Санкт-Петербургский государственный университет

ИГНАТЬЕВ Артур Андреевич

Выпускная квалификационная работа

Оценки на коммуникационную сложность булевых функций и игр Карчмера-Вигдерсона в разных моделях

Уровень образования: бакалавриат
Направление *01.03.01 “Математика”*
Основная образовательная программа *СВ.5000.2018 “Математика”*

Научный руководитель:
доцент, Факультет математики
и компьютерных наук СПбГУ,
Авдюшенко Александр Юрьевич

Рецензент:
м.н.с. ПОМИ РАН,
Софронова Анастасия Александровна

Санкт-Петербург
2022

Содержание

1 Введение

Определение 1

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 2

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 3

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 1

Для любой булевой функции f верно

$$\log_2 L(f) \leq D(f) \leq 1.82 \log_2 L(f).$$

Первое неравенство верно в силу того, что размер двоичного дерева не больше чем 2^d, где d — глубина дерева. Второе неравенство верно, так как формулы можно сбалансировать с небольшим увеличением глубины (подробнее см. в [Juk12]).

Доказательство оценок на сложность булевых формул и схем является одной из основных задач в теории сложности вычислений. Еще в 1942 году Риордан и Шеннон [RS42] показали, что если выбрать булевую функцию от n переменных случайно, то с вероятностью близкой к 1 она будет иметь формульную сложность не менее $2^n / \log n$. Но до сих пор неизвестны явно заданные функции из классов P или NP большой сложности.

На протяжении более 40 лет разрабатывались методы доказательства нижних оценок, начиная с работ Субботовской [Sub61] и Храпченко [Khr71], вплоть до знаменитой работы Хостада [Hås98]. В итоге, удалось достичь кубической нижней оценки на формульную сложность явной булевой функции (функция Андреева). Эту нижнюю оценку не удаётся превзойти уже более 20 лет. Результат Хостада был улучшен Талом [Tal14], но улучшение касается только членов второго порядка.

Карчмер, Раз и Вигдерсон [KRW95] предложили подход для доказательства суперполиномиальной нижней оценки на размера формулы для булевых функций из класса **P** (из этого следовало бы $\mathbf{P} \not\subseteq \mathbf{NC}^1$). Предлагаемый подход заключается в доказательстве нижних оценок на глубину блочной композиции двух произвольных булевых функций (KRW гипотеза).

Определение 4

Пусть $f : \{0,1\}^m \to \{0,1\}$ и $g : \{0,1\}^n \to \{0,1\}$ – булевые функции. *Блочная композиция* $f \diamond g : (\{0,1\}^n)^m \to \{0,1\}$ определяется как

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

где $x_1, \ldots, x_m \in \{0,1\}^n$.

Гипотеза 1 (KRW гипотеза)

Пусть $f : \{0,1\}^m \to \{0,1\}$ и $g : \{0,1\}^n \to \{0,1\}$ — неконстантные функции. Тогда

$$\mathrm{D}(f \diamond g) \approx \mathrm{D}(f) + \mathrm{D}(g).$$

Теорема 1

Если KRW гипотеза верна, то $\mathbf{P} \not\subseteq \mathbf{NC}^1$.

Доказательство. Рассмотрим функцию $h : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$, которая на вход принимает таблицу истинности функции $f : \{0,1\}^{\log n} \to \{0,1\}$ и строку x, и вычисляет значение блочной композиции $\log n / \log\log n$ функций f на входе x:

$$h(f, x) = (\underbrace{f \diamond \cdots \diamond f}_{\log n / \log\log n})(x).$$

Нетрудно заметить, что $h \in \mathbf{P}$. Чтобы показать, что $h \notin \mathbf{NC}^1$, обозначим через $\tilde{f}$ функцию с максимальной глубиной формулы. Из теоремы Риордана — Шеннона $\tilde{f}$ имеет глубину $\log n$. Тогда $\tilde{f} \diamond \cdots \diamond \tilde{f}$ имеет глубину примерно в $\log n \cdot (\log n / \log\log n) = \omega(\log n)$, следовательно, $\tilde{f} \diamond \cdots \diamond \tilde{f} \notin \mathbf{NC}^1$. Любая формула для h должна вычислять $\tilde{f} \diamond \cdots \diamond \tilde{f}$, если мы в качестве f подставим $\tilde{f}$, поэтому $h \notin \mathbf{NC}^1$. □

Стоит отметить, что это доказательство будет работать даже при условии более слабой версии гипотезы KRW, например $\mathrm{D}(f \diamond g) \geq \mathrm{D}(f) + \epsilon \cdot \mathrm{D}(g)$ или $\mathrm{D}(f \diamond g) \geq \epsilon \cdot \mathrm{D}(f) + \mathrm{D}(g)$ для некоторых $\epsilon > 0$.

Основным подходом к доказательству KRW гипотезы является коммуникационная сложность. В данной работе рассматривается коммуникационная сложность булевых функций и отношений Карчмера — Вигдерсона [KW88]. Вместе с классической коммуникационной сложностью, введеннной Яо [Yao79], рассматриваются полудуплексные модели коммуникационной сложности, рассмотренные в статье [HIMS18b], а также коммуникационная сложность с оракулом EHD_ℓ и EQ.

В классической коммуникационной сложности Алиса и Боб пытаются вычислить некоторую функцию $f(x, y)$, при условии, что Алиса знает только функцию f и вход x, а Боб функцию f и вход y. Игроки могут общаться, посылая биты друг другу, по одному биту за раунд, и в конце общения оба игрока должны знать результат $f(x, y)$. Существенным

свойством этой классической модели является то, что в каждом раунде общения один игрок отправляет бит, а другой его получает.

Существует множество расширений этой модели коммуникации, таких как рандомизированная коммуникационная сложность, недетерминированная коммуникационная сложность [KN97], различные типы моделей коммуникации с несколькими игроками [CFL83] и другие. В [HIMS18b] авторы предложили рассмотреть модель коммуникации, в которой игроки разговаривают по полудуплексному каналу связи. Хорошо известным примером полудуплексной коммуникации является связь с использованием рации: один игрок удерживает кнопку “push-to-talk”, чтобы поговорить с другим игроком, который в свою очередь держит ее отпущенной, чтобы слушать. Если два человека пытаются говорить одновременно, тогда они не слышат друг друга. Формально говоря, в каждом раунде каждый игрок выбирает одно из трех действий: *отправить 0*, *отправить 1* или *получить*. Существует три различных типа раундов: классический раунд, когда один игрок отправляет некоторый бит, в то время как другой получает, потерянный раунд, когда оба игрока отправляют биты (эти биты теряются), и тихий раунд, когда оба игрока получают. В [HIMS18b] авторы определили три варианта полудуплексной модели, основанные на том, что происходит в тихом раунде, мы рассмотрим данную модель в разделе 3.

Еще одним вариантом расширения является коммуникационная модель с оракулом [BFS86]. Теперь игроков трое: Алиса, Боб и Чарли, выполняющий роль оракула. Алиса и Боб каждый раунд отправляют Чарли по одному биту или нескольким сразу. Чарли по ним вычисляет некоторую функцию $A(a,b)$ и говорит ответ. Цель игроков с данным оракулом A вычислить функцию $f(x,y)$. В разделе 5 мы подробнее рассмотрим данную модель.

Целью данной работы является доказательство оценок на формульную сложность булевых функций с использованием коммуникационной сложности.

Обзор результатов:

1. В разделах 3.2, 3.3, 3.4 мы докажем оценки на функции DISJ, GT, игры Карчмера — Вигдерсона для функций MODp в различных полудуплексных моделях.

2. В 3.5 рассмотрим недетерминированную полудуплексную сложность и покажем её связь с классической моделью.

3. В главе 4 рассмотрим технику случайных ограничений для обобщенных игр Карчмера — Вигдерсона.

4. В разделе 5.2 мы докажем оценку на функцию EHD_k с оракулом EHD_1.

5. В разделе 5.3 докажем оценку на функцию EHD_k с оракулом EHD_ℓ при $k \geq l$.

6. В разделе 5.4 покажем как с помощью оракула $\mathrm{HD}_{\leq \ell}$ эффективно вычислить функцию $\mathrm{HD}_{\leq k}$.

7. В разделе 5.5 рассмотрим оракул однобитового равенства, докажем, что случайная функция имеет сложность $n - o(n)$, покажем точную оценку на функцию EHD_1.

2 Основные определения

Мы будем исследовать сложность следующих функций.

Определение 5

- $\mathrm{EQ}_n : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ такая, что $\mathrm{EQ}_n(x,y) = 1 \iff x = y$.
- $\mathrm{GT}_n\{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ такая, что $\mathrm{GT}_n(x,y) = 1 \iff x > y$, как двоичные числа.
- $\mathrm{IP}_n : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ такая, что $\mathrm{IP}_n(x,y) = \bigoplus_{i\in[n]} x_i y_i$.
- $\mathrm{DISJ}_n : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ такая, что $\mathrm{DISJ}_n(x,y) = 1 \iff \forall i \in [n],\ x_i y_i = 0$.
- $\mathrm{MOD}p_n(x) = 0 \iff x_1 + \ldots + x_n = 0 \mod p$.

2.1 Классическая коммуникационная сложность

В данном разделе предложены базовые сведения о коммуникационной сложности, более подробно в [KN97].

Пусть X, Y, Z — конечные множества, и пусть $f : X \times Y \to Z$. Множества X, Y, Z и функцию f знают оба игрока. Алисе дан некоторый $x \in X$, а Бобу некоторый $y \in Y$. Их цель вычислить $f(x,y)$. Каждый раунд они могут отправлять друг другу битовые сообщения. Будем считать, что Алиса и Боб решили задачу, если оба игрока знают значение $f(x,y)$.

Определение 6

Коммуникационный протокол для функции $f : X \times Y \to Z$ — это корневое двоичное дерево с метками. Каждая внутренняя вершина v помечена “A” или “B”, а каждый лист помечен значением из множества Z. Кроме того, для каждой вершины v, помеченной “A”, определена функция $g_v : X \to \{0,1\}$, а для каждой вершины u с пометкой “B” определена функция $h_v : Y \to \{0,1\}$. Каждая внутренняя вершина имеет двух потомков, ребро к первому потомку помечено 0, а ребро ко второму потомку помечено 1.

Несложно заметить, что общение по такому протоколу на некоторой паре входов (x,y) соответствует пути от корня к некоторому листу. Игроки начинают с корня и далее спускаются к листу, находясь во внутренней вершине v с пометкой “A” или “B”, игрок отправляет сообщение $g_v(x)$ или $h_v(y)$ в зависимости от пометки. После игроки переходят в одного из потомков вершины v по ребру, пометка которого совпадает с битом, отправленным в вершине v. Когда игроки достигают листа, то задача решена и результатом является метка в этом листе.

Определение 7

Коммуникационный протокол вычисляет функцию f, если для любой пары входов (x,y) общение игроков завершается в листе с меткой $f(x,y)$.

Определение 8

Коммуникационная сложность функции f — наименьшая глубина протокола, вычисляющего функцию f. Обозначим ее за $D(f)$.

Утверждение 2

Для любой функции $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ выполнено $D(f) \leq n+1$.

Доказательство. Алиса посылает свой вход x Бобу, используя n бит. Боб отправляет $f(x,y)$ за 1 бит Алисе. □

Стоит отметить, что определение коммуникационных протоколов и коммуникационной сложности можно обобщить на более широкий класс задач, если допустить, что вместо функции $f : X \times Y \to Z$, Алиса и Боб решают коммуникационную задачу для отношения $R \subset X \times Y \times Z$.

Рассмотрим коммуникационный протокол для некоторого отношения $F \subset X \times Y \times Z$. Для каждой вершины протокола v можно определить множество всех пар $(x,y) \in X \times Y$, для которых общение проходит через вершину v, обозначим это множество за R_v. По индукции можно показать, что R_v является комбинаторным прямоугольником, т.е. существуют такие $X_v \subset X$ и $Y_v \subset Y$, что $R_v = X_v \times Y_v$.

Определение 9

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.

Таким образом, листья коммуникационного протокола для отношения F задают разбиение прямоугольника $X \times Y$ на одноцветные прямоугольники. Обозначим через $\chi(F)$ минимальное количество одноцветных прямоугольников для F, покрывающих $X \times Y$.

Утверждение 3

$D(f) \geq \log \chi(F)$.

Доказательство. Пусть L — число листьев в коммуникационном протоколе для F, то $d \geq \log L \geq \log \chi(F)$. □

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 $X \times Y$. Пусть для любого одноцветного прямоугольника R верно $\mu(R) \leq M$, $M > 0$.

Утверждение 4

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

2.2 Игры Карчмера — Вигдерсона

Определение 10

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.

Теорема 2 (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.

Рассмотрим обобщенную игру Карчмера — Вигдерсона для функции, действующей в r бит, для таких отношений уже нет соответствий Карчмера — Вигдерсона.

Определение 11

Обобщенная игра Карчмера — Вигдерсона (обобщенная KW*)* для функции $f : \{0,1\}^n \to \{0,1\}^r$ – это следующая коммуникационная задача: Алиса получает $x \in \{0,1\}^n$, Боб получает $y \in \{0,1\}^n$, и входы, удовлетворяют $f(x) \neq f(y)$. Их цель найти такое $i \in [n]$, что $x_i \neq y_i$. Эта задача соответствует коммуникационной задаче для *обобщенного отношения Карчмера — Вигдерсона для* f:

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

3 Полудуплексная коммуникационная сложность

В полудуплексной модели каждый раунд каждый игрок выбирает одно из трех действий: отправить 0, отправить 1 или получить. Итак, есть три различных типа раундов.

- *Классический* раунд: один игрок посылает какой-то бит, а другой получает его.
- *Потраченный* раунд: оба игрока посылают биты, и эти биты теряются.
- *Тихий* раунд: оба игрока получают.

В [HIMS18b] авторы рассмотрели три варианта этой модели, основанные на том, что происходит в тихих раундах.

- *Полудуплексная модель коммуникации с тишиной*. В тихом раунде оба игрока получают специальный символ *тишины*, поэтому оба игрока могут отличить тихий раунд от классического. Сложность функций в этой модели будем обозначать $\mathrm{D}_{\mathrm{s}}^{\mathrm{hd}}(f)$.

