Санкт–Петербургский государственный университет

УШАКОВ Михаил Сергеевич

Выпускная квалификационная работа

О некоторых вопросах полудюплексной коммуникационной сложности булевых функций

Уровень образования: бакалавриат
Направление 01.03.01 «Математика»
Основная образовательная программа СВ.5000.2018 «Математика»

Научный руководитель:
доцент, к.ф.-м.н. А. Ю. Авдюшенко

Рецензент:
Разработчик ООО «техкомпания Хуавей»
М. Г. Слободкин

Санкт-Петербург
2022 г.

Содержание

Введение

В классической модели коммуникационной сложности, предложенной Яо [6], два игрока — Алиса и Боб хотят вычислить значение $f(x, y)$ для некоторой булевой функции f. Изначально Алиса имеет только битовую строчку x, а Боб — y. Они могут общаться, посылая друг другу биты, по одному за раунд. В конце коммуникации игроки должны знать результат $f(x, y)$. Например Алиса может отправить все биты своей строки Бобу, после чего он может посчитать значение функции $f(x, y)$ и отправить результат Алисе. Однако обычно существуют более эффективные с точки зрения количества отправленных друг другу битов коммуникационные протоколы.

Важным ограничением классической модели является то, что за один раунд только один игрок может посылать бит. В статье [2] рассматривается расширение модели, суть которого заключается в том, что игрокам позволяется посылать биты одновременно. Такой канал связи называется полудуплексным. Пример такого канала — общение по рации. Особенность этой модели заключается в том, что в один момент времени игрок может либо только говорить, либо только слушать. То есть если собеседники попытаются говорить одновременно, то оба ничего не услышат.

В такой модели каждый раунд каждый игрок совершает одно из следующих действий: *отправить 1*, *отправить 0* или *принимать*. Если один игрок посылает, а другой принимает, то такой раунд ничем не отличается от классического, его называют *нормальным*. Если оба игрока посылают биты, то эти биты теряются, будем называть такие раунды *потерянными*. Если оба игрока принимают, то такие раунды будем называть *тихими*. В зависимости от канала связи в тихом раунде могут возникать разные ситуации, в связи с этим определены три модели.

- *Модель с нулем*: оба игрока в тихом раунде получают 0. В этом случае они не могут отличить ноль, полученный от другого игрока, от нуля, полученного в результате тихого раунда. Сложность функции f в этой модели обозначается как $\mathrm{D}_0^{hd}(f)$.

- *Модель с тишиной*: в тихом раунде игроки получают специальный символ тишины, то есть, в отличие от случая с тишиной, игроки различают тихие раунды. Сложность функции f в этой модели обозначается как $\mathrm{D}_s^{hd}(f)$.

- *Модель с противником*: в тихом раунде каждый игрок получает либо 0, либо 1. Можно представить что есть некий противник, который пытается помешать коммуникации, выбирая какой бит Алиса и Боб услышат в тихом раунде. В такой модели игроки не могут отличить тихий раунд от нормального. Сложность функции f в этой модели обозначается как $\mathrm{D}_a^{hd}(f)$.

Цель данной работы — исследовать описанные выше модели полудуплексной коммуникационной сложности, сравнить их с классической моделью и между собой. Мы получим верхнюю оценку в модели с нулём для функции дизъюнктности, классическая коммуникационная сложность которой уже известна. Это поможет нам понять то, что модели с нулем и противником не равны.

1. Обзорный раздел по предметной области

1.1. Используемые определения

Определение 1.1.

- Функция равенства $\mathrm{EQ}_n\colon \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ оперделяется следующим отношением:

$$\mathrm{EQ}_n(x,y) = 1 \iff x = y.$$

- Функция внутреннего произведения $\mathrm{IP}_n\colon \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ оперделяется следующим отношением:

$$\mathrm{IP}_n(x,y) = \bigoplus_{i=0}^{n} x_i y_i.$$

- Функция дизъюнктности $\mathrm{DISJ}_n\colon \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ оперделяется следующим отношением:

$$\mathrm{DISJ}_n(x,y) = 1 \iff \forall i\ x_i \neq 1 \ \textit{или}\ y_i \neq 1.$$

Определение 1.2. *Игра Карчмера-Вигдерсона для функции* $f\colon \{0,1\}^n \to \{0,1\}$ — это следующая коммуникационная игра: Алиса получает $x \in f^{-1}(0)$, Боб получает $y \in f^{-1}(1)$. Далее они вместе пытаются найти $i \in [n]$, такой что $x_i \neq y_i$. Иначе говоря, игра Карчмера-Вигдерсона — это коммуникационная задача для отношения

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

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

Определение 1.3. $\mathrm{AC}^0[3]$ — это класс булевых функций, которые вычисля-

ются схемами полиномиальной длины и константной глубины над базисом $\{\wedge, \vee, \mathrm{mod}_3, \neg\}$.

