Санкт-Петербургский государственный университет

СИДЕЛЬНИК Вячеслав Андреевич

Выпускная квалификационная работа

Новые оценки на полудуплексную коммуникационную сложность игр Карчмера-Вигдерсона для булевых функций

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

Научный руководитель:
Авдюшенко Александр Юрьевич

Рецензент:
Смирнов Петр Юрьевич

Санкт-Петербург
2022

1. Введение

Коммуникационная сложность это мощный инструмент, который находит свое применение в алгоритмах, формульной сложности, сложности доказательств и многих других областях теоретической информатики. В классической коммуникационной модели, введенной Эндрю Яо в 1979 [14], два игрока, Алиса и Боб, пытаются вычислить значение $f(x, y)$, для некоторой функции f и входов x, y, где Алиса знает только x, а Боб знает только y. Игроки могут общаться, посылая друг другу по одному биту за раунд, а в конце их общения оба игрока должны знать значение $f(x, y)$. Важным свойством данной модели является то, что в каждом раунде коммуникации один игрок посылает бит, а другой его получает.

Существует множество расширений данной базовой модели, такие как рандомизированная коммуникационная сложность [14], недетерменированная коммуникационная сложность [2], коммуникационная модель с несколькими игроками [3], и т.д. Мы рассмотрим полудуплексную коммуникационную модель, предложенную в статье [5]. Основным отличием этой модели от классической является то, что игроки разговаривают по полудуплексному каналу связи. Ярким примером такого канала связи является использование рации. При разговоре по рации игрок должен удерживать кнопку "push-to-talk", а принимающий игрок должен держать ее не нажатой. Если же они пытаются говорить одновременно, то они не услышат друг друга. Более формально, авторы статьи [5] предлагают игрокам на каждом раунде выбирать одно из трех действий: *отправить 0*, *отправить 1* или *принимать*. В результате появляются три различных типа раундов:

1. *Классический*: один игрок посылает какой-то бит, а другой его получает. Общение работает, как в классическом случае.

2. *Потерянный*: оба игрока отправляют биты во время раунда. Эти биты теряются.

3. *Тихий*: оба игрока принимают.

Можно по-разному определить, что происходит в тихих раундах. Авторы [5] определяют три полудуплексные коммуникационные модели:

- *Модель с тишиной*: во время тихого раунда игроки получают специальный символ тишины s. Они могут отличить тихий раунд от классического.

- *Модель с нулем*: оба игрока в тихом раунде получают 0. Игроки не могут отличить тихий раунд от классического раунда, в котором другой игрок посылает 0.

- *Модель с противником*: игроки во время тихого раунда получают произвольные биты, не обязательно одинаковые. Игроки не могут отличить тихий раунд от классического.

Мотивация рассматривать полудплексные коммуникационные модели происходит из изучения игр Карчмера-Вигдерсона [8] для мультиплексорного отношения [4]. В статье [10], использовались результаты из полудуплексной коммуникационной сложности, для доказательства нижней оценки на композицию универсального отношения с игрой Карчмера-Вигдерсона для некоторой функции. Авторы данной статьи предполгают, что лучшее понимание полудуплексной коммуникационной сложности может помочь в исследование KRW гипотезы [7].

Цель работы:

Данная работа продолжает исследование полудуплексную коммуникационную сложность для игр Карчмера-Вигдерсона симметрических функций, в частности для пороговой функции, и для рекурсивной функции большинства. Изучение сложности этих функций в полудуплексных моделях, может помочь в понимание полудуплексной модели.

Задачи работы:

- Получение оценок на полудуплексную коммуникационную сложность игр Карчмера-Вигдерсона для различных пороговых функций.
- Получение верхних оценок на полудуплексную коммуникационную сложность игр Карчмера-Вигдерсона для рекурсивной функции большиснтва в модели с тишиной и с нулем.

2. Определения

Определим полудуплексную коммуникационную задачу, следующим образом.

Определение 2.1. Пусть X, Y, Z — конечные и непустые множества. Будем говорить, что Алиса и Боб решают *полудуплексную коммуникационную задачу* для отношения $R \subset X \times Y \times Z$, в следующем случае множества X, Y, Z и отношение R известны обоим участникам. Алисе дан некоторый $x \in X$, Бобу дан некоторый $y \in Y$. Их цель — найти такой $z \in Z$, что $(x, y, z) \in R$. Игроки могут общаться через полудуплексный коммуникационный канал, и их общение разбито на раунды. Во время любого раунда, каждый игрок решает какое из трех действий ему совершить: отправить 0, отправить 1, принимать сообщение от другого игрока. Решение каждого игрока основывается только на своем входе и предыдущей коммуникации. Мы будем говорить, что коммуникационная задача для R решается в полудуплексной модели, если в конце коммуникации оба игрока знают некоторый (один и тот же) $z \in Z$, такой что $(x, y, z) \in R$.

Теперь можно определить полудуплексный коммуникационный протокол в различных моделях.

Определение 2.2. *Полудуплексный коммуникационный протокол с тишиной*, решающий коммуникационную задачу для отношения $R \subset X \times Y \times Z$ — пара корневых деревьев (T_A, T_B), которые описывают коммуникацию Алисы и Боба на всех парах входов

$(x, y) \in X \times Y$. Каждая вершина дерева T_A — состояние Алисы, а каждая вершина дерева T_B — состояние Боба. Каждый лист l помечен некоторым элеменетом $z_l \in Z$. Определим множество возможных *действий* игрока $\mathcal{A} = \{$послать(0), послать(1), принимать$\}$, и множество возможных *событий* для игрока $\mathcal{E} = \{$послал(0), послал(1), получил(0), получил(1), тишина$\}$. Для каждой вершины v дерева T_A (дерева T_B) определим две функции $g_v : X \to \mathcal{A}$ (соответственно, $g_v : Y \to \mathcal{A}$) и $h_v : \mathcal{E} \to C(v)$, где $C(v)$ — множество потомков вершины v. Корневые вершины деревьев T_A и T_B соответствуют начальным состояниям Алисы и Боба. Если Алиса находится в вершине v, то она соовершает действие $g_v(x)$. Аналогичное верно и для Боба. Следущая вершина определяется при помощи функции h. Когда игроки достигают листьев они завершают игру.

Определение 2.3. *Полудуплексный коммуникационный протокол с нулем* определяется аналогично, только теперь множество действий $\mathcal{A} = \{$послать(1), принимать$\}$, и множество событий $\mathcal{E} = \{$послал(1), получил(0), получил(1)$\}$. В дной модели серди событий отсутствует тишина. Также игроки не посылают 0, вместо этого они молчт. Заметим, что игроки не посылают 0, вместо этого молчат.

Следующие определение верно для моделей с тишиной и с нулем.

Определение 2.4. Протокол является*корректным*, если для любой пары входов $(x, y) \in X \times Y$ коммуникация заканчивается в паре листьев (один в дереве T_A, другой в дереве T_B), помеченных $z \in Z$, таким что $(x, y, z) \in R$.

