# Квантовые алгоритмы: возможности и ограничения. Лекция 4: Полиномиальная эквивалентность числа квантовых и классических запросов. Коммуникационная сложность

М. Вялый

Вычислительный центр
им. А.А.Дородницына
Российской Академии наук

Санкт-Петербург, 2011

# План

# Формулировка

## Теорема о полиномиальной эквивалентности

Для любой всюду определенной булевой функции $f$

$$\mathrm{Q}_{1/3}(f) \leqslant \mathrm{R}_{1/3}(f) \leqslant \mathrm{D}(f) = O\big(\mathrm{Q}_{1/3}(f)^6\big).$$

## Нижняя оценка квантовой сложности через степень приближения

Для любой булевой функции $\widetilde{\deg}(f) \leqslant 2\mathrm{Q}_{1/3}(f)$.

Поэтому достаточно доказать, что $\mathrm{D}(f) = O\big(\widetilde{\deg}(f)^6\big)$.

---

## Определение

$\widetilde{\deg}(f)$ — наименьшая степень такого многочлена $p(x)$, что

$$|p(x) - f(x)| < \frac{1}{3} \quad \text{для всех } x.$$

# Формулировка

## Теорема о полиномиальной эквивалентности

Для любой всюду определенной булевой функции $f$

$$\mathrm{Q}_{1/3}(f) \leqslant \mathrm{R}_{1/3}(f) \leqslant \mathrm{D}(f) = O\big(\mathrm{Q}_{1/3}(f)^6\big).$$

## Нижняя оценка квантовой сложности через степень приближения

Для любой булевой функции $\widetilde{\deg}(f) \leqslant 2\mathrm{Q}_{1/3}(f)$.

Поэтому достаточно доказать, что $\mathrm{D}(f) = O\big(\widetilde{\deg}(f)^6\big)$.

---

## Определение

$\widetilde{\deg}(f)$ — наименьшая степень такого многочлена $p(x)$, что

$$|p(x) - f(x)| < \frac{1}{3} \quad \text{для всех } x.$$

# Формулировка

## Теорема о полиномиальной эквивалентности

Для любой всюду определенной булевой функции $f$

$$\mathrm{Q}_{1/3}(f) \leqslant \mathrm{R}_{1/3}(f) \leqslant \mathrm{D}(f) = O\big(\mathrm{Q}_{1/3}(f)^6\big).$$

## Нижняя оценка квантовой сложности через степень приближения

Для любой булевой функции $\widetilde{\deg}(f) \leqslant 2\mathrm{Q}_{1/3}(f)$.

Поэтому достаточно доказать, что $\mathrm{D}(f) = O\big(\widetilde{\deg}(f)^6\big)$.

---

## Определение

$\widetilde{\deg}(f)$ — наименьшая степень такого многочлена $p(x)$, что

$$|p(x) - f(x)| < \frac{1}{3} \quad \text{для всех } x.$$

# Сертификаты

Частичное присваивание значений переменных

$$C\colon S \to \{0,1\}, \quad S \subseteq \{1,2,\ldots,n\}.$$

## $b$-сертификат ($b \in \{0,1\}$)

Такое частичное присваивание $C$, что $f(x) = b$ для всех $x$, согласованных с $C$, т. е. $x_i = C(i)$ при $i \in S$.

## Сертификатная сложность

$C_x(f)$ — длина наименьшего $f(x)$-сертификата, согласованного с $x$.

$$C(f) = \max_x C_x(f), \quad C^{(1)}(f) = \max_{x:f(x)=1} C_x(f), \quad C^{(0)}(f) = \max_{x:f(x)=0} C_x(f).$$

## Пример: дизъюнкция

$$C^{(1)}(OR) = 1; \quad C^{(0)}(OR) = C(OR) = n.$$

# Сертификаты

Частичное присваивание значений переменных

$$C\colon S \to \{0,1\}, \quad S \subseteq \{1,2,\ldots,n\}.$$

## $b$-сертификат ($b \in \{0,1\}$)

Такое частичное присваивание $C$, что $f(x) = b$ для всех $x$, согласованных с $C$, т. е. $x_i = C(i)$ при $i \in S$.

## Сертификатная сложность

$C_x(f)$ — длина наименьшего $f(x)$-сертификата, согласованного с $x$.

$$C(f) = \max_x C_x(f), \quad C^{(1)}(f) = \max_{x:f(x)=1} C_x(f), \quad C^{(0)}(f) = \max_{x:f(x)=0} C_x(f).$$

## Пример: дизъюнкция

$$C^{(1)}(OR) = 1; \quad C^{(0)}(OR) = C(OR) = n.$$

# Сертификаты

Частичное присваивание значений переменных

$$C\colon S \to \{0,1\}, \quad S \subseteq \{1,2,\ldots,n\}.$$

## $b$-сертификат ($b \in \{0,1\}$)

Такое частичное присваивание $C$, что $f(x) = b$ для всех $x$, согласованных с $C$, т. е. $x_i = C(i)$ при $i \in S$.

## Сертификатная сложность

$C_x(f)$ — длина наименьшего $f(x)$-сертификата, согласованного с $x$.

$$C(f) = \max_x C_x(f), \quad C^{(1)}(f) = \max_{x:f(x)=1} C_x(f), \quad C^{(0)}(f) = \max_{x:f(x)=0} C_x(f).$$

## Пример: дизъюнкция

$C^{(1)}(OR) = 1; \quad C^{(0)}(OR) = C(OR) = n.$

# Сертификаты

Частичное присваивание значений переменных

$$C\colon S \to \{0,1\}, \quad S \subseteq \{1,2,\ldots,n\}.$$

## $b$-сертификат ($b \in \{0,1\}$)

Такое частичное присваивание $C$, что $f(x) = b$ для всех $x$, согласованных с $C$, т. е. $x_i = C(i)$ при $i \in S$.

## Сертификатная сложность

$C_x(f)$ — длина наименьшего $f(x)$-сертификата, согласованного с $x$.

$$C(f) = \max_x C_x(f), \quad C^{(1)}(f) = \max_{x:f(x)=1} C_x(f), \quad C^{(0)}(f) = \max_{x:f(x)=0} C_x(f).$$

## Пример: дизъюнкция

$C^{(1)}(OR) = 1; \quad C^{(0)}(OR) = C(OR) = n.$

# Жадный алгоритм детерминированного вычисления $f$

1. Строим частичное присваивание, начиная с пустого.
2. Повторить не более $t$ раз:
   1. выбрать совместимый с текущим присваиванием 1-сертификат $C$;
   2. если такого нет, закончить работу с ответом 0;
   3. запросить значения переменных из $C$ (какие еще неизвестны);
   4. если полученные значения согласованы с $C$, закончить работу с результатом 1.
3. Выбрать любой $y$, согласованный с с текущими значениями переменных и выдать ответ $f(y)$.

**Вопрос**

Количество запросов в алгоритме не более $C^{(1)}(f)t$. При каких $t$ алгоритм работает корректно?

# Жадный алгоритм детерминированного вычисления $f$

1. Строим частичное присваивание, начиная с пустого.
2. Повторить не более $t$ раз:
   1. выбрать совместимый с текущим присваиванием 1-сертификат $C$;
   2. если такого нет, закончить работу с ответом 0;
   3. запросить значения переменных из $C$ (какие еще неизвестны);
   4. если полученные значения согласованы с $C$, закончить работу с результатом 1.
3. Выбрать любой $y$, согласованный с с текущими значениями переменных и выдать ответ $f(y)$.

**Вопрос**

Количество запросов в алгоритме не более $C^{(1)}(f)t$. При каких $t$ алгоритм работает корректно?

# Жадный алгоритм детерминированного вычисления $f$

1. Строим частичное присваивание, начиная с пустого.
2. Повторить не более $t$ раз:
   1. выбрать совместимый с текущим присваиванием 1-сертификат $C$;
   2. если такого нет, закончить работу с ответом 0;
   3. запросить значения переменных из $C$ (какие еще неизвестны);
   4. если полученные значения согласованы с $C$, закончить работу с результатом 1.
3. Выбрать любой $y$, согласованный с с текущими значениями переменных и выдать ответ $f(y)$.

**Вопрос**

Количество запросов в алгоритме не более $C^{(1)}(f)t$. При каких $t$ алгоритм работает корректно?

# Жадный алгоритм детерминированного вычисления $f$

1. Строим частичное присваивание, начиная с пустого.
2. Повторить не более $t$ раз:
   1. выбрать совместимый с текущим присваиванием 1-сертификат $C$;
   2. если такого нет, закончить работу с ответом 0;
   3. запросить значения переменных из $C$ (какие еще неизвестны);
   4. если полученные значения согласованы с $C$, закончить работу с результатом 1.
3. Выбрать любой $y$, согласованный с с текущими значениями переменных и выдать ответ $f(y)$.

**Вопрос**

Количество запросов в алгоритме не более $C^{(1)}(f)t$. При каких $t$ алгоритм работает корректно?