- *Полудуплексная модель коммуникации с нулем*. В тихом раунде оба игрока получают 0, то есть игроки не могут отличить тихий раунд от классического раунда, в котором другой игрок посылает 0. Сложность функций в этой модели будем обозначать $D_0^{hd}(f)$.

- *Полудуплексная модель коммуникации с противником*. В тихом раунде каждый игрок получает произвольный бит, не обязательно такой же, как у другого игрока. Сложность функций в этой модели будем обозначать $D_a^{hd}(f)$.

В полудуплексной модели с нулем нет необходимости отправлять нули, игрок может выбрать вместо этого прием, и другой игрок не заметит разницы. Вместо одного дерева протоколов, как в классическом случае, в полудуплексном случае протокол описывается двумя деревьями, по одному для каждого игрока. Деревья протоколов будут пятиричными в полудуплексной модели с тишиной, троичными в модели с нулем и четверичными в модели с противником. Формальное определение протоколов полудуплексной модели коммуникации приведено в работе [HIMS18a]. Следует отметить, что, несмотря на различия, каждая вершина полудуплексного протокола имеет соответсвующий ей прямоугольник, а каждый прямоугольник, соответствующий листу, является одноцветным.

Минимальная глубина протокола, решающего коммуникационную задачу R, является коммуникационной сложностью R. Для классической модели коммуникации, обозначим ее через $D(R)$, для полудуплексных моделей с тишиной, с нулем и с противником мы обозначаем ее $D_s^{hd}(R), D_0^{hd}(R)$, и $D_a^{hd}(R)$ соответственно.

Мотивацией полудуплексной коммуникацинной сложности может служить KRW гипотеза. Подробнее можно ознакомиться в [MS20, Mei20].

Все результаты данной главы можно найти в совместной работе [DIS+21].

3.1 Методы доказательства нижних оценок

В статье [HIMS18b] авторы разработали методы доказательства нижних оценок в полудуплексных моделях. Рассмотрим некоторые из них.

Классический метод прямоугольников. Вершинам полудуплексного протокола можно поставить в соответствие прямоугольники, аналогично классическим протоколам. Рассмотрим полудуплексный коммуникационный протокол Π для коммуникационной задачи $P \subseteq X \times Y \times Z$. Для каждой вершины v из деревьев Алисы или Боба определим $R_v \subseteq X \times Y$ — можество всех пар $(x, y) \in X \times Y$, для которых общение проходит через вершину v. Для того, чтобы это утверждение было верно и для модели с противником, следует рассматривать протокол для фиксированной стратегии противника.

Утверждение 5

Для всех вершин v протокола Π множество R_v является комбинаторным прямоугольником.

Таким образом, можно использвать методы доказательства нижних оценок, аналогичные классической коммуникационной сложности. Но стоит учитывать арность дерева протокола, поэтому основание логарифма для полудуплексной коммуникационной сложности будет больше двух.

Утверждение 6

Пусть для коммуникационного отношения $P \subseteq X \times Y \times Z$ задана полуаддитивная мера μ на подмножествах $X \times Y$ такая, что мера всего множества не меньше μ_r, а мера любого одноцветного прямоугольника не превосходит μ_ℓ. Тогда

- $\mathrm{D}_{\mathrm{s}}^{\mathrm{hd}}(f) \geq \log_5(\mu_r/\mu_\ell)$,
- $\mathrm{D}_{0}^{\mathrm{hd}}(f) \geq \log_3(\mu_r/\mu_\ell)$,
- $\mathrm{D}_{\mathrm{a}}^{\mathrm{hd}}(f) \geq \log_4(\mu_r/\mu_\ell)$.

Метод элиминации раундов. Рассмотрим полудуплексный протокол Π для некоторой задачи и посмотрим на первый раунд. Изначальный прямоугольник входов $X \times Y$ можно разбить на девять прямоугольников (см. таблицу 1). Определим два прямоугольника $R_{good} = R_{00} \cup R_{01} \cup R_{0r}$ и $R_{bad} = R_{0r} \cup R_{1r}$. Заметим, что если сузить задачу на прямоугольник R_{good}, то первый раунд больше не нужен, игроки уже все знают. Если же сузить задачу на R_{bad}, то первый раунд остается нужным, Боб может получить 0 или 1.

Таблица 1. Разбиение прямоугольника входов в первом раунде

Алиса\Боб	`отправить 0`	`отправить 1`	`принять`
`отправить 0`	R_{00}	R_{01}	R_{0r}
`отправить 1`	R_{10}	R_{11}	R_{1r}
`принять`	R_{r0}	R_{r1}	R_{rr}

Определение 12

Прямоугольник $R' \subseteq R$ называется хорошим для полудуплексного протокола Π на прямоугольнике R, если сужение коммуникационной задачи на прямоугольник R' делает первый раунд протокола Π ненужным.

Можно сформулировать следующую Лемму, основанную на сужение рассматриваемой задачи на хорошие прямоугольники.

Лемма 1 ([HIMS18b])

Пусть μ — полуаддитивная мера на прямоугольниках такая, что $\mu(X \times Y) \geq \mu_r$ и для любого прямоугольника соответствующего листу R_l, $\mu(R_l) \leq \mu_\ell$. Если для любого прямоугольника R найдется хороший подпрямоугольник для функции f, суженной на прямоугольник R, имеющий меру хотя бы $\alpha \cdot \mu(R)$, тогда глубина протокола хотя бы $\log_{1/\alpha} \frac{\mu_r}{\mu_\ell}$.

3.2 Оценки на функцию дизъюнктности

В этой главе мы доказываем оценки на функцию DISJ_n и закрываем некоторые вопросы из работы [HIMS18b].

Теорема 3

$\mathrm{D}_{0}^{\mathrm{hd}}(\mathrm{DISJ}_n) \leq 5n/6 + 2\log n + O(1)$.

Доказательство. Без ограничения общности можно считать, что n чётно.

Рассмотрим следующий протокол: Алиса и Боб разбивают свои строки на подстроки длины 2, всего таких подстрок получится $n/2$. Через $\sharp(ab)$ обозначим количество подстрок ab среди получившихся кусочков. Заметим, что возможны три случая:

1. $\sharp(00) \geq n/6$, тогда $\sharp(01) + \sharp(10) + \sharp(11) \leq n/2 - n/6 = n/3$.
2. $\sharp(01) \geq n/6$, тогда $\sharp(00) + \sharp(10) + \sharp(11) \leq n/2 - n/6 = n/3$.
3. $\sharp(00) + \sharp(01) < n/3$.

В самом начале Боб должен решить, к какому случаю относится его строка, и сообщить Алисе с помощью двух битов.

Случай 1. Алиса и Боб обрабатывают свои входные данные по два бита за раунд. Каждый раунд они действуют согласно следующей таблице.

Символ	**Алиса**	**Боб**
00	`принять`	`отправить 1`
01	`отправить 1`	`принять`
10	`принять`	`принять`
11	`принять`	`принять`

В данной таблице Алисе и Бобу надо уметь отличать ситуации, когда их строки пересекаются, то есть отличать пары (01,01), (01,11), (10,10), (10,11), (11,01), (11,10), (11,11) от других. Будем ставить “+” в таблицу, если научились отличать какую-то из этих ситуаций.

Алиса\Боб	`00`	`01`	`10`	`11`
`00`				
`01`		+		+
`10`			+	+
`11`		+	+	+

После $n/2$ раундов Боб сообщает Алисе получал ли он 1 с его входом 11 или 01, если получал, то у Алисы было 01, и тогда их строки пересекаются (научились различать пару (01,11),(01,01)). Далее, Алиса говорит Бобу, был ли у неё тихий раунд с её входом 11. Если был, то у Боба был вход 01, 10 или 11, и их строки пересекаются (научились отличать пары (11,01), (11,10), (11,11)).

Нам осталось научиться различать пары (10,10), (10,11). Для этого Алисе нужно как-то отличать нули, полученные от Боба с входом 10 или 11, от нулей со входа 01.

Боб последовательно (начиная с его первого тихого раунда со входом 01,10 или 11) проходит по всем своим входам 01, 10, 11, в которых он получал от Алисы 0, и отправляет Алисе 1, если был вход 10 или 11, и отправляет 0, если вход 01.

Алиса знает сколько битов ей отправит Боб, так как он отправляет ей только те раунды, когда он молчал и она молчала. Алиса проходится по своим входам, на которых был тихий раунд. И смотрит, что ей отправил Боб, если Боб отправил 1, то у него в этом раунде был вход 11 или 10, иначе у него был вход 01, таким образом Алиса узнает пересекается ли ее вход в этом раунде с входом Боба в том же раунде. Алиса переходит к следующему тихому раунду и аналогично проверяет свой вход с входом Боба.

Когда Алиса проверит так весь свой вход, она отправит Бобу 1, если у нее был вход, пересекающийся с входом Боба, и отправит 0, иначе. В итоге, мы проверили все пересекающиеся входы и всего было $2 + n/2 + n/3 + 3 = 5n/6 + 5$ раундов.

Случай 2. Действуем аналогично случаю 1 по следующей таблице.

Символ	**Алиса**	**Боб**
00	`принять`	`принять`
01	`отправить 1`	`отправить 1`
10	`принять`	`принять`
11	`принять`	`принять`

После $n/2$ раундов Боб сообщает Алисе получал ли он 1 с его входом 11, если получал, то у Алисы было 01, и тогда их строки пересекаются (научились различать пару (01,11)). Алиса сообщает был ли раунд с ее входом 11, когда она получила от Боба 1 (научились различать пару (11,01)). Боб сообщает количество раундов, в которых он отправлял 1, а Алиса количество 1, которые она слышала. Если эти два числа равны, то в процессе общения не было потраченного раунда (01,01), иначе был раунд (01,01) и их строки пересекаются (научились различать пару (01,01)).

Осталось научиться различать пары (10,10), (10,11), (11,10), (11,11). Для этого Алисе надо отличать 0, полученные от Боба с входом 10 или 11, от нулей со входа 00.

Боб последовательно (начиная с его первого тихого раунда со входом 00, 10 или 11) проходит по всем своим входам 00, 10, 11, в которых он получал от Алисы 0, и отправляет Алисе 1, если был вход 10 или 11, и отправляет 0, если вход 00.

Далее они действуют аналогично случаю 1. В итоге получаем $2 + n/2 + n/3 + 2\log n + 3 = 5n/6 + 2\log n + 5$ раундов.

Случай 3. Действуем аналогично случаю 1 по следующей таблице.

Символ	**Алиса**	**Боб**
00	`отправить 1`	`принять`
01	`принять`	`принять`
10	`принять`	`отправить 1`
11	`принять`	`принять`

После $n/2$ раундов Боб сообщает Алисе был ли тихий раунд с его входом 11, если был, то у Алисы был вход 01, 10 или 11 и их строки пересекаются (научились различать пары (01,11),(10,11),(11,11)). Алиса говорит был ли у нее раунд с ее входом 10 или 11, в который она получила 1, если был, то у Боба был вход 10, и их строки пересекаются (научились различать пару (10,10), (11,10)).

Осталось научиться различать пары (01,01), (11,01). Для этого Алисе надо отличать 0, полученные от Боба с входом 00, от нулей со входа 01.

Боб последовательно (начиная с его первого тихого раунда со входом 00 или 01) проходит по всем своим входам 00, 01, в которых он получал от Алисы 0. И отправляет Алисе 1, если был вход 00, и отправляет 0, если вход 01.

Все остальное аналогично случаю 1. Получаем $2 + n/2 + n/3 + 3 = 5n/6 + 5$ раундов. □

Лемма 2

Для функции DISJ в 1-прямоугольнике не больше одной пары $(x, \overline{x})$.

Доказательство. Пусть две пары $(x, \overline{x}), (y, \overline{y})$ и $x \neq y$, тогда в прямоугольнике есть и пары $(x, \overline{y}), (y, \overline{x})$ (подробнее [KN97]) и $x, \overline{y}$ или $y, \overline{x}$ пересекаются. □

Теорема 4

$\mathrm{D}_0^{\mathrm{hd}}(\mathrm{DISJ}) \geq n \log_3 2 > 0.63n$.

Доказательство. Пусть R_c — прямоугольник всех возможных входов и $\mu(R)$ — число пар $(x, \overline{x})$ в прямоугольнике R. Рассмотрим покрытие R_c множеством хороших прямоугольников: $R_{1*} = R_{11} \cup R_{1r}, R_{r1}, R_{rr}$. Тогда мера одного из хороших прямоугольников хотя бы $\mu(R_c)/3$, так как μ – полуаддитивная мера.

Применим теорему 1 для $\alpha = 1/3, \mu_r = 2^n, \mu_l = 1$. Получаем $\mathrm{D}_0^{\mathrm{hd}}(\mathrm{DISJ}) \geq \log_3 2^n = n \log_3 2$. □

Теорема 5

$\mathrm{D}_{\mathrm{s}}^{\mathrm{hd}}(\mathrm{DISJ}) \geq n \log_5 2 > 0.43n$.

Доказательство. $\mu(R)$ — число пар $(x, \overline{x})$ в прямоугольнике R. Рассмотрим покрытие R_c множеством хороших прямоугольников:$R_{0*} = R_{00} \cup R_{01} \cup R_{0r}, R_{1*} = R_{10} \cup R_{11} \cup R_{1r}$, и R_{r0}, R_{r1}, R_{rr}. Тогда мера одного из хороших прямоугольников хотя бы $\mu(R_c)/5$, так как μ – полуаддитивная мера.

Далее аналогично доказательству теоремы 4 для $\alpha = 1/5$, получаем $\mathrm{D}_{\mathrm{s}}^{\mathrm{hd}}(\mathrm{DISJ}) \geq \log_5 2^n = n \log_5 2$. □

Теорема 6

$\mathrm{D}_{\mathrm{a}}^{\mathrm{hd}}(\mathrm{DISJ}) \geq n \log_{2.5} 2 > 0.75n$.

Доказательство. $\mu(R)$ — число пар $(x, \overline{x})$ в прямоугольнике R. Рассмотрим покрытие R_c множеством хороших прямоугольников:$R_{spent} = R_{00} \cup R_{01} \cup R_{10} \cup R_{11}$, и

$$
\begin{aligned}
R_{\overline{11}} &= R_{00} \cup R_{0r} \cup R_{r0} \cup R_{rr}, \\
R_{\overline{01}} &= R_{10} \cup R_{1r} \cup R_{r0} \cup R_{rr}, \\
R_{\overline{10}} &= R_{01} \cup R_{0r} \cup R_{r1} \cup R_{rr}, \\
R_{\overline{00}} &= R_{11} \cup R_{1r} \cup R_{r1} \cup R_{rr},
\end{aligned}
$$

где Алиса не отправляла α и Боб не отправлял β.