Определение 2.5. *Полудуплексный коммуникационный протокол с противником*, решающий коммуникационнуб задачу для отношения $R \subset X \times Y \times Z$ — пара корневых деревьев (T_A, T_B), которые описывают коммуникацию Алисы и Боба на всех парах входов $(x, y) \in X \times Y$ и для всех стратегий противника $w \in \{0, 1\}^*$. Определим множество возможных *действий* $\mathcal{A} = \{$послать(0), послать(1), принимать$\}$, и множество возможных *событий* $\mathcal{E} = \{$послал(0), послал(1), получил(0), получил(1)$\}$. Причем, если в некотором раунде i оба игрока решили принимать сообщения, то Алиса получает бит w_{2i-1}, а Боб бит w_{2i}. Протокол является *корректным*, если для любой пары входов $(x, y) \in X \times Y$ и для любой стратегии противника $w \in \{0, 1\}^*$, коммуникация заканчивается в паре листьев (один в дереве T_A, другой в дереве T_B), помеченных $z \in Z$, таким что $(x, y, z) \in R$.

Следующие определение верно для любых трех моделей.

Определение 2.6. Определим понятие *расшифровка*, как пару (π_A, π_B) последовательностей из $\mathcal{E}$, в которой перечислены все события наблюдаемые Алисой и Бобом соответственно, после запуска некоторого протокола на входе (x, y).

Определение 2.7. Будем говорить, что полудуплексный коммуникационный протокол *решает коммуникационную задачу для функции* $f : X \times Y \to Z$, если он решает коммуникационную задачу для отношения $R(f) = \{(x, y, f(x, y)) \mid x \in X, y \in Y\}$.

Теперь можно определить полудуплексную коммуникационную сложность.

Определение 2.8. *Полудуплексная коммуникационная сложность функции* f определяется, как минимальная глубина полудуплексного коммуникационного протокола, решающего коммуникационную задачу для функции f с тишиной, с нулем, с противником. Будем обозначать соответствующую сложность через $D_s^{hd}(f)$ в модели с тишиной, $D_0^{hd}(f)$ в модели с нулем, и $D_a^{hd}(f)$ в модели с противником. Аналогично определяется *полудуплексная коммуникационная сложность для отношения* R.

Для изучения полудуплексной сложность булевых функций, рассмотрим следующую игру.

Определение 2.9. *Игра Карчмера-Вигдерсона для функции* f — 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 $x_i \neq y_i$. Другими словами, игра Карчмера-Вигдерсона — это коммуникационная задача для отношения Карчмера-Вигдерсона.

Другими словами, игра Карчмера-Вигдерсона — это коммуникационная задача для отношения

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

Данное отношение KW_f называется *отношением Карчмера-Вигдерсона* для булевой функции f.

Опишем как связаны игры Карчмера-Вигдерсона с формулами в базисе Де Моргана, для этого введем следующие определение:

Определение 2.10. *Формула в базисе Де Моргана для функции* $f\colon \{0,1\}^n \to \{0,1\}$ — это булевая формула с булевыми переменными $\{x_1, \ldots, x_n\}$, соответствующими отдельным битам входа f, и со связками (гейтами) $\{\wedge, \vee, \neg\}$, вычисляющая функцию f. Структура формулы Де Моргана представляет собой корневое дерево: листья соответствуют переменным, а внутренние вершины — логическим связкам.

Теорема 1 (Карчмер-Вигдерсон [8])**.** *Для каждой формулы* ϕ*, вычисляющей* f*, существует такой протокол* $\mathcal{P}_\phi$ *для отношения Карчмера-Вигдерсона* KW_f*, что его дерево совпадает с деревом, описывающим структуру формулы* ϕ*. Верно и обратное: если есть протокол для* R_f *, то есть и формула для* f *с такой же структурой.*

Для доказательства нижних оценок на полудуплексную коммуникационную сложность коммуникационных задач, рассмотрим теоретико-информационный подход. Сначала введем необходимые определения.

Определение 2.11. Пусть случаная величина $\mathcal{A}$ принимает значения из множества $\{a_1, a_2, \ldots, a_k\}$ с вероятностями $\{p_1, p_2, \ldots, p_k\}$, где $\sum_{i=1}^k p_i = 1$. *Энтропия Шеннона* случайной величины $\mathcal{A}$ определяется как

$$H(\mathcal{A}) = \sum_{i=1}^{k} p_i \cdot \log_2 \frac{1}{p_i},$$

при $p_i = 0$ полагаем, что $p_i \cdot \log_2 \frac{1}{p_i} = 0$. Другими словами, энотропия Шеннона опредляет количество информации $H(\mathcal{A})$ в распределении вероятностей для некоторой случайной величины $\mathcal{A}$, принимающей значения из конечного множества.

Утверждение 2.1. *Для энтропии Шеннона верно следующие.*

- $H(\mathcal{A}) \geq 0$, *причем* $H(\mathcal{A}) = 0$ *тогда и только тогда, когда распределение случайной величины* $\mathcal{A}$ *вырождено.*
- $H(\mathcal{A}) \leq \log_2 k$, *причем* $H(\mathcal{A}) = \log_2 k$ *тогда и только тогда, когда случайная величина* $\mathcal{A}$ *распределена равномерно*

Энотропия совместного распредления пары случайных величин $\mathcal{A}$ и $\mathcal{B}$ обозначется $H(\mathcal{A}, \mathcal{B})$.

Утверждение 2.2. *Для энтропии свместного распредления верно следующие:*

- $H(\mathcal{AB}) \leq H(\mathcal{A}) + H(\mathcal{B})$, *причем равенство достигается тогда и только тогда, когда случайные величины независимы.*
- $H(\mathcal{A}) \leq H(\mathcal{A}, \mathcal{B})$, *причем равенство достигается тогда и только тогда, когда случайная величина* $\mathcal{B} = f(\mathcal{A})$, *то есть полностью определяется значением* $\mathcal{A}$.

Определение 2.12. Энтропия $\mathcal{A}$ при условии $\mathcal{B} = b_j$ определяется следующим образом

$$H(\mathcal{A} \mid \mathcal{B} = b_j) = \sum_i \Pr[\mathcal{A} = a_i \mid \mathcal{B} = b_j] \cdot \log_2 \frac{1}{\Pr[\mathcal{A} = a_i \mid \mathcal{B} = b_j]}.$$

Определение 2.13. *Условная энтропия* $\mathcal{A}$ отн осительно $\mathcal{B}$

$$H(\mathcal{A} \mid \mathcal{B}) = \sum_j \Pr[\mathcal{B} = b_j] \cdot H(\mathcal{A} \mid \mathcal{B} = b_j).$$

Утверждение 2.3. *Для условной энтропии верно следующие.*

- $H(\mathcal{A} \mid \mathcal{B}) \geq 0$.
- $H(\mathcal{A} \mid \mathcal{B}) = 0$ *тогда и только тогда, когда* $\mathcal{A}$ *однозначно определяется по* $\mathcal{B}$.
- $H(\mathcal{A}, \mathcal{B}) = H(\mathcal{B}) + H(\mathcal{A} \mid \mathcal{B}) = H(\mathcal{A}) + H(\mathcal{B} \mid \mathcal{A})$.

Определим понятие взаимной информации.