# Жадный алгоритм детерминированного вычисления $f$

1. Строим частичное присваивание, начиная с пустого.
2. Повторить не более $t$ раз:
   1. выбрать совместимый с текущим присваиванием 1-сертификат $C$;
   2. если такого нет, закончить работу с ответом 0;
   3. запросить значения переменных из $C$ (какие еще неизвестны);
   4. если полученные значения согласованы с $C$, закончить работу с результатом 1.
3. Выбрать любой $y$, согласованный с с текущими значениями переменных и выдать ответ $f(y)$.

**Вопрос**

Количество запросов в алгоритме не более $C^{(1)}(f)t$. При каких $t$ алгоритм работает корректно?

# Жадный алгоритм детерминированного вычисления $f$

1. Строим частичное присваивание, начиная с пустого.
2. Повторить не более $t$ раз:
   1. выбрать совместимый с текущим присваиванием 1-сертификат $C$;
   2. если такого нет, закончить работу с ответом 0;
   3. запросить значения переменных из $C$ (какие еще неизвестны);
   4. если полученные значения согласованы с $C$, закончить работу с результатом 1.
3. Выбрать любой $y$, согласованный с с текущими значениями переменных и выдать ответ $f(y)$.

**Вопрос**

Количество запросов в алгоритме не более $C^{(1)}(f)t$. При каких $t$ алгоритм работает корректно?

# Жадный алгоритм детерминированного вычисления $f$

1. Строим частичное присваивание, начиная с пустого.
2. Повторить не более $t$ раз:
   1. выбрать совместимый с текущим присваиванием 1-сертификат $C$;
   2. если такого нет, закончить работу с ответом 0;
   3. запросить значения переменных из $C$ (какие еще неизвестны);
   4. если полученные значения согласованы с $C$, закончить работу с результатом 1.
3. Выбрать любой $y$, согласованный с с текущими значениями переменных и выдать ответ $f(y)$.

**Вопрос**

Количество запросов в алгоритме не более $C^{(1)}(f)t$. При каких $t$ алгоритм работает корректно?

# Жадный алгоритм детерминированного вычисления $f$

1. Строим частичное присваивание, начиная с пустого.
2. Повторить не более $t$ раз:
   1. выбрать совместимый с текущим присваиванием 1-сертификат $C$;
   2. если такого нет, закончить работу с ответом 0;
   3. запросить значения переменных из $C$ (какие еще неизвестны);
   4. если полученные значения согласованы с $C$, закончить работу с результатом 1.
3. Выбрать любой $y$, согласованный с с текущими значениями переменных и выдать ответ $f(y)$.

**Вопрос**

Количество запросов в алгоритме не более $C^{(1)}(f)t$. При каких $t$ алгоритм работает корректно?

# Блочная чувствительность

Отождествляем множество $S \subseteq [1, \ldots, n]$ и его характеристический вектор $\chi(S)$ ($\chi_k(S) = 1 \Leftrightarrow k \in S$).

## Определение

Блочная чувствительность $\mathrm{bs}_x(f)$ функции $f$ в точке $x$ равна такому максимальному $b$, что существует набор из $b$ попарно непересекающихся подмножеств $B_1, \ldots, B_b$, для которых $f(x) \neq f(x \oplus B_i)$.

Блочная чувствительность $\mathrm{bs}(f)$ функции $f$ равна $\max_x \mathrm{bs}_x(f)$.

## Утверждение

Жадный алгоритм работает корректно при $t \geqslant \mathrm{bs}(f)$.

# Блочная чувствительность

Отождествляем множество $S \subseteq [1, \ldots, n]$ и его характеристический вектор $\chi(S)$ ($\chi_k(S) = 1 \Leftrightarrow k \in S$).

## Определение

Блочная чувствительность $\mathrm{bs}_x(f)$ функции $f$ в точке $x$ равна такому максимальному $b$, что существует набор из $b$ попарно непересекающихся подмножеств $B_1, \ldots, B_b$, для которых $f(x) \neq f(x \oplus B_i)$.

Блочная чувствительность $\mathrm{bs}(f)$ функции $f$ равна $\max_x \mathrm{bs}_x(f)$.

## Утверждение

Жадный алгоритм работает корректно при $t \geqslant \mathrm{bs}(f)$.

# Блочная чувствительность

Отождествляем множество $S \subseteq [1, \ldots, n]$ и его характеристический вектор $\chi(S)$ ($\chi_k(S) = 1 \Leftrightarrow k \in S$).

## Определение

Блочная чувствительность $\mathrm{bs}_x(f)$ функции $f$ в точке $x$ равна такому максимальному $b$, что существует набор из $b$ попарно непересекающихся подмножеств $B_1, \ldots, B_b$, для которых $f(x) \neq f(x \oplus B_i)$.

Блочная чувствительность $\mathrm{bs}(f)$ функции $f$ равна $\max_x \mathrm{bs}_x(f)$.

## Утверждение

Жадный алгоритм работает корректно при $t \geqslant \mathrm{bs}(f)$.

# Блочная чувствительность

Отождествляем множество $S \subseteq [1, \ldots, n]$ и его характеристический вектор $\chi(S)$ ($\chi_k(S) = 1 \Leftrightarrow k \in S$).

## Определение

Блочная чувствительность $\mathrm{bs}_x(f)$ функции $f$ в точке $x$ равна такому максимальному $b$, что существует набор из $b$ попарно непересекающихся подмножеств $B_1, \ldots, B_b$, для которых $f(x) \neq f(x \oplus B_i)$.

Блочная чувствительность $\mathrm{bs}(f)$ функции $f$ равна $\max_x \mathrm{bs}_x(f)$.

## Утверждение

Жадный алгоритм работает корректно при $t \geqslant \mathrm{bs}(f)$.

# Анализ алгоритма

- Ошибка возможна только на последнем шаге.
- В этом случае алгоритм запросил сертификаты $C_1, \ldots, C_t$ и существуют $y$, $y'$, согласованные со всеми известными значениями $x$ и такие, что $f(y) = 0$, $f(y') = 1$.
- Пусть $B_j$ — множество переменных, по которым различаются $C_j$ и $y$, а $B_{t+1} = y \oplus y'$.
- $B_j \neq \varnothing$ по построению ($f(y) = 0$, $y \neq y'$).
- Если $r \in B_j$, то $x_r = y_r \neq C_j(r)$.
- При $k > j$ сертификат $C_k$ согласован со всеми известными к этому времени значениями $x$, поэтому $r \in B_j \Rightarrow r \notin B_k$, т. е. $B_j \cap B_k = \varnothing$.
- Поэтому $\mathrm{bs}_y(f) \geqslant t + 1$ и утверждение доказано.

# Анализ алгоритма

- Ошибка возможна только на последнем шаге.
- В этом случае алгоритм запросил сертификаты $C_1, \ldots, C_t$ и существуют $y$, $y'$, согласованные со всеми известными значениями $x$ и такие, что $f(y) = 0$, $f(y') = 1$.
- Пусть $B_j$ — множество переменных, по которым различаются $C_j$ и $y$, а $B_{t+1} = y \oplus y'$.
- $B_j \neq \varnothing$ по построению ($f(y) = 0$, $y \neq y'$).
- Если $r \in B_j$, то $x_r = y_r \neq C_j(r)$.
- При $k > j$ сертификат $C_k$ согласован со всеми известными к этому времени значениями $x$, поэтому $r \in B_j \Rightarrow r \notin B_k$, т. е. $B_j \cap B_k = \varnothing$.
- Поэтому $\mathrm{bs}_y(f) \geqslant t + 1$ и утверждение доказано.

# Анализ алгоритма

- Ошибка возможна только на последнем шаге.
- В этом случае алгоритм запросил сертификаты $C_1, \ldots, C_t$ и существуют $y$, $y'$, согласованные со всеми известными значениями $x$ и такие, что $f(y) = 0$, $f(y') = 1$.
- Пусть $B_j$ — множество переменных, по которым различаются $C_j$ и $y$, а $B_{t+1} = y \oplus y'$.
- $B_j \neq \varnothing$ по построению ($f(y) = 0$, $y \neq y'$).
- Если $r \in B_j$, то $x_r = y_r \neq C_j(r)$.
- При $k > j$ сертификат $C_k$ согласован со всеми известными к этому времени значениями $x$, поэтому $r \in B_j \Rightarrow r \notin B_k$, т. е. $B_j \cap B_k = \varnothing$.
- Поэтому $\mathrm{bs}_y(f) \geqslant t + 1$ и утверждение доказано.

# Анализ алгоритма

- Ошибка возможна только на последнем шаге.
- В этом случае алгоритм запросил сертификаты $C_1, \ldots, C_t$ и существуют $y$, $y'$, согласованные со всеми известными значениями $x$ и такие, что $f(y) = 0$, $f(y') = 1$.
- Пусть $B_j$ — множество переменных, по которым различаются $C_j$ и $y$, а $B_{t+1} = y \oplus y'$.
- $B_j \neq \varnothing$ по построению ($f(y) = 0$, $y \neq y'$).
- Если $r \in B_j$, то $x_r = y_r \neq C_j(r)$.
- При $k > j$ сертификат $C_k$ согласован со всеми известными к этому времени значениями $x$, поэтому $r \in B_j \Rightarrow r \notin B_k$, т. е. $B_j \cap B_k = \varnothing$.
- Поэтому $\mathrm{bs}_y(f) \geqslant t + 1$ и утверждение доказано.

