЗНОСТЬ$_n\colon \{0,\dots,2^n-1\} \times \{0,\dots,2^n-1\} \to \{-2^n+1,\dots,2^n-1\}$ вычисляет разность целых чисел x и y: РАЗНОСТЬ$_n(x,y) = x - y$.

Задача 3.7 (4 балла). *Докажите, что* $C(\text{РАЗНОСТЬ}_n) = 2n$.

Задача 3.8 (5 баллов). *Функция* $\mathrm{DISJ}_n\colon \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ *проверяет, есть ли позиция, в которой и у Алисы, и у Боба стоят единицы:* $\mathrm{DISJ}_n(x,y) = 0$ *тогда и только тогда, когда существует* $i \in \{1,\dots,n\}$ *такое, что* $x[i] = y[i] = 1$ *(здесь и далее* $x[i]$ *обозначает* i*-й бит строки* x*). Докажите, что существует такая константа* $c > 0$*, что* $C(\mathrm{DISJ}_n) \geq c \cdot n$*.*

Функция СРЕДНИЙ$_n(x,y)\colon \{0,1\}^n \times \{0,1\}^n \to \{1,\dots,n\}$, определяет центральный элемент в упорядоченной по возрастанию последовательности, содержащей все номера позиций, на которых в строках x и y встречаются единицы (если в позиции i у обоих игроков

стоят единицы, то i в последовательности встречается дважды). Если число элементов нечётно и равно $2m+1$, функция возвращает элемент на позиции $m+1$. В случае, если число элементов чётно и равно $2m$, функция возвращает элемент на позиции $m+1$.

Задача 3.9 (3 балла)**.** *Докажите, что существует такая константа $c > 0$, что для любого $n = 2^k$ выполняется $C(\text{СРЕДНИЙ}_n) \leq c \cdot k^2$.*

Задача 3.10 (10 баллов)**.** *Докажите, что существует такая константа $c > 0$, что для любого $n = 2^k$ выполняется $C(\text{СРЕДНИЙ}_n) \leq c \cdot k$.*

4 Коммуникационная сложность

Область теоретической информатики, которая занимается такими задачами про Алису и Боба, называется *коммуникационная сложность*. Она была разработана Эндрю Яо в 1979 году для доказательства сложности некоторых задач параллельных вычислений, а в дальнейшем нашла применения и других областях компьютерных наук. Коммуникационная сложность естественным образом возникает в потоковых и распределённых алгоритмах, схемной сложности и сложности доказательств, и в ряде других областей. Основная литература по коммуникационной сложности написана на английском. На русском можно прочесть небольшой обзор области тут, а также главу про коммуникационную сложность в этой книге.

4.1 Базовые утверждения и понятия

Мы уже ввели определение коммуникационного протокола 3.1 и коммуникационной сложности 3.2. Нам также понадобятся другие понятия для нашего удобства.

Входное пространство коммуникационной задачи можно вопринимать как матрицу. Каждой функции f будем сопоставлять матрицу $X \times Y$, в которой в клетке (x_i, y_j) стоит значение $f(x_i, y_j)$.

Утверждение 4.1

Рассмотрим дерево протокола со входом из множества $X \times Y$. Рассмотрим в нём произвольную вершину u. Тогда все входы, из которых можно прийти в вершину u, образуют прямоугольник $R_u = X_u \times Y_u \subseteq X \times Y$.

Доказательство. Это можно доказать двумя способами.

Первый способ: пусть на входах (x_1, y_1) и (x_2, y_2) мы приходим в вершину u. Тогда нетрудно убедиться, что на входе (x_1, y_2) Алиса и Боб будут делать те же действия, что и на входах (x_1, y_1) и (x_2, y_2) соответственно. Отсюда видно, что входы, приводящие в вершину u, образуют прямоугольник $R_u = X_u \times Y_u \subseteq X \times Y$.

Второй способ: Рассмотрим таблицу элементов $X \times Y$. После первого хода Боба табличка делится пополам горизонтальной линией, так как при одних $x \in X$ Боб посылает Алисе 1, а при других — 0. Потом Алиса посылает свой бит Бобу, и каждый из двух получившихся прямоугольников делится своей вертикальной прямой, и так далее. В итоге мы получим разбиение $X \times Y$ на непересекающиеся прямоугольники, и каждый из этих прямоугольников соответствует листу в коммуникационном протоколе. □

Про прямоугольник R_u можно думать в следующим образом: если мы находимся в вершине протокола u, то нам необходимо решить задачу (то есть построить протокол) для всех входов из прямоугольника R_u. В частности этот подход можно рассмотреть, как комбинаторное определение протокола: бинарное дерево, в котором каждой вершине сопоставлен прямоугольник входов. И если вершины a, b являются потомками u, то $R_u \subseteq R_a \cup R_b$.

Определение 4.1

Прямоугольник $R \subset X \times Y$ называется одноцветным для отношения F, если существует $z \in Z$, что для всех $(x, y) \in R$ верно $(x, y, z) \in F$. Такой прямоугольник будем называть z-одноцветным.

Рассмотрим величину $\chi_0(f)$, равную минимальному числу прямоугольников, которыми можно дизъюнктно покрыть нули в матрице. Аналогично определяется $\chi_1(f)$. Тогда

листьев в коммуникационном протоколе будет хотя бы $\chi(f) = \chi_0(f) + \chi_1(f)$. Эти рассуждения дают следующую оценку:

$$C(f) \geq \log \chi(f) = \log(\chi_0(f) + \chi_1(f)).$$

Эта оценка не всегда точна. Это нам даёт понять следующий пример:

Пример 1. Рассмотрим такой пример разбиения таблицы $X \times Y$ на прямоугольники: в центре находится прямоугольник из 1, а вокруг него расположены 4 прямоугольника из 0. Покажем, что для этого разбиения не существует дерева протокола. Действительно, рассмотрим первое действие игроков. После него таблица должна поделиться на две части, но на рисунке 4 видно, что нет разреза, проходящего через всю таблицу.

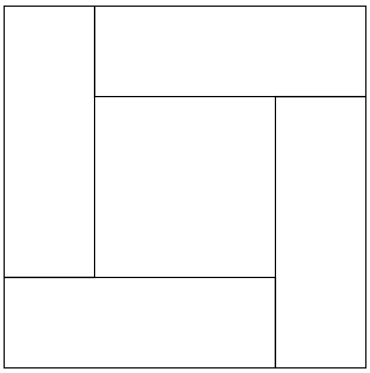
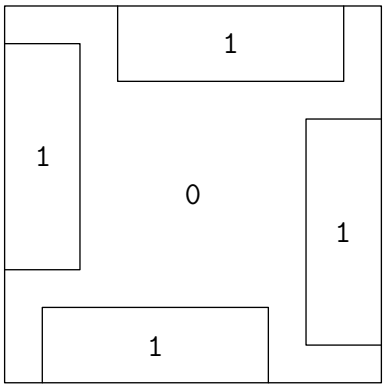


Рис. 4. Разбиение матрицы на одноцветные прямоугольники, которое не соотвествует никакому протоколу.

Задача 4.1. *Приведите пример, когда* $L(f) > \chi(f)$.



Метод трудного множества. Возьмем некоторый набор входов $(x_1, y_1), \ldots, (x_m, y_m)$, для которого выполнено, что никакие два входа не могут лежать в одном одноцветном прямоугольнике. Тогда для каждой такой пары входов должен быть свой одноцветный прямоугольник в разбиение. Значит, $\chi(f) \geq m$, а следовательно $D(f) \geq \log m$.

Метод полуаддитивной меры. Данный метод является обобщение метода трудного множеста. Определим некоторую полуаддитивную меру μ на подмножествах $X \times Y$ ($\mu(R_1 \cup R_2) \leq \mu(R_1) + \mu(R_2)$). Пусть для любого одноцветного прямоугольника R верно $\mu(R) \leq \alpha$, $\alpha > 0$.

Утверждение 4.2

Верно следующее $C(f) \geq \log \dfrac{\mu(X \times Y)}{\alpha}$.

Метод ранга. Пусть M_f — матрица некоторой функции f со значениями из $\{0,1\}$. Пусть $x_1, \ldots, x_k$ — листы коммуникационного протокола для функции f, а $R_{x_1}, \ldots, R_{x_n}$ — соответствующие им прямоугольники в M_f. Из алгебры мы знаем, что $\operatorname{rank}(M_f) \leq \sum \operatorname{rank}(R_i)$, а $\operatorname{rank}(R_i) = 1$ для любого i. Отсюда можно сделать вывод, что количество листьев в протоколе не меньше $\operatorname{rank} M_f$, а коммуникационная сложность — не меньше $\log \operatorname{rank}(M_f)$.

4.2 Игра для отношения

Обобщим игру Алисы и Боба на случай *трёхместного отношения*. Пусть X, Y и Z — непустые конечные множества, а $R \subset X \times Y \times Z$ — трёхместное отношение, в котором для любых $x \in X$ и $y \in Y$ всегда найдётся $z \in Z$ (не обязательно единственный) такой, что $(x,y,z) \in R$. В игре для отношения R цель Алисы и Боба заключается в том, что бы по входам $x \in X$ и $y \in Y$ узнать элемент $z \in Z$ (один и тот же для обоих игроков) такой, что $(x,y,z) \in R$. (Проверьте, что определения 3.1 и 3.2 легко обобщаются на случай такого трёхместного отношения.)

Частным случаем такого трёхместное отношения является *игра Карчмера — Вигдерсона* для функции $f : \{0,1\}^n \to \{0,1\}$, обозначается KW_f и определяется так:

Определение 4.2

Игра Карчмера — Вигдерсона для функции $f : \{0,1\}^n \to \{0,1\}$ — это следующая коммуникационная игра: Алиса получает $x \in f^{-1}(0)$, Боб получает $y \in f^{-1}(1)$, и они вместе пытаются найти такое $i \in [n]$, что $x_i \neq y_i$. Иначе говоря, игра Карчмера — Вигдерсона — это коммуникационная задача для *отношения*

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

Отношение KW_f называется *отношением Карчмера — Вигдерсона* для функции f.

