

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ
ФГАОУ ВО НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»

Факультет компьютерных наук
Образовательная программа «Прикладная математика и информатика»

**Отчет об исследовательском проекте на тему:
Полудуплексная коммуникационная сложность**

Выполнил:

студент группы БПМИ229
Маркелов Юрий Сергеевич

(подпись)

(дата)

Принял руководитель проекта:

Николай Константинович Верещагин
Штатный преподаватель
Факультета компьютерных наук НИУ ВШЭ

(подпись)

(дата)

Москва 2024

Аннотация

В данной статье рассматриваются модели коммуникационной сложности, обобщающие классическую модель Анрю Яо: модели с полудуплексным каналом и различными вариантами тихого раунда, в том числе со "слабым противником". Оценивается коммуникационная сложность функции в различных моделях. Предложен улучшенный протокол, с помощью которого удалось сократить множество одного из игроков в модели со слабым противником. А также впервые предложен протокол для функции с образом $\{0, 1\}$, отделяющий классическую коммуникационную сложность от полудуплексной сложности со слабым противником. Полученные результаты позволяют лучше понять границы коммуникационной сложности в различных моделях.

Список ключевых слов: коммуникационная сложность, полудуплексный канал, тихий раунд, алгоритм, оценка, стратегия.

Содержание

1. Введение

1.1 Определение классической коммуникационной модели

1.2 Определение полудуплексной модели

1.3 Определение коммуникационной сложности

2. Полудуплексная коммуникационная сложность со слабым противником

3. Пример улучшенного протокола

4. Пример протокола для функции с образом $\{0, 1\}$

5. Выводы и дальнейшие исследования

Источники

1. Введение

1.1 Определение классической коммуникационной модели

В классической модели коммуникационной сложности, введённой Андрю Яо в работе [3], рассматривается игра для двух игроков, Алисы и Боба, которые хотят вычислить $f(x,y)$ для некоторой функции f , причём Алисе известно только значение x , а Бобу — только значение y . Для решения этой задачи Алиса и Боб могут общаться, посылая друг другу битовые сообщения по одному биту за раунд. Важное свойство этой коммуникационной модели заключается в том, что на каждом раунде общения один из игроков посылает некоторое битовое сообщение, а другой игрок обязательно его принимает.

1.2 Определение полудуплексной модели

В работе Hoover, K., Impagliazzo, R., Mihajlin, I., Smal, A. V. [4] определены три новые модели коммуникационной сложности, которые обобщают классическую модель и описывают общение по так называемому полудуплексному каналу. Широко известный пример полудуплексного канала в обычной жизни — это общение при помощи раций: для передачи сообщения по рации нужно нажать кнопку передачи (принцип «push-to-talk»), в то же время на принимающей стороне в этот момент кнопка должна быть отпущена. Если два человека пытаются передавать сообщения одновременно (т.е. у обоих рации находятся в режиме передачи), то они не слышат друг друга. Мы будем рассматривать коммуникационные модели, в которых игрокам разрешено передавать сообщения одновременно, но в этом случае эти сообщения теряются.

Общение точно так же будет разбито на раунды. На каждом раунде каждый игрок выбирает одно из трёх действий: отправить 0, отправить 1 или принимать. Таким образом, могут быть три типа раундов:

- 1) Если один из игроков посылает некоторый бит, а другой игрок принимает (классический раунд), в котором гарантируется, что принимающий игрок получит именно то сообщение, которое было передано посылающим игроком.
- 2) Если оба игрока посылают некоторые биты, то такой раунд называется потерянным, при этом игроки об этом не знают.
- 3) Если оба игрока принимают сообщение, то раунд называется тихим. Модели различаются вариациями в тихом раунде. В работе А.В. Смаля [2] рассмотрены 3 варианта модели: оба игрока понимают в тихом раунде, что произошел тихий раунд (модель с “тишиной”), оба игрока получают 0 в тихом раунде (модель с нулём) и оба игрока получают случайные биты, которые могут быть разными в разных раундах (модель с противником).

1.3 Определение коммуникационной сложности

Определения взяты из работы А.В. Смаля [2]:

Определение 1 Коммуникационный протокол для функции $f: X \times Y \rightarrow Z$ — это корневое двоичное дерево с пометками. Каждая внутренняя вершина v помечена меткой «А» или «Б», а каждый лист помечен значением из множества Z . Кроме того, для каждой вершины, помеченной «А», определена функция $g_v: X \rightarrow \{0,1\}$, а для каждой вершины u с пометкой «Б» определена функция $h_u: Y \rightarrow \{0,1\}$. Каждая внутренняя вершина имеет двух потомков, ребро к первому потомку помечено 0, а ребро ко второму потомку помечено 1.