Определение 2.14. *Информация в* $\mathcal{A}$ *о величине* $\mathcal{B}$ *(взаимная информация случайных величин* $\mathcal{A}$ *и* $\mathcal{B}$*)* определяется следующим соотношением.

$$I(\mathcal{A} : \mathcal{B}) = H(\mathcal{B}) - H(\mathcal{B} \mid \mathcal{A}).$$

Утверждение 2.4. *Для взаимной информации верно следующие.*

- $I(\mathcal{A} : \mathcal{B}) \leq H(\mathcal{A})$.
- $I(\mathcal{A} : \mathcal{B}) \leq H(\mathcal{B})$.
- $I(\mathcal{A} : \mathcal{A}) = H(\mathcal{A})$.
- $I(\mathcal{A} : \mathcal{B}) = I(\mathcal{B} : \mathcal{A})$.
- $I(\mathcal{A} : \mathcal{B}) = H(\mathcal{A}) + H(\mathcal{B}) - H(\mathcal{A}, \mathcal{B})$.

Определение 2.15. Пусть $\mathcal{A}, \mathcal{B}, \mathcal{C}$ — случайные величины. Определим *взаимную информацию в $\mathcal{A}$ о $\mathcal{B}$ при условии $\mathcal{C}$* следующим образом:

$$I(\mathcal{A} : \mathcal{B} \mid \mathcal{C}) = H(\mathcal{B} \mid \mathcal{C}) - H(\mathcal{B} \mid \mathcal{A}, \mathcal{C}).$$

Утверждение 2.5. *Для взаимной информации верно следующие.*

1. $I((\mathcal{A}, \mathcal{B}) : \mathcal{C}) = I(\mathcal{A} : \mathcal{C}) + I(\mathcal{B} : \mathcal{C} \mid \mathcal{A})$.
2. $I((\mathcal{A}, \mathcal{B}) : \mathcal{C} \mid \mathcal{D}) = I(\mathcal{A} : \mathcal{C} \mid \mathcal{D}) + I(\mathcal{B} : \mathcal{C} \mid \mathcal{A}, \mathcal{D})$.

Теперь опишем сам теоретико-информационный подход к доказательству нижних оценок для коммуникационных задач. Данное описание опирается на работу [13].

Для описания этого подхода рассмотрим некоторую коммуникационную задачу $P \subset X \times Y \times Z$ и коммуникационный протокол $\mathcal{P}$ для P. Пусть $\mathcal{D}$ — вероятностное распределение на $X \times Y$. Рассмотрим совместно распределённые случайные величины $\mathcal{X}, \mathcal{Y}, \pi$, индуцированные распределением $\mathcal{D}$, где $\mathcal{X}$ и $\mathcal{Y}$ распределены на входах Алисы и Боба, а π распределена на листьях протокола $\mathcal{P}$, соответствующих результату коммуникации игроков на входах $\mathcal{X}$ и $\mathcal{Y}$.

Определение 2.16. *Внешнее информационное разглашение протокола $\mathcal{P}$* на распределении $\mathcal{D}$ определяется как

$$IC^{ext}_{\mathcal{D}}(\mathcal{P}) = I(\pi : \mathcal{X}, \mathcal{Y}).$$

Определение 2.17. *Внутреннее информационное разглашение протокола $\mathcal{P}$* на распределении $\mathcal{D}$ определяется как

$$IC^{int}_{\mathcal{D}}(\mathcal{P}) = I(\pi : \mathcal{X} \mid \mathcal{Y}) + I(\pi : \mathcal{Y} \mid \mathcal{X}).$$

Рассмотрим следующую теорему, которая связывает глубину протокола $D(\mathcal{P})$ и внешнее, и внутреннее информационное разглашение. Данная теорема описывает, как связаны гулбина протокола и информационные разглашения.

Теорема 2 ([6]). *Для любого коммуникационного протокола $\mathcal{P}$ и любого распредления $\mathcal{D}$ верно:*

$$D(\mathcal{P}) \geq IC^{ext}_{\mathcal{D}}(\mathcal{P}) \geq IC^{int}_{\mathcal{D}}(\mathcal{P}),$$

Теорема 3 ([13]). *Для любого коммуникационного протокола $\mathcal{P}$ и любого распредления $\mathcal{D}$ верно:*

$$\log_2(L(\mathcal{P})) \geq IC^{ext}_{\mathcal{D}}(\mathcal{P}),$$

где $L(\mathcal{P})$ — число листьев протокола $\mathcal{P}$.

Для доказательства нижних оценок на полудуплексную коммуникационную сложность, рассмотрим адаптацию вышеописанного подхода для полудуплексных моделей [5]. Данная адаптация необходима, поскольку в полудуплексных моделях игроки получают больше информации о входах друг друга в процессе коммуникации, чем в классической модели.

Для описания адаптации этого подхода рассмотрим некоторую коммуникационную задачу $P \subset X \times Y \times Z$ и коммуникационный протокол $\mathcal{P}$ для P. Пусть $\mathcal{D}$ — вероятностное распределение на $X \times Y$. Рассмотрим совместно распределённые случайные величины $\mathcal{X}, \mathcal{Y}, \Pi_A, \Pi_B$, индуцированные распределением $\mathcal{D}$, где $\mathcal{X}$ и $\mathcal{Y}$ распределены на входах Алисы и Боба, а Π_A и Π_B распределены на расшифровках Алисы и Боба.

Определение 2.18. *Внутреннее информационное разглашение протокола $\mathcal{P}$* на распределении $\mathcal{D}$ определяется как

$$IC_{\mathcal{D}}(\mathcal{P}) = I(\mathcal{X} : \Pi_B \mid \mathcal{Y}) + I(\mathcal{Y} : \Pi_A \mid \mathcal{X}).$$

Определение 2.19. Обозначим через Π^k_A и Π^k_B префиксы длины k значений случайных величин Π_A и Π_B, для $k \in \mathbb{N}$. Тогда внутреннее информационное разглашение первых k раундов протокола $\mathcal{P}$ по распределению $\mathcal{D}$ определяется следующим образом:

$$IC^k_{\mathcal{D}}(\mathcal{P}) = I(\mathcal{X} : \Pi^k_B \mid \mathcal{Y}) + I(\mathcal{Y} : \Pi^k_A \mid \mathcal{X}).$$

Следующие теоремы определяют верхнюю оценку на количество информации, которую игроки суммарно могут узнать в одном раунде.

Теорема 4 (Теоерема 4 в [11]). *Для любого полудуплексного коммуникационного протокола $\mathcal{P}$ с тишиной, любого распределения на входах $X \times Y$ и для любого $k \in \mathbb{N}$ верно:*

$$IC^k_{\mathcal{D}}(\mathcal{P}) = I(\mathcal{X} : \Pi^k_B \mid \mathcal{Y}) + I(\mathcal{Y} : \Pi^k_A \mid \mathcal{X}) \leq 2k.$$

Аналогичная теорема для модели с нулем.

Теорема 5 (Теоерема 4 в [11]). *Для любого полудуплексного коммуникационного протокола $\mathcal{P}$ с нулем, любого распределения на входах $X \times Y$ и для любого $k \in \mathbb{N}$ верно:*

$$IC^k_{\mathcal{D}}(\mathcal{P}) = I(\mathcal{X} : \Pi^k_B \mid \mathcal{Y}) + I(\mathcal{Y} : \Pi^k_A \mid \mathcal{X}) \leq 1.389k.$$

Для модели с противником доказана более сильная оценка:

Теорема 6 (Лемма 26 в [5]). *Для любого полудуплексного коммуникационного протокола $\mathcal{P}$ с противником, любого распределения на входах $X \times Y$ и для любого $k \in \mathbb{N}$ верно:*

$$IC^k_{\mathcal{D}}(\mathcal{P}) = I(\mathcal{X} : \Pi^k_B \mid \mathcal{Y}) + I(\mathcal{Y} : \Pi^k_A \mid \mathcal{X}) \leq k.$$

Рассмотрим следующие функции:

Определение 2.20. Пороговой k-функцией назвается булева функция $\mathrm{THR}_{k,n} : \{0,1\}^n \to \{0,1\}$, такая что

$$\mathrm{THR}_{k,n}(x) = 1 \iff \sum_{i=1}^{n} x_i \geq k.$$

В классическом случае известно, что коммуникационная сложность пороговой функции ограничена сверху $\mathcal{O}(\log_2(k^{4,3} n \log_2(n)))$ [1], и ограничена снизу $\log_2(\lfloor \frac{k}{2} \rfloor n \log_2(\frac{n}{k-1}))$ [12].