Функция чётности $\oplus_n : \{0,1\}^n \to \{0,1\}$ определяется так:

$$\oplus_n(x) = x[1] + x[2] + \cdots + x[n] \mod 2.$$

Другими словами, что $\oplus_n(x) = 0$ тогда и только тогда, когда в x чётное число единиц. В игре для отношения $\mathrm{KW}_{\oplus_n}$ Алиса получает строку с чётным числом единиц, а Боб — с нечётным. Их задача найти такое число i, что соответствующие биты $x[i]$ и $y[i]$ различны. Заметим, что такое i всегда существует.

Задача 4.2. *Для $n = 2^k$ покажите, что $C(\mathrm{KW}_{\oplus_n}) \leq 2k$.*

Функция логического «или» $\vee_n : \{0,1\}^n \to \{0,1\}$ определяется так:

$$\vee_n(x) = x[1] \vee x[2] \vee \cdots \vee x[n].$$

Другими словами, $\vee_n(x) = 0$ только для строки состоящей из всех нулей. На всех остальных входах $\vee_n$ принимает значение 1.

Задача 4.3. *Для $n = 2^k$ покажите, что $C(\mathrm{KW}_{\vee_n}) = k$.*

4.3 Формулы и коммуникационная сложность

В этой главе мы посмотрим на применение коммуникационной сложности для доказательства оценок на формульную сложность.

Определение 4.3

Формула в базисе Де Моргана для функции $f\colon \{0,1\}^n \to \{0,1\}$ — это булевая формула с переменными $\{x_1, \ldots, x_n\}$, соответствующим отдельным битам входа f, и со связками (гейтами) $\{\wedge, \vee, \neg\}$, вычисляющая функцию f. Законы Де Моргана позволяют нам предполагать, что все $\neg$ находятся непосредственно перед переменными. Структура формулы Де Моргана представляет собой корневое дерево (листья соответствуют переменным, а внутренние вершины — логическим связкам). Размером формулы называется количество листьев, а глубиной формулы — высота дерева, т.е. количество рёбер в самом длинном простом пути от корня до некоторого листа.

Определение 4.4

Будем говорить, что семейство булевых функций $f_n : \{0,1\}^n \to \{0,1\}$ вычисляется формулами Де Моргана размера $s(n)$, если для каждого $n \in \mathbb{N}$ существует формула Де Моргана размера $s(n)$, вычисляющая f_n. Формульной сложностью $L(f)$ функции f называется минимальная функция s, такая что f вычисляется формулами Де Моргана размера $s(n)$.

Определение 4.5

Будем говорить, что семейство булевых функций $f_n : \{0,1\}^n \to \{0,1\}$ вычисляется формулами Де Моргана глубины $d(n)$, если для каждого $n \in \mathbb{N}$ существует формула Де Моргана глубины $d(n)$, вычисляющая f_n. Формульной глубиной $D(f)$ функции f называется минимальная функция d, такая что f вычисляется формулами Де Моргана глубины $d(n)$.

Есть некоторая связь между этими двумя характеристиками.

Утверждение 4.3

Для любой булевой функции f верно

$$\log_2 L(f) \leq D(f) \leq 3 \log_2 L(f).$$

Оказывается, что формульная сложность функции f связана с коммуникационной сложностью для отношения KW_f. Мы формулируем теорему Карчмера — Вигдерсона, которая связывает две эти сложности.

Теорема 4.1 (Карчмер — Вигдерсон)

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

4.4 Задачи для разминки

Задача 4.4. *У Алисы имеется n-битная строка x, а у Боба n-битная строка y. Известно, что y получен из x инвертированием одного бита.*

а) Придумайте детерминированный коммуникационный протокол сложности $\mathcal{O}(\log n)$, который позволяет Бобу узнать x.

b) *Придумайте однораундовый детерминированный коммуникационный протокол сложности $\mathcal{O}(\log n)$, который позволяет Бобу узнать x. (В однораундовом протоколе Алиса посылает некоторое сообщение Бобу, после чего Боб вычисляет результат).*

Задача 4.5. *Пусть дан граф G без петель. Алиса и Боб получают две вершины данного графа x, y и хотят узнать существует ли ребро (x, y). Докажите, что детерминированная сложность данной задачи не менее $\log \chi(G)$, где $\chi(G)$ — хроматическое число графа G.*
Подсказка: *попробуйте предъявить хорошую раскраску, если есть короткий коммуникационный протокол.*

Задача 4.6. *Докажите, что $C(\mathrm{CIS}_G) = \mathcal{O}(\log^2 n)$. Где x интерпретируется как характеристическая функция некоторой клики в графе G, а y — как характеристическая функция некоторого независимого множества в графе G. $\mathrm{CIS}_G(x, y) = 1$, если клика и независимое множество имеют общую вершину, обе стороны знают граф G.*

Задача 4.7. *Постройте детерминированный коммуникационный протокол, который вычисляет функцию GT, передавая в среднем константу битов. Функция $\mathrm{GT}(x, y)$ определена на парах x, y целых чисел в интервале $\{0, \ldots, 2^n - 1\}$ и принимает значение 1, если $x > y$, и значение 0, иначе. Говоря о среднем, мы имеем в виду, что x, y выбираются случайно и независимо среди всех чисел указанного интервала с равномерным распределением.*

Определение 4.6

Внутреннее произведение $\mathrm{IP}_n \colon \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ задаётся соотношением

$$\mathrm{IP}_n(x, y) = x[1]y[1] + x[2]y[2] + \cdots + x[n]y[n] \mod 2.$$

Задача 4.8. *Докажите, что коммуникационная сложность* IP *равна $n - \mathcal{O}(1)$.*

4.5 Исследовательские задачи

Задачи в таких секциях являются исследовательскими. Их решение может потребовать значительно больше времени и сил. Предложенные задачи имеют различную сложность. В частности, решение открытых задач неизвестно. Поэтому перед тем, как браться за эти задачи, стоит подумать над решением обычных задач в секциях 4.5, 5.6, 7.2.

Функция подсчёта $\mathrm{MOD}p_n : \{0,1\}^n \to \{0,1\}$ для натурального $p > 1$ определяется следующим соотношением $\mathrm{MOD}p_n(x) = 0 \iff x[1] + x[2] + \cdots + x[n] = 0 \mod p$. Отметим, что $\oplus_n$ — это в точности $\mathrm{MOD}2_n$.

Открытая задача 4.9 (очень сложно)

Предлагается улучшить верхнюю оценку из статьи Andrew Chin для отношения $\mathrm{KW}_{\mathrm{MOD}p_n}$ для конкретного значения $p > 2$.

a) Для $p = 3$ лучше $2.881 \log_2 n$,

b) Для $p = 5$ лучше $3.475 \log_2 n$,

c) Для $p = 11$ лучше $4.930 \log_2 n$.

Задача 4.10. *Улучшите константу в балансировке протоколов. Доказать, что $C(f) \leq c \log_2 L(f)$ для $c < 3$.*

5 Коммуникационная сложность с оракулом

В этой главе мы будем исследовать коммуникационную сложность с оракулом. В данной модели Алиса и Боб отправляют сообщения третьему игроку Чарли, выполняющему роль оракула, он вычисляет некоторую функцию g и отправляет результат игрокам, цель Алисы и Боба — вычислить с помощью Чарли функцию f.

Одним из наиболее исследованных оракулов в коммуникационной сложности является задача равенства EQ. Она является сложной для детерминированной коммуникационной сложности, но вероятностно решается за константное количество раундов в модели с публичными случайными битами. В коммуникационной сложности с оракулом EQ Алиса и Боб каждый раунд отправляют некоторые битовые строки третьему игроку, Чарли, который сообщает в ответ, равны ли они (см. рис. 5). Будем обозначать за $C^{\mathrm{EQ}}(f)$ коммуникационную сложность функции f с оракулом EQ, т.е. минимальную глубину протокола, который вычисляет функцию f с оракулом EQ. Впервые данная модель была введена [BFS86].

Задача 5.1. *Покажите, что $C(f) \geq C^{\mathrm{EQ}}(f)$. Примером лучшего разделения может служить сама же задача* EQ*, $C^{\mathrm{EQ}}(\mathrm{EQ}) = 1$, $C(\mathrm{EQ}) = \Theta(n)$.*

Для подробного изучения модели с оракулом можно почитать статью Chattopadhyay и других. Также ознакомиться со всеми доказательствами из этой главы можно тут.

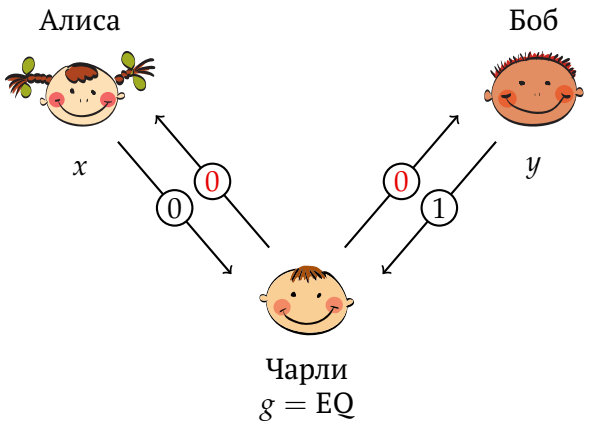


Рис. 5. Общение Алисы и Боба с оракулом Чарли.

Задача 5.2. *Придумайте решение задачи 1.0 за 2 раунда в модели с оракулом* EQ*.*

Разбор задачи 5.2. Алиса и Боб отправляют Чарли первый бит двоичной записи x и y. Чарли говорит им, равны ли они, таким образом каждый из игроков понимает какой бит был у другого. Игроки проделывают такой же раунд со втором битом своих чисел и узнают числа друг друга.

