Федеральное государственное бюджетное учреждение науки
Санкт-Петербургское отделение Математического института
им. В. А. Стеклова РАН

Представление на соискание учёной степени кандидата
физико-математических наук по специальности
01.01.06 Математическая логика, алгебра и теория чисел

Доказательство нижних оценок на размер формул для булевых функций методами коммуникационной сложности

Выступающий: А. В. Смаль
Руководитель: докт. физ.-мат. наук., профессор РАН Э. А. Гирш

Санкт-Петербург, 2022

Формулы Де Моргана

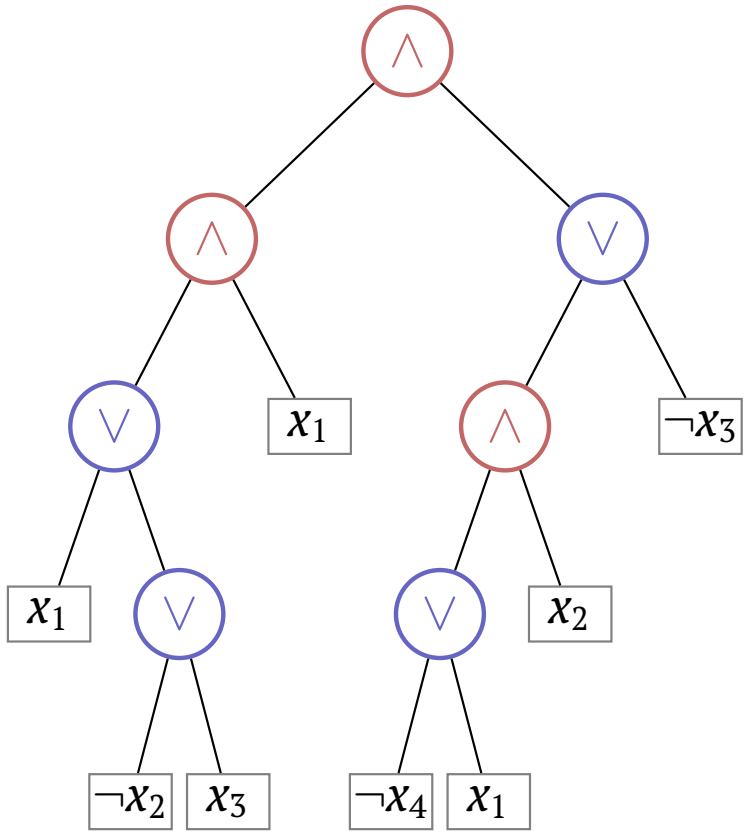
Размер — количество листьев.

Глубина — высота дерева.

$f : \{0,1\}^* \to \{0,1\}$ *вычисляется формулами Де Моргана размера* $s(n)$ *(глубины* $d(n)$*)*, если для всех $k \in \mathbb{N}$ существует формула размера $s(k)$ (глубины $d(k)$), вычисляющая $f_k = f\restriction_{\{0,1\}^k}$.

Формульная сложность f — минимальная функция s, такая что f вычисляется формулами размера $s(n)$, обозначается $L(f)$.

Формульная глубина f — минимальная функция d, такая что f вычисляется формулами размера $d(n)$, обозначается $D(f)$.



Формула Де Моргана

Утверждение

Существует такая константа $c > 1$, что для любой булевой функции $f : \{0,1\}^n \to \{0,1\}$ выполняется $\log_2 L(f) \leq D(f) \leq c \cdot \log_2 L(f)$.

Теорема (Риордан, Шеннон, 1942)

Для любого $\epsilon > 0$ доля функций $f : \{0,1\}^n \to \{0,1\}$, для которых $L(f) \leq (1-\epsilon) \cdot 2^n / \log n$, не превосходит $2^{-2^n \cdot (\epsilon - o(1))}$.

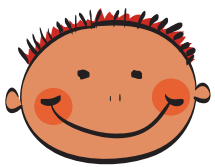
Теорема (Хостад, 1998)

Существуют константа $c > 0$ и явная функция $f : \{0,1\}^n \to \{0,1\}$, вычислимая за полиномиальное время, такие что f имеет только формулы размера $\Omega\left(n^3 / \log^c n\right)$.

Введена Эндрю Яо в 1979 году.

Алиса

Боб



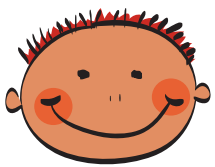
Коммуникационная модель

Введена Эндрю Яо в 1979 году.

Алиса

$x \in \{0,1\}^n$

Боб



$y \in \{0,1\}^n$

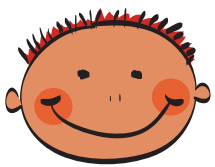
Коммуникационная модель

Введена Эндрю Яо в 1979 году.

Алиса

$x \in \{0,1\}^n$

Боб



$y \in \{0,1\}^n$

Алиса и Боб хотят вычислить $f(x,y)$.

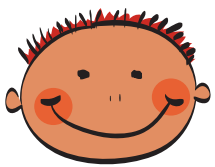
Коммуникационная модель

Введена Эндрю Яо в 1979 году.