Так же определим рекурсивную функцию большинства, но для начала рассмотрим функцию большинства для трех.

Определение 2.21. *Функцией большинства для трех* называется булева функция $\mathrm{Maj}_3 : \{0,1\}^3 \to \{0,1\}$, такая что:

$$\mathrm{Maj}_3(x_1, x_2, x_3) = 1 \iff \sum_{i=1}^{3} x_i \geqslant 2.$$

Определение 2.22. Будем считать, что $n = 3^k$, то есть в последующих теоремах, будем считать, что n — степень тройки. Функция $\mathrm{RecMaj}\colon \{0,1\}^n \to \{0,1\}$ определяется следующим соотношением

$$\mathrm{RecMaj}(x_1, \ldots, x_n) = \\ \mathrm{Maj}_3(\mathrm{RecMaj}(x_1, \ldots, x_{\frac{n}{3}}), \mathrm{RecMaj}(x_{\frac{n}{3}}, \ldots, x_{\frac{2n}{3}}), \mathrm{RecMaj}(x_{\frac{2n}{3}}, \ldots, x_n)).$$

В классическом случае известно, что коммуникационная сложность RecMaj находится между $2\log_3(n)$ и $3\log_3(n)$ [9]. Структура этой функции идеально подходит для реализации троичного поиска.

3. Результаты

Рассмотрим отношение Карчмера-Вигдерсона для функции RecMaj. Структура данной функции отлично подходит для троичного поиска. Основываясь на этом замечании, докажем следующие верхние оценки.

Теорема 7. $\mathrm{D}_s^{hd}(\mathrm{KW}_{\mathrm{RecMaj}_n}) \leq 2\log_3(n)$.

Доказательство. Пусть у Алисы $x \in \mathrm{RecMaj}_n^{-1}(1)$, а у Боба $y \in \mathrm{RecMaj}_n^{-1}(0)$. Предъявим протокол, в котором Алиса и Боб реализуют троичный поиск. На каждом шаге игроки делят свои строки на три части и считают для них $\mathrm{RecMaj}_{\frac{n}{3^k}}$, где k — номер шага. При этом, на каждом шаге игроки переходят в ту подстроку, где у Алисы стоит 1, а у Боба стоит 0. После разбиения текущей строки на три части и подсчета RecMaj для каждой части, у Алисы могут получиться следующие случаи (1 обозначает, что RecMaj для соответствующей части равен 1, 0 — RecMaj равен 0):

1. 111, 110;

2. 101;

3. 011.

Аналогично у Боба могут получиться следующие случаи:

1. 000, 001;

2. 010;

3. 100.

На каждом шаге, Алиса будет отправлять номер своего случая (1)–(3) (Алиса закодирует номер своего случая в троичной записи и отправит получившийся код Бобу, для этого потребуется один бит), а Боб будет сообщать, в какую подстроку им нужно переходить (Боб будет отправлять 0, если надо перейти в первую подстроку, 1, если надо перейти во вторую подстроку, и слушать, если надо перейти в третью подстроку). В итоге потребуется сделать $\log_3(n)$ шагов, и на каждом шаге потребуется отправить или принять 2 сообщения, то есть:

$$\mathrm{D}_s^{hd}(\mathrm{KW}_{\mathrm{RecMaj}_n}) \leq 2\log_3(n). \qquad \square$$

Покажем анлогичную оценку в модели с нулем.

Теорема 8. $\mathrm{D}_0^{hd}(\mathrm{KW}_{\mathrm{RecMaj}_n}) \leq 2\log_3(n)$.

Доказательство. Пусть у Алисы $x \in \mathrm{RecMaj}_n^{-1}(1)$, а у Боба $y \in \mathrm{RecMaj}_n^{-1}(0)$. Предъявим протокол, в котором Алиса и Боб будут реализуют троичный поиск. На каждом шаге игроки делят свои строки на три части и считают для них $\mathrm{RecMaj}_{\frac{n}{3^k}}$, где k — номер шага. При этом, на каждом шаге игроки переходят в ту подстроку, где у Алисы стоит 1, а у Боба стоит 0. Случаи у Алисы и Боба такие же, как и в предыдущей теореме. Коммуникация по раундам осуществляется следующим образом:

1. Боб молчит, если у него в первой подстроке стоит 0, иначе он отправляет 1. Алиса молчит, если у нее в первой подстроке 1, иначе она отправляет 1.

2. Боб молчит, если у него во втором куске 0, иначе он отправляет 1. Алиса молчит, если у нее в втором куске 1, иначе она отправляет 1.

Покажем, что протокол корректен. Заметим, что оба раунда не могут быть потерянными. Тогда в следующих случаях Алиса и Боб могут идти в первую подстроку:

- оба раунда тихие;

- первый раунд тихий, второй раунд потерянный;

- первый раунд потерянный, второй раунд тихий;

Если Боб в первом раунде получил 1, значит у Алисы случай — 011, и тогда если Боб во втором раунде молчит, то они идут во вторую подстроку. Если же он отправляет 1, то они идут в третью подстроку. Аналогично, если Алиса в первом раунде получила 1.

Если Боб во втором раунде получил 1, значит у Алисы случай — 101, и тогда если Боб в первом раунде молчал, то они идут в первую подстроку. Если же он отправлял 1, то они идут в третью подстроку. Аналогично, если Алиса во втором раунде получила 1. В итоге потребуется сделать $\log_3(n)$ шагов, и на каждом шаге потребуется отправить или принять 2 сообщения, то есть:

$$\mathrm{D}_0^{hd}(\mathrm{KW}_{\mathrm{RecMaj}_n}) \leq 2\log_3(n). \qquad \square$$

Рассмотрим отношение Карчмера-Вигдерсона для функции $\mathrm{THR}_{2,n}$. Игроки будут реализовывать троичный поиск и на каждом шаге, после деления текущей строки на 3 подстроки, будут считать для них THR_1, чтобы они смогли определить подстроку для дальнейшего перехода.

Теорема 9. $\mathrm{D}_s^{hd}(\mathrm{KW}_{\mathrm{THR}_{2,n}}) \leq \log_3(n) + \log_3(\log_3(n)) + 6$.

Доказательство. Пусть у Алисы $x \in \mathrm{THR}_{2,n}^{-1}(1)$, а у Боба $y \in \mathrm{THR}_{2,n}^{-1}(0)$. Заметим, что если $\sum\limits_{i=1}^{n} x_i > 2$, то Алиса может оставить только две единицы, инвертировав все оставшиеся. Поэтому достаточно рассмотреть случай, когда во входе Алисы только две единицы.