5.1 Протокол с оракулом

Пусть A — семейство коммуникационных задач $A_m : \{0,1\}^m \times \{0,1\}^m \to \{0,1\}$ для $m \in \mathbb{N}$. Если входы игроков $(x,y) \in \{0,1\}^n \times \{0,1\}^n$, то каждое сообщение в модели с оракулом A — это пара входов $(g_1(x), g_2(y)) \in \{0,1\}^m \times \{0,1\}^m$ для функции A_m, где g_1 и g_2 выбраны заранее, а выход $A_m(g_1(x), g_2(y))$ виден обоим игрокам. Сложность такого

протокола — это число вызовов оракула. $C^A(f)$ — это минимальная сложность по всем протоколам для функции f.

Фактически, в нашем анализе после обращения к оракулу мы разбиваем набор входов на набор прямоугольников. Для доказательства нижних оценок нам будет удобнее работать с более сильной моделью, в которой все возможные наборы ответов заранее разбиты на прямоугольники, и оракул сообщает игрокам не только ответ на их запрос, но и к какому прямоугольнику в разбиении относятся их вход, без каких-либо дополнительных затрат.

Заметим, что вызов функции A_m со входом, преобразованным g_1 и g_2, эквивалентен вызову функции $B = A_m \circ (g_1, g_2)$, и что матрица B может быть получена из матрицы A_m путем удаления, дублирования и перестановки некоторых строк или столбцов. Каждой матрице M оракула мы сопоставляем некоторое разбиение $\mathcal{R}(M)$ матрицы на одноцветные прямоугольники. В общем, таких вариантов может быть много; правильный выбор будет иметь решающее значение для нашей техники доказательства нижней оценки. Единственное требование заключается в том, что это разбиение на одноцветные прямоугольники.

Протокол в модели с оракулом A, вычисляющий функцию $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ — это дерево, где каждая вершина соответствует прямоугольнику $R \subseteq \{0,1\}^n \times \{0,1\}^n$ входов. Каждая вершина связана с матрицей M оракула тех же размеров, что и R, и имеет по одному сыну для каждого прямоугольника $R' \in \mathcal{R}(M)$. Находясь в вершине, помеченной R, игроки переходят к сыну с прямоугольником R', который содержит их входы. Каждый лист помечен 0 или 1, а метка листа R равна $f(x,y)$ для каждого $(x,y) \in R$.

Аналогично тому, как один бит детерминированной коммуникации обновляет разделение входного пространства, где каждый прямоугольник делится на два. Один вызов оракула обновляет разделение пространства, где каждый прямоугольник R заменяется на разбиение $\mathcal{R}(M(R))$, связанное с матрицей оракула $M(R)$ того же размера. Это значит, что все начинается с одного прямоугольника $\mathcal{R}_0 = \{\{0,1\}^n \times \{0,1\}^n\}$, и после обращения к оракулу, получается раздел $\mathcal{R}_i = \cup_{R \in \mathcal{R}_{i-1}} \mathcal{R}(M(R))$. Если протокол вычисляет функцию f после C вызовов, то разбиение $\mathcal{R}_C$ является разбиением матрицы M_f функции f на одноцветные прямоугольники.

Для простоты изложения предположим, что мы ограничиваем возможный вход оракула A длиной не более n (т.е. у игроков есть доступ к оракулам A_m, где $m \leq n$, или что тоже самое $g_1, g_2 : \{0,1\}^n \to \{0,1\}^m$, $m \leq n$). Но все рассуждения можно обобщить на случай неограниченного m.

5.2 Оракул единичного расстояния Хэмминга

Следующие секции посвящены изучению сложности функций в модели с оракулом расстояния Хэмминга.

Определение 5.1

Точное расстояние Хэмминга $\mathrm{EHD}_k(x,y) = 1$ тогда и только тогда, когда расстояние Хэмминга (количество различающихся битов) между x и y равно ровно k, где $x, y \in \{0,1\}^n$.

Для разбиения $\mathcal{R} = \bigcup R_i$, где $R_i = A_i \times B_i$, обозначим за $p(\mathcal{R}) = \sum_{R_i} |A_i| + |B_i|$ полупериметр разбиения $\mathcal{R}$. За $p(M)$ обозначим минимальный периметр по всем разбиениям матрицы M на одноцветные прямоугольники.

Лемма 5.1

Для матрицы M оракула EQ размера $a \times b$ существует разбиение $\mathcal{R}$ на одноцветные прямоугольники такое, что $p(\mathcal{R}) \leq 2(a+b)\log(a+b)$.

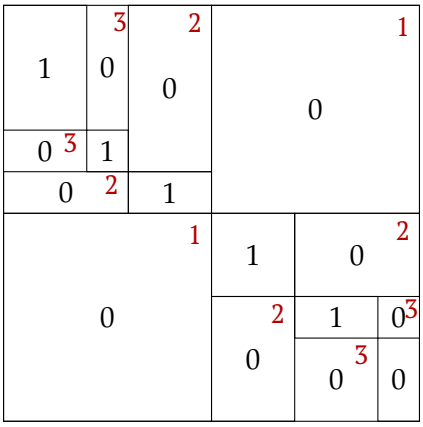


Рис. 6. Матрица оракула EQ.

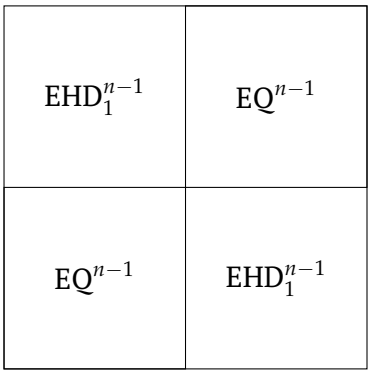


Рис. 7. Матрица EHD_1.

Лемма 5.2

Пусть $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ — булева функция, которая в модели с оракулом EHD_1 имеет сложность C. Тогда существует разбиение $\mathcal{R}$ коммуникационной матрицы f на одноцветные прямоугольники с периметром $p(\mathcal{R}) \leq 2^{n+1}(2n^2)^C$.

Теперь нам нужна оценка на размер одноцветных прямоугольников матрицы EHD_k, в случае константного k мы докажем лемму 5.3. Будем доказывать двойной индукцией по параметру функции k и размеру входа n.

Лемма 5.3

Для любого 1-прямоугольника R матрицы EHD_k верно $|R| \leq 2n^k$.

Теорема 5.1

Коммуникационная сложность $C^{\mathrm{EHD}_1}(\mathrm{EHD}_k)$ не менее $\frac{k}{5}$.

5.3 Оракул точного расстояния Хэмминга равного ℓ

Лемма 5.4

Пусть $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ — булева функция, которая в модели с оракулом EHD_ℓ имеет сложность C. Тогда существует разбиение $\mathcal{R}$ коммуникационной матрицы f на одноцветные прямоугольники с периметром $p(\mathcal{R}) \leq 2^{n+1}(2n^{\ell+1})^C$.

Теорема 5.2

Коммуникационная сложность $C^{\mathrm{EHD}_\ell}(\mathrm{EHD}_k)$ не менее $\frac{k}{2(\ell+2)}$.

5.4 Верхняя оценка с оракулом расстояние Хэмминга не более ℓ

Определение 5.2

$\mathrm{HD}_{\leq k}(x,y) = 1$ тогда и только тогда, когда расстояние Хэмминга между x и y не более k.

Несложно заметить, что матрица задачи $\mathrm{HD}_{\leq k}$ имеет схожую EHD_k структуру, поэтому полученная оценка верна и для задачи $\mathrm{HD}_{\leq k}$ с оракулом $\mathrm{HD}_{\leq \ell}$.

Несложно понять, что используя оракул $\mathrm{HD}_{\leq \ell}$ как EQ задача $\mathrm{HD}_{\leq k}$ может быть решена за $2k \cdot \log n$. Аналогичное верно и для задачи EHD_k с оракулом EHD_ℓ. Непонятно как использовать оракул EHD_ℓ более эффективно. Для случая задачи $\mathrm{HD}_{\leq k}$ с оракулом $\mathrm{HD}_{\leq \ell}$ получается доказать более точную верхнюю оценку.

Теорема 5.3

$$C^{\mathrm{HD}_{\leq \ell}}(\mathrm{HD}_{\leq k}) \leq 2 \cdot \frac{k}{\ell} \cdot \log \ell \cdot \log n.$$

5.5 Оракул однобитового равенства

Для получения нижних оценок на формулы в полном булевом базисе можно переносить нижние оценки на коммуникационную сложность игр Карчмера — Вигдерсона в модели с однобитовым оракулом EQ_1.

По формуле в полном булевом базисе для функции f можно получить протокол для KW_f с оракулом EQ_1 такой же глубины. Алиса получает $x \in f^{-1}(0)$, Боб $y \in f^{-1}(1)$, если формула $\phi = \phi_1 \wedge \phi_2$ ($\phi = \phi_1 \vee \phi_2$) Алиса (Боб) отправляет в какой подформуле у нее (него) $\phi_i(x) = 0$ ($\phi_i(y) = 1$) и они переходят в нужную подформулу. Если $\phi = \phi_1 \oplus \phi_2$, то Алиса отправляет 1 в оракул EQ_1, если $\phi_1(x) = 1$ и $\phi_2(x) = 1$, и 0, если $\phi_1(x) = 0$ и $\phi_2(x) = 0$, Боб отправляет 1 в оракул, если $\phi_1(y) = 0$ и $\phi_2(y) = 1$, и 0, иначе. Тогда если биты Алисы и Боба равны, то они идут в левую подформулу ϕ_1, иначе идут в правую подформулу ϕ_2. Таким образом, получаем протокол для KW_f в модели с оракулом EQ_1 такой же глубины как и формула для f, значит $C^{\mathrm{EQ}_1}(\mathrm{KW}_f) \leq C(f)$.