# Анализ алгоритма

- Ошибка возможна только на последнем шаге.
- В этом случае алгоритм запросил сертификаты $C_1, \ldots, C_t$ и существуют $y$, $y'$, согласованные со всеми известными значениями $x$ и такие, что $f(y) = 0$, $f(y') = 1$.
- Пусть $B_j$ — множество переменных, по которым различаются $C_j$ и $y$, а $B_{t+1} = y \oplus y'$.
- $B_j \neq \varnothing$ по построению ($f(y) = 0$, $y \neq y'$).
- Если $r \in B_j$, то $x_r = y_r \neq C_j(r)$.
- При $k > j$ сертификат $C_k$ согласован со всеми известными к этому времени значениями $x$, поэтому $r \in B_j \Rightarrow r \notin B_k$, т. е. $B_j \cap B_k = \varnothing$.
- Поэтому $\mathrm{bs}_y(f) \geqslant t + 1$ и утверждение доказано.

# Анализ алгоритма

- Ошибка возможна только на последнем шаге.
- В этом случае алгоритм запросил сертификаты $C_1, \ldots, C_t$ и существуют $y$, $y'$, согласованные со всеми известными значениями $x$ и такие, что $f(y) = 0$, $f(y') = 1$.
- Пусть $B_j$ — множество переменных, по которым различаются $C_j$ и $y$, а $B_{t+1} = y \oplus y'$.
- $B_j \neq \varnothing$ по построению ($f(y) = 0$, $y \neq y'$).
- Если $r \in B_j$, то $x_r = y_r \neq C_j(r)$.
- При $k > j$ сертификат $C_k$ согласован со всеми известными к этому времени значениями $x$, поэтому $r \in B_j \Rightarrow r \notin B_k$, т. е. $B_j \cap B_k = \varnothing$.
- Поэтому $\mathrm{bs}_y(f) \geqslant t + 1$ и утверждение доказано.

# Анализ алгоритма

- Ошибка возможна только на последнем шаге.
- В этом случае алгоритм запросил сертификаты $C_1, \ldots, C_t$ и существуют $y$, $y'$, согласованные со всеми известными значениями $x$ и такие, что $f(y) = 0$, $f(y') = 1$.
- Пусть $B_j$ — множество переменных, по которым различаются $C_j$ и $y$, а $B_{t+1} = y \oplus y'$.
- $B_j \neq \varnothing$ по построению ($f(y) = 0$, $y \neq y'$).
- Если $r \in B_j$, то $x_r = y_r \neq C_j(r)$.
- При $k > j$ сертификат $C_k$ согласован со всеми известными к этому времени значениями $x$, поэтому $r \in B_j \Rightarrow r \notin B_k$, т. е. $B_j \cap B_k = \varnothing$.
- Поэтому $\mathrm{bs}_y(f) \geqslant t + 1$ и утверждение доказано.

# Что дальше?

## Доказано

$\mathrm{D}(f) \leqslant \mathrm{bs}(f) C^{(1)}(f)$.

## Лемма 1

$C^{(1)}(f) \leqslant C(f) \leqslant \mathrm{s}(f)\mathrm{bs}(f) \leqslant \mathrm{bs}(f)^2$.

## Лемма 2 (теорема Нисана – Сегеди)

$\mathrm{bs}(f) \leqslant 6\widetilde{\deg}(f)^2$.

## Получим из лемм и оценки $\widetilde{\deg}(f) \leqslant 2\mathrm{Q}_{1/3}(f)$

$\mathrm{D}(f) \leqslant \mathrm{bs}(f)^3 \leqslant 216\widetilde{\deg}(f)^6 \leqslant 13824\mathrm{Q}_{1/3}(f)^6$,
что доказывает теорему о полиномиальной эквивалентности.

# Что дальше?

## Доказано

$\mathrm{D}(f) \leqslant \mathrm{bs}(f) C^{(1)}(f)$.

## Лемма 1

$C^{(1)}(f) \leqslant C(f) \leqslant \mathrm{s}(f)\mathrm{bs}(f) \leqslant \mathrm{bs}(f)^2$.

## Лемма 2 (теорема Нисана – Сегеди)

$\mathrm{bs}(f) \leqslant 6\widetilde{\deg}(f)^2$.

## Получим из лемм и оценки $\widetilde{\deg}(f) \leqslant 2\mathrm{Q}_{1/3}(f)$

$\mathrm{D}(f) \leqslant \mathrm{bs}(f)^3 \leqslant 216\widetilde{\deg}(f)^6 \leqslant 13824\mathrm{Q}_{1/3}(f)^6$,
что доказывает теорему о полиномиальной эквивалентности.

# Что дальше?

## Доказано

$\mathrm{D}(f) \leqslant \mathrm{bs}(f) C^{(1)}(f)$.

## Лемма 1

$C^{(1)}(f) \leqslant C(f) \leqslant \mathrm{s}(f)\mathrm{bs}(f) \leqslant \mathrm{bs}(f)^2$.

## Лемма 2 (теорема Нисана – Сегеди)

$\mathrm{bs}(f) \leqslant 6\widetilde{\deg}(f)^2$.

## Получим из лемм и оценки $\widetilde{\deg}(f) \leqslant 2\mathrm{Q}_{1/3}(f)$

$\mathrm{D}(f) \leqslant \mathrm{bs}(f)^3 \leqslant 216\widetilde{\deg}(f)^6 \leqslant 13824\mathrm{Q}_{1/3}(f)^6$,

что доказывает теорему о полиномиальной эквивалентности.

# Что дальше?

## Доказано

$\mathrm{D}(f) \leqslant \mathrm{bs}(f) C^{(1)}(f)$.

## Лемма 1

$C^{(1)}(f) \leqslant C(f) \leqslant \mathrm{s}(f)\mathrm{bs}(f) \leqslant \mathrm{bs}(f)^2$.

## Лемма 2 (теорема Нисана – Сегеди)

$\mathrm{bs}(f) \leqslant 6\widetilde{\deg}(f)^2$.

## Получим из лемм и оценки $\widetilde{\deg}(f) \leqslant 2\mathrm{Q}_{1/3}(f)$

$\mathrm{D}(f) \leqslant \mathrm{bs}(f)^3 \leqslant 216\widetilde{\deg}(f)^6 \leqslant 13824\mathrm{Q}_{1/3}(f)^6$,
что доказывает теорему о полиномиальной эквивалентности.

# Доказательство леммы 1 ($C(f) \leqslant \mathrm{s}(f)\mathrm{bs}(f) \leqslant \mathrm{bs}(f)^2$)

- Рассмотрим для некоторого $x$ максимальный набор чувствительных блоков $B_1, \ldots, B_b$, причем каждый блок выберем минимальным по включению.
- Присваивание $X : \cup_i B_i \overset{x}{\mapsto} \{0,1\}$ является $f(x)$-сертификатом:
  - если $y$ согласован с $X$ и $f(y) \neq f(x)$, то $\{B_j\} \cup \{y \oplus x\}$ является системой чувствительных блоков для $x$.
- Размер каждого блока $B_j$ не больше $\mathrm{s}_{x \oplus B_j}(f) \leqslant \mathrm{s}(f)$:
  - $f(x \oplus B_j \oplus e_k) = f(x \oplus b) = f(x) \neq f(x \oplus e_k)$.
- Следовательно, $C(f) \leqslant \mathrm{s}_x(f)\mathrm{bs}_x(f) \leqslant \mathrm{s}(f)\mathrm{bs}(f) \leqslant \mathrm{bs}(f)^2$.

# Доказательство леммы 1 ($C(f) \leqslant \mathrm{s}(f)\mathrm{bs}(f) \leqslant \mathrm{bs}(f)^2$)

- Рассмотрим для некоторого $x$ максимальный набор чувствительных блоков $B_1, \ldots, B_b$, причем каждый блок выберем минимальным по включению.
- Присваивание $X\colon \cup_i B_i \overset{x}{\mapsto} \{0,1\}$ является $f(x)$-сертификатом:
  - если $y$ согласован с $X$ и $f(y) \neq f(x)$, то $\{B_j\} \cup \{y \oplus x\}$ является системой чувствительных блоков для $x$.
- Размер каждого блока $B_j$ не больше $\mathrm{s}_{x \oplus B_j}(f) \leqslant \mathrm{s}(f)$:
  - $f(x \oplus B_j \oplus z) = f(x \oplus z) = f(x) \neq f(x \oplus B_j)$.
- Следовательно, $C(f) \leqslant \mathrm{s}_x(f)\mathrm{bs}_x(f) \leqslant \mathrm{s}(f)\mathrm{bs}(f) \leqslant \mathrm{bs}(f)^2$.