Алиса и Боб ищут бит различия, с помощью троичного поиска. На каждом шаге Алиса и Боб делят свои строки на три равные части и считают для каждой части $\mathrm{THR}_{1,\frac{n}{3^k}}$, где k — номер шага. У Алисы могут быть следующие случаи (1 обозначает, что THR_1 для соответствующей части равен 1, 0 — THR_1 равен 0):

(a) 110, 101, 011;

(b) 100, 010, 001.

У Боба могут быть следующие случаи:

(c) 000;

(d) 100, 010, 001.

В самом начале протокола Боб сообщает Алисе есть ли у него единица или нет. Если у Боба нет единицы, то Алиса отправляет Бобу номер любой своей единицы. Для этого она кодирует номер своей единицы в троичной записи и отправляет получившийся код. В этом случае потребуется $\lceil \log_3(n) \rceil + 1$ раундов.

Если у Боба есть единица, то может быть два случая в троичном поиске, в зависимости от того, как выглядит вход Алисы:

1. $(a) \to (b)$;

2. $(b) \to (a) \to (b)$.

Первый случай обозначает, что при первом разбиение строки на три части, мы получили две единицы, и потом перешли в ту часть, где одна единица. Второй случай обозначает, что первое разбиение нам дает только одну единицу и следующие несколько шагов поиска тоже будут только с одной единицей, пока мы не получим разбиение с двумя единицами, откуда перейдем в часть с одной единицей.

После сообщения Боба о наличие единицы, Алиса сообщает, какой сценарий троичного поиска будет у них. В первом случае Алиса сообщает Бобу какое у нее разбиение из (a), Боб сообщает, куда они должны перейти. Дальше Алиса сообщает в какую часть им надо переходить. В этом случае потребуется $\lceil \log_3(n) \rceil + 4$ раундов.

Основная сложность второго случая заключается в том, что Алиса без информации от Боба, не знает в какую часть нужно переходить, когда у нее разбиение из (a). Чтобы сделать правильный выбор ей нужно знать, какой случай у Боба. Алиса знает на каком шаге троичного поиска у нее появится две единицы в подстроке. Она сообщает Бобу номер уровня i в троичном дереве поиска и разбиение из (a). Боб смотрит на все подстроки, которые находятся на уровне i и выбирает ту подстроку, где есть единица и сообщает Алисе какой у него случай из (d). Для этого Боб отправляет: 0, если первый случай, 1, если второй случай, слушает, если третий случай. Эта информация, позволит Алисе понять, в какую часть им нужно идти, и Алиса сообщит Бобу номер этой части. В этом случае потребуется $\lceil \log_3(n) \rceil + \lceil \log_3(\log_3(n)) \rceil + 4$ раундов. В итоге:

$$\mathrm{D}_s^{hd}(\mathrm{KW}_{\mathrm{THR}_{2,n}}) \leq \log_3(n) + \log_3(\log_3(n)) + 6. \qquad \square$$

Рассмотрим отношение Карчмера-Вигдерсона для функции $\mathrm{THR}_{3,n}$. Покажем аналогичную оценку для этого отношения, используя похожую идею.

Теорема 10. $\mathrm{D}_s^{hd}(\mathrm{KW}_{\mathrm{THR}_{3,n}}) \leq \log_3(n) + \log_3(\log_3(n)) + 8.$

Доказательство. Пусть у Алисы $x \in \mathrm{THR}_{3,n}^{-1}(1)$, а у Боба $y \in \mathrm{THR}_{3,n}^{-1}(0)$. Заметим, что если $\sum_{i=1}^{n} x_i > 3$, то Алиса может оставить только три единицы, инвертировав все оставшиеся. Поэтому достаточно рассмотреть случай, когда во входе Алисы только три единицы.

Алиса и Боб ищут бит отличия с помощью троичного поиска. На каждом шаге Алиса и Боб делят свои строки на три равные части и считают для каждой части $\mathrm{THR}_{1,\frac{n}{3^k}}$, где k — номер шага. У Алисы могут быть следующие случаи (1 обозначает, что THR_1 для соответствующей части равен 1, 0 — THR_1 равен 0):

(a) 111;

(b) 110, 101, 011;

(c) 100, 010, 001.

У Боба могут быть следующие случаи:

(d) 000;

(e) 110, 101, 011;

(f) 100, 010, 001.

В самом начале протокола, Боб сообщает Алисе есть ли у него единицы или нет. Если у Боба нет единиц, то Алиса отправляет Бобу номер любой своей единицы. В этом случае потребуется $\lceil \log_3(n) \rceil + 1$ раундов.

Если у Боба есть единицы, то может быть несколько случаев в троичном поиске, в зависимости от того, как выглядит вход Алисы:

1. $(a) \to (c)$;
2. $(b) \to (b) \to (c)$;
3. $(b) \to (c) \to (b) \to (c)$;
4. $(c) \to (a) \to (c)$;
5. $(c) \to (b) \to (b) \to (c)$;
6. $(c) \to (b) \to (c) \to (b) \to (c)$;

Эти случаи описываются аналогично случаям в предыдущей теореме. После сообщения Боба о наличие единицы, Алиса сообщает, какой сценарий троичного поиска у них.

В первом случае Алиса сообщает, что у нее разбиение из трех единиц, Боб сообщает Алисе номер подстроки, в которой у него стоит ноль. После этого Алиса сообщает номер подстроки, в которую они переходят. Игроки переходят в подстроку, в которой у Алисы стоит 1, а у Боба стоит 0. В этом случае потребуется $\lceil \log_3(n) \rceil + 5$ раундов.

Во втором случае Алиса сообщает какое у нее разбиение из (b), Боб сообщает, какое у него разбиение, Алиса сообщает, в какую подстроку им надо перейти и новое разбиение из (b), после чего Боб в последний раз сообщает, какой у него случай Алисе, и дальше она собщает Бобу в какую подстроку им надо перейти. Игроки будут переходить в подстроку, в которой у Алисы стоит 1, а у Боба стоит 0. В этом случае потребуется $\lceil \log_3(n) \rceil + 5$ раундов.

В третьем случае Алиса сообщает Бобу свое разбиение из (b), Боб сообщает какой у него случай, Алиса говорит, в какую часть им надо перейти. Заметим, что если Боб переходит в 0, то Алиса знает об этом и она может дальше сообщать Бобу, куда им идти. Если Боб переходит в 1, то в поддереве, которое соответствует этой единице, будет только одна 1. Алиса смотрит на свое троичное дерево поиска и отправляет Бобу номер уровня i, в котором у нее во второй раз появляется случай из (b), и само разбиение. Боб смотрит, какой у него случай из разбиения (f) находится на уровне i, и сообщает об этом Алисе. После чего Алиса говорит, куда им надо и идти. В этом случае потребуется $\lceil \log_3(n) \rceil + \lceil \log_3(\log_3(n)) \rceil + 5$ раундов.

Четвертый случай аналогичен первому. В самом начале Алиса сообщает Бобу номер шага i, на котором у нее появится разбиение из (a) и Боб, спустя i сообщений от Алисы, собщает какое у него разбиение, чтобы Алиса приняла решение куда им дальше идти. Игроки будут переходить в подстроку, в которой у Алисы стоит 1, а у Боба стоит 0. В этом случае потребуется $\lceil \log_3(n) \rceil + \lceil \log_3(\log_3(n)) \rceil + 4$ раундов.