Рассмотрим сложность булевых функций от $2n$ бит с разделенным входом для Алисы и Боба. Покажем, что сложность случайной функции равняется $n - o(n)$.

Теорема 5.4

Существует функция $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$, которая имеет сложность $C^{\mathrm{EQ}_1}(f) = n - o(n)$.

Задача 5.3. $C^{\mathrm{EQ}_1}(\mathrm{EHD}_1) = n/2 + \mathcal{O}(1)$.

5.6 Исследовательские задачи

Задача 5.4. *Оцените сложность $C^{\mathrm{EQ}_1}(\mathrm{EHD}_k)$ в зависимости от k.*

Открытая задача 5.5 (сложно)

Оцените сложность $C^{\mathrm{EQ}}(\mathrm{EHD}_k)$ в зависимости от k.

Открытая задача 5.6 (сложно)

Попробуйте улучшить нижнюю оценку на $C^{\mathrm{EHD}_\ell}(\mathrm{EHD}_k)$.

Открытая задача 5.7

Попробуйте улучшить верхнюю оценку на $C^{\mathrm{EHD}_\ell}(\mathrm{EHD}_k)$ и $C^{\mathrm{HD}_{\leq \ell}}(\mathrm{HD}_{\leq k})$.

6 Вероятностная коммуникационная сложность

Определение 6.1 (Вероятностная коммуникационная сложность)

Пусть у Алисы и Боба есть доступ к общей последовательности случайных битов r. Теперь они знают, что их партнер видит ту же последовательность r, и действие каждого игрока в вершине протокола зависит от его входа, предыдущей коммуникации и последовательности r. *Вероятностной коммуникационной сложностью функции f с публичными битами r* называется следующая величина:

$$\mathrm{R}_{\varepsilon}^{\mathrm{pub}}(f) = \min_{\Pi} \max_{(x,y)}(\sharp\text{переданных битов}),$$

где протоколы Π удовлетворяют условию $\Pr_r[\Pi(x,y) \neq f(x,y)] \leq \varepsilon$. Количество переданных бит считается в худшем случае по всем случайным битам r, но большой разницы нет, если вместо этого считать матожидание.
Аналогично можно определить коммуникационную сложность в случае с отдельными последовательностями случайных битов. Будем обозначать ее за $\mathrm{R}_{\varepsilon}^{\mathrm{pr}}$.

Утверждение 6.1

$\mathrm{R}_{\frac{1}{10}}^{\mathrm{pub}}(\mathrm{EQ}) = \mathcal{O}(1)$.

Задача 6.1. *Докажите, что* $R_{\varepsilon}^{pub}(\mathrm{EQ}) \leq \mathcal{O}(\log \frac{1}{\varepsilon})$.

Задача 6.2. *Докажите, что* $\mathrm{R}_{\frac{1}{10}}^{pub}(\mathrm{GT}) = \mathcal{O}(\log n \cdot \log\log n)$.

Задача 6.3. $\mathrm{R}_{\frac{1}{2}}^{pr}(\mathrm{EQ}) = \mathcal{O}(\log n)$.

Утверждение 6.2

$\mathrm{R}_{\frac{1}{10}}^{\mathrm{pub}}(\mathrm{DISJ}_n^{\leq k}) = \mathcal{O}(2^{2k})$, где в функции $\mathrm{DISJ}_n^{\leq k}$ множества игроков имеют размеры не больше k, $\mathrm{DISJ}_n^{\leq k}(x,y) = 1$, если множества не пересекаются.

Давайте покажем связь между классической коммуникационной сложность и вероятностной.

Теорема 6.1

$\mathrm{R}_{\varepsilon}^{\mathrm{pub}} \leq C(f) \leq 2^{\mathrm{R}_{\varepsilon}^{\mathrm{pub}}}(\log(\frac{1}{1/2-\varepsilon}) + \mathrm{R}_{\varepsilon}^{\mathrm{pub}})$.

Несложно заметить, что сложность с приватными случайными битами не менее сложности с публичными битами. Оказаывается, что вероятностная сложность в приватном случае отличается не более чем на $\log n$ от публичного случая.

Теорема 6.2 (Ньюман)

$\mathrm{R}_{2\varepsilon}^{\mathrm{pr}}(f) \leq \mathrm{R}_{\varepsilon}^{\mathrm{pub}}(f) + \mathcal{O}(\log n)$.

7 Полудуплексная коммуникационная сложность

Коммуникационное устройство, используемое Алисой и Бобом в предыдущих разделах, обладало следующим свойством: в каждый момент один игрок посылал некоторый бит, а другой его принимал. Рассмотрим аналогичную игру, но с другим коммуникационным устройством. Теперь Алиса и Боб будут использовать устройство, принцип работы которого похож на работу рации: для того, чтобы отправить сообщение, нужно нажать на кнопку, переводящую устройство в режим передачи, а для того, чтобы вернуться в режим приёма сообщений, нужно эту кнопку отпустить. Если оба игрока пытаются одновременно передать сообщение, то их сообщения «теряются». Если, наоборот, оба игрока находятся в принимающем состоянии, то они слышат «тишину».

Давайте опишем взаимодействие игроков с таким передающим устройством более подробно. Будем считать, что кроме передающего устройства у игроков есть некоторый способ синхронизации (например, у них есть синхронизированные часы), которые позволяют разбить взаимодействие игроков на *раунды*. Для простоты будем считать, что каждый раунд длится одну минуту. В начале каждой минуты начинается новый раунд, и каждый из игроков выбирает одно из трёх *действий*: «принимать», «послать „`0`“», «послать „`1`“». Если один из игроков принимает, а другой посылает, то устройство работает так же, как и раньше, будем называть это *классическим раундом*. Если оба игрока посылают, то их сообщения теряются (и они об этом не знают), будет называть это *потерянным раундом*. Если оба игрока принимают, то они слушают «тишину», будем называть это *тихим раундом*. Тихие раунды можно определить по-разному. Мы будем рассматривать два варианта.

1. В тихом раунде игроки получают «символ тишины» отличный от «`0`» и «`1`». В таком случае будем говорить о *полудуплексной коммуникационной модели с тишиной*.

2. В тихом раунде игроки получают «`0`», т.е. игрок не может отличить тихий раунд от классического раунда, в котором другой игрок посылает ему «`0`». В таком случае будем говорить о *полудуплексной коммуникационной модели с нулём*.

В дальнейшем нам потребуется определить понятие *полудуплексного коммуникационного протокола*, но первые задачи можно решить без этого определения.

Задача 7.1. *Придумайте решение задачи 1.0 за два раунда в полудуплексной модели с тишиной.*

Давайте разберём эту задачу, чтобы понять, чем коммуникация в такой модели отличается от того, что мы видели раньше.

Разбор задачи 7.1. Предлагается следующий протокол из двух раундов.

Вход	Алиса	Боб
0	послать «0»	принимать
1	послать «1»	принимать
2	принимать	принимать

Первый раунд

Вход	Алиса	Боб
0	принимать	послать «0»
1	принимать	послать «1»
2	принимать	принимать

Второй раунд

Получается, что, если ни один игрок не получил 2, то их общение похоже на классический протокол, в котором Алиса и Боб просто обмениваются числами. Если один из них получил 2 (или оба), то первый или второй раунд (или оба) будут *тихими*. В модели с тишиной игроки могут отличить тихий раунд от классического; поэтому Боб в первом раунде или Алиса во втором смогут понять, что произошёл тихий раунд и, следовательно, у другого игрока вход 2. Таким образом, в этой модели игроки смогут обменяться входами за два раунда.

Задача 7.2. *Придумайте решение задачи 1.0 за три раунда в полудуплексной модели с нулём, либо докажите, что его не существует.*

Пусть X, Y и Z — непустые конечные множества, а $R \subset X \times Y \times Z$ — трёхместное отношение, в котором для любых $x \in X$ и $y \in Y$ всегда найдётся $z \in Z$ (не обязательно единственный) такой, что $(x, y, z) \in R$. Рассмотрим игру для отношения R в полудуплексных моделях коммуникации. Определим *полудуплексную коммуникационную сложность отношения R в моделях с тишиной и нулём*, $C_т(R)$ и $C_0(R)$, как минимальное количество раундов, необходимое Алисе и Бобу для решения игры для R в модели с тишиной и нулём, соответственно (пока это неформальное определение, далее мы его уточним).

Задача 7.3. *Докажите, что $C_т(R) \leq C_0(R)$.*

Задача 7.4. *Докажите, что $C_0(R) \leq C(R)$.*

Задача 7.5. *Докажите, что $C_0(R) \geq C(R)/2$.*

Задача 7.6. *Докажите, что $C_т(R) \geq C(R)/3$.*

Задача 7.7. *Докажите, что в полудуплексной модели с нулём игроки могут обойтись без действия «послать „0“», сохранив при этом количество раундов.*

Теперь давайте определим понятие *полудуплексного коммуникационного протокола*. В классическом случае коммуникационный протокол задаётся двоичным корневым деревом, которое описывает коммуникацию игроков на всех возможных входах: каждая внутренняя вершина протокола задаёт текущее состояние коммуникации и определяет, какой из игроков в данный момент посылает бит, а какой — принимает. В отличие от классической модели, в полудуплексной коммуникации игрок не всегда знает, какое действие совершил его собеседник в этом раунде — информация об этом “теряется” в потерянных раундах, а тихие и классические раунды могут быть неотличимы. Таким образом, игрок не всегда сможет определить, какой узел дерева соответствует текущему состоянию коммуникации. Поэтому в полудуплексной модели протокол определяется как пара корневых деревьев (не обязательно двоичных).