# Доказательство леммы 1 ($C(f) \leqslant \mathrm{s}(f)\mathrm{bs}(f) \leqslant \mathrm{bs}(f)^2$)

- Рассмотрим для некоторого $x$ максимальный набор чувствительных блоков $B_1, \ldots, B_b$, причем каждый блок выберем минимальным по включению.
- Присваивание $X\colon \cup_i B_i \overset{x}{\mapsto} \{0,1\}$ является $f(x)$-сертификатом:
  - если $y$ согласован с $X$ и $f(y) \neq f(x)$, то $\{B_j\} \cup \{y \oplus x\}$ является системой чувствительных блоков для $x$.
- Размер каждого блока $B_j$ не больше $\mathrm{s}_{x \oplus B_j}(f) \leqslant \mathrm{s}(f)$:
  - $f(x \oplus B_j \oplus e_k) = f(x \oplus B_j) = f(x) \neq f(x \oplus B_j)$.
- Следовательно, $C(f) \leqslant \mathrm{s}_x(f)\mathrm{bs}_x(f) \leqslant \mathrm{s}(f)\mathrm{bs}(f) \leqslant \mathrm{bs}(f)^2$.

# Доказательство леммы 1 ($C(f) \leqslant \mathrm{s}(f)\mathrm{bs}(f) \leqslant \mathrm{bs}(f)^2$)

- Рассмотрим для некоторого $x$ максимальный набор чувствительных блоков $B_1, \ldots, B_b$, причем каждый блок выберем минимальным по включению.
- Присваивание $X\colon \cup_i B_i \overset{x}{\mapsto} \{0,1\}$ является $f(x)$-сертификатом:
  - если $y$ согласован с $X$ и $f(y) \neq f(x)$, то $\{B_j\} \cup \{y \oplus x\}$ является системой чувствительных блоков для $x$.
- Размер каждого блока $B_j$ не больше $\mathrm{s}_{x \oplus B_j}(f) \leqslant \mathrm{s}(f)$:
  - $f(x \oplus B_j \oplus e_k) = f(x \oplus B'_j) = f(x) \neq f(x \oplus B_j)$.
- Следовательно, $C(f) \leqslant \mathrm{s}_x(f)\mathrm{bs}_x(f) \leqslant \mathrm{s}(f)\mathrm{bs}(f) \leqslant \mathrm{bs}(f)^2$.

# Доказательство леммы 1 ($C(f) \leqslant \mathrm{s}(f)\mathrm{bs}(f) \leqslant \mathrm{bs}(f)^2$)

- Рассмотрим для некоторого $x$ максимальный набор чувствительных блоков $B_1, \ldots, B_b$, причем каждый блок выберем минимальным по включению.
- Присваивание $X\colon \cup_i B_i \overset{x}{\mapsto} \{0,1\}$ является $f(x)$-сертификатом:
  - если $y$ согласован с $X$ и $f(y) \neq f(x)$, то $\{B_j\} \cup \{y \oplus x\}$ является системой чувствительных блоков для $x$.
- Размер каждого блока $B_j$ не больше $\mathrm{s}_{x \oplus B_j}(f) \leqslant \mathrm{s}(f)$:
  - $f(x \oplus B_j \oplus e_k) = f(x \oplus B'_j) = f(x) \neq f(x \oplus B_j)$.
- Следовательно, $C(f) \leqslant \mathrm{s}_x(f)\mathrm{bs}_x(f) \leqslant \mathrm{s}(f)\mathrm{bs}(f) \leqslant \mathrm{bs}(f)^2$.

# Доказательство леммы 1 ($C(f) \leqslant \mathrm{s}(f)\mathrm{bs}(f) \leqslant \mathrm{bs}(f)^2$)

- Рассмотрим для некоторого $x$ максимальный набор чувствительных блоков $B_1, \ldots, B_b$, причем каждый блок выберем минимальным по включению.
- Присваивание $X: \cup_i B_i \overset{x}{\mapsto} \{0,1\}$ является $f(x)$-сертификатом:
  - если $y$ согласован с $X$ и $f(y) \neq f(x)$, то $\{B_j\} \cup \{y \oplus x\}$ является системой чувствительных блоков для $x$.
- Размер каждого блока $B_j$ не больше $\mathrm{s}_{x \oplus B_j}(f) \leqslant \mathrm{s}(f)$:
  - $f(x \oplus B_j \oplus e_k) = f(x \oplus B_j') = f(x) \neq f(x \oplus B_j)$.
- Следовательно, $C(f) \leqslant \mathrm{s}_x(f)\mathrm{bs}_x(f) \leqslant \mathrm{s}(f)\mathrm{bs}(f) \leqslant \mathrm{bs}(f)^2$.

# Доказательство леммы 2 ($\mathrm{bs}(f) \leqslant 6\widetilde{\deg}(f)^2$)

- Пусть
  - в точке $a$ набор $B_1, \ldots, B_b$ достигает $\mathrm{bs}(f)$,
  - мультилинейный многочлен $p(x)$ степени $d$ приближает $f(x)$,
  - $f(a) = 0$ (не ограничивая общности).
- Строим многочлен $q(y_1, \ldots, y_b)$ подстановками в $p(x)$:
  - если $a_j = 0$ и $j \in B_k$, то $x_j := y_k$;
  - если $a_j = 1$ и $j \in B_k$, то $x_j := 1 - y_k$;
  - в противном случае $x_j := a_j$.
- Свойства $q(y)$
  - $\deg q(y) \leqslant d$, $q(y)$ — мультилинейный;
  - $1/3 \leqslant q(y) \leqslant 2/3$ при $y \in \{0,1\}^b$;
  - $|q(0) - p(a)| \leqslant 1/3$;
  - $q(e_i) = p(a \oplus e_i)$, $(a \oplus e_i)_j = 1$, поэтому $|q(e_i) - 1| \leqslant 1/3$.
- Применим нижнюю оценку степени многочлена через неравенство Маркова к $\tilde{q}$ — симметризации и специализации $q$.

# Доказательство леммы 2 ($\mathrm{bs}(f) \leqslant 6\widetilde{\deg}(f)^2$)

- Пусть
  - в точке $a$ набор $B_1, \ldots, B_b$ достигает $\mathrm{bs}(f)$,
  - мультилинейный многочлен $p(x)$ степени $d$ приближает $f(x)$,
  - $f(a) = 0$ (не ограничивая общности).
- Строим многочлен $q(y_1, \ldots, y_b)$ подстановками в $p(x)$:
  - если $a_j = 0$ и $j \in B_k$, то $x_j := y_k$;
  - если $a_j = 1$ и $j \in B_k$, то $x_j := 1 - y_k$;
  - в противном случае $x_j := a_j$.
- Свойства $q(y)$
  - $\deg q(y) \leqslant d$, $q(y)$ — мультилинейный;
  - $1/3 \leqslant q(y) \leqslant 2/3$ при $y \in \{0,1\}^b$;
  - $|q(0) - p(a)| \leqslant 1/3$;
  - $q(e_i) = p(a \oplus B_i)$, $|q(e_i) - q(0)| \geqslant 1/3$, поэтому $|\partial_i q| \geqslant 1/3$.
- Применим нижнюю оценку степени многочлена через неравенство Маркова к $\tilde{q}$ — симметризации и специализации $q$.

# Доказательство леммы 2 ($\mathrm{bs}(f) \leqslant 6\widetilde{\deg}(f)^2$)

- Пусть
  - в точке $a$ набор $B_1, \ldots, B_b$ достигает $\mathrm{bs}(f)$,
  - мультилинейный многочлен $p(x)$ степени $d$ приближает $f(x)$,
  - $f(a) = 0$ (не ограничивая общности).
- Строим многочлен $q(y_1, \ldots, y_b)$ подстановками в $p(x)$:
  - если $a_i = 0$ и $i \in B_k$, то $x_i := y_k$;
  - если $a_i = 1$ и $i \in B_k$, то $x_i := 1 - y_k$;
  - в противном случае $x_i := a_i$.
- Свойства $q(y)$
  - $\deg q(y) \leqslant d$, $q(y)$ — мультилинейный;
  - $\frac{1}{3} \leqslant q(y) \leqslant \frac{2}{3}$ при $y \in \{0,1\}^b$;
  - $|q(0) - p(a)| \leqslant 1/3$;
  - $q(e_i) = p(a \oplus B_i)$, $|q(e_i) - p(a)| \geqslant \frac{1}{3}$, поэтому $|q(e_i) - q(0)| \geqslant \frac{1}{3}$.
- Применим нижнюю оценку степени многочлена через неравенство Маркова к $\tilde{q}$ — симметризации и специализации $q$.