Алиса

b_1

Боб



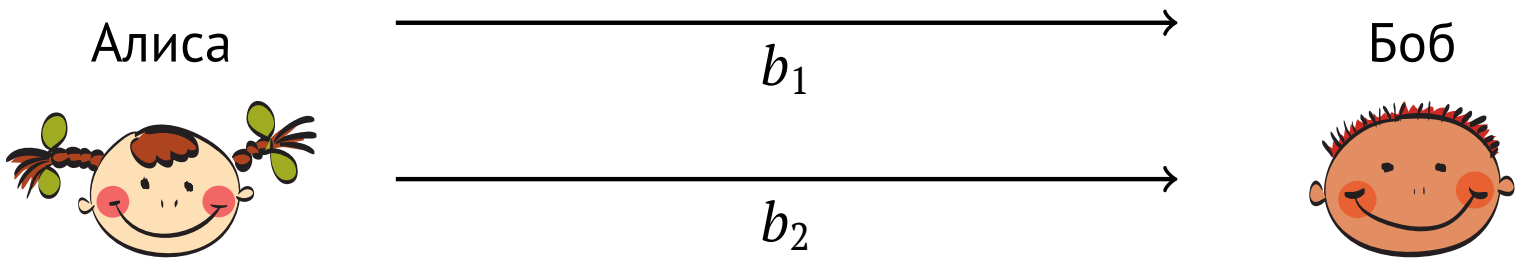
$x \in \{0,1\}^n$

$y \in \{0,1\}^n$

Алиса и Боб хотят вычислить $f(x,y)$.

Коммуникационная модель

Введена Эндрю Яо в 1979 году.

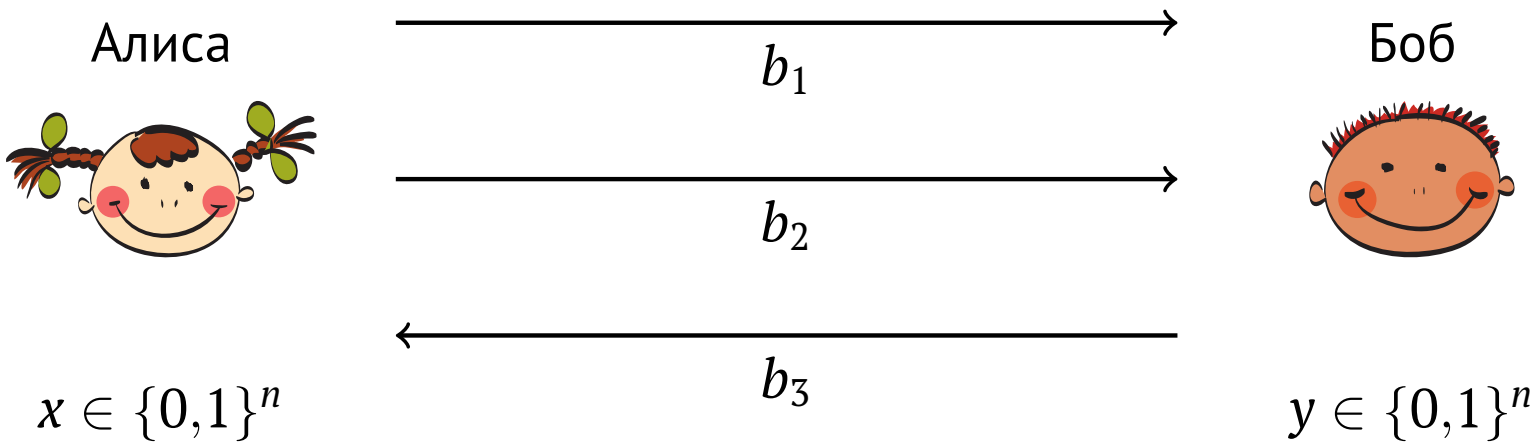


$x \in \{0,1\}^n$ $y \in \{0,1\}^n$

Алиса и Боб хотят вычислить $f(x,y)$.

Коммуникационная модель

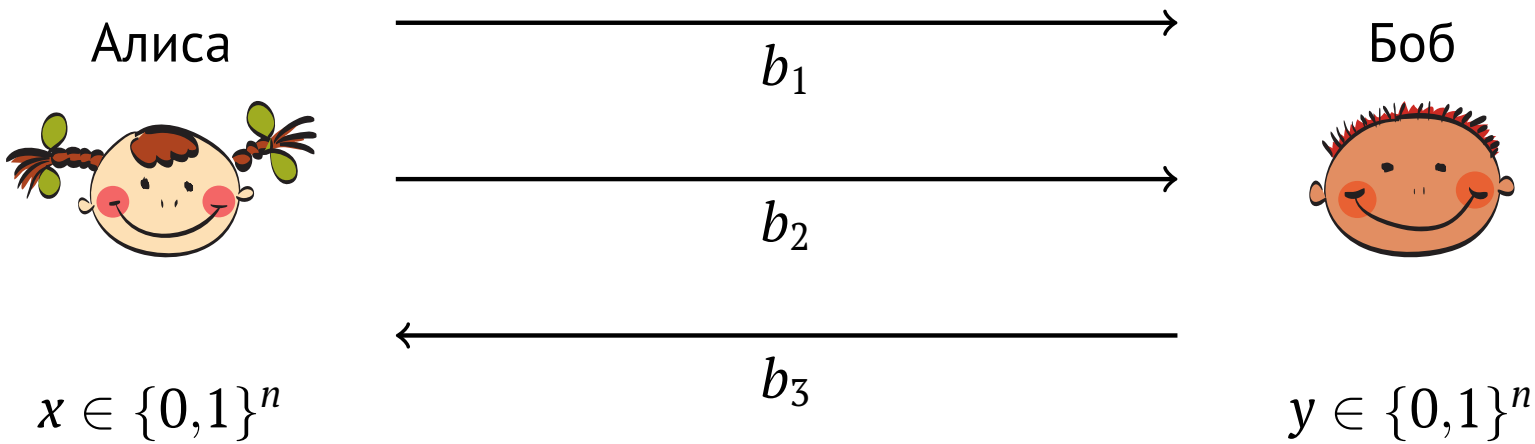
Введена Эндрю Яо в 1979 году.