Определение 7.1. *Полудуплексный коммуникационный протокол с тишиной*, решающий коммуникационную задачу для отношения $R \subset X \times Y \times Z$, — это пара корневых деревьев (T_A, T_B), в которых каждая внутренняя вершина имеет не более пяти потомков, и, кроме того,

- каждый лист l помечен некоторым элементом $z_l \in Z$,

- для каждой вершины v дерева T_A определены две функции $g_v : X \to \mathcal{A}$ и $h_v : \mathcal{E} \to D(v)$, где $D(v)$ обозначает множество потомков вершины v, $\mathcal{A}$ — *множество действий*,

$$\mathcal{A} = \{\texttt{послать(0)}, \texttt{послать(1)}, \texttt{принимать}\},$$

а $\mathcal{E}$ — *множество событий*,

$$\mathcal{E} = \{\texttt{передано(0)}, \texttt{передано(1)}, \texttt{получено(0)}, \texttt{получено(1)}, \texttt{тишина}\}.$$

- для каждой вершины u дерева T_B определены функции $g_u : Y \to \mathcal{A}$ и $h_u : \mathcal{E} \to D(u)$.

Пути Алисы и Боба $\pi_A(x,y)$ и $\pi_B(x,y)$ на входе (x,y) — это последовательности вершин $u_1,\dots,u_n$ и $v_1,\dots,v_n$ деревьев T_A и T_B соответственно, определяемые следующими условиями:

- u_1 и v_1 — корни деревьев T_A и T_B;
- u_n или v_n — лист дерева T_A или T_B;
- для каждого $i \in \{1,\dots,n-1\}$ выполнено

$$v_{i+1} = h_{v_i}(\phi_A(g_{v_i}(x), g_{u_i}(y))),$$
$$u_{i+1} = h_{u_i}(\phi_B(g_{u_i}(x), g_{v_i}(y))),$$

где функция $\phi_A : \mathcal{A} \times \mathcal{A} \to \mathcal{E}$ задается следующей таблицей:

$g_v(x)$ \ $g_u(y)$	послать(0)	послать(1)	принимать
послать(0)	передано(0)	передано(0)	передано(0)
послать(1)	передано(1)	передано(1)	передано(1)
принимать	получено(0)	получено(1)	тишина

Функция $\phi_B : \mathcal{A} \times \mathcal{A} \to \mathcal{E}$ задается аналогично.

Протокол Π называется *корректным* протоколом для отношения R, если на любой паре входов (x,y) оба пути $\pi_A(x,y)$ и $\pi_B(x,y)$ заканчиваются в листьях с одной и той же пометкой z, такой, что $(x,y,z) \in R$. Соответствующее значение z называется *результатом* протокола Π на входе (x,y) и обозначается $\Pi(x,y)$.

Полудуплексный коммуникационный протокол с нулём определяется аналогично, но множества действий и событий отличаются:

$$\mathcal{A} = \{\texttt{послать(1)}, \texttt{принимать}\}, \quad \mathcal{E} = \{\texttt{передано(1)}, \texttt{получено(0)}, \texttt{получено(1)}\},$$

т.е. среди событий отсутствует тишина (она неотличима от получения нуля), но при этом игроки никогда не посылают 0 (см. задачу 7.7). Как следствие, внутренние вершины деревьев T_A и T_B могут иметь не более трёх потомков.

Классическая коммуникационная сложность функции f, $C(f)$, определена в терминах минимальной глубины протокола, решающего коммуникационную задачу для f. Аналогичным образом на основе определения полудуплексного протокола мы определяем полудуплексную коммуникационную сложность. Так как мы определили протокол сразу же для отношения, будем говорить, что полудуплексный коммуникационный протокол решает коммуникационную задачу для функции $f : X \times Y \to Z$, если он решает коммуникационную задачу для отношения $R(f) = \{(x,y,f(x,y)) \mid x \in X, y \in Y\}$.

Определение 7.2

Через $C_{\text{т}}(R)$ будем обозначать *полудуплексную коммуникационную сложность R с тишиной* — минимальную глубину полудуплексного коммуникационного протокола с тишиной, решающего коммуникационную задачу для отношения R.
Аналогично, через $C_0(R)$ обозначим *полудуплексную коммуникационную сложность R с нулём* — минимальную глубину полудуплексного коммуникационного протокола с нулём, решающего коммуникационную задачу для отношения R.

В задаче 3.4 мы доказали, что в классическом случае протокол обладает следующим свойством: если двум парам входов (x_1, y_1) и (x_2, y_2) соответствует один и тот же лист, то он соответствует и парам входов (x_1, y_2) и (x_2, y_1). Множество пар с таким свойством называют *комбинаторным прямоугольником*. Другими словами, это множество пар, которое является декартовым произведением двух множеств. В утверждение 4.1 мы доказали более сильное утверждение.

Теперь докажите аналогичный факт для полудуплексных протоколов.

Задача 7.8. *Докажите, что для каждой вершины полудуплексного протокола (в обоих деревьях) множество пар входов, при которых путь проходит через эту вершину, является комбинаторным прямоугольником.*

При решение следующих задач полезно вспомнить, как доказывались аналогичные оценки в классической коммуникационной сложности.

Задача 7.9. *Докажите, что для любого $n \in \mathbb{N}$, $C_{\text{т}}(\text{EQ}_n) \geq \log_5 2^n = n/\log 5$,*

Задача 7.10. *Докажите, что для любого $n \in \mathbb{N}$, $C_0(\text{EQ}_n) \geq \log_3 2^n = n/\log 3$,*

Задача 7.11. *Докажите, что для любого $n \in \mathbb{N}$, $C_{\text{т}}(\text{DISJ}_n) \geq \log_5 2^n = n/\log 5$,*

Задача 7.12. *Докажите, что для любого $n \in \mathbb{N}$, $C_0(\text{DISJ}_n) \geq \log_3 2^n = n/\log 3$,*

Задача 7.13. *Пусть $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$. Докажите, что $C_{\text{т}}(f) \leq \lceil n/\log_2 3 \rceil + 1$.*

Рассмотрим некоторую функцию μ, определённую на подмножествах $X \times Y$, принимающую неотрицательные вещественные значения и удовлетворяющую следующему свойству: $\mu(A \cup B) \leq \mu(A) + \mu(B)$, если $A \cap B = \varnothing$. Будем называть такую функцию *полуаддитивной мерой*. Будем называть комбинаторный прямоугольник R *одноцветным* для задачи $\mathcal{P}$, если существует такой z, что он является ответом для всех входов из R.

Задача 7.14. *Пусть для коммуникационной задачи $\mathcal{P} \subset X \times Y \times Z$ задана полуаддитивная мера μ на подмножествах $X \times Y$ такая, что существует константа $M > 0$, что для любого одноцветного прямоугольника $R \subset X \times Y$ верно $\mu(R) \leq M$. Докажите, что*

$$C_{\text{т}}(\mathcal{P}) \geq \log_5 \frac{\mu(X \times Y)}{M}, \text{ и } C_0(\mathcal{P}) \geq \log_3 \frac{\mu(X \times Y)}{M}.$$

7.1 Связь коммуникационной сложности с оракулом и полудуплексной

Оказывается существует связь между коммуникационной сложность с орукулом EQ_1 и полудуплексной сложностью. Стоит отметить, что какая-либо нетривиальная связь между полудуплескной коммуникационной сложностью с тишиной и коммуникационной сложность с оракулом EQ_1 неясна. В каких-то частных случаях сложности отличаются, например, для функции EQ в модели с тишиной сложность равна $n/\log 5 + o(n)$, с другой стороны в модели с оракулом EQ_1 сложность равна $n/2 + O(1)$.

Утверждение 7.1

Для любой функции f верно $C(f)/2 \leq C^{\text{EQ}_1}(f) \leq C_0(f) \leq C_a(f)$.

Доказательство. Заметим, что коммуникацию с оракулом EQ_1 можно воспринимать как модель, в которой Алиса и Боб могут говорить одновременно и получают сообщения друг друга. Таким образом, из протокола в полудуплексной коммуникационной сложности можно получить протокол с оракулом EQ_1, если кто-то из игроков принимал, то теперь он будет отправлять 0 в модели с оракулом EQ_1, если отправлял 1, то также отправляет 1. Второе неравенство справедливо в силу того, что в модели с противником в тихом раунде игроки могут получать любой бит. □

Следствие 7.1

Случайная функция в полудуплексной коммуникационной сложности с нулем и противником равна $n - o(n)$.

7.2 Исследовательские задачи

Открытая задача 7.15

Можно ли получить какую-то связь между коммуникационной сложность с оракулом EQ_1 и полудуплексной сложность с тишиной?

a) Пример функции, на которой сложность не совпадают $C^{\mathrm{EQ}_1}(f) < C_{\mathrm{т}}(f)$. Пример, на котором $C^{\mathrm{EQ}_1}(f) > C_{\mathrm{т}}(f)$.

b) Можно ли получить какую-то явную связь?

Известные оценки на полудуплексную сложность набора функций представлены в таблице 1.

Модель \ Функция	EQ	IP	DISJ
$C_{\mathrm{т}}$	$\geq n/\log 5$ $\leq n/\log 5 + o(n)$	$\geq n/2$ $\leq n/2 + O(1)$	$\geq n/\log 5$ $\leq n/2 + 2$
C_0	$\geq n/\log 3$ $\leq n/\log 3 + o(n)$	$\geq n/\log \frac{2}{3-\sqrt{5}}$ $\leq 7n/8 + O(1)$	$\geq n/\log 3$ $\leq 3n/4 + o(n)$
C_{a}	$\geq n/\log 2.5$	$\geq n/\log(7/3)$	$\geq n/\log 2.5$

Таблица 1. Известные результаты

Задача 7.16. *Предложите более эффективный полудуплексный протокол для* EQ_n

a) в модели с тишиной (лучше $n/\log_2 3$*),*

b) в модели с нулём (лучше n*).*

Задача 7.17. *Предложите эффективный полудуплексный протокол для* GT_n

a) в модели с тишиной (лучше $n/\log_2 3$*),*

b) в модели с нулём (лучше n*).*

Задача 7.18. *Предложите эффективный полудуплексный протокол для* DISJ_n

a) в модели с тишиной (лучше $n/\log_2 3$*),*

b) в модели с нулём (лучше n*).*

Задача 7.19. *Предложите эффективный полудуплексный протокол для* IP_n

a) в модели с тишиной (лучше $n / \log_2 3$),

b) в модели с нулём (лучше n).