Эти прямоугольники покрывают множество возможных входов дважды. Значит, мера одного из них хотя бы $2/5 \cdot \mu(R_c)$.

Далее аналогично доказательству теоремы 4 для $\alpha = 2/5$, получаем $D_a^{hd}(DISJ) \geq \log_{2.5} 2^n = n \log_{2.5} 2$. □

3.3 Оценки на игры Карчмера — Вигдорсона

В работе [Chi90] автор доказал верхние оценки на $KW_{\mathrm{MOD}p}$ для некоторых конкретных p, которые на данный момент являются наилучшими, а также в этой же работе получена общая оценка на $KW_{\mathrm{MOD}p}$ при произвольном p, но данная оценка с увеличением числа p становится хуже известной оценки на симметрические функции [BH96]. Мы рассмотрим сложность отношения Карчмера — Вигдерсона для MODp в полудуплексных моделях.

Определение 13

Отношение $KW_{\mathrm{MOD}p} = \{((x,y),i) \mid \mathrm{MOD}p(x) = 0, \mathrm{MOD}p(y) \neq 0, x_i \neq y_i\}$.

Теорема 7

$\mathrm{D}_0^{\mathrm{hd}}(KW_{\mathrm{MOD2}}) \geq 2\log_3 n$ и $\mathrm{D}_{\mathrm{s}}^{\mathrm{hd}}(KW_{\mathrm{MOD2}}) \geq 2\log_5 n$.

Доказательство. Начнем со сложности в модели с нулем. Рассмотрим протокол Алисы – троичное дерево. Пусть d – глубина дерева, r – минимальное количество одноцветных прямоугольников в покрытие $X \times Y$, тогда $r \leq$ количество листьев $\leq 3^d$. Из теоремы Храпченко [Khr71] знаем, что $r \geq n^2$, значит $d \geq \log_3 r \geq 2\log_3 n$ (аналогично для модели с тишиной). □

Теорема 8

$\mathrm{D}_0^{\mathrm{hd}}(KW_{\mathrm{MOD2}}) \leq 3\log_3 n$.

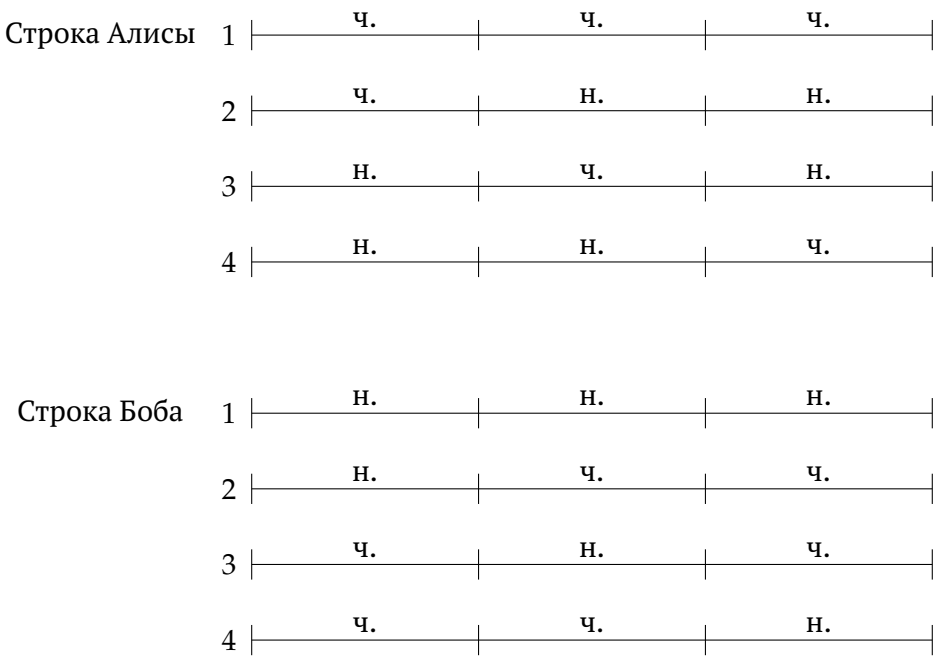

Рис. 1.

Доказательство. Игроки будут реализовывать троичный поиск. Алиса и Боб делят строки на три куска, возможны 4 случая (см. рис. 1, ч. – означает, что в куске длины $n/3$ чётное количество единиц, н. – нечётно).

В первом раунде Алиса и Боб отправляют 1, если у них 1 случай и молчат, иначе.

- Если оба игрока молчат, то оба знают, что у них не 1 случай. Дальше Алиса молчит, если у нее в первом куске н., иначе посылает 1. Боб молчит, если у него в первом куске ч., иначе посылает 1. Третий раунд аналогичный. Тогда, если второй раунд тихий, то в первом куске у них отличие и они идут в него, если третий раунд тихий, то во втором куске отличие и идут в него. Если не было тихих раундов, тогда отличие в третьем куске, так как обязательно есть кусок, где у Алисы н., а у Боба ч.
- Если кто-то из игроков отправил 1. Дальше Алиса молчит, если у нее в первом куске ч., иначе посылает 1. Боб молчит, если у него в первом куске н., иначе посылает 1. Третий раунд аналогичный. Тогда, если второй раунд тихий, то в первом куске у них отличие и они идут в него, если третий раунд тихий, то во втором куске отличие и идут в него. Если не было тихих раундов, тогда отличие в третьем куске, так как у Алисы или Боба первый случай, то обязательно есть кусок, где у Алисы ч., а у Боба н.

Таким образом, за три раунда игроки определили кусок, в котором отличие. Всего таких шагов будет не более $\log_3 n$. Значит, $\mathrm{D}_0^{\mathrm{hd}}(KW_{\mathrm{MOD2}}) \leq 3\log_3 n$. □

Теорема 9

$\mathrm{D}_{\mathrm{s}}^{\mathrm{hd}}(KW_{\mathrm{MOD3}}) \leq 1.89 \log n$.

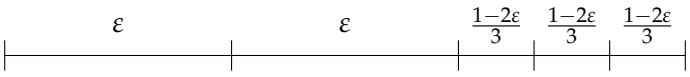

Рис. 2.

Доказательство. Разобьем входы Алисы и Боба, как на рис. 2 (отрезок – это строка из нулей и единиц).

1. Алиса молчит, если у нее в первом отрезке $\sum_{i=1}^{\varepsilon n} a_i \equiv 0 \pmod 3$.
2. Алиса отправляет 0, если у нее в первом отрезке $\sum_{i=1}^{\varepsilon n} a_i \equiv 1 \pmod 3$.
3. Алиса отправляет 1, если у нее в первом отрезке $\sum_{i=1}^{\varepsilon n} a_i \equiv 2 \pmod 3$.

Аналогично Алиса делает со вторым отрезком. Эти два раунда Боб принимает. Боб отправляет номер отрезка, в котором у них отличиие $\sum a_i \not\equiv \sum b_i \pmod 3$.

1. Боб отправляет 0, если отличие в первом отрезке.
2. Боб отправляет 1, если отличие во втором отрезке.
3. Боб молчит, иначе.

Во время раунда Боба, Алиса молчит. Если у Боба был случай 1 или 2, то они, соответственно, переходят в отрезок 1 или 2. Иначе Алиса отправляет остатки в отрезках 3 и 4 (в 5 отрезке Боб может узнать остаток сам, так как знает сумму остатков), и Боб, отправляет номер отрезка, в котором отличие, теперь они могут перейти к новому отрезку.

Оценим сложность. Получается система рекуррентных соотношений:

$$\begin{cases} T(n) = 2 + 1 + T(\varepsilon n) \\ T(n) = 3 + 2 + 1 + T(\frac{1-2\varepsilon}{3} n) \end{cases}$$

Здесь $T(n)$ — это количество отправленных битов.

$$\begin{cases} T(n) = 3 \log_{\frac{1}{\varepsilon}} n \\ T(n) = 6 \log_{\frac{3}{(1-2\varepsilon)}} n \end{cases} \quad \Longrightarrow \quad \frac{1}{2} = \frac{\log \varepsilon}{\log \frac{1-2\varepsilon}{3}}$$

Отсюда $\varepsilon = \frac{1}{3}$, следовательно $T(n) = 3 \log_3 n = 1.89 \log n$. □

Теорема 10

$\mathrm{D}_{\mathrm{s}}^{\mathrm{hd}}(KW_{\mathrm{MOD5}}) \leq 2.46 \log n$.

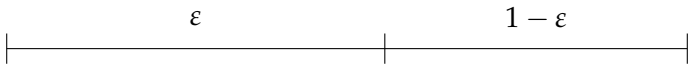

Рис. 3.

Доказательство. Рассмотрим следующий протокол, Алиса и Боб разбивают свои входы на два отрезка первый длины εn, второй $(1-\varepsilon)n$ (Рис. 3). Алиса отправляет остаток в первом отрезке ($\sum_{i=1}^{\varepsilon n} a_i \bmod 3$). Далее, каждый раунд игрок будет сообщать совпал ли у него остаток в соответствующем отрезке с прошлым игроком и остаток в следующем отрезке, к которому они переходят (более формально [Chi90]), согласно таблице 2 (код должен быть префиксным, чтобы каждый игрок знал сколько раундов нужно слушать). Пока один игрок передает сообщение, второй молчит. Переменная BALANCE говорит,

Таблица 2. Код для MOD5

BALANCE	Остаток	Сообщение
0	0	00
0	1	01
0	2	0s
0	3	10
0	4	11
1	0	s00
1	1	s01
1	2	s0s
1	3	s10
1	4	s11

равен ли остаток в отрезке, который отправил игрок (А. или Б.) на прошлом шаге, остатку в соответствующем отрезке у другого игрока.

Получаем систему рекуррентных соотношений:

$$\begin{cases} T(n) = 2 + T(\varepsilon n) \\ T(n) = 3 + T((1-\varepsilon)n) \end{cases}$$

$$\begin{cases} T(n) = 2\log_{\frac{1}{\varepsilon}} n \\ T(n) = 3\log_{\frac{1}{1-\varepsilon}} n \end{cases} \Longrightarrow \frac{2}{3} = \frac{\log \varepsilon}{\log(1-\varepsilon)}$$

Отсюда $\varepsilon = 0.57$, следовательно $T(n) = 2.466 \log n$. □

Теорема 11

$\mathrm{D}_{\mathrm{s}}^{\mathrm{hd}}(KW_{\mathrm{MOD11}}) \leq 3.48 \log n$.

Доказательство. Действуем аналогично теореме 10, согласно таблице 3.

Таблица 3. Код для MOD11

BALANCE	Остаток	Сообщение
0	0	000
0	1	001
⋮	⋮	⋮
0	10	101
1	0	s000
1	1	s001
⋮	⋮	⋮
1	10	s101

$$\begin{cases} T(n) = 3 + T(\varepsilon n) \\ T(n) = 4 + T((1-\varepsilon)n) \end{cases} \Longrightarrow \begin{cases} T(n) = 3\log_{\frac{1}{\varepsilon}} n \\ T(n) = 4\log_{\frac{1}{1-\varepsilon}} n \end{cases}$$

Отсюда $\frac{3}{4} = \frac{\log \varepsilon}{\log(1-\varepsilon)}$, следовательно $\varepsilon = 0.55$, значит $T(n) = 3.48 \log n$. □

Теорема 12 (Обобщение теорем 10,11)

Для любого n и p верно $\mathrm{D}_{\mathrm{s}}^{\mathrm{hd}}(KW_{\mathrm{MOD}p}) \leq \dfrac{1 + \lceil \log_3 \frac{p}{2} \rceil}{\log\left(\frac{2}{\sqrt{5}-1}\right)} \log n$.

Доказательство. Алгоритм аналогичен 10, нужен префиксный код для сообщений А. и Б. для MOD p.

- Если $BALANCE = 0$, то кодовое слово начинается с 0 или 1, а затем идут любые символы (s,0,1).
- Если $BALANCE = 1$, то кодовое слово начинается с s, а затем идут любые символы (s,0,1).

Длина кодовых слов при $BALANCE = 0$ равна $1 + \log_3 p/2$. При $BALANCE = 1$ длина равна $1 + \log_3 p$.

Таблица 4. Код для MODp

BALANCE	Остаток	Сообщение
0	`0`	`0...`
⋮	⋮	⋮
0	`p`	`1...`
1	`0`	`s...`
⋮	⋮	⋮
1	`p`	`s...`

$$\begin{cases} T(n) = 1 + \lceil \log_3 \frac{p}{2} \rceil + T(\varepsilon n) \\ T(n) = 1 + \lceil \log_3 p \rceil + T((1-\varepsilon)n) \end{cases} \implies \begin{cases} T(n) = (1 + \lceil \log_3 \frac{p}{2} \rceil) \log_{\frac{1}{\varepsilon}} n \\ T(n) = (1 + \lceil \log_3 p \rceil) \log_{\frac{1}{1-\varepsilon}} n \end{cases}$$

$$\frac{1 + \lceil \log_3 \frac{p}{2} \rceil}{1 + \lceil \log_3 p \rceil} = \frac{\log \varepsilon}{\log(1-\varepsilon)}$$

Заметим, что правая часть последнего уравнения уменьшается с ε, а левая часть увеличивается с p. Таким образом, легко видеть, что $\frac{1+\lceil \log_3 \frac{p}{2} \rceil}{1+\lceil \log_3 p \rceil} \in [\frac{1}{2}, 1)$, и таким образом $\varepsilon \in (\frac{1}{2}, \frac{\sqrt{5}-1}{2}]$. Следовательно, $T(n) \leq \dfrac{1 + \lceil \log_3 \frac{p}{2} \rceil}{\log \frac{2}{\sqrt{5}-1}} \log n$. □

Как получить нетривиальную верхнюю оценку на $KW_{\text{MOD}p}$ в модели с нулем остается открытым вопросом.

3.4 Оценки на функцию “больше”

По мотивам статьи [HIMS18b], где авторы рассмотрели полудуплексную сложность функции равенства EQ_n, мы рассмотрим сложность функции GT_n. Аналогично протоколам для EQ_n можно получить протоколы для GT_n.