Пятый случай аналогичен второму. В самом начале Алиса сообщает через какое число шагов у них второй случай. Дальше они будут действовать, как во втором случае. В сумме потребуется $\lceil \log_3(n) \rceil + \lceil \log_3(\log_3(n)) \rceil + 5$ раундов.

В шестом случае Алиса отправляет Бобу номер уровня i, на котором у нее второй раз появится случай из (b). Боб сообщает Алисе, что у него происходит на уровне i. На нем могут быть либо две подстроки с одной 1, либо одна подстрока с двумя 1, либо одна подстрока с одной 1. Если у Боба одна подстрока с двумя 1, то Алисе, при первом появление разбиения из (b), нужно идти в ту часть с 1, в которой по итогу находится только одна единица. После i шагов поиска, Боб сообщает, какой у него случай. Либо игроки дальше продолжают переходить в единицу Алисы, либо игроки будут переходить в единицу Боба. Если у Боба одна подстрока с одной 1 или две подстроки с двумя 1, то Алисе, при первом появление разбиения из (b), надо идти в ту часть, в которой по итогу надоходится две единицы, и чтобы Алисе понять, в какую часть на шаге i надо перейти, Боб после i шагов отправляет какой у него случай из (f). Дальше игроки переходят в подстроку, в которой у Алисы стоит 1, а у Боба стоит 0. В этом случае потребуется $\lceil \log_3(n) \rceil + \lceil \log_3(\log_3(n)) \rceil + 6$ раундов.

Итого:

$$\mathrm{D}_s^{hd}(\mathrm{KW}_{\mathrm{THR}_{3,n}}) \leq \lceil \log_3(n) \rceil + \lceil \log_3(\log_3(n)) \rceil + 6. \qquad \square$$

Рассмотрим отношение Карчмера-Вигдерсона для функции $\mathrm{THR}_{4,n}$. Для этого отношения покажем менее слабую оценку, с использованием похожей идеи.

Теорема 11. $\mathrm{D}_s^{hd}(\mathrm{KW}_{\mathrm{THR}_{4,n}}) \leq \log_3(n) + 3\log_3\log_9(n) + 12$.

Доказательство. Пусть у Алисы $x \in \mathrm{THR}_{4,n}^{-1}(1)$, а у Боба $y \in \mathrm{THR}_{4,n}^{-1}(0)$. Заметим, что если $\sum_{i=1}^{n} x_i > 4$, то Алиса может оставить только четыре единицы, инвертировав все оставшиеся. Поэтому достаточно рассмотреть случай, когда во входе Алисы только четыре единицы.

Алиса и Боб ищут бит отличия с помощью девятиричного посика. На каждом шаге Алиса и Боб делят свои строки на девять равных частей и считают для каждой части $\mathrm{THR}_{1,\frac{n}{9^k}}$, где k — номер шага. У Алисы могут быть следующие случаи на каждом шаге (1 обозначает, что THR_1 для соответствующей части равен 1, 0 — THR_1 равен 0):

(a) 4 единицы в подстроках;

(b) 3 единицы в подстроках;

(c) 2 единицы в подстроках;

(d) 1 единица в подстроках.

У Боба могут быть следующие случаи:

(e) 3 единицы в подстроках;

(f) 2 единицы в подстроках;

(g) 1 единица в подстроках;

(h) 0 единиц в подстроках.

В самом начале протокола Боб сообщает Алисе есть ли у него единицы или нет. Если у Боба нет единиц, то Алиса отправляет номер любой своей единицы и в этом случае потребуется $\lceil \log_3(n) \rceil + 1$ бит.

Если у Боба есть единицы, следующие шаги в поиске зависят от того, как выглядит вход у Алисы.

1. У Алисы есть подстрока, в которой четыре единицы.

2. У Алисы на каком-то уровне в дереве поиска есть подстрока, в которой две единицы и эта подстрока, на следющих уровнях дерева поиска, делится на две подстроки, в каждой из которых по две единицы.

3. У Алисы есть три последовательные подстроки, в которых по две единицы, то есть в подстроке с двумя единицами, одна единица соответствует подстроке с двумя единицами и в этой подстроке, одна из единиц соответствует еще одной подстроке с двумя в единицами.

4. У Алисы есть подстрока, в которой три единицы.

После сообщения Боба о наличие единицы, Алиса сообщает, как выглядит ее вход и в зависимости от этого у них будут разные протоколы.

В первом случае, Алиса сообщает на каком шаге поиска i у нее подстрока, состоящая из 4 единиц. Боб после i шагов сообщает как выглядит его подстрока. Заметим, что в этом случае у Алисы и Боба есть подстрока, в которой у Алисы стоит 1, а у Боба стоит 0. Именно в эту подстроку и переходят игроки. В итоге, в этом случае потребуется: $\lceil \log_3(n) \rceil + \lceil \log_3(\log_9(n)) \rceil + 11$ раундов.

Во втором случае, Алиса сообщает три номера в дереве поиске: i, j, l (j может быть равно l). Где i соответствует уровню в дереве поиска, где Алисе впервые встретилась подстрока с двумя единицами, l соответствует уровню в дереве поиска, где у Алисы второй раз находится подстрока с двумя единицами, а j соответсвует уровню в дереве поиска, где в третьи раз находится подстрока с двумя единицами. Боб смотрит на свое дерево и сообщает Алисе, какой у него случай на шаге j. У Боба могут быть следующие случаи:

1. 111;

2. 11, 1;

3. 1, 1, 1;

4. 1, 1;

5. 11;

6. 1;

Первый случаи обозначает, что на уровне j у Боба только одна подстрока, в которой находятся 3 единицы. Второй случай обозначает, что на уровне i у Боба две подстроки, в одной подстроки находятся 2 единицы, а в оставшейся находится только одна единица. Остальные случаи описываются аналогично.

Если у Боба случай (1), то Алиса на шаге i переходит в подстроку, в которой на уровне j находятся две единицы. Если после j шагов Боб оказывается в подстроке с 3 единицами, то он сообщает, где у него стоят эти единицы, и игроки переходят в подстроку, где у Алисы стоит 0, а у Боба стоит 1. Иначе, игроки переходят в подстроку, где у Алисы стоит 1, а у Боба стоит 0. Если у Боба случаи (3), (4), (6), то Алиса на шаге i переходит в подстроку, в которой на уровне j находятся две единицы. Если после j шагов Боб оказался в подстроке с одной единицей, то он сообщает ее номер, и игроки переходят в подстроку, где у Алисы стоит 1, а у Боба стоит 0. Иначе, игроки переходят в подстроку, где у Алисы стоит 1, а у Боба стоит 0. Если у Боба случай (5), то на уровне i у него только одна подстрока с одной единицей и после i шага он сообщает Алисе ее номер и игроки переходят в подстроку, где у Алисы стоит 1, а у Боба стоит 0. Иначе, игроки переходят в подстроку, где у Алисы стоит 1, а у Боба стоит 0. Если у Боба случий (2), значит у него где-то на более раннем шаге либо подстрока с одной единицей, либо подстрока с двумя единицами. Если у Боба одна единица после шага i, то игроки после i шага переходят в подстроку, где у Алисы стоит 1, а у Боба стоит 0. Если у Боба две единицы после шага i, то может быть следующие случаи:

- Единица Алисы, в которой находится две единицы на уровне j, совпала с единицей Боба, в которой находится две единицы на уровне j. Тогда Алиса после i шага переходит в подстроку, в которой находится две единицы на уровне l. Боб же после l шага, сообщает номер своей единицы и игроки переходят в подстроку, в которой у Алисы стоит 1, а у Боба стоит 0.