# Доказательство леммы 2 ($\mathrm{bs}(f) \leqslant 6\widetilde{\deg}(f)^2$)

- Пусть
  - в точке $a$ набор $B_1, \ldots, B_b$ достигает $\mathrm{bs}(f)$,
  - мультилинейный многочлен $p(x)$ степени $d$ приближает $f(x)$,
  - $f(a) = 0$ (не ограничивая общности).
- Строим многочлен $q(y_1, \ldots, y_b)$ подстановками в $p(x)$:
  - если $a_j = 0$ и $j \in B_k$, то $x_j := y_k$;
  - если $a_j = 1$ и $j \in B_k$, то $x_j := 1 - y_k$;
  - в противном случае $x_j := a_j$.
- Свойства $q(y)$
  - $\deg q(y) \leqslant d$, $q(y)$ — мультилинейный;
  - $-1/3 \leqslant q(y) \leqslant 4/3$ при $y \in \{0,1\}^b$;
  - $|q(0) - p(a)| \leqslant 1/3$;
  - $q(e_i) = p(a \oplus B_i)$, $|q(e_i) - p(a)| \geqslant 1$, поэтому $|\nabla_i q(0)| \geqslant 1/b$.
- Применим нижнюю оценку степени многочлена через неравенство Маркова к $\tilde{q}$ — симметризации и специализации $q$.

# Доказательство леммы 2 ($\mathrm{bs}(f) \leqslant 6\widetilde{\deg}(f)^2$)

- Пусть
  - в точке $a$ набор $B_1, \ldots, B_b$ достигает $\mathrm{bs}(f)$,
  - мультилинейный многочлен $p(x)$ степени $d$ приближает $f(x)$,
  - $f(a) = 0$ (не ограничивая общности).
- Строим многочлен $q(y_1, \ldots, y_b)$ подстановками в $p(x)$:
  - если $a_j = 0$ и $j \in B_k$, то $x_j := y_k$;
  - если $a_j = 1$ и $j \in B_k$, то $x_j := 1 - y_k$;
  - в противном случае $x_j := a_j$.
- Свойства $q(y)$
  - $\deg q(y) \leqslant d$; $q(y)$ — мультилинейный;
  - $\frac{1}{3} \leqslant q(y) \leqslant \frac{2}{3}$ при $y \in \{0,1\}^b$;
  - $|q(0) - p(a)| \leqslant 1/3$;
  - $q(e_i) = p(a \oplus B_i)$, $|q(e_i) - q(0)| \geqslant 1/3$, поэтому $\|\tilde{q}'\| \geqslant 1/b$.
- Применим нижнюю оценку степени многочлена через неравенство Маркова к $\tilde{q}$ — симметризации и специализации $q$.

# Доказательство леммы 2 ($\mathrm{bs}(f) \leqslant 6\widetilde{\deg}(f)^2$)

- Пусть
  - в точке $a$ набор $B_1, \ldots, B_b$ достигает $\mathrm{bs}(f)$,
  - мультилинейный многочлен $p(x)$ степени $d$ приближает $f(x)$,
  - $f(a) = 0$ (не ограничивая общности).
- Строим многочлен $q(y_1, \ldots, y_b)$ подстановками в $p(x)$:
  - если $a_j = 0$ и $j \in B_k$, то $x_j := y_k$;
  - если $a_j = 1$ и $j \in B_k$, то $x_j := 1 - y_k$;
  - в противном случае $x_j := a_j$.
- Свойства $q(y)$
  - $\deg q(y) \leqslant d$, $q(y)$ — мультилинейный;
  - $\frac{1}{3} \leqslant q(y) \leqslant \frac{2}{3}$ при $y \in \{0,1\}^b$;
  - $|q(0) - p(a)| \leqslant 1/3$;
  - $q(e_i) = p(a \oplus B_i)$, $|e_i| = b_i = 1$, поэтому $|q(e_i) - 1/2| \geqslant 1/6$.
- Применим нижнюю оценку степени многочлена через неравенство Маркова к $\tilde{q}$ — симметризации и специализации $q$.

# Доказательство леммы 2 ($\mathrm{bs}(f) \leqslant 6\widetilde{\deg}(f)^2$)

- Пусть
  - в точке $a$ набор $B_1, \ldots, B_b$ достигает $\mathrm{bs}(f)$,
  - мультилинейный многочлен $p(x)$ степени $d$ приближает $f(x)$,
  - $f(a) = 0$ (не ограничивая общности).
- Строим многочлен $q(y_1, \ldots, y_b)$ подстановками в $p(x)$:
  - если $a_j = 0$ и $j \in B_k$, то $x_j := y_k$;
  - если $a_j = 1$ и $j \in B_k$, то $x_j := 1 - y_k$;
  - в противном случае $x_j := a_j$.
- Свойства $q(y)$
  - $\deg q(y) \leqslant d$; $q(y)$ — мультилинейный;
  - $|q(y)| \leqslant \frac{1}{3}$ при $y \in \{0,1\}^b$;
  - $|q(0)| \geqslant \frac{2}{3}$;
  - $q(e_i) = p(a \oplus B_i)$, $\{e_1, \ldots, e_b\}$ — стандартный базис $\mathbb{R}^b$.
- Применим нижнюю оценку степени многочлена через неравенство Маркова к $\tilde{q}$ — симметризации и специализации $q$.

# Доказательство леммы 2 ($\mathrm{bs}(f) \leqslant 6\widetilde{\deg}(f)^2$)

- Пусть
  - в точке $a$ набор $B_1, \ldots, B_b$ достигает $\mathrm{bs}(f)$,
  - мультилинейный многочлен $p(x)$ степени $d$ приближает $f(x)$,
  - $f(a) = 0$ (не ограничивая общности).
- Строим многочлен $q(y_1, \ldots, y_b)$ подстановками в $p(x)$:
  - если $a_j = 0$ и $j \in B_k$, то $x_j := y_k$;
  - если $a_j = 1$ и $j \in B_k$, то $x_j := 1 - y_k$;
  - в противном случае $x_j := a_j$.
- Свойства $q(y)$
  - $\deg q(y) \leqslant d$, $q(y)$ — мультилинейный;
  - $|q(y) - q(0)| \leqslant 1/3$ при $y \in \{0,1\}^b$;
  - $|q(0) - p(a)| < 1/3$;
  - $q(e_i) - q(0) \in \{1, 0, -1\}$, поэтому $|q(e_i) - q(0)| \leqslant 1/3$.
- Применим нижнюю оценку степени многочлена через неравенство Маркова к $\tilde{q}$ — симметризации и специализации $q$.

# Доказательство леммы 2 ($\mathrm{bs}(f) \leqslant 6\widetilde{\deg}(f)^2$)

- Пусть
  - в точке $a$ набор $B_1, \ldots, B_b$ достигает $\mathrm{bs}(f)$,
  - мультилинейный многочлен $p(x)$ степени $d$ приближает $f(x)$,
  - $f(a) = 0$ (не ограничивая общности).
- Строим многочлен $q(y_1, \ldots, y_b)$ подстановками в $p(x)$:
  - если $a_j = 0$ и $j \in B_k$, то $x_j := y_k$;
  - если $a_j = 1$ и $j \in B_k$, то $x_j := 1 - y_k$;
  - в противном случае $x_j := a_j$.
- Свойства $q(y)$
  - $\deg q(y) \leqslant d$, $q(y)$ — мультилинейный;
  - $-1/3 < q(y) < 4/3$ при $y \in \{0,1\}^n$;
  - $|q(0) = p(a)| < 1/3$;
  - $q(e_j) = p(a \oplus B_j)$, $f(a \oplus B_j) = 1$, поэтому $|q(e_j) - 1| < 1/3$.
- Применим нижнюю оценку степени многочлена через неравенство Маркова к $\tilde{q}$ — симметризации и специализации $q$.

# Доказательство леммы 2 ($\mathrm{bs}(f) \leqslant 6\widetilde{\deg}(f)^2$)

- Пусть
  - в точке $a$ набор $B_1, \ldots, B_b$ достигает $\mathrm{bs}(f)$,
  - мультилинейный многочлен $p(x)$ степени $d$ приближает $f(x)$,
  - $f(a) = 0$ (не ограничивая общности).
- Строим многочлен $q(y_1, \ldots, y_b)$ подстановками в $p(x)$:
  - если $a_j = 0$ и $j \in B_k$, то $x_j := y_k$;
  - если $a_j = 1$ и $j \in B_k$, то $x_j := 1 - y_k$;
  - в противном случае $x_j := a_j$.
- Свойства $q(y)$
  - $\deg q(y) \leqslant d$, $q(y)$ — мультилинейный;
  - $-1/3 < q(y) < 4/3$ при $y \in \{0,1\}^n$;
  - $|q(0) = p(a)| < 1/3$;
  - $q(e_j) = p(a \oplus B_j)$, $f(a \oplus B_j) = 1$, поэтому $|q(e_j) - 1| < 1/3$.
- Применим нижнюю оценку степени многочлена через неравенство Маркова к $\tilde{q}$ — симметризации и специализации $q$.