Задача 7.20. *Предложите эффективный полудуплексный протокол для отношения* $\mathrm{KW}_{\oplus_n}$

a) в модели с тишиной (лучше $2\log_2 n$),

b) в модели с нулём (лучше $2\log_2 n$).

Задача 7.21. *Докажите, что* $C_{\mathrm{T}}(\mathrm{KW}_{\mathrm{MOD3}_n}) \leq 3\log_3 n$.

Открытая задача 7.22

Предложите эффективный полудуплексный протокол для отношения $\mathrm{KW}_{\mathrm{MOD3}_n}$ в модели с нулём (лучше $3\log_3 n$).

Определение 7.3

Функция рекурсивного большинства $\mathrm{RecMaj}_k : \{0,1\}^{3^k} \to \{0,1\}$ для натурального k определяется следующими соотношениями

$$\mathrm{RecMaj}_1(a,b,c) = \begin{cases} 0, & a+b+c < 2 \\ 1, & a+b+c \geq 2. \end{cases}$$

$$\mathrm{RecMaj}_k(a_1,\ldots,a_{3^k}) = \mathrm{RecMaj}_1(\mathrm{RecMaj}_{k-1}(a_1,\ldots,a_{3^{k-1}}),$$
$$\mathrm{RecMaj}_{k-1}(a_{3^{k-1}+1},\ldots,a_{2\cdot 3^{k-1}}),\mathrm{RecMaj}_{k-1}(a_{2\cdot 3^{k-1}+1},\ldots,a_{3^k}))$$

Задача 7.23. *Предложите эффективный полудуплексный протокол для отношения* $\mathrm{KW}_{\mathit{RecMaj}_k}$

a) в модели с тишиной (лучше $3\log_3 n$),

b) в модели с нулём (лучше $3\log_3 n$).

Открытая задача 7.24

Предложите эффективный полудуплексный протокол для отношения $\mathrm{KW}_{\mathrm{RecMaj}_k}$

a) в модели с тишиной (лучше $2\log_3 n$),

b) в модели с нулём (лучше $2\log_3 n$).

Задача 7.25. *Алиса получает строку длины n с ровно одной единицей, а Боб получается строку с не менее двумя единицами. Их задача найти индекс бита, в котором их входы различаются. Предложите эффективный протокол для этой задачи*

a) в классической модели (лучше $2\log_2 n$),

b) в модели с тишиной (лучше $\log_2 n$),

c) в модели с нулём (лучше придуманного вами в пункте «a»).

Открытая задача 7.26 (сложно)

Улучшите известные оценки (из таблицы 1) на функцию DISJ_n.

Открытая задача 7.27 (сложно)

Улучшите известные оценки (из таблицы 1) на функцию IP_n.

Открытая задача 7.28

Покажите оценку на сложность случайной функции в полудуплексной модели с тишиной.

8 Недетерминированная коммуникационная сложность

Определение 8.1

Три игрока: Алиса, Боб и Чарли. Алиса получает строку $x \in \{0,1\}^n$, Боб — строку $y \in \{0,1\}^n$. Чарли посылает Алисе и Бобу одинаковую подсказку $w \in \{0,1\}^m$. Далее Алиса и Боб общаются как обычно. Сложность

$$nc_1 := m + \#(\text{переданных битов между Алисой и Бобом}) .$$

Ответ 1, если существует подсказка w, для которой Алиса и Боб вычислят 1. Ответ 0, если для всех подсказок они вычислят 0.

Пример. Рассмотрим функцию NEQ. Чарли посылает позицию различия. Алиса и Боб за два бита проверяют. Сложность $nc_1(\text{NEQ}) \leq \lceil \log n \rceil + 2$.

Определение 8.2

Чарли посылает Алисе подсказку w_x, а Бобу — подсказку w_y. Далее Алиса и Боб общаются как обычно. Сложность

$$nc_2 := \#(\text{переданных битов между Алисой и Бобом}) ,$$

уже без платы за подсказки. Ответ 1 $\Leftrightarrow$ существует пара (w_x, w_y), на которой Алиса и Боб выдадут 1.

Пример. Рассмотрим функцию NEQ. Чарли посылает Алисе позицию различия. Алиса пересылает ее Бобу. Дальше за два бита они ее проверяют. Сложность $nc_2(\text{NEQ}) \leq \lceil \log n \rceil + 2$.

Теорема 8.1

Сложности функции в определениях 8.1 и 8.2 совпадают с точностью до аддитивной константы. А именно, для любой функции $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$

$$nc_1(f) = nc_2(f) + \Theta(1).$$

Обозначим $c^1(f)$ — минимальное число 1-прямоугольников, покрывающих все единицы M_f (возможно с пересечением), $N^1(f) := \lceil \log c^1(f) \rceil$.

Теорема 8.2

$$N^1(f) = nc_1(f) + \Theta(1).$$

Определение 8.3

Будем называть $N^1(f)$ *недетерминированной коммуникационной сложностью* f.

Задача 8.1. *Докажите, что для любого* $z \in \{0,1\}$

$$C(f) \leq c^z(f) + 1.$$

Задача 8.2. *Докажите, что*

a) $N^1(\text{EQ}) = n$;

b) $N^0(\mathrm{EQ}) = \log n + \Theta(1)$.

Задача 8.3. *Докажите, что* $N^0(\mathrm{GT}) = n$ *и* $N^1(GT) = n$.

Теорема 8.3

$$C(f) = \mathcal{O}(N^0(f) \cdot N^1(f))$$

Задача 8.4. *Докажите, что* $C(f) = \mathcal{O}(\log c^0(f) \cdot \log c^1(f))$.

9 Универсальные протоколы

В этой главе мы предлагаем читателям исследовать следующую модификацию классической коммуникационной модели: Алиса и Боб договорились о протоколе заранее, до получения задачи, то есть они фиксировали всю структуру протокола, кроме пометок на листьях и своих функций в вершинах. И мы хотим ответить на вопрос: сколько различных задач сможет решить такой протокол, если в зависимости от полученной задачи мы можем менять только ответы, которые написаны в листьях, и функции в вершинах? Более конкретно, нас будет интересовать следующее свойство: при каких условиях существует универсальный протокол, решающий все задачи, для которых $C(R) \leq d$, то есть которые решаются некоторым протоколом глубины не более d?

Такая постановка задачи не только интересна сама по себе, но и имеет полезные приложения. С одной стороны, универсальные графовые структуры интересны с точки зрения прикладных вычислений: при разработке арифметических схем оказывается крайне важно, чтобы наиболее компактные структуры (схемы, формулы, и т.д.) вычисляли наиболее широкий класс задач. А с другой стороны, изучение универсальный протоколов — один из подходов к доказательству гипотезы Карчмера — Раза — Вигдерсона, краеугольного камня в коммуникационной сложности наших дней. Подробнее об этом можно почитать здесь.

9.1 Связь протоколов и формул. Универсальные формулы

Однако после недолгого раздумья становится понятно, что смотреть на такую задачу в терминах протоколов неудобно. Потому что для каждой конкретной задачи потребуется описать не только значения в листьях, но и функции игроков в вершинах, а затем еще сверить исходную задачу с интерпретацией вложения. В общем, слишком много описательных усилий для каждой пары протоколов. Вместо этого, используя спользуя теорему Карчмера — Вигдерсона 4.3 мы можем перейти от изучения протоколов к изучению булевых формул в базисе Де Моргана и получить тем самым задачу о вложении булевых формул (напомним, что основные определения, касающиеся формул Де Моргана, представлены в разделе 4.3).

Определение 9.1

Формула $\varphi_1(x_1, \ldots, x_k)$ вкладывается в формулу $\varphi_2(y_1, \ldots, y_n)$, где $n \geq k$, если можно сделать такую подстановку $L : \{y_1, \ldots, y_n\} \to \{0, 1\} \cup \{x_1, \ldots, x_k, \neg x_1, \ldots, \neg x_k\}$, что полученная формула $\varphi_2[L](x_1, \ldots, x_k)$ вычисляет ту же функцию, что и φ_1.

Пример вложения формул можно видеть на рисунке 8.

Мы уже упомянули выше, что хотим перейти от задачи вложения протоколов к задаче вложения формул. Но чтобы такой переход был корректен, требуется еще одно важное замечание. Мы знаем, что существует соответствие формул и коммуникационных протоколов для отношения Карчмера — Вигдерсона. А задачу вложения можно задать на произвольных протоколах. Чтобы разрешить эту сложность, можно воспользоваться следующим утверждением.

Утверждение 9.1. *Произвольный коммуникационный протокол для произвольного отношения $R \subseteq \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$ можно рассматривать как протокол для решения игры Карчмера — Вигдерсона для некоторой функции f.*

Используя этот факт, нетрудно показать, что формульная задача вложения является полной для коммуникационных протоколов. То есть, если не существует формулы глубины D, в которую вкладываются все формулы глубины d, то и не существует протокола глубины D, решающего любую задачу сложности не выше d.