Определение 1.4. $\mathrm{PARITY}_n \colon \{0,1\}^n \to \{0,1\}$ — *функция четности*,

$$\forall x \in \{0,1\}^n \;\; \mathrm{PARITY}_n(x) = \bigoplus_{i=1}^{n} x_i.$$

Определение 1.5. Полином $p \colon \mathbb{F}_3^n \to \mathbb{F}_3$ называется *правильным*, если он отображает $\{0,1\}^n$ на $\{0,1\}$.

Определение 1.6. $\mathrm{Maj}_3 \colon \{0,1\}^3 \to \{0,1\}$

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

Определение 1.7. $\mathrm{RecMaj} \colon \{0,1\}^n \to \{0,1\}$

$$\mathrm{RecMaj}(x_1, \ldots, x_n) =$$

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

1.2. Используемые факты

Лемма 1. *Для любого* $n \in \mathbb{N}$,

$$\mathrm{D}(\mathrm{DISJ}_n) = \mathrm{D}(\mathrm{EQ}_n) = \mathrm{D}(\mathrm{IP}_n) = n + 1.$$

Теорема 1 ([3])**.** *Для любого* $n \in \mathbb{N}$,

$$\mathrm{D}_s^{hd}(\mathrm{DISJ}_n) \geq n/\log 5, \mathrm{D}_0^{hd}(\mathrm{DISJ}_n) \geq n/\log 3, \mathrm{D}_a^{hd}(\mathrm{DISJ}_n) \geq n/\log 2.5.$$

В статьях [4, 5, 1] рассматриваются следующие определения и утверждения.

Лемма 2 ([1]). *Пусть* $g\colon \mathbb{F}_3^n \to \mathbb{F}_3$ *— правильный полином степени не более* $\sqrt{n}$*. Тогда* g *совпадает с* PARITY_n *не более чем на* $49/50$ *от всех входов из* $\{0,1\}^n$.

Лемма 3 ([1]). *Пусть* $t \geq 0$*, и* $C \in \mathrm{AC}^0[3]$ *— схема глубины* d*. Тогда существует правильный полином степени хотя бы* $(2t)^d$*, который совпадает с* C *на* $1 - \mathrm{SIZE}(C)/2^t$ *доле от всех входов из* $\{0,1\}^n$.

Теорема 2. $\mathrm{PARITY} \notin \mathrm{AC}^0[3]$

Доказательство. Предположим, что $\mathrm{PARITY} \in \mathrm{AC}^0[3]$. Тогда существует фиксированное положительное целое число d, такое что для входа любого размера существует схема глубины d из $\mathrm{AC}^0[3]$, вычисляющая PARITY_n.

Возьмём $t = \frac{n^{1/2d}}{2}$ и применим лемму 3. Тогда существует правильный полином степени не больше $\sqrt{n}$, который совпадает с PARITY_n на

$$1 - \frac{\mathrm{SIZE}(C)}{\sqrt{2}^{n^{\frac{1}{2d}}}}$$

входах. Тогда по лемме 2

$$\mathrm{SIZE}(C) \geq \left(\frac{1}{50}\right) \cdot \sqrt{2}^{n^{\frac{1}{2d}}},$$

что противоречит полиномиальному размеру C. □

2. Верхняя оценка на функцию дизъюнктности

Теорема 3. $\mathrm{D}_0^{hd}(\mathrm{DISJ}) \leqslant \frac{3}{4}n + o(n)$.

Доказательство. Будем считать, что n чётно, иначе Алиса и Боб могут приписать к своей строке ноль, от чего значение функции не поменяется. Тогда протокол выглядит следующим образом: Алиса и Боб разбивают свои строки на подстроки из двух битов. Всего таких подстрок $n/2$. Через $\sharp(ab)$ обозначим количество подстрок ab среди получившихся кусков, где $a, b \in \{0, 1\}$. 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. $\sharp(00) + \sharp(01) < n/3$.