- Ни одна единица Боба не совпала с единицами Алисы. Тогда игроки иепереходят в подстроку, в которой у Алисы стоит 1, а у Боба стоит 0.

- Единица Алисы, в которой находится две единицы на уровне l, совпала с единицей Боба, в которой находится две единицы на уровне j. Тогда Алиса после i шага переходит в подстроку, в которой находится две единицы на уровне j. Боб же после j шагов, сообщает номер своей единицы и игроки переходят в подстроку, в которой у Алисы стоит 1, а у Боба стоит 0.

В итоге, в этом случае потребуется: $\lceil \log_3(n) \rceil + 3\lceil \log_3(\log_9(n)) \rceil + 10$ раундов.

В третьем случае, Алиса сообщает два номера в дереве поиске: i и j, где i соответствует шагу, где Алиса впервые встретила подстроку с двумя единицами, а j соответствует шагу, где Алисе в последний раз встретила подстроку с двумя единицами. Боб смотрит на свое дерево и сообщает Алисе, какой у него случай (1) — (6) на шаге j. Если у Боба слуйчай (1), то Алиса на шаге i переходит в ту подстроку, в которой суммарно находится 3 единицы. Если после j шагов Боб оказывается в подстроке с 3 единицами, то он сообщает их номера. Дальше игроки переходят в подстроку, где у Алисы стоит 0, а у Боба стоит 1. Иначе, игроки переходят в подстроку, где у Алисы стоит 1, а у Боба стоит 0. Если у Боба случаи (3), (4), (6), то Алиса на шаге i переходит в ту подстроку, в которой суммарно находится 3 единицы. Боб через j шагов сообщает их номера в текущей подстроке и игроки переходят в ту подстроку, где у Алисы стоит 1, а у Боба стоит 0. Если у Боба случай (5), то Алиса на шаге i переходит в ту подстроку, в которой находится одна единица. Если после j шагов Боб оказавается в подстроке с 2 единицами, то он сообщает их номера. Игроки переходят в подстроку, где у Алисы стоит 0, а у Боба стоит 1. Иначе, игроки переходят в подстроку, где у Алисы стоит 1, а у Боба стоит 0. Если у Боба случай (2), значит у него где-то на более раннем шаге либо подстрока с одной единицей, либо подстрока с двумя единицами. Боб через i шагов сообщает Алисе номера свох диниц. Если у Боба одна единица, то игроки переходят в подстроку, где у Алисы стоит 1, а у Боба стоит 0. Если у Боба две единицы, то могут быть следующие случаи:

- Единица Алисы, в которой в сумме находится три единицы, совпала с 1 Боба, в которой находится две единицы на уровне j. Тогда Алиса на шаге i переходит в подстроку, в которой у нее в сумме три единицы. При следующем появление подстроки с двумя единицами, она переходит в 1 с ровно одной единицей на уровне j. Боб на шаге j сообщает Алисе номера своих единицы. Дальше игроки переходят в подстроку, в которой у Алисы стоит 0, а у Боба стоит 1. Иначе, в подстроку, в которой у Алисы стоит 1, а у Боба стоит 0.

- Единица Боба, в которой находится две едницы на уровне j, совпала с 1 Алисы в которой нахдится одна единица на уровне j. Тогда Алиса переходит в подстроку, в которой у нее одна единица на уровне j. Боб на шаге j сообщает Алисе номера своих единицы. Дальше игроки переходят в подстроку, в которой у Алисы стоит 0, а у Боба стоит 1. Иначе, в подстроку, в которой у Алисы стоит 1, а у Боба стоит 0.

- Ни одна единица Боба не совпала с единицами Алисы. Тогда игроки переходят в подстроку, в которой у Алисы стоит 1, а у Боба стоит 0.

В итоге, в этом случае потребуется: $\lceil \log_3(n) \rceil + \lceil \log_3(\log_9(n)) \rceil + 10$ раундов.

В последнем случае, Алиса отправляет два номера уровней в своем дереве. Первый номер i соответствует уровню, где у Алисы впервые появляется подстрока с тремя единицами. Второй номер j соответствует уровню, когда у Алисы появляется подстрока

с двумя единицами. Боб смотрит на свое дерево, а именно на уровень j и сообщает Алисе, какой у него случай (1) — (6). Если у Боба случаи (1), (3), (4), (6), то Алиса на уровне i переходит в 1, в которой находится две единицы на уровне j. Боб после j раундов от Алисы сообщает нмоера своих единиц. Дальше игроки переходят либо в подстроку, где у Алисы стоит 1, а у Боба стоит 0, либо в подстроку, где у Алисы стоит 0, а у Боба стоит 1 и меняются ролями, то есть теперь Боб сообщает, в какую подстроку им переходить. Если у Боба случай (5), то Алиса на уровне i переходит в 1, где стоит одна единица. Боб после j раундов сообщает номера своих единиц. Дальше игроки переходят либо в подстроку, где у Алисы стоит 1, а у Боба 0, либо в подстроку, где у Алисы стоит 0, а у Боба стоит 1 и меняются ролями. Если у Боба случай (2), то Боб через i шагов сообщает нмоера своих единиц. В ответ, Алиса сообщает номер подстроки, куда им надо перейти. Заметим, что в этом случае игроки перейдут в ту подстроку, где у Алисы стоит 1, а у Боба стоит 0.

Итого:

$$\mathrm{D}_s^{hd}(\mathrm{KW}_{\mathrm{THR}_{4,n}}) \leq \log_3(n) + 3\log_3\log_9(n) + 12. \qquad \square$$

Следующая теорема устанавливает нижние оценки на полудуплексную коммуникационную сложность игр Карчмера-Вигдерсона для пороговых функций.

Теорема 12. *Для константы $k > 4$ верно:*

1. $\mathrm{D}_s^{hd}(\mathrm{KW}_{\mathrm{THR}_{k,n}}) \geq \frac{\log_2(k(n-k+1))}{2}$,
2. $\mathrm{D}_0^{hd}(\mathrm{KW}_{\mathrm{THR}_{k,n}}) \geq 0.71\log_2(k(n-k+1))$,
3. $\mathrm{D}_a^{hd}(\mathrm{KW}_{\mathrm{THR}_{k,n}}) \geq \log_2(k(n-k+1))$.