# Доказательство леммы 2 ($\mathrm{bs}(f) \leqslant 6\widetilde{\deg}(f)^2$)

- Пусть
  - в точке $a$ набор $B_1, \ldots, B_b$ достигает $\mathrm{bs}(f)$,
  - мультилинейный многочлен $p(x)$ степени $d$ приближает $f(x)$,
  - $f(a) = 0$ (не ограничивая общности).
- Строим многочлен $q(y_1, \ldots, y_b)$ подстановками в $p(x)$:
  - если $a_j = 0$ и $j \in B_k$, то $x_j := y_k$;
  - если $a_j = 1$ и $j \in B_k$, то $x_j := 1 - y_k$;
  - в противном случае $x_j := a_j$.
- Свойства $q(y)$
  - $\deg q(y) \leqslant d$, $q(y)$ — мультилинейный;
  - $-1/3 < q(y) < 4/3$ при $y \in \{0,1\}^n$;
  - $|q(0) = p(a)| < 1/3$;
  - $q(e_j) = p(a \oplus B_j)$, $f(a \oplus B_j) = 1$, поэтому $|q(e_j) - 1| < 1/3$.
- Применим нижнюю оценку степени многочлена через неравенство Маркова к $\tilde{q}$ — симметризации и специализации $q$.

# Доказательство леммы 2 ($\mathrm{bs}(f) \leqslant 6\widetilde{\deg}(f)^2$)

- Пусть
  - в точке $a$ набор $B_1, \ldots, B_b$ достигает $\mathrm{bs}(f)$,
  - мультилинейный многочлен $p(x)$ степени $d$ приближает $f(x)$,
  - $f(a) = 0$ (не ограничивая общности).
- Строим многочлен $q(y_1, \ldots, y_b)$ подстановками в $p(x)$:
  - если $a_j = 0$ и $j \in B_k$, то $x_j := y_k$;
  - если $a_j = 1$ и $j \in B_k$, то $x_j := 1 - y_k$;
  - в противном случае $x_j := a_j$.
- Свойства $q(y)$
  - $\deg q(y) \leqslant d$, $q(y)$ — мультилинейный;
  - $-1/3 < q(y) < 4/3$ при $y \in \{0,1\}^n$;
  - $|q(0) = p(a)| < 1/3$;
  - $q(e_j) = p(a \oplus B_j)$, $f(a \oplus B_j) = 1$, поэтому $|q(e_j) - 1| < 1/3$.
- Применим нижнюю оценку степени многочлена через неравенство Маркова к $\tilde{q}$ — симметризации и специализации $q$.

# Доказательство леммы 2 ($\mathrm{bs}(f) \leqslant 6\widetilde{\deg}(f)^2$)

- Пусть
  - в точке $a$ набор $B_1, \ldots, B_b$ достигает $\mathrm{bs}(f)$,
  - мультилинейный многочлен $p(x)$ степени $d$ приближает $f(x)$,
  - $f(a) = 0$ (не ограничивая общности).
- Строим многочлен $q(y_1, \ldots, y_b)$ подстановками в $p(x)$:
  - если $a_j = 0$ и $j \in B_k$, то $x_j := y_k$;
  - если $a_j = 1$ и $j \in B_k$, то $x_j := 1 - y_k$;
  - в противном случае $x_j := a_j$.
- Свойства $q(y)$
  - $\deg q(y) \leqslant d$, $q(y)$ — мультилинейный;
  - $-1/3 < q(y) < 4/3$ при $y \in \{0,1\}^n$;
  - $|q(0) = p(a)| < 1/3$;
  - $q(e_j) = p(a \oplus B_j)$, $f(a \oplus B_j) = 1$, поэтому $|q(e_j) - 1| < 1/3$.
- Применим нижнюю оценку степени многочлена через неравенство Маркова к $\tilde{q}$ — симметризации и специализации $q$.

# Доказательство леммы 2 ($\mathrm{bs}(f) \leqslant 6\widetilde{\deg}(f)^2$)

- Пусть
  - в точке $a$ набор $B_1, \ldots, B_b$ достигает $\mathrm{bs}(f)$,
  - мультилинейный многочлен $p(x)$ степени $d$ приближает $f(x)$,
  - $f(a) = 0$ (не ограничивая общности).
- Строим многочлен $q(y_1, \ldots, y_b)$ подстановками в $p(x)$:
  - если $a_j = 0$ и $j \in B_k$, то $x_j := y_k$;
  - если $a_j = 1$ и $j \in B_k$, то $x_j := 1 - y_k$;
  - в противном случае $x_j := a_j$.
- Свойства $q(y)$
  - $\deg q(y) \leqslant d$, $q(y)$ — мультилинейный;
  - $-1/3 < q(y) < 4/3$ при $y \in \{0,1\}^n$;
  - $|q(0) = p(a)| < 1/3$;
  - $q(e_j) = p(a \oplus B_j)$, $f(a \oplus B_j) = 1$, поэтому $|q(e_j) - 1| < 1/3$.
- Применим нижнюю оценку степени многочлена через неравенство Маркова к $\tilde{q}$ — симметризации и специализации $q$.

# Доказательство леммы 2 ($\mathrm{bs}(f) \leqslant 6\widetilde{\deg}(f)^2$)

- Свойства $q(y)$:
  - $\deg q(y) \leqslant d$, $q(y)$ — мультилинейный;
  - $-1/3 < q(y) < 4/3$ при $y \in \{0,1\}^n$;
  - $|q(0) = p(a)| < 1/3$;
  - $q(e_j) = p(a \oplus B_j)$, $f(a \oplus B_j) = 1$, поэтому $|q(e_j) - 1| < 1/3$.
- Симметризация многочлена:

$$q^{sym}(y_1, \ldots, y_b) = \frac{1}{b!} \sum_{\sigma \in S_b} q(y_{\sigma(1)}, y_{\sigma(2)}, \ldots, y_{\sigma(n)}).$$

- Специализация

$$\tilde{q}(t) = q^{sym}(t, t, \ldots, t).$$

удовлетворяет условиям теоремы о нижней оценке.

**Теорема (нижняя оценка на степень многочлена)**

Пусть $f(x)$ — многочлен и $|f(0)| < 1/3$, $|f(1) - 1| < 1/3$, а $-1/3 < f(k) < 4/3$ при $2 \leqslant k \leqslant n$.
Тогда $\deg f \geqslant \sqrt{n/6}$.

# Доказательство леммы 2 ($\mathrm{bs}(f) \leqslant 6\widetilde{\deg}(f)^2$)

- Свойства $q(y)$:
  - $\deg q(y) \leqslant d$, $q(y)$ — мультилинейный;
  - $-1/3 < q(y) < 4/3$ при $y \in \{0,1\}^n$;
  - $|q(0) = p(a)| < 1/3$;
  - $q(e_j) = p(a \oplus B_j)$, $f(a \oplus B_j) = 1$, поэтому $|q(e_j) - 1| < 1/3$.
- Симметризация многочлена:

$$q^{sym}(y_1, \ldots, y_b) = \frac{1}{b!} \sum_{\sigma \in S_b} q(y_{\sigma(1)}, y_{\sigma(2)}, \ldots, y_{\sigma(n)}).$$

- Специализация

$$\tilde{q}(t) = q^{sym}(t, t, \ldots, t).$$

удовлетворяет условиям теоремы о нижней оценке.

**Теорема (нижняя оценка на степень многочлена)**

Пусть $f(x)$ — многочлен и $|f(0)| < 1/3$, $|f(1) - 1| < 1/3$, а $-1/3 < f(k) < 4/3$ при $2 \leqslant k \leqslant n$.
Тогда $\deg f \geqslant \sqrt{n/6}$.

# Доказательство леммы 2 ($\mathrm{bs}(f) \leqslant 6\widetilde{\deg}(f)^2$)

- Свойства $q(y)$:
  - $\deg q(y) \leqslant d$, $q(y)$ — мультилинейный;
  - $-1/3 < q(y) < 4/3$ при $y \in \{0,1\}^n$;
  - $|q(0) = p(a)| < 1/3$;
  - $q(e_j) = p(a \oplus B_j)$, $f(a \oplus B_j) = 1$, поэтому $|q(e_j) - 1| < 1/3$.
- Симметризация многочлена:
$$q^{sym}(y_1, \ldots, y_b) = \frac{1}{b!} \sum_{\sigma \in S_b} q(y_{\sigma(1)}, y_{\sigma(2)}, \ldots, y_{\sigma(n)}).$$
- Специализация
$$\tilde{q}(t) = q^{sym}(t, t, \ldots, t).$$
удовлетворяет условиям теоремы о нижней оценке.

**Теорема (нижняя оценка на степень многочлена)**

Пусть $f(x)$ — многочлен и $|f(0)| < 1/3$, $|f(1) - 1| < 1/3$, а $-1/3 < f(k) < 4/3$ при $2 \leqslant k \leqslant n$.
Тогда $\deg f \geqslant \sqrt{n/6}$.