Общение по такому протоколу на конкретной паре входов (x,y) соответствует пути от корня к некоторому листу. Игроки начинают «находясь» в корне и дальше спускаются к листу. В каждой внутренней вершине v этого пути в зависимости от пометки либо Алиса (пометка «А»), либо Боб (пометка «Б») пересылает один бит, который равен, соответственно, $g_v(x)$ или $h_v(y)$. После этого игроки «переходят» в одного из потомков вершины v по ребру, пометка которого совпадает с битом, переданным в вершине v . Когда игроки достигают листа, то их общение завершается. Результатом является пометка в этом листе.

Определение 2 Будем говорить, что коммуникационный протокол вычисляет функцию f , если для всех пар $(x,y) \in X \times Y$ общение игроков завершается в листе с пометкой $f(x,y)$.

Теперь можно дать формальное определение коммуникационной сложности функции f .

Определение 3 Коммуникационная сложность функции f определяется как наименьшая глубина протокола (максимальная рёберная длина пути от корня до листа), вычисляющего функцию f , и обозначается через $CC(f)$.

Определение 4 Полудуплексный коммуникационный протокол с противником, решающий коммуникационную задачу для функции $f: X \times Y \rightarrow Z$ — это пара корневых деревьев (TA, TB) , которые описывают коммуникацию Алисы и Боба на всех парах входов $(x,y) \in X \times Y$ и для всех стратегий противника $w \in \{0,1\}^*$. Множества возможных действий и множество возможных событий определяются как $\mathcal{A} = \{\text{послать}(0), \text{послать}(1), \text{принимать}\}$ и $\mathcal{B} = \{\text{послал}(0), \text{послал}(1), \text{получил}(0), \text{получил}(1)\}$. Если в некотором раунде i оба игрока решили принимать сообщения, то Алиса получает бит w_{2i-1} , а Боб — 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 $f(x,y)$.

Определение 5 Минимальная глубина полудуплексного коммуникационного протокола, решающего коммуникационную задачу для функции f с противником определяет полудуплексную коммуникационную сложность функции f с противником $CC_a^{hd}(f)$. (hd - half duplex, a - adversary)

2. Полудуплексная коммуникационная сложность со слабым противником

Мы будем рассматривать четвертую вариацию этой модели, введенную в совместной работе Дегтярева и Верещагина [1]. В этой модели в тихом раунде Алиса и Боб получают одинаковые биты 0 и 0 или 1 и 1, в разных тихих раундах полученные биты могут отличаться. Модель называется моделью со слабым противником (в оригинале “weak” adversary).

Несложно заметить, что любую коммуникацию в классической модели можно повторить и в полудуплексной модели используя только классические раунды. В то же время, полудуплексную коммуникацию со слабым противником можно моделировать в классической модели, если удвоить число раундов. Таким образом, полудуплексная коммуникационная сложность функции ограничена сверху классической сложностью, а снизу — классической сложностью деленной на два.

Наша цель уточнить эту оценку для полудуплексной модели со слабым противником.

В работе Верещагина и Дегтярева [1] был приведен пример, в котором полудуплексная сложность со слабым противником не более 3, а классическая сложность хотя бы 4. В рассматриваемом примере множества Алисы и Боба состоят из 5 элементов.

3. Пример улучшенного протокола

Мне удалось усовершенствовать вышеупомянутую модель - изменить протокол, так что появилась возможность сократить множество Боба до 4 элементов.

Пусть множество Алисы $X = \{r, 00, 01, 10, 11\}$, множество Боба $Y = \{r, 00, 01, 10\}$ и множество исходов $Z = \{0, 1, 2\}$. Сначала мы спроектируем 3-раундовый полудуплексный протокол, вычисляющий функцию $f: X \times Y \rightarrow Z$ (против слабого противника), и затем мы докажем, что его классическая сложность хотя бы 4.

В этом протоколе только первый раунд не является классическим. В этом раунде оба игрока в зависимости от своих входов выбирают одно из трех действий. Это действие определяется первым символом входа: r означает "получить", а $0,1$ - "отправить $0,1$ ", соответственно. Во втором раунде Боб отправляет бит, а Алиса получает, а в третьем раунде - наоборот. Если Боб в первом раунде получал бит, то он во втором раунде отправляет Алисе обратный бит от полученного в первом раунде. Если Алиса в первом раунде получала бит, то она отправляет этот же бит в третьем раунде. В противном случае игроки отправляют вторые биты своих входов.