Доказательство. Путь $(\mathcal{X}, \mathcal{Y})$ пара случайных величин, задающие совместное распределение на входах Алисы и Боба, где случайная величина $\mathcal{X}$ равномерно распределена на множестве: $\{x \in \{0,1\}^n \mid \|x\|_1 = k\}$, которое соответсвует входам Алисы, а случайная величина $\mathcal{Y}$ отличается от случайной величины $\mathcal{X}$ ровно в одном бите, где у $\mathcal{X}$ стоит единица. Следовательно $H(\mathcal{X} \mid \mathcal{Y}) \geq \log_2(n-k+1)$, а $H(\mathcal{Y} \mid \mathcal{X}) \geq \log_2(k)$. То есть, перед началом коммуникации верно.

$$H(\mathcal{X} \mid \mathcal{Y}) + H(\mathcal{Y} \mid \mathcal{X}) \geq \log_2(k(n-k+1)) \geq \log_2(n).$$

С другой стороны, по паре входов из распределения $(\mathcal{X}, \mathcal{Y})$ игроки могут однозначно определить индекс бита различия. Следовательно, по завершению коммуникации, оба игрока знают входы друг друга. То есть, верно.

$$H(\mathcal{X} \mid \mathcal{Y}, \Pi_A) + H(\mathcal{Y} \mid \mathcal{X}, \Pi_B) = 0,$$

где случайные величины Π_A и Π_B соответствуют расшифровкам протокола Алисы и Боба. Таким образом, за коммуникацию игроки должны передать хотя бы $\log_2(k(n-k+1))$ бит информации. Применяя оценки на количество информации передаваемые в одном раунде, получаем соответсвующие оценки.

1. Из теоремы 4 получаем нижнюю оценку в полудуплексной модели с тишиной: $\mathrm{D}_s^{hd}(\mathrm{KW}_{\mathrm{THR}_{k,n}}) \geq \frac{\log_2(k(n-k+1))}{2}$.

2. Из теоремы 5 получаем нижнюю оценку в полудуплексной модели с нулем: $\mathrm{D}_0^{hd}(\mathrm{KW}_{\mathrm{THR}_{k,n}}) \geq 0.71 \log_2(k(n-k+1))$.

3. Из теоермы 6 получаем нижнюю оценку в полудуплексной модели с противником: $\mathrm{D}_a^{hd}(\mathrm{KW}_{\mathrm{THR}_{k,n}}) \geq \log_2(k(n-k+1))$. □

Следствие 3.1. *Для $k = \frac{n}{2}$ верно:*

1. $\mathrm{D}_s^{hd}(\mathrm{KW}_{\mathrm{THR}_{k,n}}) \geq \log_2(n)$,

2. $\mathrm{D}_0^{hd}(\mathrm{KW}_{\mathrm{THR}_{k,n}}) \geq 1.42 \log_2(n)$,

3. $\mathrm{D}_a^{hd}(\mathrm{KW}_{\mathrm{THR}_{k,n}}) \geq 2 \log_2(n)$.

4. Заключение

В данной работе, продолжено исследование полудуплексной коммуникационной сложности, начатое в статье [5]. Была изучена сложность пороговых функции. Получены верхние оценки на полудуплексную коммуникационную сложность в модели с тишиной, и нижние оценки для всех трех моделей. В частности получены нижние оценки на полудуплексную коммуникационную сложность для функции большинства во всех трех моделях. Помимо пороговых функции была изучена рекурсивная функция большинства, для которой получены верхние оценки в моделях с тишиной и с нулем.

Список литературы

[1] Boppana R. B. Amplification of probabilistic boolean formulas // 2013 IEEE 54th Annual Symposium on Foundations of Computer Science. — Los Alamitos, CA, USA : IEEE Computer Society. — 1985. — P. 20–29. — Access mode: https://doi.ieeecomputersociety.org/10.1109/SFCS.1985.5.

[2] Buhrman H. Communication complexity: Eyal Kushilevitz, Noam Nisan, Cambridge University Press, Cambridge, 1997. ISBN 0-56067-5 // Science of Computer Programming. — 1999. — Vol. 33.

[3] Chandra A. K., Furst M. L., Lipton R. J. Multi-Party Protocols // Proceedings of the 15th Annual ACM Symposium on Theory of Computing, 25-27 April, 1983, Boston, Massachusetts, USA / ed. by Johnson D. S., Fagin R., Fredman M. L. et al. — ACM. — 1983. — P. 94–99. — Access mode: https://doi.org/10.1145/800061.808737.

[4] Communication complexity towards lower bounds on circuit depth / Edmonds J., Impagliazzo R., Rudich S., and Sgall J. // Comput. Complex. — 2001. — Vol. 10, no. 3. — P. 210–246. — Access mode: https://doi.org/10.1007/s00037-001-8195-x.

[5] Half-Duplex Communication Complexity / Hoover K., Impagliazzo R., Mihajlin I., and Smal A. V. // 29th International Symposium on Algorithms and Computation, ISAAC 2018, December 16-19, 2018, Jiaoxi, Yilan, Taiwan / ed. by Hsu W., Lee D., Liao C. — Schloss Dagstuhl - Leibniz-Zentrum für Informatik. — 2018. — Vol. 123 of LIPIcs. — P. 10:1–10:12. — Access mode: https://doi.org/10.4230/LIPIcs.ISAAC.2018.10.

[6] How to compress interactive communication / Barak B., Braverman M., Chen X., and Rao A. // STOC '10. — 2010.

[7] Karchmer M., Raz R., Wigderson A. Super-Logarithmic Depth Lower Bounds Via the Direct Sum in Communication Complexity // Comput. Complex. — 1995. — Vol. 5, no. 3/4. — P. 191–204. — Access mode: https://doi.org/10.1007/BF01206317.

[8] Karchmer M., Wigderson A. Monotone Circuits for Connectivity Require Super-logarithmic Depth // Proceedings of the 20th Annual ACM Symposium on Theory of Computing, May 2-4, 1988, Chicago, Illinois, USA / ed. by Simon J. — ACM. — 1988. — P. 539–550. — Access mode: https://doi.org/10.1145/62212.62265.

[9] Laplante S., Lee T., Szegedy M. The Quantum Adversary Method and Classical Formula Size Lower Bounds // 20th Annual IEEE Conference on Computational Complexity (CCC 2005), 11-15 June 2005, San Jose, CA, USA. — IEEE Computer Society. — 2005. — P. 76–90. — Access mode: https://doi.org/10.1109/CCC.2005.29.

[10] Mihajlin I., Smal A. Toward Better Depth Lower Bounds: The XOR-KRW Conjecture // 36th Computational Complexity Conference, CCC 2021, July 20-23, 2021, Toronto, Ontario, Canada (Virtual Conference) / ed. by Kabanets V. — Schloss Dagstuhl - Leibniz-Zentrum für Informatik. — 2021. — Vol. 200 of LIPIcs. — P. 38:1–38:24. — Access mode: https://doi.org/10.4230/LIPIcs.CCC.2021.38.

[11] New bounds on the half-duplex communication complexity / Dementiev Y., Ignatiev A., Sidelnik V., Smal A., and Ushakov M. // Electron. Colloquium Comput. Complex. — 2020. — P. 117. — Access mode: https://eccc.weizmann.ac.il/report/2020/117.

[12] Radhakrishnan J. Better Lower Bounds for Monotone Threshold Formulas // J. Comput. Syst. Sci. — 1997. — Vol. 54. — P. 221–226.

[13] Toward better formula lower bounds: an information complexity approach to the KRW composition conjecture / Gavinsky D., Meir O., Weinstein O., and Wigderson A. // Proceedings of the forty-sixth annual ACM symposium on Theory of computing. — 2013.

[14] Yao A. C. Some Complexity Questions Related to Distributive Computing (Preliminary Report) // Proceedings of the 11h Annual ACM Symposium on Theory of Computing, April 30 - May 2, 1979, Atlanta, Georgia, USA / ed. by Fischer M. J., DeMillo R. A., Lynch N. A. et al. — ACM. — 1979. — P. 209–213. — Access mode: https://doi.org/10.1145/800135.804414.