Теорема 13

$\text{D}_{\text{s}}^{\text{hd}}(\text{GT}) \leq n/\log 5 + O(\log^2 n)$.

Доказательство. Алиса и Боб кодируют свои входы в пятеричной системе. Затем они последовательно обрабатывают свои входы по символам за $\lceil n/\log 5 \rceil$ раундов. В раунде i они обрабатывают символ i следующим образом.

Символ	Алиса	Боб
0	`отправить 0`	`принять`
1	`отправить 1`	`принять`
2	`принять`	`отправить 0`
3	`принять`	`отправить 1`
4	`принять`	`принять`

После этого Алисе и Бобу надо найти первый символ отличия или проверить что строки равны и выдать ответ 0.

Боб находит первый раунд, в котором он нашел отличие между их входами, т.е. если Боб с символом 4 получил от Алисы 0 или 1, если с символом 0 он получил от Алисы 1 или с символом 1 получил от Алисы 0, если с символом 0 или 1 тишина (у Алисы 2, 3 или 4).

Алиса находит первый раунд, в котором она нашла отличие между входами, т.е. если она с символом 4 получила от Боба 0 или 1, если она с символом 2 получила от Боба 1 или с символом 3 получила 0, если с символом 2 или 3 слышит тишину.

После этого Алиса отправляет свой первый раунд (если он был, иначе Боб), в котором было отличие, после этого Боб говорит у кого отличие раньше, и они обмениваются символами в этой позиции. Такими образом, мы нашли первую позицию, где символы Алисы и Боба отличаются, такие отличия обозначим $+$. Остается несколько отличий, которые мы не нашли, обозначим их $*$.

Алиса\Боб	0	1	2	3	4
0	$\cdot$	$+$	$*$	$*$	$+$
1	$+$	$\cdot$	$*$	$*$	$+$
2	$+$	$+$	$\cdot$	$+$	$+$
3	$+$	$+$	$+$	$\cdot$	$+$
4	$+$	$+$	$+$	$+$	$\cdot$

Для начала поймем есть ли $*$, т.е. надо узнать был ли потраченный раунд, Алиса отправляет сколько было раундов, где она принимала 0 или 1, Боб проверяет равно ли это числу раундов, где он отправлял, если равно, то потраченных раундов не было. Если не равно, то есть потраченный раунд и надо найти первый потраченных раунд, чтобы понять какое было отличие.

Найдем первый потраченный раунд двоичным поиском по раундам, Алиса отправляет сколько классических раундов у нее было в первой половине входной строки, Боб проверяет совпадает ли это с числом раундов в первой половине его входа, в которых он отправлял, если не совпадает, то игроки идут в первую половину входной строки, если совпадает идем во вторую половину входной строки. Так они найдут первый потраченный раунд, символ $*$ в табличке. На это понадобится $\log n \cdot \log n$ раундов.

В конце Алиса и Боб проверяют, в какой позиции было самое первое различие символов, и выясняют, у кого в этой позиции больше цифра. Игроки поняли у кого больше число и нашли ответ. Если Алиса и Боб не нашли отличие, значит их входы равны и ответ 0.

□

Теорема 14

$\mathrm{D}_0^{\mathrm{hd}}(\mathrm{GT}) \leq n/\log 3 + O(\log^2 n)$.

Доказательство. Аналогично теореме 13.

Алиса и Боб кодируют свои входы в троичной системе. Затем они последовательно обрабатывают свои входы по символам за $\lceil n/\log 3 \rceil$ раундов. В раунде i они обрабатывают символ i следующим образом.

Символ	**Алиса**	**Боб**
0	`принять`	`принять`
1	`отправить 1`	`принять`
2	`принять`	`отправить 1`

Далее Алиса и Боб ищут первый раунд, в котором нашли отличие. Получаем такую табличку, где $+$ то различие в символах, которое они уже нашли.

Алиса\Боб	0	1	2
0	$\cdot$	$+$	$+$
1	$+$	$\cdot$	$*$
2	$+$	$+$	$\cdot$

Алиса и Боб находят первый потраченный раунд и после узнают первый раунд, в котором было несовпадение символов, выясняют у кого было больше число. Если не было раунда, где символы не совпадают, то числа равны и ответ 0.

□

Теорема 15

- $D_s^{hd}(GT) \geq n/\log 5$,
- $D_0^{hd}(GT) \geq n/\log 3$.

Доказательство. Рассмотрим трудное множество $\{(x,x) \mid x \in \{0,1\}^n\}$ (подробнее смотреть в [KN97]). Никакие два элемента этого множества не лежат в одном 0-прямо-угольнике, иначе 0-прямоугольник содержит элементы $(x,x), (x',x'), (x,x')$, (x',x), но тогда $x' \geq x \geq x'$, и значит $x = x'$, противоречие. Следовательно, листьев не менее 2^n.

Дальше пользуемся тем, что протокол в случае модели с тишиной является пятеричным деревом, а в модели с нулем – троичным деревом. □

Теорема 16

$D_a^{hd}(GT) \geq n \log_{2.5} 2 > 0.75n$.

Доказательство. Рассмотрим меру $\mu(R)$, равную количеству пар (x,x) в прямоугольнике R. Рассмотрим покрытие R_c множеством хороших прямоугольников:$R_{spent} = R_{00} \cup R_{01} \cup R_{10} \cup R_{11}$, и

$$R_{\overline{11}} = R_{00} \cup R_{0r} \cup R_{r0} \cup R_{rr},$$
$$R_{\overline{01}} = R_{10} \cup R_{1r} \cup R_{r0} \cup R_{rr},$$
$$R_{\overline{10}} = R_{01} \cup R_{0r} \cup R_{r1} \cup R_{rr},$$
$$R_{\overline{00}} = R_{11} \cup R_{1r} \cup R_{r1} \cup R_{rr},$$

где Алиса не отправляла α и Боб не отправлял β. Эти прямоугольники покрывают множество возможных входов дважды. Значит, мера одного из них хотя бы $2/5 \cdot \mu(R_c)$. Далее применяем лемму 1 для $\alpha = 2/5$, получаем $D_a^{hd}(GT) \geq \log_{2.5} 2^n = n \log_{2.5} 2$. □

3.5 Недетерминированная полудуплексная сложность

Мы рассмотрим эквивалентные определения недетерминированной коммуникационной сложности в классической модели, подробнее можно посмотреть в [MS21].

Определение 14 (Классическое определение)

Функция $f : X \times Y \to \{0,1\}$ имеет *недетерминированный коммуникационный протокол* сложности d, если существуют две функции $A : X \times \{0,1\}^d \to \{0,1\}$ и $B : Y \times \{0,1\}^d \to \{0,1\}$, такие что

- $\forall (x,y) \in f^{-1}(1)\ \exists w \in \{0,1\}^d : A(x,w) = B(y,w) = 1$,
- $\forall (x,y) \in f^{-1}(0)\ \forall w \in \{0,1\}^d : A(x,w) = 0 \vee B(y,w) = 0$.

Недетерминированная коммуникационная сложность $\mathrm{N}(f)$ функции f — это минимальное d, для которого существует недетерминированный коммуникационный протокол для f сложности d.

Определение 15 (Альтернативное определение, [MS21, DIS+21, KN97])

Функция $f : X \times Y \to \{0,1\}$ имеет *приватный недетерминированный коммуникационный протокол* сложности d, если существуют функция $\tilde{f} : (X \times \{0,1\}^*) \times (Y \times \{0,1\}^*) \to \{0,1\}$ детерминированной коммуникационной сложности не более d, такая что

- $\forall (x,y) \in f^{-1}(1)\ \exists w_x, w_y \in \{0,1\}^* : \tilde{f}((x,w_x),(y,w_y)) = 1$,
- $\forall (x,y) \in f^{-1}(0)\ \forall w_x, w_y \in \{0,1\}^* : \tilde{f}((x,w_x),(y,w_y)) = 0$.

Приватная недетерминированная коммуникационная сложность $\mathrm{N}'(f)$ функции f — это минимальное d, для которого существует приватный недетерминированный коммуникационный протокол для f сложности d.

Мы рассмотрим определение 15 в полудуплексной модели коммуникации и покажем, что недетерминированная полудуплексная сложность неравносильна 14.

Определение 16

$\mathrm{N}_s^{hd}, \mathrm{N}_0^{hd}, \mathrm{N}_a^{hd}$ — недетерминированная полудуплексная сложность (в смысле определения 15) с полудуплексной коммуникацией с тишиной, нулем, противником, соответственно.

Теорема 17

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

- $\mathrm{N}_s^{hd}(f) \geq \mathrm{N}(f)/\log 5$,
- $\mathrm{N}_0^{hd}(f) \geq \mathrm{N}(f)/\log 3$,
- $\mathrm{N}_a^{hd}(f) \geq \mathrm{N}(f)/\log 3$.

Доказательство. В полудуплексной модели с тишиной протокол – это пара пятиричных деревьев. Покажем как получить из недетерминированного полудуплексного протокола Π получить классический. Алиса и Боб публично угадывают путь от корня к листу π_A в дереве Π, соответствующем Алисе. Алиса проверяет, что эта подсказка является действительно правильным путем для ее входа. Боб проверяет, что существует путь от корня к листу π_B в его дереве, который является допустимым для его входа, и также проверяет,

что π_B соответствует π_A (во всех раундах, где Алиса получала в π_A, Боб в π_B посылал тот же бит, что Алиса получила, и во всех раундах, где Алиса посылает, Боб получает соответствующий бит или посылает какой-то бит). Если Π имеет глубину d, то длина описания π_A — это $\lceil d \cdot \log 5 \rceil$.

Аналогично с полудуплексной моделью с нулем, протокол — пара троичных деревьев. Таким образом, существует классический недетерминированный протокол сложности $\lceil d \cdot \log 3 \rceil$.

В полудуплексной модели с противником, мы можем рассмотреть только протоколы, где в каждом тихом раунде игроки получают только 0. Тогда, мы получаем такую же оценку как в модели с нулем. □

Теорема 18

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

- $\mathrm{N}_s^{hd}(f) \leq \mathrm{N}(f)/\log 5 + O(\log \mathrm{N}(f))$,
- $\mathrm{N}_0^{hd}(f) \leq \mathrm{N}(f)/\log 3 + O(\log \mathrm{N}(f))$.

Доказательство. Для любого (классического) недетерминированного протокола, Алиса и Боб могут угадать общую подсказку w, затем проверить, что они взяли одинаковые подсказки. Для этого они решат задачу равенства на строках длины $\mathrm{N}(f)$ в модели с тишиной и нулем соответственно. Из верхней оценки на задачу равенства [HIMS18a], мы получаем нужную оценку. □

Таким образом, для моделей с тишиной и нулем мы получаем точные оценки, для модели с противником неизвестно нетривиальной оценки на EQ, если получить такую оценку, то сразу получается верхняя оценка на недетерминированную сложность с противником.

4 Сжатие протоколов

В этом разделе мы покажем, что можно адаптировать метод случайных ограничений для коммуникационных протоколов обобщенных игр Карчмера−−Вигдерсона. В статье [Hås98] анализируется ожидаемый размер формулы после того, как она была подвергнута случайному ограничению. Его результат позволяет показать лучшую нижнюю оценку на формульную сложность явной булевой функции. *Ограничение* для формулы на n переменных является элементом $\{0,1,*\}^n$. Для $p \in [0,1]$ случайное ограничение ρ из R_p выбирается тем, что мы случайным образом и независимо устанавливаем каждой переменной значение $*$ с вероятностью p и $0,1$ с равными вероятностями $\frac{1-p}{2}$. Интерпретация присвоения переменной значения $*$ заключается в том, что она остается переменной, в то время как в других случаях данная константа подставляется в качестве значения переменной в формулу. Основная теорема о сжатии [Hås98], теорема 7.1 ограничивает ожидаемый размер результирующей формулы.

Теорема 19 (Теорема 7.1 в [Hås98])

Пусть ϕ — формула размера L и ρ случайное ограничение из R_p. Тогда ожидаемый размер $\phi\restriction_\rho$ оценивается как

$$O\left(p^2(1+(\log(\min(1/p,L)))^{3/2})L+p\sqrt{L}\right).$$

Мы хотим показать, что точно такие же рассуждения могут быть применены к протоколу для обобщенного отношения Карчмера — Вигдерсона, и, следовательно, мы получим аналогичный результат.

Замечание. Обобщенная игра Карчмера — Вигдерсона для функции f представляет собой коммуникационную задачу с *обещанием*, что у игроков $f(x)\neq f(y)$. Поэтому возможно, что в протоколе для KW_f есть лист с пометкой i, такой, что для некоторой пары входов в этом листе $x_i=0$ и $y_i=1$, а для другой пары входов ситуация противоположная $x_i=1$ и $y_i=0$. Такого не бывает, если рассматривать коммуникационные задачи без обещания, так как в таком случае входы в вершинах протокола образуют комбинаторные прямоугольники. Каждый протокол для KW_f можно изменить таким образом, чтобы каждый лист с пометкой i содержал только входы одного из этих типов, в листе Алиса скажет чему равен x_i, значит размер протокола увеличится не более чем в два раза. Поэтому будем предполагать, что протоколы удовлетворяют этому условию.

Для обобщенных игр Карчмера—Вигдерсона мы можем синтаксически перевести протокол в формулу, но неясно, как полученная формула связана с функцией (с несколькими выводами) в протоколе. Поэтому нам надо проанализировать упрощения, использованные Хостадом. Он предлагает использовать следующие упрощения для формул после применения случайного ограничения.

1. Если одному входу в $\vee$-гейте ($\wedge$-гейте) присвоено значение 0 (значение 1), этот вход стирается и другой вход этого гейта занимает место выхода гейта.

2. Если одному входу в $\vee$-гейте ($\wedge$-гейте) присвоено значение 1 (значение 0), гейт заменяется на константу 1 (константу 0).

3. Если один вход $\vee$-гейта ($\wedge$-гейта) сводится к единственному литералу $x_i/\bar{x}_i$, то $x_i=0/x_i=1$ ($x_i=1/x_i=0$) подставляется в подформулу, дающую другой вход для этого гейта. Если возможно, то производятся дальнейшие упрощения в этой подформуле.

Покажем, что все эти упрощения формулы Де Моргана могут быть переформулированы в терминах соответствующего коммуникационного протокола для обобщенной игры Карчмера — Вигдерсона. Для этого определим случайное ограничение для протоколов.