Алиса и Боб хотят вычислить $f(x,y)$.

Коммуникационная модель

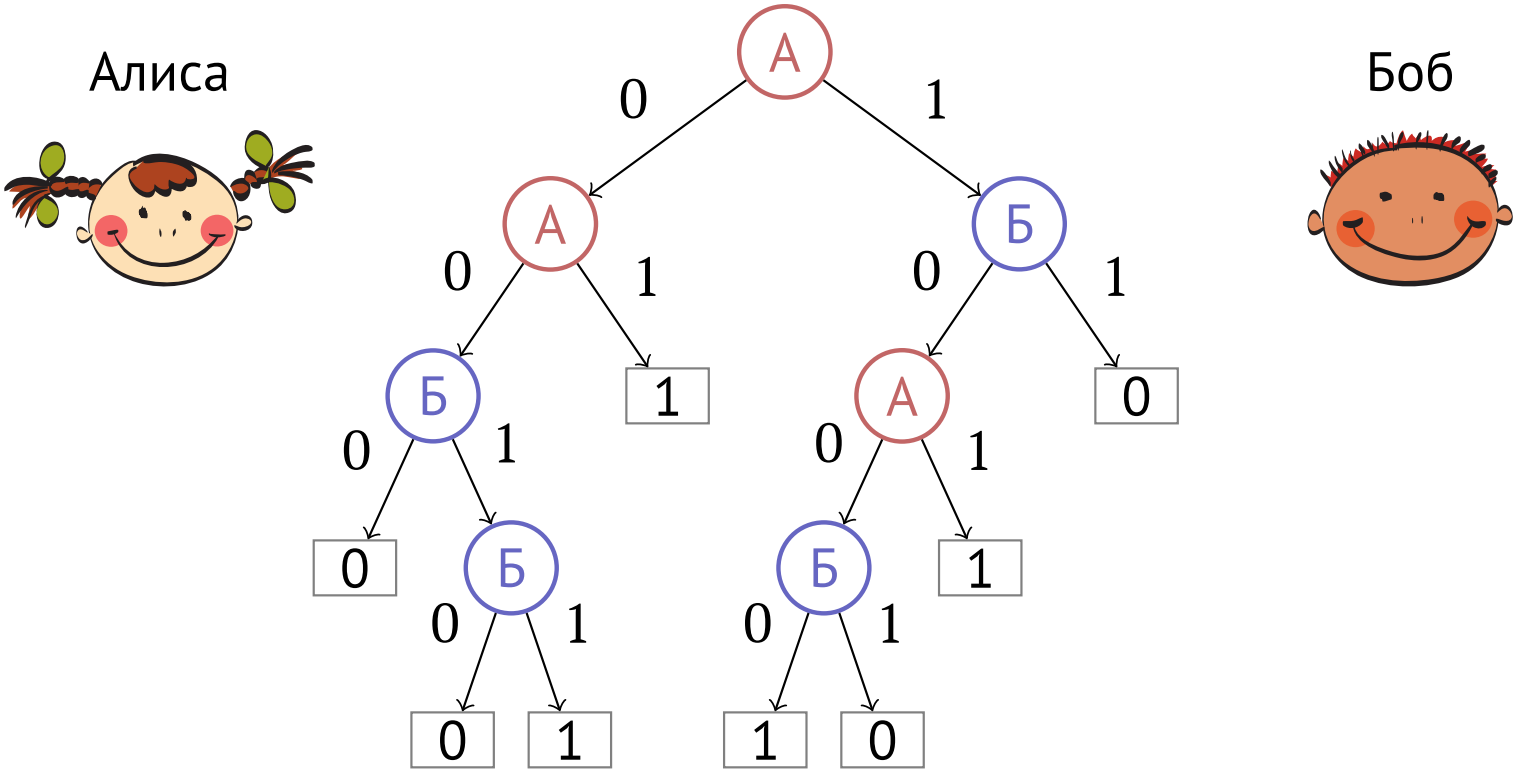
Введена Эндрю Яо в 1979 году.



Алиса и Боб хотят вычислить $f(x,y)$.

Можно обобщить на трёхместные отношения: если для пары (x,y) есть несколько значений z, удовлетворяющих трёхместному отношению, то игроки должны сойтись на каком-то одном.