Сначала Боб определяет, какому из неравенств выше удовлетворяет его строка, и сообщает об этом Алисе, используя два бита коммуникации.

Рассмотрим все три случая:

- **Случай 1**

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

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

Таблица 1.

  Тогда Алисе и Бобу нужно уметь различать ситуации, когда их строки пересекаются, то есть пары (01,01), (01,11), (10,10), (10,11), (11,01), (11,10), (11,11) отличать от других. Если у Алисы была пара 01, а

у Боба 01 или 11, то, согласно протоколу действия, Боб услышал 1. Теперь он знает что их строки пересекаются, и позже может сообщить об этом Алисе. Если у Алисы была пара 11 и она слышит 0, то это значит, что у Боба была одна из пар 01, 10, 11. Значит теперь Алиса знает, что их строки пересекаются, и может сообщить об этом Бобу. В таблице 2 знаком "+" обозначены пары входов, которые Алиса и Боб уже умеют отличать от остальных. Теперь им осталось отличить только пары (10,10) и (10, 11).

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

Таблица 2.

После $n/2$ раундов Боб смотрит на 01, 10 и 11 со своего входа на которых он слышал ноль. Он записывает новую строку, назовём её $\tilde{y}$, так: вместо 10 и 11 пишет 0, вместо 01 — 1. Аналогично, Алиса смотрит на 11, 00 и 01 на которых был тихий раунд. Новая строка, назовём её $\tilde{x}$, выглядит следующим образом: вместо 11 она записывает 1, вместо оставшихся — 0. Нетрудно понять, что ответом на исходную задачу будет результат применения DISJ к новым битовым строчкам размера не больше $\frac{n}{3}$,

$$\mathrm{DISJ}_n(x, y) = \mathrm{DISJ}_{\frac{n}{3}}(\tilde{x}, \tilde{y}),$$

где x, y — изначальные входы Алисы и Боба соответственно.

- **Случай 2**

  Действуем аналогично случаю 1 по следующей таблице (3).

  После $n/2$ раундов Боб смотрит на 00, 01 и 11 со своего входа, на которых он слышал ноль. Он записывает новую строку так: вместо

Символ	Алиса	Боб
00	`принимать`	`принимать`
01	`отправить 1`	`отправить 1`
10	`принимать`	`принимать`
11	`принимать`	`принимать`

Таблица 3.

10 и 11 пишет 1, вместо 00 — 0. Аналогично, Алиса смотрит на 00, 10 и 11, на которых был тихий раунд. Вместо 11 и 10 она записывает 1, вместо 00 — 0. Снова получили DISJ от новых битовых строчек размера не больше $\frac{n}{3}$.

- **Случай 3**

  Действуем аналогично случаю 1 по следующей таблице (4).

Символ	Алиса	Боб
00	`отправить 1`	`принимать`
01	`принимать`	`принимать`
10	`принимать`	`отправить 1`
11	`принимать`	`принимать`

Таблица 4.

После $n/2$ раундов Боб смотрит на 00 и 01 со своего входа, на которых он слышал ноль. Аналогично другим случаям Боб вместо 01 пишет 1, вместо 00 — 0. Алиса смотрит на 01, 10 и 11, на которых был тихий раунд. Вместо 11 и 01 она записывает 1, вместо 10 — 0. Снова получили DISJ от новых битовых строчек размера не больше $n/3$.

Таким образом, во всех 3-х случаях Алисе и Бобу после $n/2$ отправленных битов остается решить DISJ для входов длины не более чем $n/3$,

$$\mathrm{D}_0^{hd}(\mathrm{DISJ}_n) \leqslant \frac{n}{2} + \mathrm{D}_0^{hd}(\mathrm{DISJ}_{\frac{n}{3}}).$$

Отсюда получаем:

$$\mathrm{D}_0^{hd}(\mathrm{DISJ}_n) \leqslant \sum_{i=0}^{\lceil \log_3(n) \rceil} \frac{n}{2 \cdot 3^i} + o(n) \leqslant \sum_{i=0}^{\infty} \frac{n}{2 \cdot 3^i} + o(n) = \frac{3n}{4} + o(n).$$

□

Эта теорема разделяет DISJ в моделях с нулем и противником. Известные нам оценки [3] собраны в таблице 5.