Пусть $f:\{0,1\}^n\to\{0,1\}^m$ — неконстантная функция и Π — протокол для KW_f. *Ограничения* для протоколов — элемент $\{0,1,*\}^n$. Для $p\in[0,1]$ случайное ограничение ρ в R_p выбирается так, что мы случайно и независимо для каждого бита i оставляем его ($\rho(i)=*$) с вероятностью p и фиксируем бит i у Алисы и Боба равным 0 или 1 ($\rho(i)=0$ или $\rho(i)=1$) с вероятностью $\frac{1-p}{2}$.

После действия случайного ограничения, используются следующие правила упрощения:

1. Предположим, что $\rho(i)=1$, т.е. у Алисы и Боба i-ый бит равен 1. Рассмотрим лист l, помеченный значением i, и пусть в этом листе $a_i=0, b_i=1$ и этому листу соответствует прямоугольник $C\times B$. После ограничения ρ умирает часть Алисы C. Рассмот-

рим вершину v перед этим листом, она соответсвует Алисе или Бобу, рассмотрим два случая.

Пусть в вершине v ход Алисы, $A \times B$ прямоугольник, соответствующий этой вершине, тогда в вершине v происходит разделение по A. Тогда второму потомку вершины v соответствует прямоугольник $D \times B$. Так как умирает только часть Алисы A, то умирает только лист l, а лист v можно объединить со вторым потомком (Рис. 4).

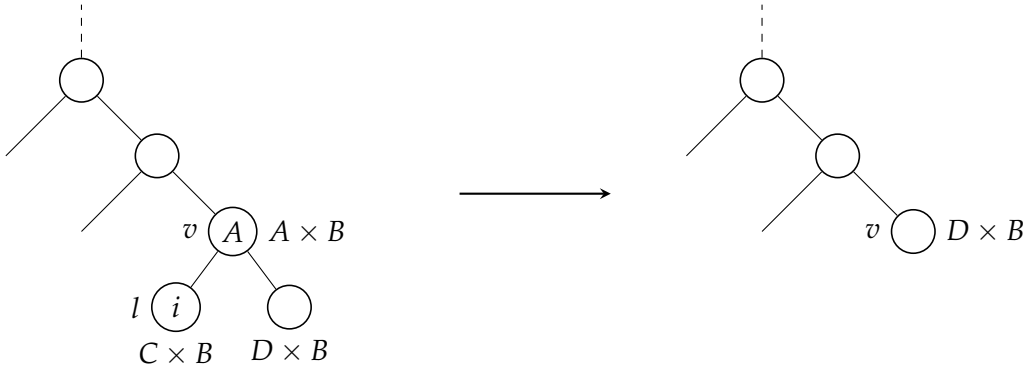

Рис. 4. Упрощение 1

2. Пусть в v ход Боба, $A \times B$ прямоугольник в вершине v, тогда происходит разделение по B и двум потомкам соответствуют прямоугольники $A \times C, A \times D$, тогда после ограничения умирают эти два листа и их предок, вершина v, т.к. у них у всех одна из сторон A. Эти три вершины удаляются, а вершины v_2, v_3 можно объединить в одну (Рис. 5).

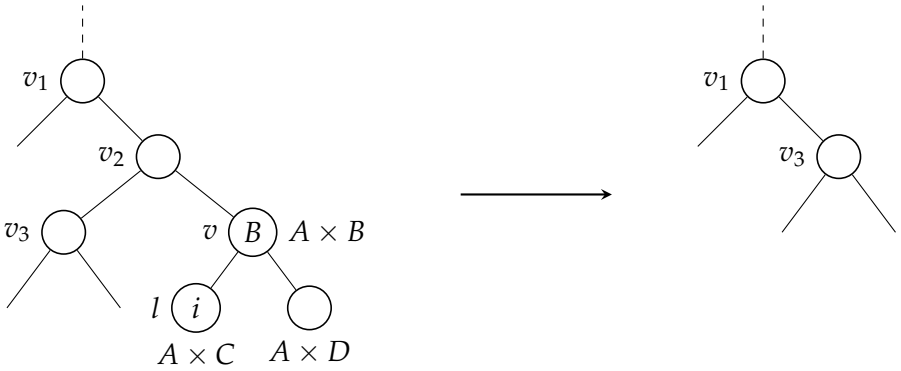

Рис. 5. Упрощение 2

3. Если какой-то подпротокол упростился до одного листа l, соответствующего значению i, и пусть в этом листе $a_i = 0, b_i = 1$. Рассмотрим v предка этого листа, пусть в вершине v ход Алисы и этой вершине соответсвует прямоугольник $A \times B$, у второго потомка v есть подпротокол Π'. Хотим упростить подпротокол Π', выкинув листы подпротокола Π' со значением i, и реализовать их с помощью листа l.

   Рассмотрим лист s с прямоугольником $C \times D$ подпротокола Π' со значением i, заметим, что листу l соответствует прямоугольник $A_2 \times B$ и второму потомку вершины v соответствует прямоугольник $A_1 \times B$, тогда в листе s написано $c_i = 0, d_i = 1$ (Рис. 6).

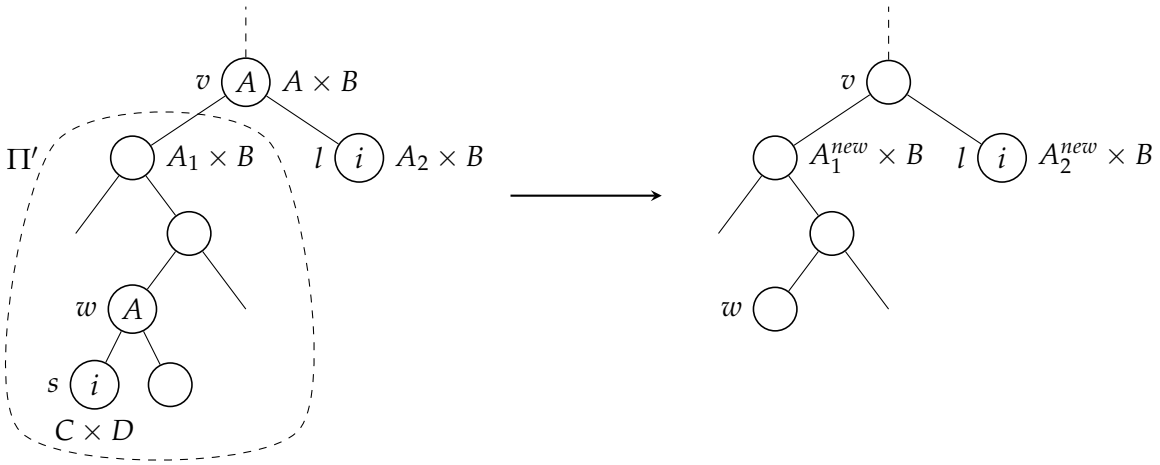

Рис. 6. Упрощение 3

Рассмотрим предка s — вершина w. Пусть в w ход Алисы. Тогда можно сделать ограничение “в i-ом бите у Алисы и Боба стоит 1” в подпротоколе Π', и рассмотреть новый протокол Π, в котором $A_1^{new} = A_1 \setminus C, A_2^{new} = A_2 \cup C$.

4. Пусть в вершине w ($C \times D$) ход Боба. Обозначим второго потомка w за w' с прямоугольником $C \times D_2$, заметим, что листу w' можно сопоставить ответ i, так как первая сторона прямоугольника $C \times D_2$ совпадает с первой стороной листа s и вторая сторона $D_2 \subseteq B$, то $c_i = 0, d_i = 1$. Аналогично с вершиной w. Тогда можно сделать ограничение “в i-ом бите у Алисы и Боба стоит 1” в подпротоколе Π', упростить подпротокол и рассмотреть новый протокол Π, в котором $A_1^{new} = A_1 \setminus C, A_2^{new} = A_2 \cup C$ (см. рис. 7).

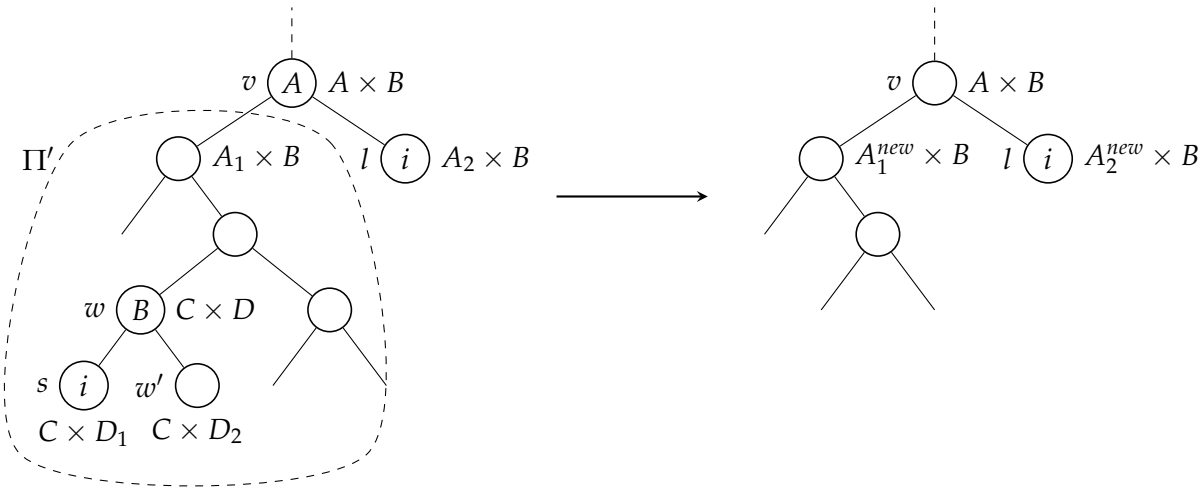

Рис. 7. Упрощение 4

Таким образом, с помощь данных упрощений (аналогичных упрощениям Хостада для формул, первое правило убивает хотя бы один лист, второе правило хотя бы два листа) и дальнешего доказательсва Хостада для формул [Hås98] получается доказать следующую теорему.

Теорема 20

Пусть Π протокол для обобщенного отношения Карчмера—Вигдерсона размера L и ρ случайное ограничение в R_p. Тогда ожидаемый размер протокола $\Pi\restriction_\rho$ оценивается как

$$O\left(p^2(1+(\log(\min(1/p,L)))^{3/2})L+p\sqrt{L}\right).$$

Данный результат находит применение при доказательстве суперкубической оценки на размер коммуникационного протокола обобщенных игр Карчмера—Вигдерсона некоторой явной булевой функции $f:\{0,1\}^n\to\{0,1\}^{\log n}$, подробнее в [IMS22].

5 Вычисления с оракулом

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 строки третьему игроку, Чарли, который сообщает в ответ, равны ли они. Будем обозначать за $\mathsf{P}^{\mathrm{EQ}}(f)$ 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], легко заметить, что $D(f)\geq\mathsf{P}^{\mathrm{EQ}}(f)$. Примером лучшего разделения может служить сама же задача EQ, $\mathsf{P}^{\mathrm{EQ}}(f)=1$, $D(f)=\Theta(n)$.

Интересным является вопрос о связи между $\mathsf{P}^{\mathrm{EQ}}(f)$ и $R(f)$, где $R(f)$ вероятностная коммуникационная сложность в модели с публичными случайными битами (по теореме Ньюмана сложность с публичными и приватными битами отличается не более чем на $\mathcal{O}(\log n)$, поэтому будем рассматривать только модель с публичными битами). Так как вероятностно EQ можно решить за константное число раундов, то верна следующая оценка $R(f)\leq\mathcal{O}(\mathsf{P}^{\mathrm{EQ}}(f))$. Можно было бы предположить, что есть какая-то обратная связь, т.е. каждая функция с небольшой вероятностной коммуникационной сложностью имеет небольшую коммуникационную сложность с оракулом равенства. Одним из примеров, который показывает, что это неверно, является задача расстояния Хэмминга с разрывом (GHD) [PSS14], это *частичная* функция, равная 1, если расстояние между x и y не меньше $\frac{2}{3}n$, и 0, если расстояние не более чем $\frac{1}{3}n$,

$$R(GHD)=\mathcal{O}(1),\quad \mathsf{P}^{\mathrm{EQ}}(GHD)=\Omega(n).$$

Из этого мы можем заключить, что такой связи между этими мерами сложности нет. Однако остается вопрос о связи для *всюду определенных* функций. В статье [CLV19] авторы показали, что для функции целочисленного внутреннего произведения достигается экспоненциальное разделение между вероятностной сложностью и сложностью с оракулом EQ.

Определение 17

Целочисленное внутренние произведение $IIP_{m,t}(x,y)=1$, тогда и только тогда, когда $\sum_{i=1}^{t}x_iy_i=0$, где $x,y\in[-M,M]^t$, $M=2^m$. Обозначим через IIP_t семейство функций $IIP_{m,t}$ с фиксированным $t=\mathcal{O}(1)$ и растущим m. Можно заметить, что входной размер $IIP_{m,t}$ равен $n=(m+1)t$.

Определение 18

Множество функций, которые могут быть вычислены с помощью некоторого протокола в модели с оракулом EQ за $\mathrm{polylog}(n)$ бит, называется P^{EQ}. Множество функций, которые имеют вероятностные протоколы сложности $\mathrm{polylog}(n)$, называется BPP.

Теорема 21 ([CLV19])

Для любого $t \geq 6$ всюду определенная функция IIP_t на n битах может быть вычислена с помощью $\mathcal{O}(\log n)$ бит рандомизированной коммуникации, но для решения с помощью протоколов в модели P^{EQ} требуется $\Omega(n)$ бит.

Как только стало ясно, что EQ недостаточно для моделирования BPP, потому что P^{EQ} не может эффективно решать IIP, следующим естественным кандидатом на оракул A, таким что $\mathsf{P}^A = \mathsf{BPP}$, стала сама функция IIP. Однако в работе [CLV19] также показали, что для любого фиксированного t оракула IIP_t недостаточно для моделирования BPP, и фактически классы сложности, определенные оракулами IIP, образуют строгую бесконечную иерархию.