Коммуникационный протокол

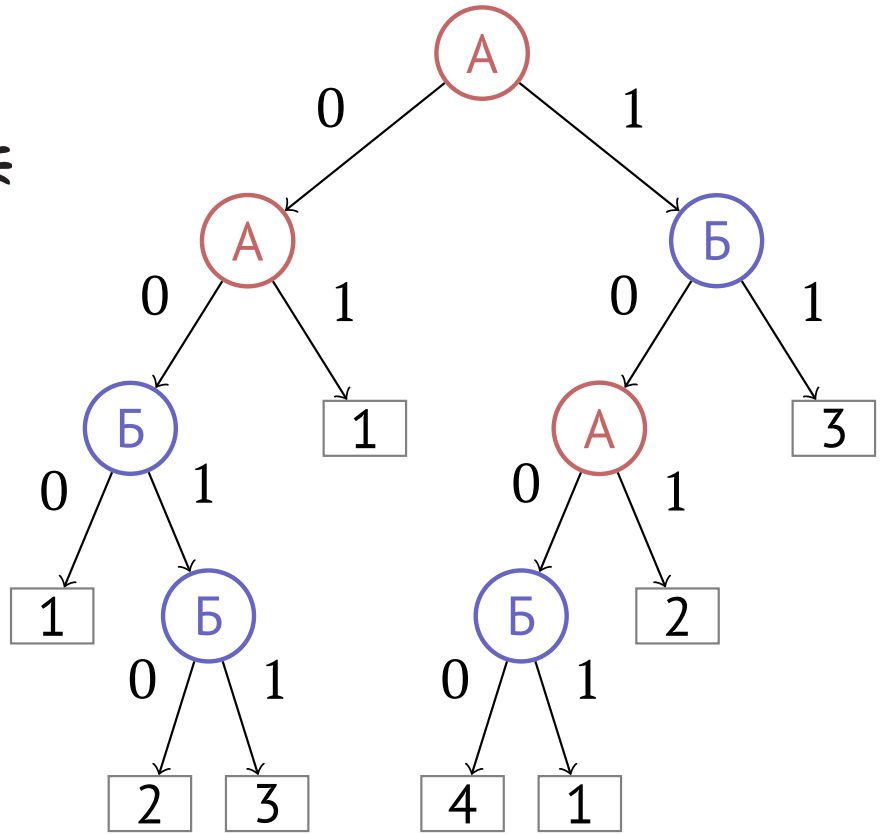


Коммуникационная сложность f — это минимальная глубина протокола, который вычисляет f, обозначается $\mathrm{CC}(f)$.

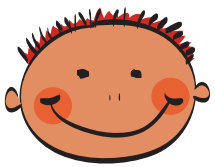
Игра Карчмера — Вигдерсона для $f : \{0,1\}^n \to \{0,1\}$