	DISJ_n
D_s^{hd}	$n/\log(5) \leq \cdots \leq n/2 + O(1)$
D_0^{hd}	$n/\log(3) \leq \cdots \leq 3n/4 + o(n)$
D_a^{hd}	$\geq n/\log(2.5)$

Таблица 5.

3. Другие результаты

3.1. Функция рекурсивного голосования

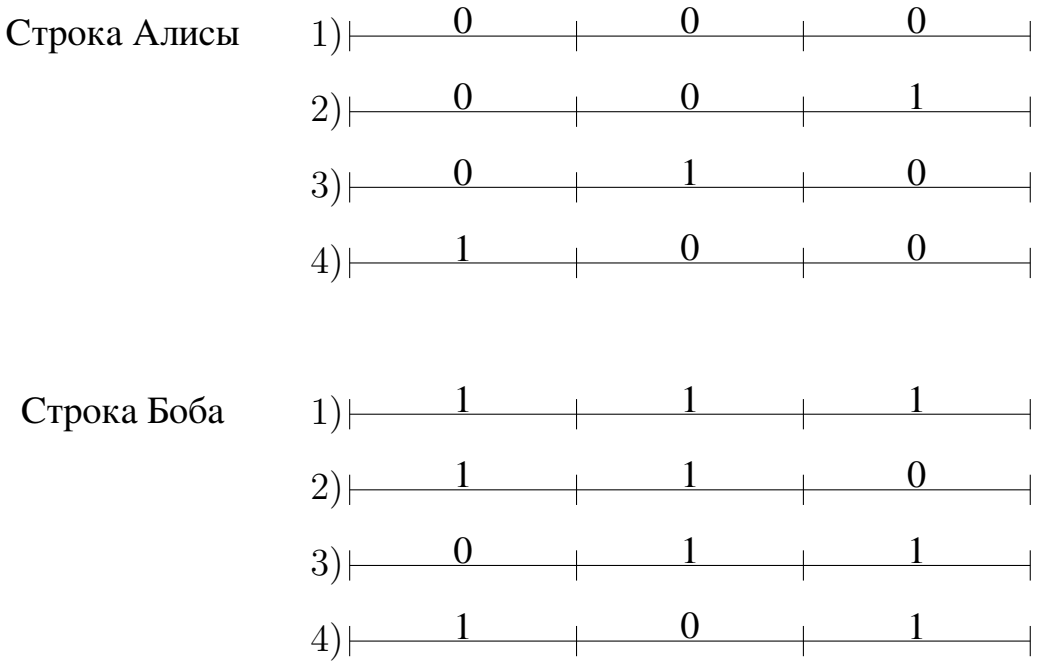

Рис. 1.

Утверждение 3.1. *Для любого $n \in \mathbb{N}$, такого что n является степенью 3,* $\mathrm{D}(KW_{\mathrm{RecMaj}_n}) \leqslant 3\log_3(n)$.

Доказательство. У Алисы есть строка x, такая что $\mathrm{RecMaj}(x) = 0$, а у Боба — y, такой что $\mathrm{RecMaj}(y) = 1$. На каждом шаге игроки делят свои строки на 3 подстроки одинаковой длины. Возможные случаи Алисы и Боба изображены на рис. 1, бит в соответствующем куске означает значение функции RecMaj от него.

В начале каждого шага Боб отправляет Алисе значение RecMaj от первой подстроки размера $n/3$. Далее, в зависимости от того, какой первый бит у Боба, возникают следующие возможные случаи:

- Первый бит Боба — 0. Тогда Алиса отправляет Бобу, в какой из двух оставшихся частей у неё ноль (это корректно, так как у Алисы вход из

прообраза нуля, а значит хотя бы на одной из этих подстрок RecMaj принимает значение 0).

- Первый бит Боба — 1. Тогда Алиса отправляет Бобу свой первый бит. Если это 0, то они переходят к следующему шагу для первой (из трёх) подстроки длины $n/3$. Иначе Боб отправляет 0, если нужно перейти во вторую подстроку, или 1 — если в третью.