Результат протокола - это функция битов, отправленных (и полученных) во втором и третьем раундах (в дальнейшем мы будем называть его 2-3-транскриптом). Поскольку эти

раунды являются классическими, это гарантирует, что Алиса и Боб выдадут один и тот же результат, что бы ни произошло в первом раунде.

Давайте посмотрим, чему равен результат протокола. Если вход Боба равен r , а вход Алисы нет, то 2-3-транскрипт состоит из отрицания первого бита входа Алисы и её второго бита. Если вход Алисы равен r , а Боба нет, то 2-3-транскрипт совпадает с развёрнутым входом Боба. Если оба входа Алисы и Боба равны 0, 1, то 2-3-транскрипт формируется из вторых битов Боба и Алисы. Наконец, если оба входа Алисы и Боба равны r , то 2-3-транскрипт равен либо 01, либо 10, так как мы предполагаем слабого противника.

2-3-транскрипт показан в таблице 1, где вход Алисы обозначает первый столбец, а Боба - первая строка.

Таблица 1. 2-3-транскрипт - биты отправленные и полученные в 2 и 3 раундах

	r	00	01	10
r	01 или 10	00	10	01
00	10	00	10	00
01	11	01	11	01
10	00	00	10	00
11	01	01	11	01

Мы определим выходную функцию как 2-3-транскрипт с идентифицированными 01 и 10. Представим 2-3-транскрипт натуральными числами.

Таблица 2 является таблицей значений функции f , которую мы построили.

Таблица 2. Таблица значений функции f .

	r	00	01	10
r	2	0	2	2
00	2	0	2	0
01	1	2	1	2
10	0	0	2	0
11	2	2	1	2

Ключевой момент заключается в следующем: после тихого раунда мы пользуемся информацией, что в нём были получены одинаковые биты.

Чтобы оценить снизу классическую коммуникационную сложность воспользуемся методом трудного множества из книги Nisan - Kushilevitz [5] (в оригинале “fooling set”).

Определение 6 Множество $F \subseteq X \times Y$ называется трудным множеством для функции $f : X \times Y \rightarrow Z$, если для всех различных пар $(x, y), (u, v) \in F$ не все значения $f(x, y), f(u, v), f(x, v), f(u, y)$ равны.

Метод трудного множества (fooling set)

Для любого трудного множества F для функции $f : X \times Y \rightarrow Z$: $CC(f) \geq \log_2 |F|$, где $CC(f)$ - коммуникационная сложность.

В Таблице 3 указано трудное множество размера 9 для нашей функции f . Значит $CC(f)$ хотя бы 4.

Для большей наглядности и полноты изложения покажем, что $CC(f) = 4$. Построим пример протокола в классической модели для 4 раундов. В первые 2 раунда Алиса будет слушать, а во вторые два Боб. Так как у Боба множество состоит из 4 элементов, то он за 2 раунда может передать Алисе, какой элемент у него. Далее Алиса будет знать ответ из множества $Z = \{0, 1, 2\}$ и за 2 раунда сможет передать Бобу этот ответ.

Таблица 3. Трудное множество размера 9 для функции f .

	г	00	01	10
г	2	0	2	2
00	2	0	2	0
01	1	2	1	2
10	0	0	2	0
11	2	2	1	2

4. Пример протокола для функции с образом $\{0, 1\}$

Данный пример является основным результатом этого исследовательского проекта. Впервые предложен протокол для функции с образом $\{0, 1\}$, отделяющий классическую коммуникационную сложность от полудуплексной сложности со слабым противником.

Решение во многом похоже на решение пункта 4, но своими небольшими отличиями и даёт продвижение в задаче.

Пусть множество Алисы $X = \{r0, r1, 00, 01, 10, 11\}$, множество Боба $Y = \{r0, r1, 00, 01, 10, 11\}$ и множество исходов $Z = \{0, 1\}$. Поступим аналогично предыдущему примеру: спроектируем 3-раундовый полудуплексный протокол, вычисляющий функцию $f: X \times Y \rightarrow Z$ (против слабого противника), и докажем, что его классическая сложность хотя бы 4.

В этом протоколе только первый раунд не является классическим. В этом раунде оба игрока в зависимости от своих входов выбирают одно из трех действий. Это действие определяется первым символом входа: r означает "получить", а $0,1$ - "отправить $0,1$ ", соответственно. Во втором раунде Боб отправляет бит, а Алиса получает, а в третьем раунде - наоборот.

Если Боб в первом раунде получил бит 0 , то он во втором раунде отправляет Алисе обратный бит от второго символа входа. Если Боб в первом раунде получил бит 1 или отправлял, то он во втором раунде отправляет Алисе второй символ входа.

Алиса аналогично Бобу поступает в 3 раунде.