Алиса

$x \in f^{-1}(0)$



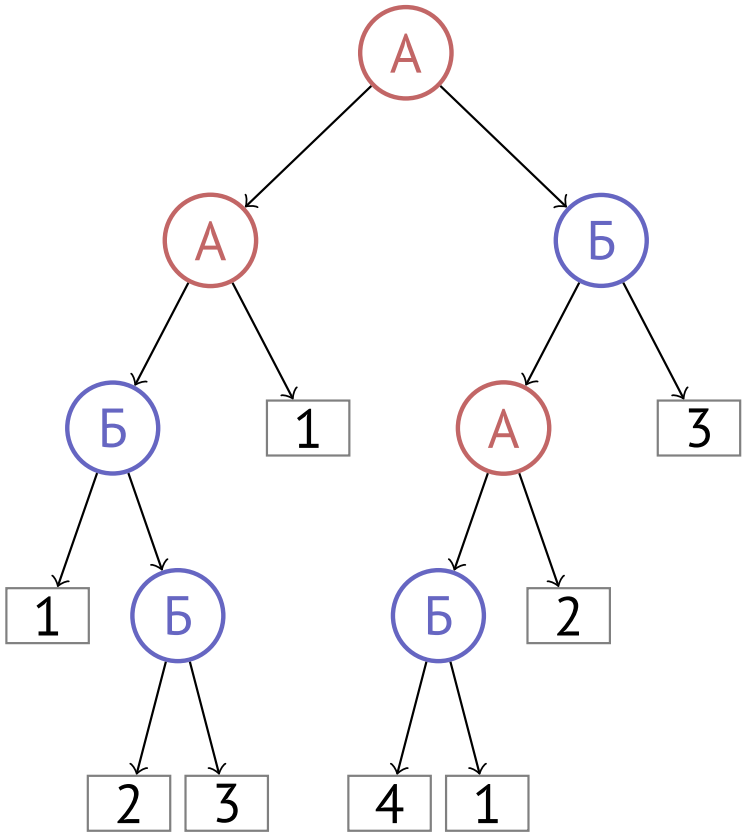
Боб



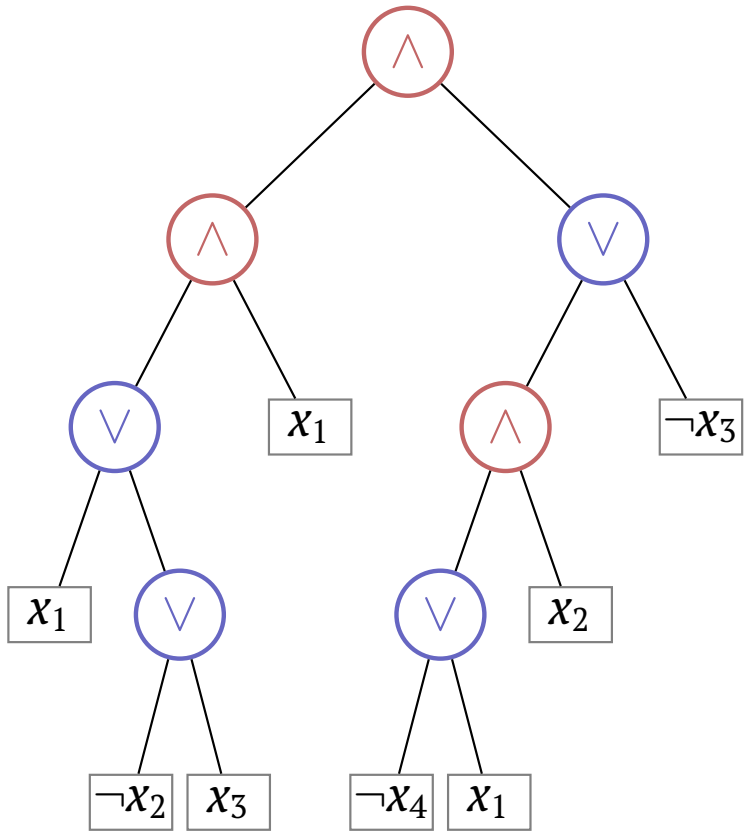
$y \in f^{-1}(1)$

Игроки хотят найти число $i \in [n]$, такое что $x_i \neq y_i$.

Теорема Карчмера — Вигдерсона



$\Leftrightarrow$



Протокол для KW_f

Формула Де Моргана для f

Цель данной работы

Целью данной работы является разработка и совершенствование новых подходов к доказательству нижних оценок на формульную сложность булевых функций с использованием методов коммуникационной сложности.

Результаты

Предсказания с помощью сертификатов

Случайная величина $X = (X_1, \ldots, X_n)$ распределена на $\{0,1\}^n$ и имеет энтропию Шеннона не менее $n - k$.

Сертификат для координаты $i \in [n]$ и $b \in \{0,1\}$ — это пара (Q, a), где $Q \subseteq [n] \setminus \{i\}$ и $a \in \{0,1\}^{|Q|}$, такая что если $X|_Q = a$, то $X_i = b$.

Длина сертификата равна $|Q|$.

Пусть X распределена на $\{0,1\}^n$, $H(X) \geq n - k$ и $q < n$.

Для всех $i \in [n]$ и $b \in \{0,1\}$ пусть σ_i обозначает вероятность того, что X содержит сертификат для i размера q.

Теорема (Меир, Вигдерсон, 2016)

$\mathbb{E}_i[\sigma_i] \leq \frac{300 \cdot k \cdot q}{n}$.

Усиление теоремы Меира — Вигдерсона

$\mathbb{E}_i[\sigma_i] \leq \frac{k \cdot (q+1)}{n}$.

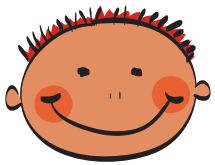
Следствием этой теоремы являются нижние оценки на размер $\wedge$-$\vee$-$\wedge$-формул, вычисляющих функции большой чувствительности.

Полудуплексная коммуникационная модель

Игроки общаются по полудуплексному каналу (по рации).

Алиса

Боб



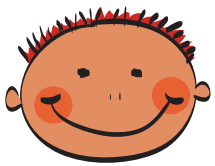
Полудуплексная коммуникационная модель

Игроки общаются по полудуплексному каналу (по рации).

Алиса

$x \in \{0,1\}^n$

Боб



$y \in \{0,1\}^n$

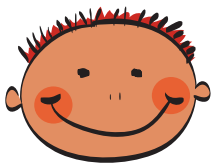
Полудуплексная коммуникационная модель

Игроки общаются по полудуплексному каналу (по рации).

Алиса

$x \in \{0,1\}^n$

Боб



$y \in \{0,1\}^n$

Алиса и Боб хотят вычислить $f(x,y)$.

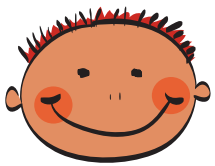
Полудуплексная коммуникационная модель

Игроки общаются по полудуплексному каналу (по рации).

Алиса

$\xrightarrow{b_1}$

Боб



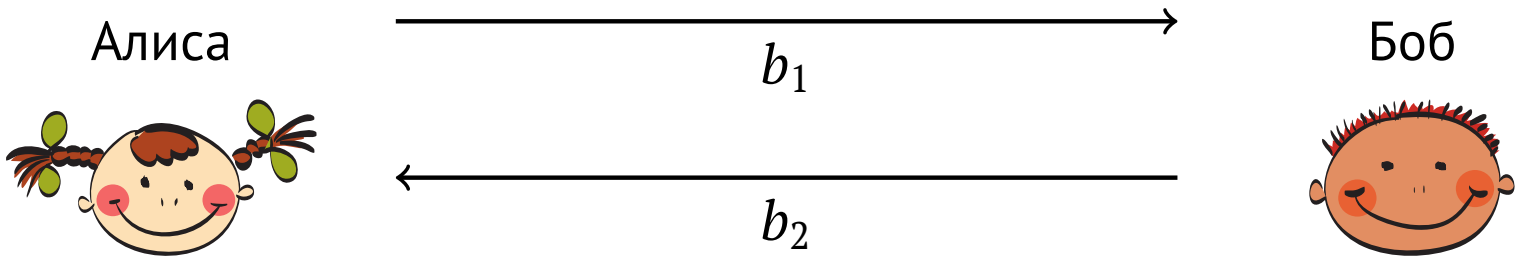
$x \in \{0,1\}^n$

$y \in \{0,1\}^n$

Алиса и Боб хотят вычислить $f(x,y)$.

Полудуплексная коммуникационная модель

Игроки общаются по полудуплексному каналу (по рации).