# Доказательство леммы 2 ($\mathrm{bs}(f) \leqslant 6\widetilde{\deg}(f)^2$)

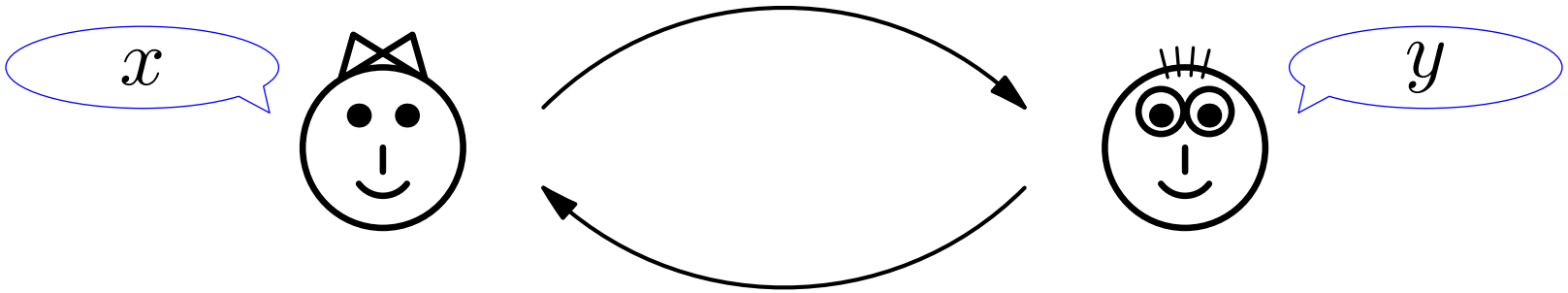
- Свойства $q(y)$:
  - $\deg q(y) \leqslant d$, $q(y)$ — мультилинейный;
  - $-1/3 < q(y) < 4/3$ при $y \in \{0,1\}^n$;
  - $|q(0) = p(a)| < 1/3$;
  - $q(e_j) = p(a \oplus B_j)$, $f(a \oplus B_j) = 1$, поэтому $|q(e_j) - 1| < 1/3$.
- Симметризация многочлена:
$$q^{sym}(y_1, \ldots, y_b) = \frac{1}{b!} \sum_{\sigma \in S_b} q(y_{\sigma(1)}, y_{\sigma(2)}, \ldots, y_{\sigma(n)}).$$
- Специализация
$$\tilde{q}(t) = q^{sym}(t, t, \ldots, t).$$
удовлетворяет условиям теоремы о нижней оценке.

**Теорема (нижняя оценка на степень многочлена)**

Пусть $f(x)$ — многочлен и $|f(0)| < 1/3$, $|f(1) - 1| < 1/3$, а $-1/3 < f(k) < 4/3$ при $2 \leqslant k \leqslant n$.
Тогда $\deg f \geqslant \sqrt{n/6}$.

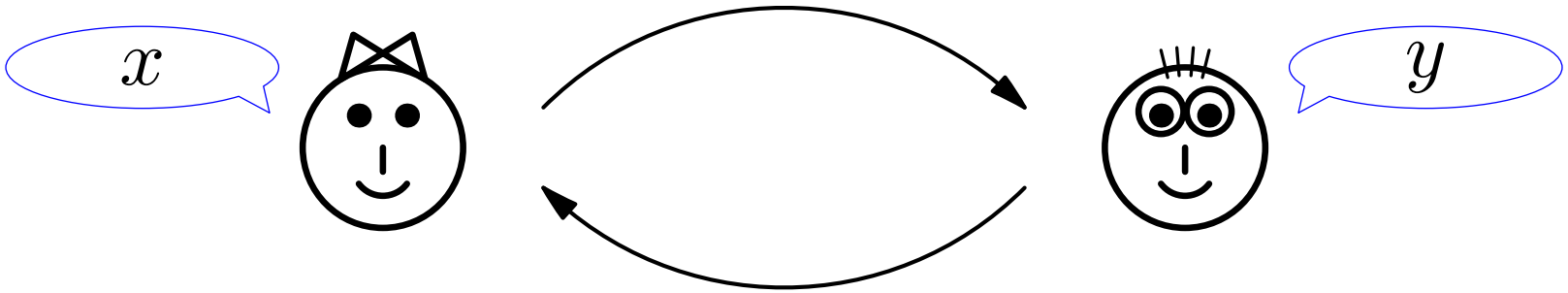
# План

# Основная модель коммуникации: детерминированная



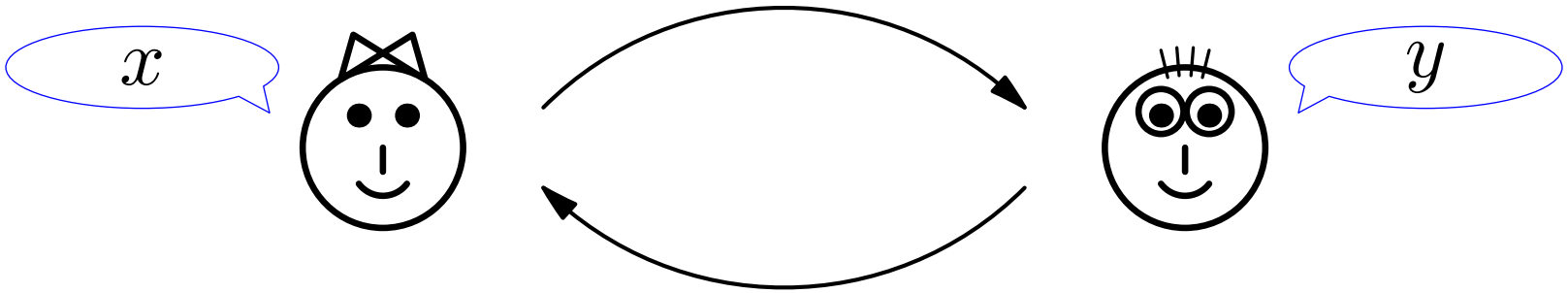

- Алиса знает $x \in \{0,1\}^n$; Боб знает $y \in \{0,1\}^n$.
- Цель: вычислить $f(x,y)$.
- Возможности: Алиса и Боб могут обмениваться сообщениями. Их действия адаптивны (зависят от полученных сообщений).
- Коммуникационная сложность $C(f)$: наименьшее количество битов в протоколе, гарантирующем вычисление $f(x,y)$ для любых $x$, $y$.

# Основная модель коммуникации: детерминированная



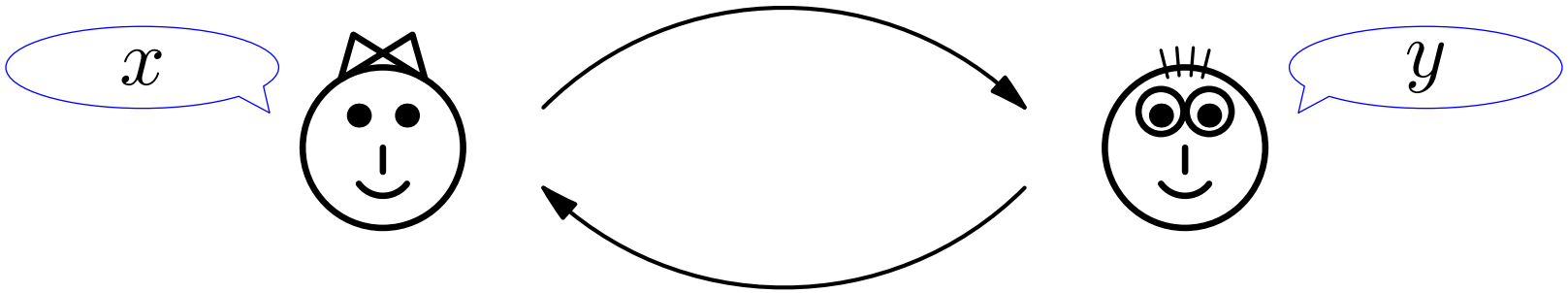

- Алиса знает $x \in \{0,1\}^n$; Боб знает $y \in \{0,1\}^n$.
- Цель: вычислить $f(x,y)$.
- Возможности: Алиса и Боб могут обмениваться сообщениями. Их действия адаптивны (зависят от полученных сообщений).
- Коммуникационная сложность $C(f)$: наименьшее количество битов в протоколе, гарантирующем вычисление $f(x,y)$ для любых $x$, $y$.

# Основная модель коммуникации: детерминированная



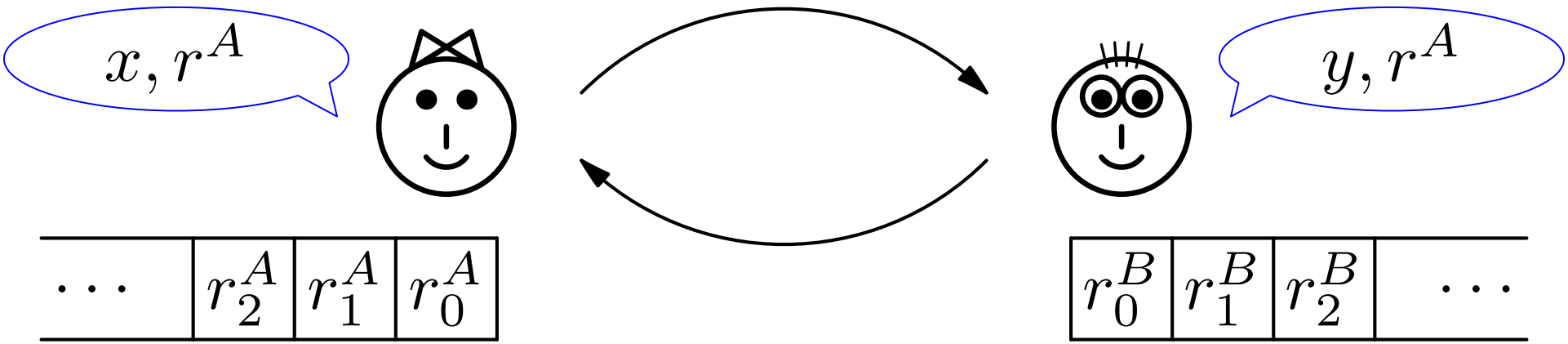

- Алиса знает $x \in \{0,1\}^n$; Боб знает $y \in \{0,1\}^n$.
- Цель: вычислить $f(x,y)$.
- Возможности: Алиса и Боб могут обмениваться сообщениями. Их действия адаптивны (зависят от полученных сообщений).
- Коммуникационная сложность $C(f)$: наименьшее количество битов в протоколе, гарантирующем вычисление $f(x,y)$ для любых $x$, $y$.