Теорема 22 ([CLV19])

Существует бесконечная последовательность $(t_i)_{i\in\mathbb{N}}$, такая что

$$\mathsf{P} \subsetneq \mathsf{P}^{\mathrm{EQ}} \subsetneq \mathsf{P}^{IIP_{t_1}} \subsetneq \cdots \subsetneq \mathsf{P}^{IIP_{t_i}} \subsetneq \cdots \subsetneq \mathsf{BPP}\,.$$

Определение 19

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

Последним примером о связи между $R(f)$ и $\mathsf{P}^{\mathrm{EQ}}(f)$ может служить функция точного расстояния Хэмминга. В неопубликованной работе [SM19] авторы показали, что

$$R(\mathrm{EHD}_1) = \mathcal{O}(1), \quad \mathsf{P}^{\mathrm{EQ}}(\mathrm{EHD}_1) = \Theta(\log n).$$

Из приведенных выше примеров мы знаем, что не существует субэкспоненциальной симуляции вида $\mathsf{P}^{\mathrm{EQ}}(f) = o(2^{R(f)}) + o(n)$ для любой функции f. Кроме того, нет симуляции вида $\mathsf{P}^{\mathrm{EQ}}(f) \leq S(R(f))$ для любой функции f и некоторой функции $S : \mathbb{N} \to \mathbb{N}$. При этом все ещё теоретически возможно, что существует симуляция вида $\mathsf{P}^{\mathrm{EQ}}(f) = 2^{R(f)} + \log n$ для любого f. Доказать или опровегнуть существование такой симуляции является интересным открытым вопросом.

В данной главе мы рассмотрим коммуникационную сложность с оракулом EHD_k и докажем некоторые оценки на EHD_ℓ для $\ell \geq k$. Мы бы хотели показать, что на вычисление EHD_k с оракулом EHD_ℓ при константных k и ℓ требуется $\Omega(\log n)$ раундов коммуникации. Учитывая, что EHD_k вероятностно можно решить за $O(1)$, из этой оценки мы получили бы возрастающую последовательность $(k_i)_{i\in\mathbb{N}}$, такую что для решения задачи $\mathrm{EHD}_{k_{i+1}}$ с оракулом EHD_{k_i} требуется $\Omega(\log n)$ бит. У нас же получится доказать лишь константную оценку при константных k и ℓ. Кроме того, докажем оценки на коммуникационную сложностью с оркулом EQ_1.

5.1 Формальная модель

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 P^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. $\mathsf{P}^A(f)$ — это минимальная сложность по всем протоколам для функции f.

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. Различных разбиений может быть много, поэтому мы будем выбирать разбиение, минимизирующее выбранную меру.

Протокол в модели P^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 $g_1, g_2 : \{0,1\}^n \to \{0,1\}^m$, $m \leq n$).

5.2 Оракул единичного расстояния Хэмминга

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

Лемма 3

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

Доказательство. Матрица оракула EQ получается из матрицы EQ удалением, дублированием и перестановкой строк и столбцов. Сначала можно применить преобразования, связанные со строками, а потом со столбцами. Таким образом, M является матрицей, у которой блоки единиц не пересекаются по сторонам, сделав перестановку строк и столбцов, матрицу M можно преобразовать в матрицу, у которой из левого верхнего угла идет блочная диагональ из единиц и нулей, а оставшаяся часть матрицы заполнена нулями.

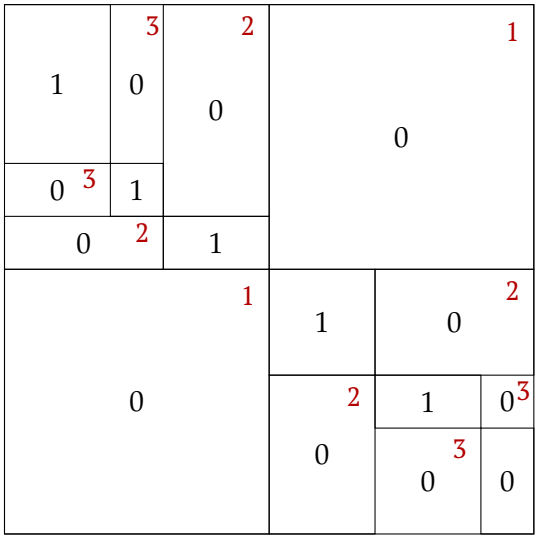

Рис. 8. Матрица оракула EQ.

Рассмотрим разбиение, состоящее из 1-прямоугольников и 0-прямоугольников на блочной диагонали. Суммарный периметр этих прямоугольников равняется $a+b$. Оставшиеся нули разбиваем на 0-прямоугольники так, как показано на рисунке 8, т.е. проводим вертикальную и горизонтальную прямую, разделяющую блочную диагональ на две части с равным числом блоков, рекурсивно проделываем данную операцию с двумя подматрицами, содержащими часть блочной диагонали, i-набором назовем набор, полученный на i уровне рекурсии. Получается $\log(\min(a,b))$ наборов, так как количество наборов не превосходит логарифма от количества блоков на диагонали. Каждый i-набор прямоугольников является непересекающимся по сторонам, а значит сумма периметров прямоугольников из i-набора не больше, чем $a+b$. Получаем разбиение $\mathcal{R}$ такое, что $\sum_{R_i}(|A_i|+|B_i|) \leq (a+b)\log(a+b)+(a+b) \leq 2(a+b)\log(a+b)$. □

Лемма 4

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

Доказательство. Для начала заметим, что матрица функции EHD_1^n состоит из 4 подматриц (Рис. 9): двух матриц EQ^{n-1} и двух матриц EHD_1^{n-1}. Далее каждую из подматриц EHD_1^{n-1} можно аналогично разбить на 4 матрицы. Таких шагов разбиения ровно $\log(2^n) = n$.

Тогда несложно понять, что матрица оракула EHD_1 выглядит как матрица, составленная из 4 подматриц оракулов (двух матриц оракула EQ и двух матриц оракула EHD_1). Аналогично, оставшиеся подматрицы оракула EHD_1 можно разбить на матрицы оракула EQ и EHD_1, пока не дойдем до одноцветных прямоугольников. Число шагов таких разбиений не больше чем число шагов для матрицы функции EHD_1^m, где $m \leq n$, так как матрица оракула была получена из нее дублированием и удалением строк, а следовательно эти действия не увеличивали число шагов разбиения. Таким образом, число шагов разбиения не более n.

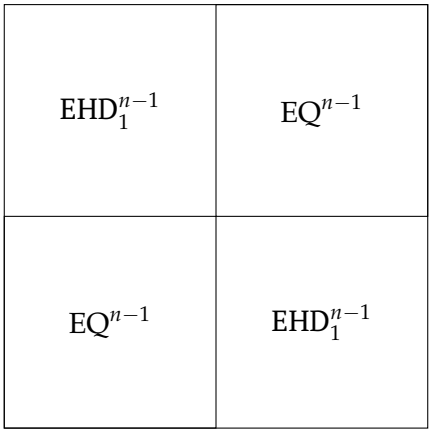

Рис. 9. Матрица EHD_1.

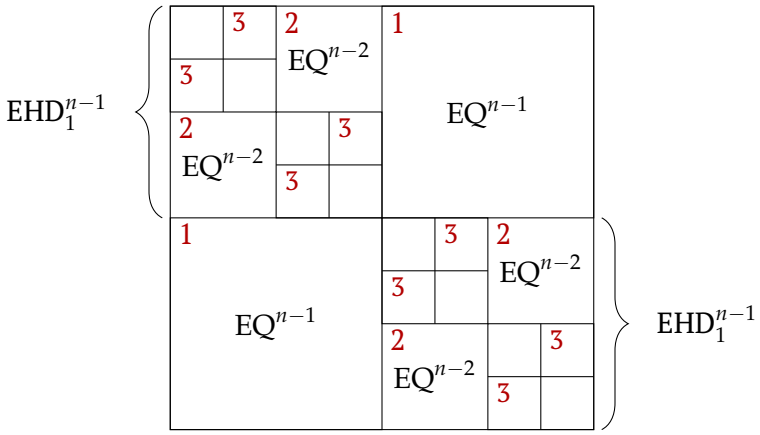

Рис. 10. Матрица EHD_1.

Пусть M — матрица оракула EHD_1 размера $a \times b$. Все матрицы оракула EQ, полученные на i-шаге разбиения, обозначим за i-набор матриц оракула EQ. Заметим, что матрицы из i-набора матриц оракула EQ попарно не пересекаются по сторонам. Воспользуемся леммой 3 для каждой матрицы из i-набора и получим разбиение на одноцветные прямоугольники i-набора, для которого верно

$$\sum_{R_k} |A_k| + |B_k| \leq \sum 2(a_j + b_j)\log(a_j + b_j)$$
$$\leq \sum 2(a_j + b_j)\log(a + b) \leq 2(a + b)\log(a + b),$$

где R_k – одноцветные прямоугольники, $a_j \times b_j$ – размеры матриц оракула EQ из i-набора. Следовательно, для любой матрицы M оракула EHD_1 верно $p(M) \leq 2n \cdot (a + b)\log(a + b)$.

Предположим, что мы имеем разбиение $\mathcal{R} = \bigcup R_i$, $R_i = A_i \times B_i$ исходной матрицы M_f, следующее разбиение мы получаем применением оракула к каждому из прямоугольников разбиения $\mathcal{R}$. Мы покажем, что существует разбиение $\mathcal{R}'$, полученное из $\mathcal{R}$, для которого

$$p(\mathcal{R}') \leq 2n^2 \cdot p(\mathcal{R}).$$

Рассмотрим M_i матрицы оракула EHD_1 для прямоугольников R_i из разбиения $\mathcal{R}$, они имееют те же размеры, что и прямоугольники R_i. Тогда существуют такие разбиения

матриц M_i оракула EHD_1 на одноцветные прямоугольники, что

$$p(\mathcal{R}') \le \sum_{R_i \in \mathcal{R}} p(M_i) \le \sum_{R_i \in \mathcal{R}} 2n(|A_i| + |B_i|)\log(|A_i| + |B_i|)$$
$$\le 2n^2 \sum_{R_i \in \mathcal{R}} |A_i| + |B_i| = 2n^2 \cdot p(\mathcal{R}).$$

Пусть $\mathcal{R}_0, \ldots, \mathcal{R}_C$ обозначают промежуточные разбиения, соответствующие протоколу, т.е. $\mathcal{R}_i$ – разбиение, полученное после i вызовов оракула EHD_1. Тогда $\mathcal{R}_0$ – изначальный прямоугольник размера $2^n \times 2^n$, $\mathcal{R}_C$ – разбиение на одноцветные прямоугольники матрицы M_f. Таким образом, $p(\mathcal{R}_0) = 2^{n+1}$ и $p(\mathcal{R}_i) \le 2n^2 \cdot p(\mathcal{R}_{i-1})$ для $i = 1, \ldots, C$, значит $p(\mathcal{R}_C) \le 2^{n+1}(2n^2)^C$. □

Теперь нам нужна оценка на размер одноцветных прямоугольников матрицы EHD_k, в случае константного k мы докажем лемму 5. Будем доказывать двойной индукцией по параметру функции k и размеру входа n.

Лемма 5

Для любого 1-прямоугольника R матрицы EHD_k верно $|R| \le c_k n^k$, где c_k — константа, зависящая от k.

Доказательство. Внешняя индукция по k. Проверим базу для $k = 1$ и $k = 2$. Докажем, что в матрице EHD_1^n есть только 1-прямоугольники размера $1 \times b$, где $b \le n$, и прямоугольники размера 2×2.

1. $k = 1$. Индукция по n (размеру входных строк). База $n = 2$: очевидно. Переход от n к $n+1$. Рассмотрим матрицу EHD_1^{n+1}. Она состоит из 4 подматриц. Размеры 1-прямоугольников, которые лежат полностью в одной строке или столбце, равны $1 \times b$, где $b \le n+1$. В подматрицах EHD_1^n размеры 1-прямоугольников, которые имеют две стороны отличные от 1, равны 2×2, но эти 1-прямоугольники нельзя дополнить до больших, так как в левом нижнем и правом верхнем углу стоят матрицы EQ^n, у которых 1 стоят только на диагонали.

2. $k = 2$. Покажем, что для матрицы EHD_2^n есть только 1-прямоугольники размера $a \times b$, где $ab \le c_2 n^2$. Индукция по n. База $n = 2$: очевидно. Переход от n к $n+1$: Рассмотрим матрицу EHD_2^{n+1}, она состоит из 4 подматриц (двух матриц EHD_2^n и двух EHD_1^n). Несложно убедиться, что если 1-прямоугольник матрицы EHD_2^{n+1} состоит из двух прямоугольников размера $x \times y$, $a \times b$ из подматриц EHD_1^n, тогда в прямоугольник входит два прямоугольника размера $x \times b$ и $a \times y$ из подматриц EHD_2^n, и один из прямоугольников в какой-то подматрице EHD_2^n имеет площадь не более чем $\max(ab, xy)$. Пусть это не так, тогда размер прямоугольников $x \times b$ и $a \times y$ из подматриц EHD_2^n больше чем размер прямоугольников из подматриц EHD_1^n, т.е. $xb > \max(ab, xy)$ и $ay > \max(ab, xy)$, следовательно, $xb > ab$ и $ay > xy$, а значит $x > a$ и $a > x$, противоречие.

   Размер прямоугольников в подматрицах EHD_1^n ограничен n. Во второй матрице EHD_2^n размер 1-прямоугольника по индукционному предположению меньше чем cn^2. Тогда размер максимального 1-прямоугольника в EHD_2^n можно оценить как

$$3n + c_2 n^2 \le c_2(n+1)^2 = c_2 n^2 + 2c_2 n + c_2,$$

   при $c_2 \ge 2$.

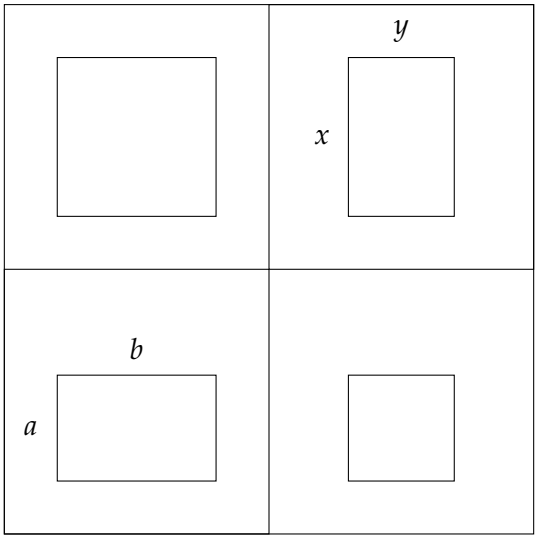

Рис. 11. Матрица EHD_{k+1}^{n+1}

3. Переход от k к $k+1$: Индукция по n. База $n = k+1$: очевидно. Переход от n к $n+1$: Рассмотрим матрицу EHD_{k+1}^{n+1}, она состоит из 4 подматриц: двух матриц EHD_{k+1}^{n} и двух EHD_{k}^{n}. Несложно убедиться, что если 1-прямоугольник матрицы EHD_{k+1}^{n+1} состоит из двух прямоугольников размера $x \times y$, $a \times b$ из подматриц EHD_{k}^{n}, то один из прямоугольников в какой-то подматрице EHD_{k+1}^{n} имеет площадь не более чем $\max(ab, xy)$.