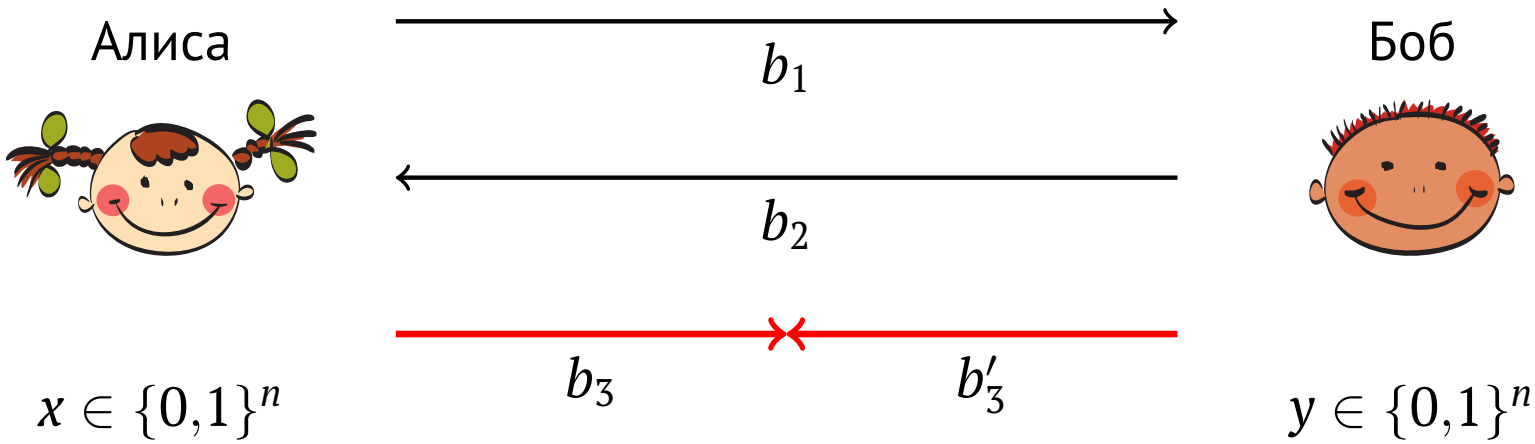
$x \in \{0,1\}^n$

$y \in \{0,1\}^n$

Алиса и Боб хотят вычислить $f(x,y)$.

Полудуплексная коммуникационная модель

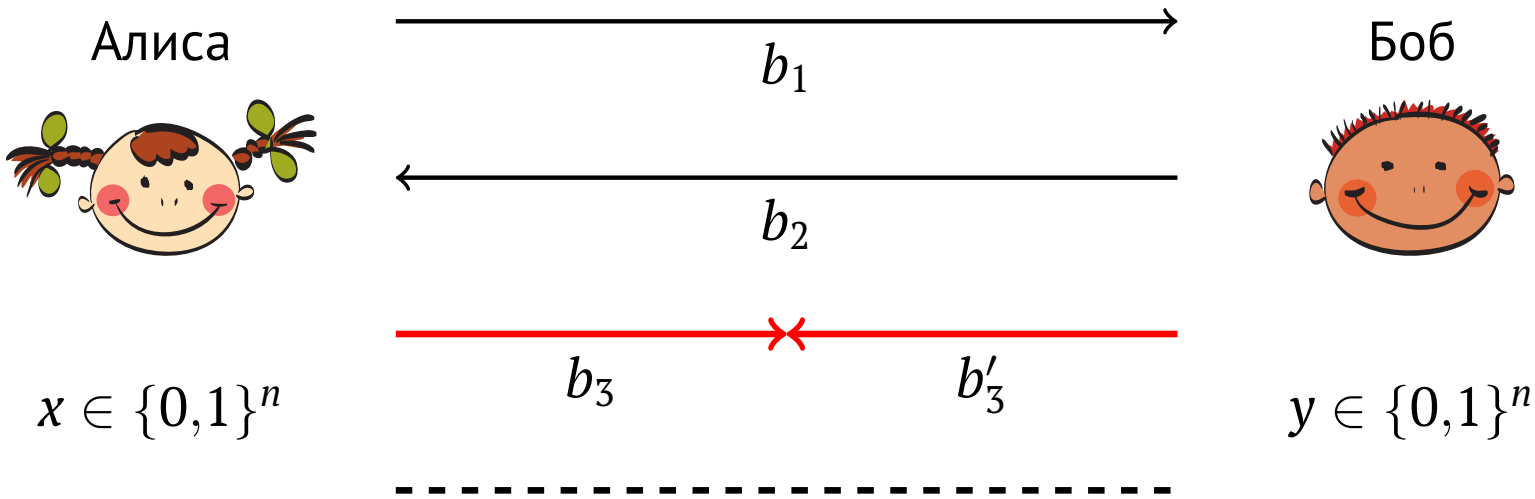
Игроки общаются по полудуплексному каналу (по рации).



Алиса и Боб хотят вычислить $f(x,y)$.