Таким образом, на каждом шаге тратится не более 3-х битов, а длина строки уменьшается в 3 раза. Всего шагов $\log_3 n$, т.е. $\mathrm{D}(KW_{\mathrm{RecMaj}_n}) \leqslant 3\log_3(n)$. □

3.2. Функция четности

Утверждение 3.2. *При глубине схемы* $d(n) = \dfrac{\log n}{\log\log n}$ *над базисом* $\{\wedge, \vee, \neg, mod_3\}$*, размер схемы, вычисляющей* PARITY_n*, суперполиномиален, т.е.* $\mathrm{SIZE}(C) \geq n^{\log n}$.

Доказательство. Аналогично доказательству теоремы 2 получаем, что при глубине схемы $d(n)$ размер ограничен снизу $\mathrm{SIZE}(C) \geq 2^{n^{\frac{1}{2d}}}$. Осталось найти при каких значениях $d(n)$ размер схемы будет превосходить полиномиальный. Это показано в следующей выкладке. Найдём функцию d(n), такую, что её размер будет ограничен снизу полиномиальным.

$$2^{n^{\frac{1}{2d}}} = n^{O(1)}$$

Прологарифмируем обе части:

$$n^{\frac{1}{2d}} = O(\log n).$$

Таким образом, верно следующее

$$2^{\frac{\log n}{2d}} = O(\log n).$$

Так как степень полинома хотя бы 1, последнее равенство означает

$$2^{\frac{\log n}{2d}} \leq C_0 \log n,\ C_0 \geq 1.$$

Снова прологарифмируем обе части

$$\frac{\log n}{2d} \leq \log\log n + C_1,\ C_1 = \log C_0 \geq 0.$$

Выразим из этого неравенства d

$$2d \geq \frac{\log n}{C_1 + \log\log n}.$$

Таким образом, при $d(n) < \dfrac{\log n}{2(C_1 + \log\log n)}$ размер схемы будет превосходить полиномиальный.

□

Заключение

На примере функции дизъюнктности мы убедились, что модель с противником и модель с нулём отличаются. Результаты данной работы вошли в публикацию [3]. Оценка на полудуплексную коммуникационную сложность функции дизъюнктности не является точной: во всех трёх полудуплексных моделях между верхней и нижней оценкой есть зазор, а в модели с противником нет верхней оценки лучше тривиальной. Будет интересно получить любое улучшение какой-либо из представленных в таблице 5 оценок.

Также известно [3], что классическая и полудуплексная сложности ведут себя по-разному. Например, для функций равенства и внутреннего произведения сложности в классическом случае совпадают, а в полудуплексном — отличаются. На данный момент нельзя утверждать, что полудуплексные коммуникационные сложности функций внутреннего произведения и дизъюнктности отличаются, но очень похоже, что это действительно так. Мы знаем, что $\mathrm{D}_0^{hd}(\mathrm{IP}_n) \geq n/\log_2(2/(3-\sqrt{5})) \approx 0.72n$ и $\mathrm{D}_0^{hd}(\mathrm{DISJ}_n) \leq 0.75n + o(n)$. Зазор между этими оценками небольшой, поэтому вполне возможно, что их получится разъединить.

Список литературы

[1] Boppana R. B., Sipser M. The Complexity of Finite Functions // Handbook of Theoretical Computer Science, Volume A: Algorithms and Complexity / ed. by van Leeuwen J. — Elsevier and MIT Press, 1990. — P. 757–804.

[2] 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.

[3] New Bounds on the Half-Duplex Communication Complexity / Dementiev Y., Ignatiev A., Sidelnik V., Smal A., and Ushakov M. // 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 / ed. by Bures T., Dondi R., Gamper J. et al. — Springer. — 2021. — Vol. 12607 of Lecture Notes in Computer Science. — P. 233–248. — Access mode: https://doi.org/10.1007/978-3-030-67731-2_17.

[4] Razborov A. A. Lower bounds on the size of bounded depth circuits over a complete basis with logical addition // Mathematical Notes of the Academy of Sciences of the USSR. — 1987. — Vol. 41, no. 4. — P. 333–338.

[5] Smolensky R. Algebraic Methods in the Theory of Lower Bounds for Boolean Circuit Complexity // Proceedings of the 19th Annual ACM Symposium on Theory of Computing, 1987, New York, New York, USA / ed. by Aho A. V. — ACM. — 1987. — P. 77–82. — Access mode: https://doi.org/10.1145/28395.28404.

[6] Yao A. C. Some Complexity Questions Related to Distributive Computing (Preliminary Report) // Proceedings of the 11h Annual ACM Sympo-

sium 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.