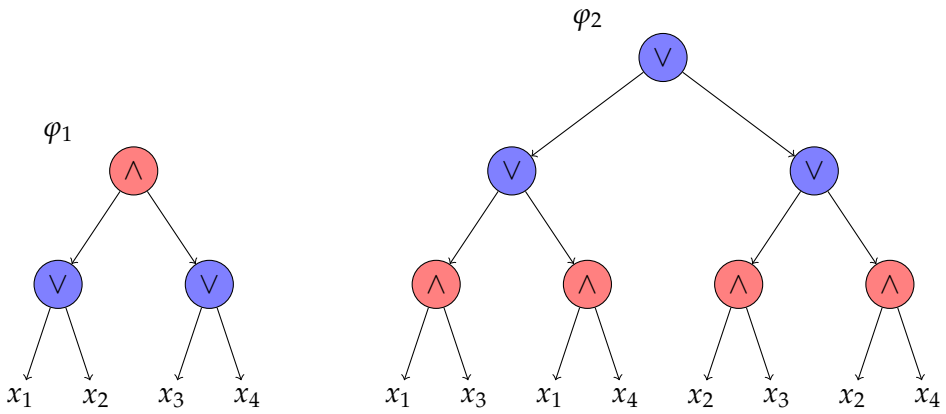


Рис. 8. Пример вложения формул Де Моргана.

Давайте рассмотрим это рассуждение. Напомним, что формулировка исходной задачи звучит следующим образом: при каких соотношениях на числа d и D, где $d \leq D$, существует коммуникационный протокол глубины D, решающий все задачи, коммуникационная сложность которых не больше d?

Предположим, что есть протокол Π_2 глубины D, и нужно понять, может ли он решить коммуникационную задачу, которую решает протокол Π_1 глубины d. Теорема Карчмера — Вигдерсона говорит нам, что существуют формулы φ_1 и φ_2, сохраняющие структуру протоколов Π_1 и Π_2, соответственно, и вычисляющие некоторые функции f_1 и f_2. Значит, если мы сможем вложить формулу φ_1 в φ_2 (обозначим результат вложения за $\varphi_2[L]$), то и на задачу с протоколом ответ положительный, так как $\Pi(\varphi_2[L])$ — подпротокол Π_2, решающий задачу Π_1. И в обратную сторону: если мы знаем, что с помощью Π_2 можно решить Π_1 (обозначим эту подстановку в протокол за $\Pi_2[L]$), то формула $\varphi(\Pi_2[L])$ реализует нам вложение φ_1 в φ_2.

Поэтому новая формулировка нашей задачи такая: при каких условиях на d и D, где $d \leq D$, существует формула глубины D, в которую вкладываются все формулы глубины d? А так же, как эффективно проверять для пары формул φ_1 и φ_2, можно ли одну из них вложить в другую?

Оказывается, что при работе с формулами можно сильно оптимизировать процесс проверки универсальности. Первое наблюдение, которое нам в этом помогает, состоит в следующем. Заметим, что если в формуле, которую мы хотим вложить, заменить литерал, соответствующий отрицанию некоторой переменной, скажем $\neg x_i$, новой переменной x_j, которой ранее в формуле не было, то вложив новую формулу, мы автоматически получим вложение и для исходной. Отсюда следует, что для проверки формулы на универсальность мы можем рассматривать только вложения формул без отрицаний, где каждый лист помечен переменной $\{x_1, \ldots, x_n\}$ — так называемые *монотонные формулы Де Моргана*.

Теперь мы готовы к тому, чтобы формально определить объект нашего изучения — универсальную формульную константу. Для натурального числа d через $\mathrm{depth}(d)$ мы обозначаем класс всех булевых функций, которые вычисляются формулами Де Моргана глубины d.

Определение 9.2

Для любого натурального числа d через α_d обозначим минимальное натуральное D, такое что существует остов T, такой что для каждой функции $f \in \mathrm{depth}(d)$ существует некоторая формула φ глубины D, вычисляющая f и имеющая остов T.
Определим *универсальную формульную константу* α как следующий предел:

$$\alpha = \lim_{d \to \infty} \frac{\alpha_d}{d}.$$

При прочтении этого определения должен возникать вопрос: почему этот предел корректно определен? Или другими словами, почему он существует и конечен? Чтобы ответить на него, давайте представим, что мы уже знаем конкретный пример универсальной формулы для некоторой глубины d. Тогда для всех формул большей глубины можно делать следующее. Резать на части глубины d, и вместо каждой из них вставлять универсальную формулу глубины α_d. Тогда мы увеличили глубину формулы примерно в $\frac{\alpha_d}{d}$ раз*.

Совершенно аналогичный показатель можно определить и для коммуникационных протоков. Давайте распишем формально.

Определение 9.3

Для любого натурального числа d через β_d обозначим минимальное натуральное D, такое что существует некоторый остов T, такой что для каждого отношения R, которое может быть решено протоколом глубины d, существует коммуникационный протокол Π глубины D, решающий R и имеющий остов T.
Определим *универсальную константу протоколов* β как следующий предел:

$$\beta = \lim_{d \to \infty} \frac{\beta_d}{d}.$$

Замечание 1. Из утверждения 9.1, в частности, следует, что универсальные константы для протоколов и формул совпадают: $\forall d \in \mathbb{N},\ \alpha_d = \beta_d$

Выше мы уже начали сужать пространство поиска и необходимой проверки формулы на универсальность, и в этом направлении можно продвинуться дальше. Для этого введем ряд естественных определений.

Определение 9.4

Булева функция f называется *монотонной*, если для любых двух входных наборов $x \preccurlyeq y$, где $x \preccurlyeq y \iff \forall i \in \{1, \ldots, n\},\ x_i \leq y_i$, выполнено $f(x) \leq f(y)$.

Определение 9.5

Формулы однократного чтения (read-once формулы) — это формулы, в которых каждая переменная встречается ровно один раз.

Будем говорить, что read-once формула φ_1 *read-once вкладывается* в формулу φ_2, если существует такое вложение, где каждая переменная из φ_1 встречается в листьях φ_2 не больше одного раза.

Определение 9.6

Для монотонной булевой функции от переменных $X = \{x_1, \ldots, x_n\}$ определены:

1. *минтермы* — это минимальные по включению подмножества $S \subseteq X$, такие что если подставить во все переменные из S значение 1, а во все остальные 0, то значение функции будет равно 1;
2. *макстермы* — это максимальные по включению подмножества $T \subseteq X$, такие что если подставить во все переменные из T значение 1, а во все остальные 0, то значение функции будет равно 0.

Заметим, что каждая (монотонная) формула Де Моргана вычисляет только одну (монотонную) булеву функцию, с другой стороны, каждая (монотонная) булева функция вычисляется многими (монотонными) формулами Де Моргана. Для монотонной булевой формулы φ за MIN_φ (MAX_φ) будем обозначать множество минтермов (макстермов) функции, которую вычисляет φ.

Замечание 2. Иногда под минтермом (макстермом) мы будем понимать не множество переменных $S \subseteq X$, а его характеристическую функцию — битовую строчку $\{0,1\}^X$, где на местах переменных, входящих в S, стоят 1, а на остальных местах стоят 0.

Теперь, когда мы ввели необходимые определения, перейдем к их применению в задаче вложения формул. На формулу φ можно смотреть как на пару (T, L), где T — остов (с пометками), а L — означивание листьев дерева (переменными и константами). Поэтому условие универсальности формулы с остовом T_2 для глубины d можно записать с помощью кванторов следующим образом:

$$\forall T_1 \; \forall L_1 \; \exists L_2 : \; \varphi(T_2, L_2) \equiv \varphi(T_1, L_1)$$

Где T_1 — остов глубины d, а эквивалентность формул означает, что они совпадают на всех подстановках переменных: $\forall x \in \{0,1\}^{2^d} \; \varphi(T_2, L_2)(x) = \varphi(T_1, L_1)(x)$. Теперь давайте оптимизируем эти кванторы:

- заметим, что на самом деле можно вкладывать только маленькие формулы, в которых все листья — различные переменные. Тогда квантор $\forall L_1$ можно опустить, и рассматривать только монотонные read-once формулы глубины d. Тогда и большие формулы можно рассматривать только монотонные;
- Для монотонных формул нас будут интересовать только монотонные вложения, поэтому перебор $\forall x \in \{0,1\}^{2^d}$ можно сократить до $\forall x \in \mathrm{MIN}_{T_1} \sqcup \mathrm{MAX}_{T_1}$.

Для read-once вложения монотонных формул задача проверки монотонного вложения является полной. То есть, если существует какое-то немонотонное вложение φ_1 в φ_2, то его можно переделать в монотонное вложение φ_1 в φ_2, заменив отрицательные литералы на подходящие константы.

Открытая задача 9.1

Доказать, что для немонотонной формулы размера s над базисом Де Моргана, вычисляющей монотонную функцию, можно найти монотонную формулу размера не более s, вычисляющую ту же функцию.

В предположении, что этот факт верен, для поиска вложений монотонных формул в общем случае также достаточно рассматривать только монотоннные вложения. Дальше мы будем рассматривать только монотонные формулы Де Моргана.

Задача 9.2. *Придумайте формулу в базисе Де Моргана для вычисления функции $\oplus_n$ размера n^2.*

Задача 9.3. *Оцените количество полных формул как функцию от глубины d.*

Задача 9.4. *Придумайте формулу глубины 4, в которую вкладываются все формулы глубины 2.*

Задача 9.5. *Придумайте формулу глубины 5, в которую вкладываются все формулы глубины 3.*

9.2 Двухцветные деревья. Частный случай вложения

В предыдущей секции мы увидели, что, хоть задачу универсальных протоколов можно свести к легко формализуемой задаче универсальных формул, доказывать нижние оценки на универсальную формульную константу сложно. Это возникает из-за того, что возможно множество нетривиальных использований подфомул. Давайте попробуем упростить себе задачу, и разрешим вкладывать формулы только "правильным"и понятным образом: чтобы маленькая формула была поддеревом большой. Сформулируем этот подход аккуратнее в терминах простого комбинаторного объекта.

Определение 9.7 (Двухцветное дерево)

Двухцветное дерево — это корневое дерево, где каждая вершина покрашена в один из двух цветов.

Определение 9.8

Для формулы Де Моргана φ определим *остов* φ — поддерево, состоящее из всех внутренних вершин с пометками, и обозначим его T_φ.