Полудуплексная коммуникационная модель

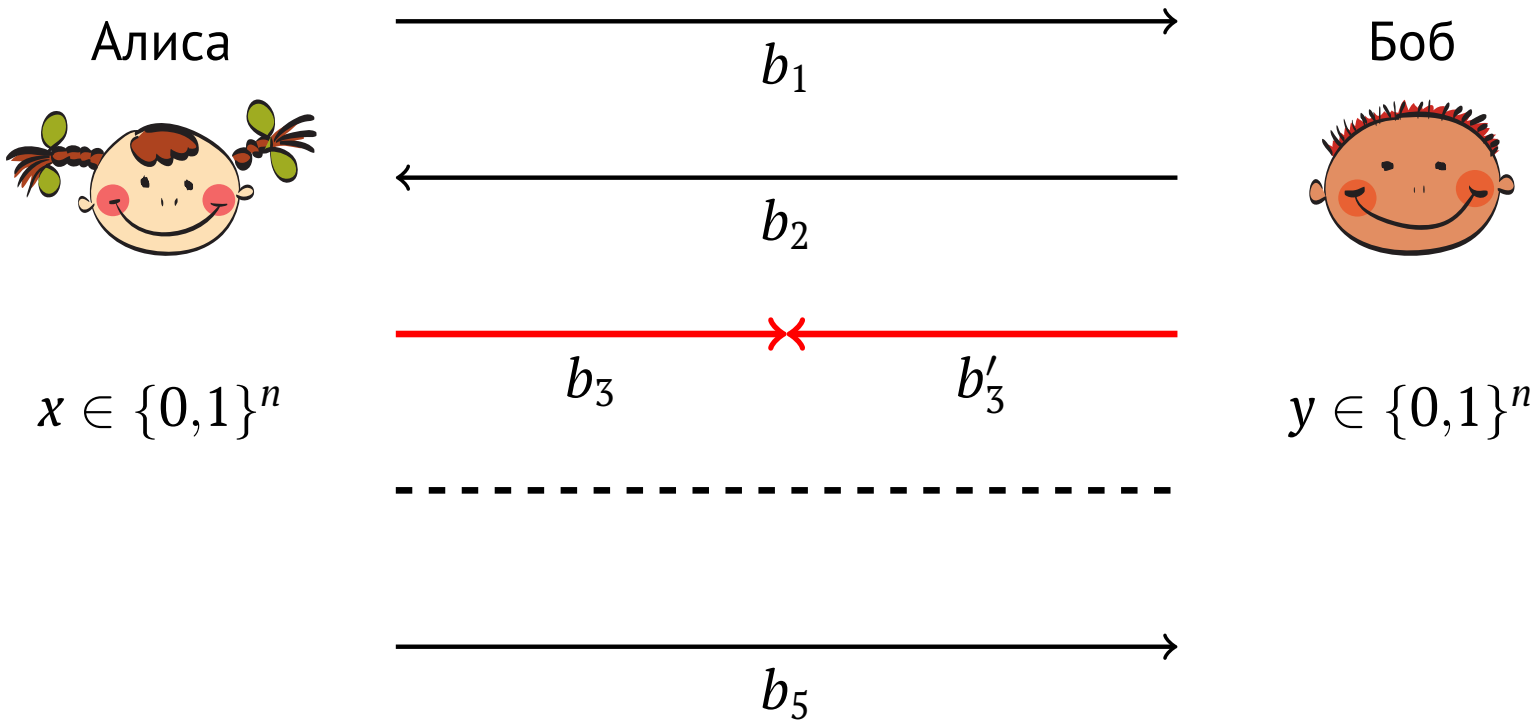
Игроки общаются по полудуплексному каналу (по рации).



Алиса и Боб хотят вычислить $f(x,y)$.

Полудуплексная коммуникационная модель

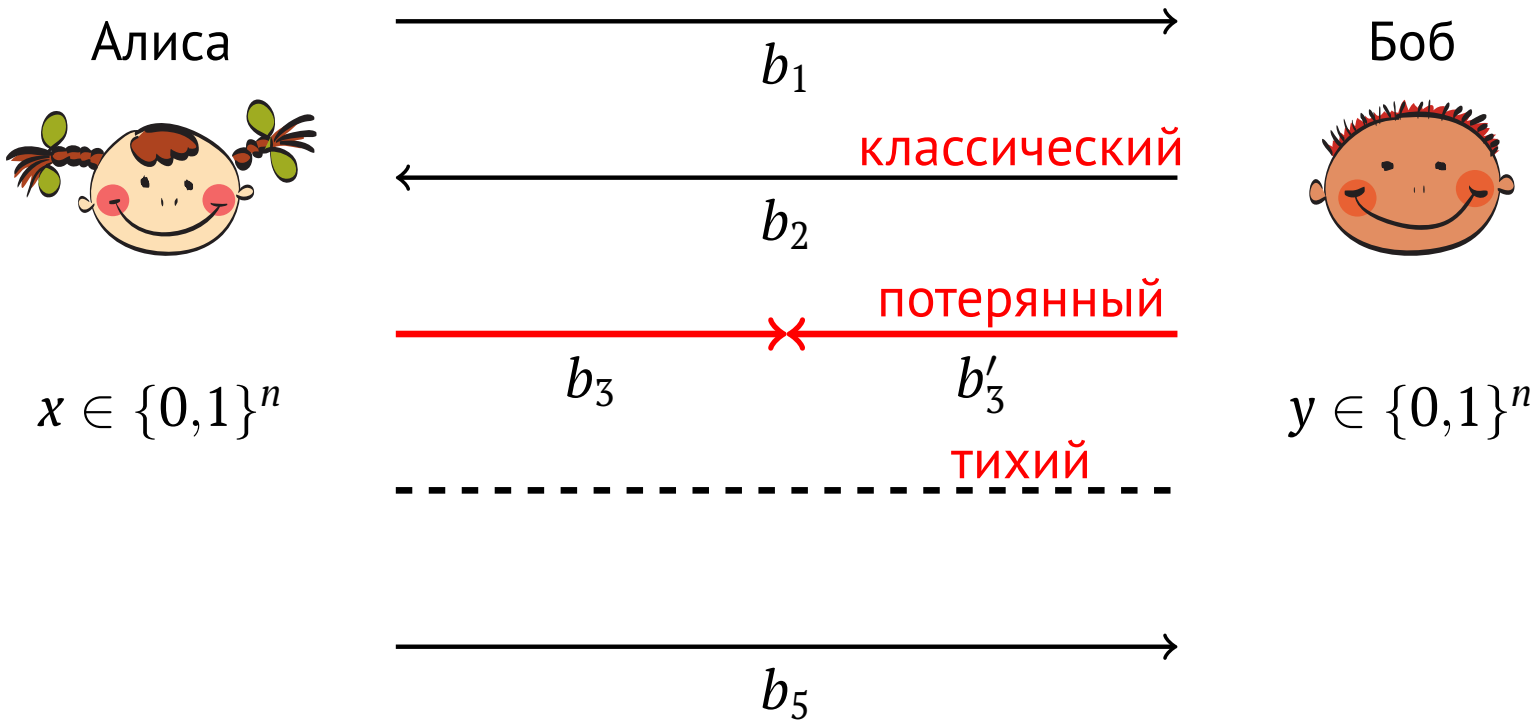
Игроки общаются по полудуплексному каналу (по рации).