   Размер прямоугольников в подматрицах EHD_{k}^{n} не более чем $c_k n^k$. Во второй подматрице EHD_{k+1}^{n} размер 1-прямоугольника по индукционному предположению меньше чем $c_{k+1} n^{k+1}$. Тогда размер максимального 1-прямоугольника в EHD_{k+1}^{n+1} можно оценить как

$$3c_k n^k + c_{k+1} n^{k+1} \leq c_{k+1}(n+1)^{k+1} = c_{k+1} n^{k+1} + c_{k+1}(k+1) n^k + \ldots + c_{k+1},$$

   при $c_{k+1} \geq 3c_k/(k+1)$.

Можно заметить, что в качестве коэффициента c_k можно взять 2 для любого k. □

Теорема 23

Коммуникационная сложность EHD_k в $\mathrm{P}^{\mathrm{EHD}_1}$ не менее $\frac{k}{5}$.

Доказательство. Пусть $\mathcal{R}$ является разбиение $\mathrm{EHD}_1^{-1}(1)$ на прямоугольники $R_i = A_i \times B_i$, которое минимизирует $p(\mathcal{R})$. По неравенству о среднем

$$p(\mathcal{R}) = \sum_{R_i \in \mathcal{R}} |A_i| + |B_i| \geq 2 \sum_{R_i \in \mathcal{R}} \sqrt{|A_i||B_i|}.$$

Обозначим за $s_i = |A_i||B_i|/2^{2n}$ нормированную площадь прямоугольника R_i. Тогда правую часть неравенства можно переписать, как

$$2^{n+1} \sum_{R_i \in \mathcal{R}} \sqrt{s_i}.$$

Пусть все s_i нормированные площади прямоугольников меньше чем β, а α — это нормированное количество единиц в матрице EHD_k, т.е. $\alpha = 2^n\binom{n}{k}/2^{2n} = \binom{n}{k}/2^n$, для фиксированного x есть ровно $\binom{n}{k}$ вариантов y, которые отличаются в k позициях. Тогда мы хотим минимизировать выражение

$$2^{n+1} \min_{\substack{\sum_i s_i = \alpha \\ 0 \le s_i \le \beta}} \sum_i \sqrt{s_i}.$$

Получаем вогнутую функцию над выпуклым многоугольником, которая минимизируется в вершине, т.е. в любой точке с $\lfloor \alpha/\beta \rfloor$ координатами, равными β, и одной координатой, равной $\alpha - \lfloor \alpha/\beta \rfloor \beta$, а остальные координаты равны 0. Следовательно,

$$p(\mathcal{R}) \ge 2^{n+1}\alpha/\sqrt{\beta}.$$

Из леммы 5 следует, что $\beta = c_k n^k/2^{2n}$. Если функция EHD_k имела протокол сложности C в $\mathrm{P}^{\mathrm{EHD}_1}$, то по лемме 4 существует разбиение $\mathcal{R}'$ такое, что

$$p(\mathcal{R}') \le 2^{n+1}(2n^2)^C.$$

Получаем, что

$$(2n^2)^C \ge \frac{\binom{n}{k}}{\sqrt{c_k n^k}} \ge \frac{n^k}{2^k k!} \cdot \frac{1}{\sqrt{c_k n^k}},$$

Прологарифмируем неравенство и получим

$$C \ge \frac{k/2\log(n)}{\log(2n^2)} - \frac{\mathcal{O}(1)}{\log(2n^2)} \implies C \ge \frac{k/2\log n}{2\log(n)+1} \ge k/5,$$

при достаточно больших n. □

5.3 Оракул точного расстояния Хэмминга равного ℓ

Лемма 6

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

Доказательство. Покажем, что для матрицы M оракула EHD_ℓ размера $a \times b$ выполнено неравенство $p(M) \le 2n^\ell \cdot (a+b)\log(a+b)$. Индукция по ℓ. База $\ell = 1$: проверили в лемме 4.

Переход от ℓ к $\ell+1$: матрица оракула $\mathrm{EHD}_{\ell+1}$ состоит из 4 подматриц оракулов (двух матриц оракула EHD_ℓ и двух матриц оракула $\mathrm{EHD}_{\ell+1}$). Аналогично, оставшиеся подматрицы оракула $\mathrm{EHD}_{\ell+1}$ можно разбить на матрицы оракула EHD_ℓ и $\mathrm{EHD}_{\ell+1}$, пока не дойдем до одноцветных прямоугольников. Число шагов таких разбиений не больше чем число шагов для матрицы функции $\mathrm{EHD}^m_{\ell+1}$, где $m \le n$, так как матрица оракула была получена из нее дублированием и удалением строк, а следовательно эти действия не увеличивали число шагов разбиения. Таким образом, число шагов разбиения не более n.

Все матрицы оракула EHD_ℓ, полученные на шаге разбиения i, обозначим за i-набор матриц оракула EHD_ℓ. Заметим, что матрицы из i-набора матриц оракула EHD_ℓ попарно

не пересекаются по сторонам, воспользуемся индукционным предположением для каждой матрицы из i-набора, тогда получаем разбиение на одноцветные прямоугольники i-набора, для которого верно

$$\sum_{R_k} |A_k| + |B_k| \le \sum 2n^\ell (a_j + b_j) \log(a_j + b_j)$$
$$\le \sum 2n^\ell (a_j + b_j) \log(a + b) \le 2n^\ell (a + b) \log(a + b),$$

где R_k – одноцветные прямоугольники, $a_j \times b_j$ – размеры матриц оракула EHD_ℓ из i-набора. Следовательно, для любой матрицы M оракула $\mathrm{EHD}_{\ell+1}$ верно $p(M) \le 2n^{\ell+1} \cdot (a + b) \log(a + b)$. Конец доказательства аналогичен доказательству леммы 4. □

Теорема 24

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

Доказательство. Аналогичено доказательству теоремы 23. Получаем неравенство

$$(2n^{\ell+1})^C \ge \frac{\binom{n}{k}}{\sqrt{c_k n^k}} \ge \frac{n^k}{2^k k!} \cdot \frac{1}{\sqrt{c_k n^k}},$$

Прологарифмируем неравенство и получим

$$C \ge \frac{k/2 \log(n)}{\log(2n^{\ell+1})} - \frac{\mathcal{O}(1)}{\log(2n^{\ell+1})} \implies C \ge \frac{k/2 \log n}{(\ell+1)\log(n) + 1} \ge \frac{k}{2(\ell+2)},$$

при достаточно больших n. □

5.4 Верхняя оценка

Определение 20

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

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

Несложно понять, что используя оракул $\mathrm{HD}_{\le \ell}$ как EQ задача $\mathrm{HD}_{\le k}$ 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 $\mathrm{HD}_{\le k}$ с оракулом $\mathrm{HD}_{\le \ell}$ получается доказать более точную верхнюю оценку.

Теорема 25

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

Доказательство. Разделим входы игроков пополам и запустим на каждой половине оракул $\mathrm{HD}_{\le \ell}$. Если в какой-то из половин у игроков оказалось не больше чем ℓ отличий, то за $\log \ell$ раундов игроки смогут найти точное количество отличий, используя оракул $\mathrm{HD}_{\le l}$ как оракул $\mathrm{HD}_{\le j}$ (можно добавить ложные биты к входу), где $j \le \ell$, и двоичный поиск,

после нахождения количества отличий игроки могут убрать данные подстроки из рассмотрения и запомнить найденное число отличий. Алиса и Боб продолжают делить все подстроки, которые остаются на рассмотрении, пополам и проделывать шаги с первого этапа.

Несложно заметить, что если на рассмотрении у Алисы и Боба остается более чем k/ℓ подстрок, то изначальные строки имели более чем k отличий, и ответ 0. Таким образом, на рассмотрении у игроков не более чем k/ℓ отрезков, иначе бы они уже решили задачу. На каждом шаге они тратят не более чем $2 \cdot \frac{k}{\ell} \cdot \log \ell$ раундов коммуникации. □

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 $\mathrm{P}^{\mathrm{EQ}^1}(KW_f) \leq D(f)$.

Рассмотрим сложность булевых функций от $2n$ бит с разделенным входом для Алисы и Боба.

Теорема 26

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

Доказательство. Оценим количество протоколов с оракулом EQ^1 глубины не более d. Для начала, количество различных деревьев можно оценить по формуле Кэли как $(2s)^{2s-2} \leq 2^{4s \log s}$, где s — размер протокола с глубиной не более d, $s \leq 4^d$, так как каждый раунд в модели с оракулом EQ^1 происходит разделение на не более чем четыре подпрямоугольника.

Оценим количество функций, которые можно расставить в вершины протокола. В корне находятся $f_a : \{0,1\}^n \to \{0,1\}$ и $g_b : \{0,1\}^n \to \{0,1\}$, получаем $(2^{2^n})^2$ вариантов расставить функции в корне. На глубине 2 изначальный прямоугольник $A \times B$ делится на не более чем четыре подпрямоугольника (в случае если он делится на два подпрямоугольника, вариантов будет меньше). Пусть прямоугольник разделился на подрямоугольники $A_1 \times B_1, A_1 \times B_2, A_2 \times B_1, A_2 \times B_2$. Тогда на глубине 2 в вершине с подрямоугольником $A_i \times B_j$ нужно выбрать функцию из A_i в $\{0,1\}$ для Алисы и функцию из B_j в $\{0,1\}$ для Боба. Для этого есть $2^{|A_i|} \cdot 2^{|B_j|}$ вариантов. Значит на глубине 2 не более чем $2^{2|A_1|+2|A_2|} \cdot 2^{2|B_1|+2|B_2|} = 2^{2|A|+2|B|} = (2^{2^n})^4$ вариантов расставить функции. Таким образом, на глубине i не более чем $(2^{2^n})^{2^i}$ вариантов расставить функции. Тогда всего вариантова расставить функции не более чем $2^{2 \cdot 2^n \cdot (1+2+\cdots+2^d)} = 2^{2 \cdot 2^n \cdot (2^{d+1}-1)}$.

Следовательно, всего протоколов глубины не более d менее

$$2^{4s\log s}\cdot 2^{2\cdot 2^n\cdot(2^{d+1}-1)} \le 2^{4\cdot 4^d\cdot 2d}\cdot 2^{2\cdot 2^n\cdot(2^{d+1}-1)}.$$

Выберем $d = n - \log n$. Тогда оценку можно переписать как

$$2^{8\frac{4^n}{n^2}\cdot(n-\log n)}\cdot 2^{2^n\cdot 2^n/n} \le 2^{8\cdot 4^n/n}\cdot 2^{2\cdot 4^n/n}.$$

Так как всего различных функций $2^{2^{2n}}$, то вероятность того, что функция f имеет протокол глубины меньше чем d, оценивается как

$$\Pr[\mathrm{P}^{\mathrm{EQ}^1}(f)\le d] \le \frac{2^{8\cdot 4^n/n}\cdot 2^{2\cdot 4^n/n}}{2^{4^n}} = 2^{4^n(10/n-1)} < 1.$$

□

Утверждение 7

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

Доказательство. **Верхняя оценка.** В первый раунд Алиса посылает в оракул первый бит своей строки a_1, а Боб посылает последний бит своей строки b_n. На шаге номер i Алиса отправляет оракулу бит a_i, а Боб отправляет бит b_{n-i+1}, где $1 \le i \le n/2$. После этих раундов Алиса будет знать вторую половину строки Боба, а Боб будет знать первую половину строки Алисы. Далее Алиса посылает 1 в оракул, если вторая половина ее строки совпадает с второй половиной строки Боба, и 0, иначе. Боб делает аналогично с первой половиной строк. Если отправленные биты не равны, то осталось проверить, что в одной половине отличие только в одном бите. Иначе или нет отличий, или более одного.

Нижняя оценка. Рассмотрим меру $\mu(R)$, равную количеству единиц в прямоугольнике R для матрицы EHD_1. В изначальной матрице EHD_1 всего $n\cdot 2^n$. Каждый раунд исходный прямоугольник делится на 4 подпрямоугольника (или меньше), значит найдется подпрямоугольник, в котором $\mu(R') \ge \frac{\mu(R)}{4}$. Так как по лемме 5 для матрицы EHD_1 размер любого 1-прямоугольника не более n, то получаем $\mathrm{P}^{\mathrm{EQ}^1}(\mathrm{EHD}_1) \ge n/2$.

□

Утверждение 8

Для любой функции f верно $\mathrm{P}^{\mathrm{EQ}^1}(f) \le \mathrm{D}_0^{\mathrm{hd}}(f) \le \mathrm{D}_{\mathrm{a}}^{\mathrm{hd}}(f)$.

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 1

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

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 EQ в модели с тишиной сложность равна $n/\log 5 + o(n)$, с другой стороны в модели с оракулом EQ^1 сложность равна $n/2 + O(1)$.

6 Заключение

В данной работе мы исследовали коммуникационную сложность булевых функций и отношений Карчмера — Вигдерсона. В главе 3 было доказано несколько оценок в полудуплексной модели на DISJ, GT, $KW_{\mathrm{MOD}p}$, показали связь между полудуплексной недетерминированной сложностью и классической недетерминированной сложностью.

В главе 4 мы показали как адаптировать технику случайных ограничений Хостада на обобщенные игры Карчмера — Вигдерсона. В главе 5 доказали оценки на коммуникационную сложность EHD_k с оракулом EHD_ℓ. Кроме того, рассмотрели вычисления с оракулом EQ^1, показали, что случайная функция с вероятностью близкой к единице имеет сложность $n - o(n)$. Из этого мы поняли, что сложность случайной функции в полудуплексной модели с нулем и противником равна $n - o(n)$.