Нетрудно видеть, что остов любой формулы Де Моргана и любого коммуникационного протокола является бинарным двухцветным деревом. Под *глубиной* двухцветного дерева будем понимать количество *вершин* в самом длинном пути из корня в лист. Следовательно, остов формулы (протокола) глубины d как двухцветное дерево тоже будет иметь глубину d.

Определение 9.9

Для двух раскрашенных деревьев T_1 и T_2 мы говорим, что T_1 *топологически вкладывается в* T_2, если существует инъекция $\phi : V(T_1) \to V(T_2)$, такая что для каждого $v \in V(T_1)$

1. $\phi(v)$ того же цвета, что и v,
2. если w является предком v, то $\phi(w)$ — предок $\phi(v)$,
3. если u и w являются детьми v, то $\phi(v)$ — наименьший общий предок $\phi(u)$ и $\phi(w)$.

Пример топологического вложения двухцветных деревьев можно представлен на рисунке 9.

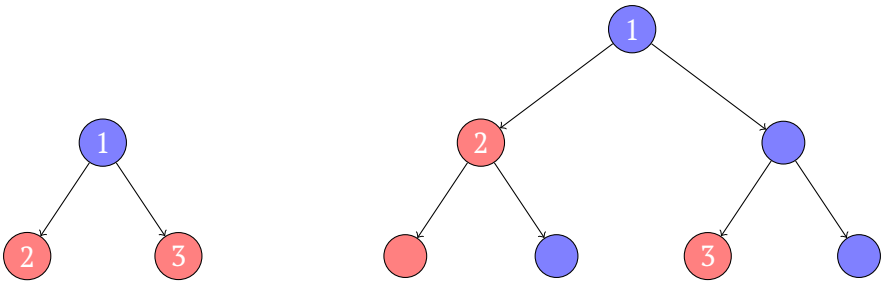


Рис. 9. Пример топологического вложения деревьев.

Определение 9.10

Для любого натурального d через γ_d обозначим минимальное натуральное D, такое что существует некоторое двухцветное бинарное дерево T глубины D, в которое топологически вкладываются все двухцветные бинарные деревья глубины d. Определим *универсальную константу двухцветных деревьев* γ как следующий предел:

$$\gamma = \lim_{d \to \infty} \frac{\gamma_d}{d}.$$

Следующее утверждение показывает, что топологическое вложение бинарных двухцветных деревьев является частным случаем вложения формул, имеющих эти деревья в качестве остовов. Из этого напрямую следует, что универсальная формульная константа не превосходит универсальную константу двухцветных деревьев.

Утверждение 9.2. *Для любого d, $\gamma_d \geq \alpha_d$.*

Задача 9.6. *Оцените количество полных двухцветных деревьев как функцию от глубины d.*

Задача 9.7. *Оцените количество всех двухцветных деревьев как функцию от глубины d.*

Задача 9.8. *Придумайте двухцветное дерево глубины 6, в которую вкладываются все двухцветные деревья глубины 3.*

Задача 9.9. *Придумайте двухцветное дерево глубины 5, в которое вкладываются все двухцветные деревья глубины 3.*

Рассмотрим теперь более общий случай: задачу о топологическом вложении n-арных деревьев, вершины которых могут быть покрашены в k цветов, где $n, k \geq 2$. Заметим, что частный случай $(n,k) = (2,2)$ является в точности задачей о топологическом вложении двухцветных бинарных деревьев. И попробуем получить нижние оценки на размер универсального дерева в терминах n и k. Основным вопросом является, при каком значении $D = D(d,n,k)$ возможно найти универсальное дерево глубины D, в которое топологически вкладываются все деревья глубины d. Отметим сначала некоторые верхние оценки.

Лемма 9.1. *Если $n \geq k-1$, то $\dfrac{D}{d} \leq 2$.*

Следствие 9.1. *Коэффициент топологического вложения $\gamma \leq 2$.*

Доказательство. Это в точности случай $(n,k) = (2,2)$. □

Лемма 9.2. *Если $n < k-1$, то $\dfrac{D}{d} \leq \lceil \log_n k \rceil + 1$.*

Теперь перейдем к нижним оценкам на отношение D/d для случая произвольной арности и числа цветов.

Теорема 9.1. *Пусть $D = (1+\delta)d$. Чтобы для параметров (n,k,d) существовало универсальное дерево с параметрами (n,k,D), необходимо, чтобы выполнялось следующее неравенство:*

$$\left(\frac{1}{\sqrt{2\pi d}}\right)^{1/d} \cdot (1+\delta) \cdot \left(\frac{1+\delta}{\delta}\right)^{\delta+1/2d} \geq k \cdot n^{-\delta}.$$

Численные нижние оценки на параметр δ для различных значений n и k приведены в таблице 2.

n	k	δ
2	2	0.20559
2	3	0.39169
2	4	0.54824
2	5	0.68268
2	6	0.80047
3	2	0.17713
3	3	0.32636
3	4	0.44728
3	5	0.54864
3	6	0.63594

Таблица 2. Нижние оценки на α для различных n и k.

Следствие 9.2. *Коэффициент топологического вложения $\gamma \geq 1.20559$.*

Стоит отметить, что полученную оценку на коэффициент γ невозможно существенно улучшить этим методом.

9.3 Применение вложения деревьев к формулам

Напомним, что согласно рассуждениям выше, для проверки формулы глубины D на универсальность достаточно рассматривать вложения в нее только монотонных read-once формул глубины d. Соответственно, и потенциально универсальные формулы глубины D достаточно рассматривать только монотонные. Поэтому далее мы будем рассматривать только монотонные формулы Де Моргана, и их монотонные вложения друг в друга, то есть использующие только положительные литералы и константы.

Замечание 3. Во избежание перегрузки нижних индексов, через $\varphi_2[L]$ будем обозначать формулу, имеющую остов φ_2, но листья которой помечены согласно вложению φ_1 в φ_2.

Рассмотрим подход к задаче поиска универсальных формул, основанный на том факте, что остов формулы Де Моргана — это двухцветное дерево. Мы покажем, что эту задачу можно рассматривать как надзадачу о вложении двухцветных деревьев. То есть перейти к рассмотрению структуры формул и пытаться вкладывать их как деревья, используя при этом некоторые преобразования.

Теорема 9.2. *Если формула φ_1 вкладывается в формулу φ_2, то можно, используя операции дистрибутивности (в обе стороны) и коммутативности, получить формулу, эквивалентную φ_1, которая топологически вложится в формулу φ_2.*

Задача 9.10. *Докажите, что для $d \geq 2$ верно, что $\alpha_d > d+1$.*

Открытая задача 9.11

Докажите, что существуют такие $d_0 \in \mathbb{N}$, $c \in \mathbb{Z}_{>1}$, что $\forall d \geq d_0 \quad \alpha_d > d + c$.

9.4 Универсальные формулы над полным базисом

Рассмотрим теперь обобщение задачи и исследуем вопрос об универсальных формулах над полным бинарным базисом вместо базиса Де Моргана. Теперь формула — это корневое двоичное дерево, каждая внутренняя вершина которого помечена одной из трех операций $\{\wedge, \vee, \oplus\}$, а каждый лист помечен одним из литералов $\{x_1, \ldots, x_n, \neg x_1, \ldots, \neg x_n\}$ или константой $\{0, 1\}$. В полном булевом базисе B_2 всего 16 функций от двух переменных, среди которых:

- 8 AND-функций вида $(x_1 \oplus a_1) \wedge (x_2 \oplus a_2) \oplus a_3$, где $a_1, a_2, a_3 \in \{0, 1\}$;
- 2 XOR-функции вида $(x_1 \oplus x_2) \oplus a_1$, где $a_1 \in \{0, 1\}$;
- 4 функции, зависящих только от одной из двух переменных $x_1, \neg x_1, x_2, \neg x_2$;
- 2 константные функции $0, 1$.

Пользуясь законами Де Моргана, а также тем фактом, что $\neg(x_1 \oplus x_2) = \neg x_1 \oplus x_2$, мы получаем, что отрицания достаточно ставить только у листьев.

В таком базисе мы аналогично можем определить задачу поиска универсальной формулы. Обозначим также универсальную формульную константу для полного базиса через α^{B_2}

Задача 9.12. *Докажите, что* $\alpha^{B_2} \leq 2$.

Открытая задача 9.13

Улучшите верхнюю оценку из предыдущей задачи.

Также, как и в случае с базисом Де Моргана, для полного булева базиса можно рассмотреть топологическое вложение формул (топологическое вложение их трехцветных остовов). С точки зрения формул это значит, что мы запрещаем моделировать $\oplus$-гейт с помощью $\wedge$, $\vee$-гейтов. Тогда топологическое вложение остовов является частным случаем вложения формул (аналогично утверждению 9.2). И тогда применима оценка, полученная ранее для раскрашенных двоичных деревьев.

Следствие 9.3. *Коэффициент топологического вложения трехцветных двоичных деревьев* $\frac{D}{d} \geq 1.39169$.

Открытая задача 9.14

Докажите верхнюю оценку на коэффициент топологического вложения трехцветных двоичных деревьев.

Известные результаты для констант:

	Верхняя, $\leq$	**Нижняя,** $\geq$
α_d	$5d/3$	$> d + 1$
α	$5/3$	1
β	$5/3$	1
γ	$5/3$	1.20559
α^{B_2}	2	1
γ^{B_2}	?	1.39169

Таблица 3. Актуальные оценки на универсальные константы.

9.5 Практические задачи

Задача 9.15. *Компьютерный поиск универсального дерева глубины 8 для вложения деревьев глубины 5.*

Задача 9.16. *Оптимизированная схема компьютерного поиска универсальных формул.*

Открытая задача 9.17

Провести компьютерный поиск универсальных формул глубины 8 для формул глубины 5.

Список литературы

[BFS86] Laszlo Babai, Peter Frankl, and Janos Simon. Complexity classes in communication complexity theory. In *27th Annual Symposium on Foundations of Computer Science (sfcs 1986)*, pages 337–347, 1986.