Алиса и Боб хотят вычислить $f(x,y)$.

Полудуплексная коммуникационная модель

Игроки общаются по полудуплексному каналу (по рации).



Алиса и Боб хотят вычислить $f(x,y)$.

Оценки для полудуплексной коммуникации

Верхние оценки

Верхние оценки на полудуплексную коммуникационную сложность для функции равенства EQ_n: $n/\log_2 5 + O(\log n)$ в модели с тишиной и $n/\log_2 3 + O(\log n)$ в модели с нулём, а также верхняя оценка $n/2 + O(1)$ на функцию дизъюнктности DISJ_n в модели с тишиной.

Нижние оценки

Нижние оценки на полудуплексную коммуникационную сложность функции внутреннего произведения IP_n: $n/2$ для модели с тишиной, $n/1.39$ для модели с нулём и $n/\log_2(7/3)$ для модели с противником.

Верхние оценки для игр Карчмера — Вигдерсона

Нижние оценки на полудуплексную коммуникационную сложность игр Карчмера — Вигдерсона для функций подсчёта: $\log n - O(1)$ и $1.439 \log n - O(1)$ в моделях с тишиной и с нулём, соответственно.

Гипотеза Карчмера — Раза — Вигдерсона

Пусть $f : \{0,1\}^m \to \{0,1\}$ и $g : \{0,1\}^n \to \{0,1\}$ — две произвольные булевы функции. *Блочная композиция* $f \diamond g : (\{0,1\}^n)^m \to \{0,1\}$ определяется соотношением

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

где $x_1, \ldots, x_m \in \{0,1\}^n$.

Гипотеза Карчмера — Раза — Вигдерсона (КРВ)

Для любых непостоянных $f : \{0,1\}^m \to \{0,1\}$ и $g : \{0,1\}^n \to \{0,1\}$

$$D(f \diamond g) \approx D(f) + D(g).$$

Если гипотеза верна, то существует явная функция $f : \{0,1\}^n \to \{0,1\}$, вычислимая за полиномиальное время и не имеющая формул полиномиального размера.

Нижняя оценка для композиции отношений

Для доказательства КРВ гипотезы предлагается изучать коммуникационную сложность отношений, которые обобщают игры Карчмера — Вигдерсона для композиций функций.

В статье [Гавинский и др., 2016] доказана нижняя оценка на композицию игры Карчмера — Вигдерсона и универсального отношения и сформулирован открытый вопрос про нижнюю оценку для композиции универсального отношения и игры Карчмера — Вигдерсона.

Нижняя оценка для композиции отношений

Доказана нижняя оценка $1.5n - o(n)$ на коммуникационную сложность композиции универсального отношения и игры Карчмера — Вигдерсона для некоторой функции для случаев XOR-композиции и блочной композиции.

Участие в конференциях

- Международная конференция «The 29th International Symposium on Algorithms and Computation» (Тайвань, 2018).
- Международная конференция «The 47th International Conference on Current Trends in Theory and Practice of Computer Science» (онлайн, 2021).
- Международная конференция «The Computational Complexity Conference» (онлайн, 2021).

Основные публикации

1. *Dementiev*, *Y.*, *Ignatiev*, *A.*, *Sidelnik*, *V.*, *Smal*, *A.*, *Ushakov*, *M.* — New Bounds on the Half-Duplex Communication Complexity. — // SOFSEM 2021. — 2021.
2. *Hoover*, *K.*, *Impagliazzo*, *R.*, *Mihajlin*, *I.*, *Smal*, *A. V.* — Half-Duplex Communication Complexity. — // ISAAC 2018. — 2018.
3. *Mihajlin*, *I.*, *Smal*, *A.* — Toward Better Depth Lower Bounds: The XOR-KRW Conjecture. — // CCC 2021. — 2021.
4. *Smal*, *A. V.*, *Talebanfard*, *N.* — Prediction from partial information and hindsight, an alternative proof. — // Inf. Process. Lett. — 2018.