Направления для дальнейших исследований. Рассмотрим несколько открытых задач, возникших по результатам данной работы.

1. Докажите точную оценку на DISJ в полудуплексной модели с нулем.
2. Докажите точную оценку на EHD_k с оракулом EHD_ℓ при константных k и ℓ.
3. Покажите оценку на сложность случайной функции в полудуплексной модели с тишиной.
4. Приведите пример явной функции со сложностью $n - o(n)$ в модели с оракулом EQ^1.
5. Установите нетривиальную связь между $\mathrm{D}_{\mathrm{s}}^{\mathrm{hd}}(f)$ и $\mathrm{P}^{\mathrm{EQ}^1}(f)$ для любой функции f, например, докажите, что $\mathrm{D}_{\mathrm{s}}^{\mathrm{hd}}(f) \leq \mathrm{P}^{\mathrm{EQ}^1}(f)$.

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.

[BH96] Gerth Stølting Brodal and Thore Husfeldt. A communication complexity proof that symmetric functions have logarithmic depth. *BRICS Report Series*, 3, 1996.

[CFL83] Ashok K. Chandra, Merrick L. Furst, and Richard J. Lipton. Multi-party protocols. In David S. Johnson, Ronald Fagin, Michael L. Fredman, David Harel, Richard M. Karp, Nancy A. Lynch, Christos H. Papadimitriou, Ronald L. Rivest, Walter L. Ruzzo, and

Joel I. Seiferas, editors, *Proceedings of the 15th Annual ACM Symposium on Theory of Computing, 25-27 April, 1983, Boston, Massachusetts, USA*, pages 94–99. ACM, 1983.

[Chi90] Andrew Chin. On the depth complexity of the counting functions. *Inf. Process. Lett.*, 35(6):325–328, 1990.

[CLV19] Arkadev Chattopadhyay, Shachar Lovett, and Marc Vinyals. Equality alone does not simulate randomness. In Amir Shpilka, editor, *34th Computational Complexity Conference, CCC 2019, July 18-20, 2019, New Brunswick, NJ, USA*, volume 137 of *LIPIcs*, pages 14:1–14:11. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019.

[DIS+21] Yuriy Dementiev, Artur Ignatiev, Vyacheslav Sidelnik, Alexander Smal, and Mikhail Ushakov. New bounds on the half-duplex communication complexity. In Tomás Bures, Riccardo Dondi, Johann Gamper, Giovanna Guerrini, Tomasz Jurdzinski, Claus Pahl, Florian Sikora, and Prudence W. H. Wong, editors, *SOFSEM 2021: Theory and Practice of Computer Science - 47th International Conference on Current Trends in Theory and Practice of Computer Science, SOFSEM 2021, Bolzano-Bozen, Italy, January 25-29, 2021, Proceedings*, volume 12607 of *Lecture Notes in Computer Science*, pages 233–248. Springer, 2021.

[EIRS01] Jeff Edmonds, Russell Impagliazzo, Steven Rudich, and Jirí Sgall. Communication complexity towards lower bounds on circuit depth. *Comput. Complex.*, 10(3):210–246, 2001.

[Hås98] Johan Håstad. The shrinkage exponent of de morgan formulas is 2. *SIAM J. Comput.*, 27(1):48–64, 1998.

[HIMS18a] Kenneth Hoover, Russell Impagliazzo, Ivan Mihajlin, and Alexander Smal. Half-duplex communication complexity. *Electronic Colloquium on Computational Complexity (ECCC)*, 25:89, 2018.

[HIMS18b] Kenneth Hoover, Russell Impagliazzo, Ivan Mihajlin, and Alexander V. Smal. Half-duplex communication complexity. In Wen-Lian Hsu, Der-Tsai Lee, and Chung-Shou Liao, editors, *29th International Symposium on Algorithms and Computation, ISAAC 2018, December 16-19, 2018, Jiaoxi, Yilan, Taiwan*, volume 123 of *LIPIcs*, pages 10:1–10:12. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2018.

[IMS22] Artur Ignatiev, Ivan Mihajlin, and Alexander Smal. Super-cubic lower bound for generalized karchmer-wigderson games. *Electron. Colloquium Comput. Complex.*, TR22-016, 2022.

[Juk12] Stasys Jukna. *Boolean Function Complexity - Advances and Frontiers*, volume 27 of *Algorithms and combinatorics*. Springer, 2012.

[Khr71] VM Khrapchenko. Complexity of the realization of a linear function in the class of ii-circuits. *Mathematical Notes of the Academy of Sciences of the USSR*, 9(1):21–23, 1971.

[KN97] Eyal Kushilevitz and Noam Nisan. *Communication complexity*. Cambridge University Press, 1997.

[KRW95] Mauricio Karchmer, Ran Raz, and Avi Wigderson. Super-logarithmic depth lower bounds via the direct sum in communication complexity. *Computational Complexity*, 5(3/4):191–204, 1995.

[KW88] Mauricio Karchmer and Avi Wigderson. Monotone circuits for connectivity require super-logarithmic depth. In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, STOC '88, page 539–550, New York, NY, USA, 1988. Association for Computing Machinery.

[Mei20] Or Meir. Toward better depth lower bounds: Two results on the multiplexor relation. *Comput. Complex.*, 29(1):4, 2020.

[MS20] Ivan Mihajlin and Alexander Smal. Toward better depth lower bounds: the XOR-KRW conjecture. *Electron. Colloquium Comput. Complex.*, 27:116, 2020.

[MS21] Ivan Mihajlin and Alexander Smal. Toward better depth lower bounds: The XOR-KRW conjecture. In Valentine Kabanets, editor, *36th Computational Complexity Conference, CCC 2021, July 20-23, 2021, Toronto, Ontario, Canada (Virtual Conference)*, volume 200 of *LIPIcs*, pages 38:1–38:24. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021.

[PSS14] Periklis Papakonstantinou, Dominik Scheder, and Hao Song. Overlays and limited memory communication. In *2014 IEEE 29th Conference on Computational Complexity (CCC)*, pages 298–308, 2014.

[RS42] John Riordan and Claude E. Shannon. The number of two-terminal series-parallel networks. *Journal of Mathematics and Physics*, 21(1-4):83–93, 1942.

[SM19] Dmitri Sokolov and Ivan Mihajlin. On deterministic communication with oracle to equality. 2019.

[Sub61] Bella Abramovna Subbotovskaya. Realization of linear functions by formulas using $\wedge$, $\vee$, $\neg$. In *Doklady Akademii Nauk*, volume 136-3, pages 553–555. Russian Academy of Sciences, 1961.

[Tal14] Avishay Tal. Shrinkage of de morgan formulae by spectral techniques. In *2014 IEEE 55th Annual Symposium on Foundations of Computer Science*, pages 551–560, 2014.

[Yao79] Andrew Chi-Chih Yao. Some complexity questions related to distributive computing (preliminary report). In Michael J. Fischer, Richard A. DeMillo, Nancy A. Lynch, Walter A. Burkhard, and Alfred V. Aho, editors, *Proceedings of the 11h Annual ACM Symposium on Theory of Computing, April 30 - May 2, 1979, Atlanta, Georgia, USA*, pages 209–213. ACM, 1979.

A Перевешивания

Теорема 27

Для отношения R, $\mathrm{D}(R) \leqslant 2.46 \log \mathrm{L}(R)$.

Доказательство. Рассмотрим двоичное дерево T произвольного протокола, пусть в нём t листьев. Покажем, что существует вершина v, такая что в каждом из двух поддеревьев её потомков содержится не более $\frac{t}{a}$ листьев, где $a \geq 2$, а в её поддереве T_v не менее $\frac{t}{a}$ листьев: начнем спускаться из корня и до тех пор, пока в поддереве хотя бы одного из потомков нашей текущей вершины больше $\frac{t}{a}$ листьев, будем спускаться в этого потомка (если таких двое, переходим в левого). Когда процесс завершится, мы будем находится в требуемой вершине.

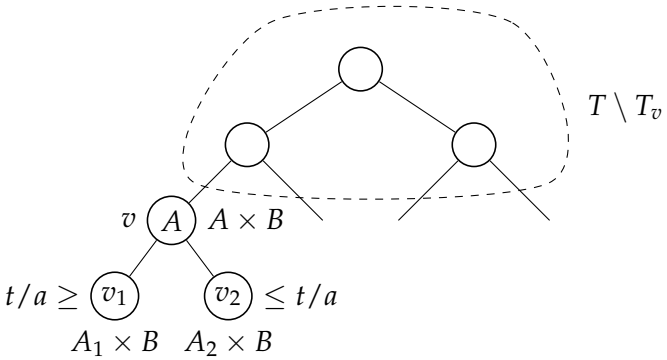

Рис. 12. Протокол до перевешивания

Алиса и Боб для своего протокола так же находят вершину v. Теперь им нужно определить, в каком из трёх поддеревьев лежит лист, соответствующий их входу (x, y): в поддереве T_{v_1} левого потомка v, в поддереве T_{v_2} правого потомка v или в поддереве $T \setminus T_v$. Н.у.о. в вершине v ход Алисы, то есть в вершине v происходит разделение по x. Пусть вершине v соответствует прямоугольник $A \times B$, тогда вершине v_1 соответствует прямоугольник $A_1 \times B$, а вершине v_2 соответствует прямоугольник $A_2 \times B$. Боб отправляет Алисе 1, если $y \in B$ и 0, иначе. Алиса отправляет

$$\begin{cases} 00, & \text{если } x \in A_1, \\ 01, & \text{если } x \in A_2, \\ 1, & \text{если } x \notin A. \end{cases}$$

Теперь они оба знают поддерево, к которому нужно переходить. При каждом таком переходе Алиса и Боб обмениваются двумя битами, если лист для (x, y) в поддереве $T \setminus T_v$, и тремя битами, если лист для (x, y) в поддереве T_{v_1} или T_{v_2}, причем $|T_{v_i}| \leq \frac{t}{a}$, для $i = 1, 2$, и $|T \setminus T_v| \leq t - \frac{t}{a}$. Получаем систему

$$\begin{cases} D(t) = 3 + D(\frac{t}{a}) \\ D(t) = 2 + D(\frac{(a-1)t}{a}) \end{cases} \implies \begin{cases} D(t) = 3\log_a t \\ D(t) = 2\log_{\frac{a}{a-1}} t \end{cases} \implies \frac{3}{\log a} = \frac{2}{\log \frac{a}{a-1}}.$$

Получаем $a = 2.32$, значит $D(t) = \frac{3}{\log a} \log t = 2.46 \log t$.

□

B Универсальное отношение

Определение 21 ([EIRS01])

Универсальное отношение длины n,

$$\mathrm{U}_n = \{(x, y, i) \mid x, y \in \{0,1\}^n, i \in [n], x_i \neq y_i\}.$$

Коммуникационная задача для универсального отношения является обобщением игры Карчмера-Вигдерсона: Алисе и Бобу даны n-битные различные строки, и их цель состоит в том, чтобы найти координату $i \in [n]$ такую, что $x_i \neq y_i$. Единственное различие с игрой KW для некоторой функции заключается в том, что у игроков нет доказательства того, что их строки отличаются. Блочная композиция универсальных отношений является более сложным объектом, который обобщает блочную композицию функций. Иногда удобнее рассматривать не обещанную версию универсального отношения, где Алисе и Бобу могут быть даны одни и те же строчки, в этом случае они должны вывести $\perp$. Эта задача соответствует не обещанному универсальному отношению длины n.

Определение 22 ([EIRS01])

Универсальное отношение без обещания длины n,

$$\mathrm{U}'_n = \mathrm{U}_n \cup \{(x, x, \perp) \mid x \in \{0,1\}^n\}.$$

Предположим мы хотим покрыть универсальное отношение несколькими отношениями Карчмера-Вигдерсона для некоторых (сложных) функций. Это может быть полезно для нижних оценок на блочную композицию универсального отношения с каким-то другим отношением. Сколько отношений Карчмера-Вигдерсона понадобится для этого (т.е. чтобы любой вход универсального отношения был покрыт каким-то KW)?

Утверждение 9

Для покрытия универсального отношения необходимо n отношений Карчмера-Вигдерсона для некоторых функций.

Доказательство. Заметим, что покрытие KW должно разделить все возможные пары входов Алисы и Боба (x, y), т.е. любую такую пару можно было бы дать на вход какому-то отношению KW_f. Изначально 2^{2n} неразделенных пар, первое отношение KW_f разделяет пространство x не более чем в два раза, значит остается набор x размера хотя бы 2^{n-1}, из которых любая пара (x_a, x_b) не может быть дана на вход KW (возьмем больший из прообразов функции f и перейдем к нему). Таким образом, необходимо хотя бы n отношений KW. □

Утверждение 10

Существует покрытие универсального отношения размера $2n$.

Доказательство. Вероятностно покажем существование покрытия. Возьмем покрытие KW размера N, функции берем независимо и равновероятно.

$$\Pr[\exists\ (x, y) : \text{покрытию нельзя дать на вход } (x, y)] \leq$$

$$\leq \sum_{i=1,j=1}^{2^n} \Pr[(x_i, y_j) \text{ нельзя дать на вход покрытию из } \mathrm{KW}_f] =$$

$$= \sum_{\substack{i=0 \\ j=0}} \prod_{k=1}^{N} \frac{1}{2} = \frac{2^{2n}}{2^N}$$

Первое равенство верно потому, что каждая функция не разделяет (x_i, y_j) с вероятностью 1/2. Мы хотим чтобы $\Pr[\mathrm{KW}_f$ является покрытием $\mathrm{U}_n] > 0$, значит надо, чтобы $\frac{2^{2n}}{2^N} < 1$, а это верно при $N > 2n$.

Явная конструкция. Возьмем отношения KW для функций f_i и $\widetilde{f_i}, i \in [n]$, где f_i и $\widetilde{f_i}$ разделяет пространство x по i биту, т.е. $f_i(x) = 0, \widetilde{f_i}(x) = 1$ для x, т.ч. $x_i = 0$, и $f_i(x) = 1, \widetilde{f_i}(x) = 0$ для x, т.ч. $x_i = 1$. Тогда любой вход (x, y) универсального отношения можно дать какому-то отношению Карчмера-Вигдерсона (легко заметить, что мы получили покрытие легкими функциями, если Алиса и Боб узнают в каком отношении лежит их вход, то они сразу же решат задачу). □