Результат протокола - это функция битов, отправленных (и полученных) во втором и третьем раундах (в дальнейшем мы будем называть его 2-3-транскриптом). Поскольку эти раунды являются классическими, это гарантирует, что Алиса и Боб выдадут один и тот же результат, что бы ни произошло в первом раунде.

Давайте посмотрим, чему равен результат протокола.

2-3-транскрипт показан в таблице 4, где вход Алисы обозначает первый столбец, а Боба - первая строка.

Таблица 4. 2-3-транскрипт - биты отправленные и полученные в 2 и 3 раундах

	r0	r1	00	01	10	11
r0	00 или 11	01 или 10	01	11	00	10
r1	01 или 10	00 или 11	00	10	01	11
00	10	00	00	10	00	10
01	11	01	01	11	01	11
10	00	10	00	10	00	10
11	01	11	01	11	01	11

Мы определим выходную функцию как 2-3-транскрипт с 0 в клетке, если биты в 2-3-транскрипте разные и с 1 , если одинаковые. Заметим, что это сохраняет корректность в случае тихого раунда.

Таблица 5 является таблицей значений функции f , которую мы построили.

Таблица 5. Таблица значений функции f .

	r0	r1	00	01	10	11
r0	1	0	0	1	1	0
r1	0	1	1	0	0	1
00	0	1	1	0	1	0
01	1	0	0	1	0	1
10	1	0	1	0	1	0
11	0	1	0	1	0	1

Ключевой момент заключается в следующем: после тихого раунда мы пользуемся информацией, что в нём были получены одинаковые биты. Оба будут или менять, или оставлять свой второй бит.

В Таблице 6 указано трудное множество размера 12 для нашей функции f . Значит $CC(f)$ хотя бы 4.

Для большей наглядности и полноты изложения вновь покажем, что $CC(f) = 4$. Построим пример протокола в классической модели для 4 раундов. Первые 3 раунда Алиса будет слушать, а последний говорить. Так как у Боба множество состоит из 6 элементов, то он за 3 раунда может передать Алисе, какой элемент у него. Дальше Алиса будет знать ответ из множества $Z = \{0, 1\}$ и за 1 раунд сможет передать Бобу этот ответ.

Таблица 6. Трудное множество размера 12 для функции f .

	r0	r1	00	01	10	11
r0	1	0	0	1	1	0
r1	0	1	1	0	0	1
00	0	1	1	0	1	0
01	1	0	0	1	0	1
10	1	0	1	0	1	0
11	0	1	0	1	0	1

5. Выводы и дальнейшие исследования

Коммуникационные модели с функцией с образом $\{0, 1\}$ хорошо изучены. Построенный пример отделяющий полудуплексную модель со слабым противником от классической модели с функцией с образом $\{0, 1\}$ открывает просторы для следующих исследований с использованием методов для этого класса моделей.

Дальнейшее исследование может развиваться в нескольких направлениях:

1. Изучение расширения этого метода на многомерные пространства, как будто Алиса и Боб играют несколько игр подряд по этим правилам.

2. Модель тихого раунда с 0 - аналогична “очень слабому” противнику, который может давать только 1 из 4 наборов: 00. Она хорошо изучена.

В модели со слабым противником, он может давать 2 из 4 наборов: 00 и 11. В нашей статье мы привели новый пример отделения этой модели от классической.

В модели с противником, он может давать все 4 набора из 4: 00, 01, 10, 11. Отделимость от классической модели - открытая проблема.

На мой взгляд, логичным продолжением будет изучение модели, в которой противник сможет давать 3 из 4 наборов Алисе и Бобу, например, 00, 01 и 10.

Источники

1. Dektiarev M., Vereshchagin N.K. Half-duplex communication complexity with adversary can be less than the classical communication complexity. (2023)
<https://eccc.weizmann.ac.il/report/2023/011/>
2. Смаль А.В. Доказательство нижних оценок на размер формул для булевых функций методами коммункационной сложности. (2022)
3. Yao, A. C.-C. Some Complexity Questions Related to Distributive Computing (Preliminary Report) // STOC 1979. — ACM, 1979. — С. 209—213. — URL: <http://doi.acm.org/10.1145/800135.804414>.
4. Hoover, K., Impagliazzo, R., Mihajlin, I., Smal, A. V. Half-Duplex Communication Complexity // ISAAC 2018. V. 123. — Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2018. — 10:1—10:12. — (LIPIcs). — <https://doi.org/10.4230/LIPIcs.ISAAC.2018.10>
5. Eyal Kushilevitz, Noam Nisan, Communication Complexity, Cambridge University Press (2006)