# Основная модель коммуникации: детерминированная




- Алиса знает $x \in \{0,1\}^n$; Боб знает $y \in \{0,1\}^n$.
- Цель: вычислить $f(x,y)$.
- Возможности: Алиса и Боб могут обмениваться сообщениями. Их действия адаптивны (зависят от полученных сообщений).
- Коммуникационная сложность $C(f)$: наименьшее количество битов в протоколе, гарантирующем вычисление $f(x,y)$ для любых $x$, $y$.

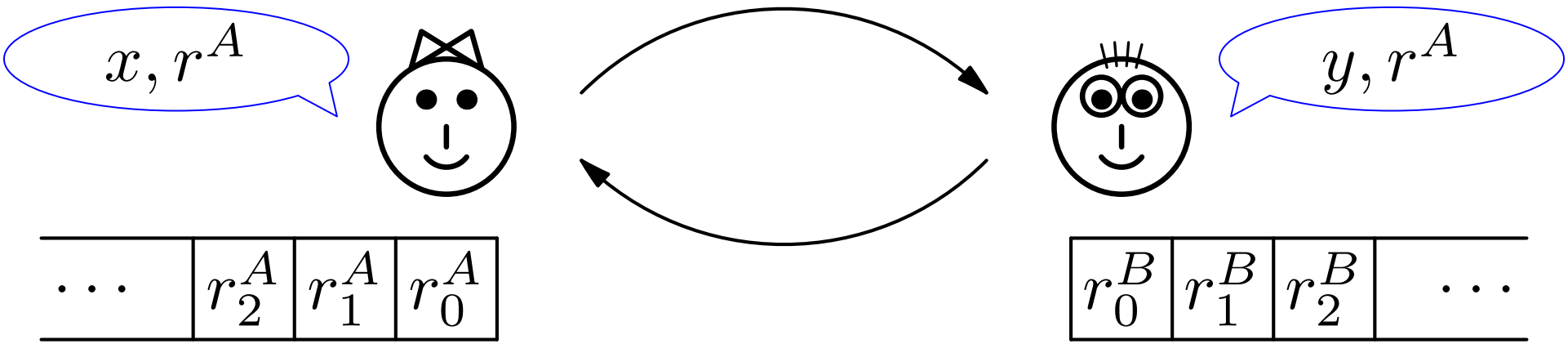
# Основная модель: вероятностная, частные генераторы




Изменения к предыдущему:

- Возможности: Алиса и Боб могут использовать генератор случайности. У каждого свой.
- Вероятностная коммуникационная сложность $R_\varepsilon(f)$: наименьшее количество битов в протоколе, гарантирующем вычисление $f(x, y)$ с ошибкой не более $\varepsilon$ для любых $x$, $y$.

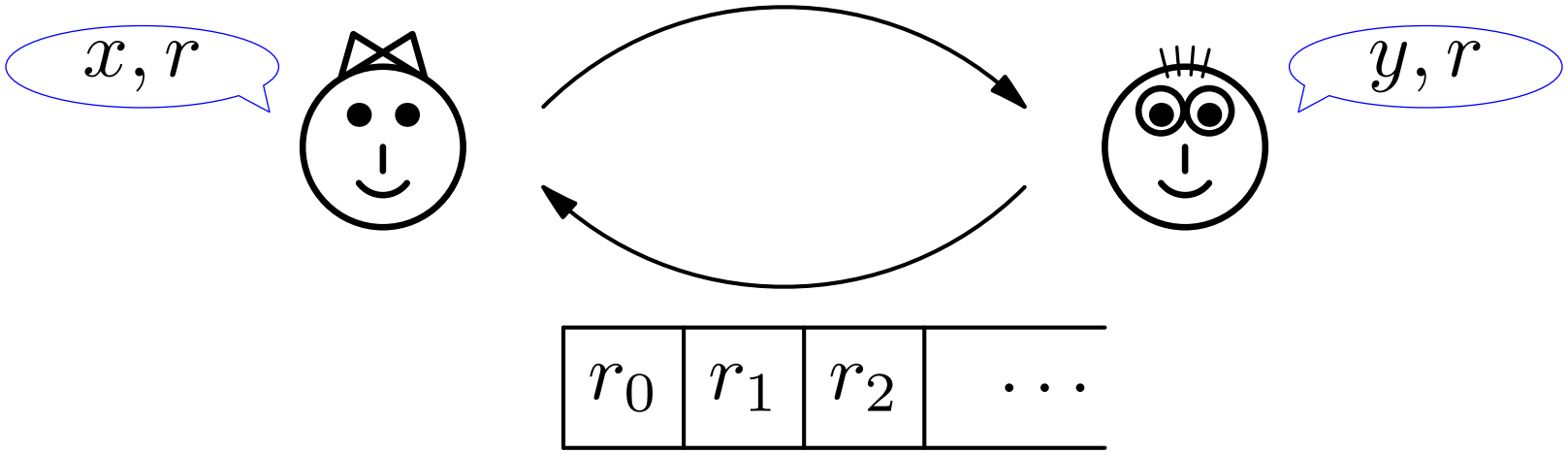
# Основная модель: вероятностная, частные генераторы




Изменения к предыдущему:

- Возможности: Алиса и Боб могут использовать генератор случайности. У каждого свой.
- Вероятностная коммуникационная сложность $R_\varepsilon(f)$: наименьшее количество битов в протоколе, гарантирующем вычисление $f(x, y)$ с ошибкой не более $\varepsilon$ для любых $x$, $y$.

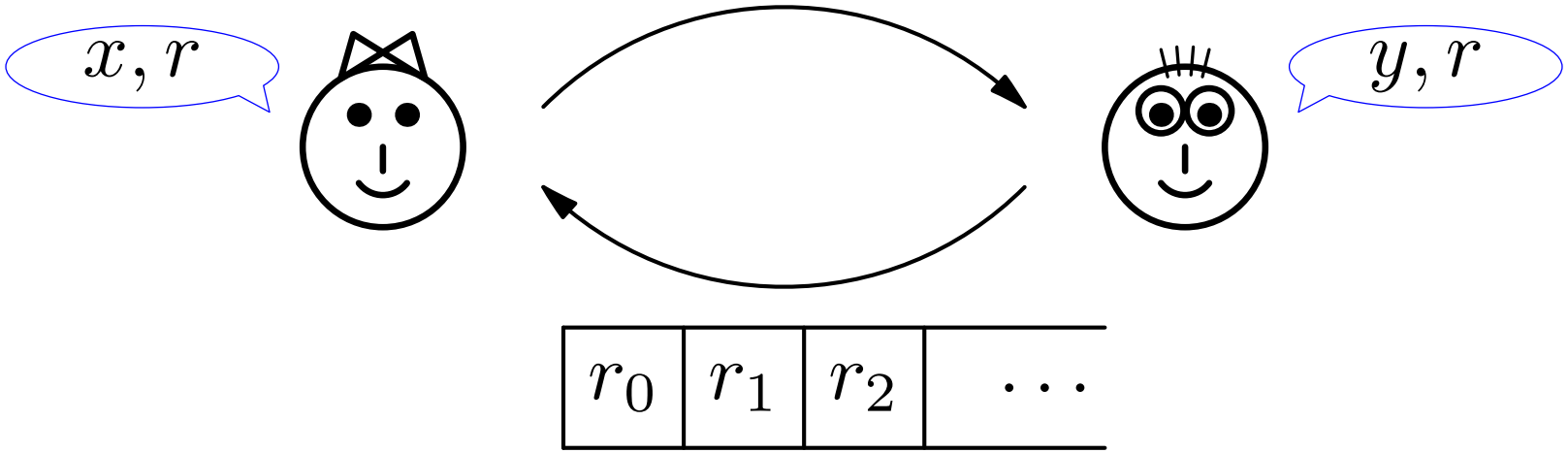
# Основная модель: вероятностная, общий генератор




Изменения к предыдущему:

- Возможности: Алиса и Боб используют один и тот же генератор случайности.
- Вероятностная коммуникационная сложность с общим генератором $R_\varepsilon^{\text{pub}}(f)$: наименьшее количество битов в протоколе, гарантирующем вычисление $f(x, y)$ с ошибкой не более $\varepsilon$ для любых $x$, $y$.

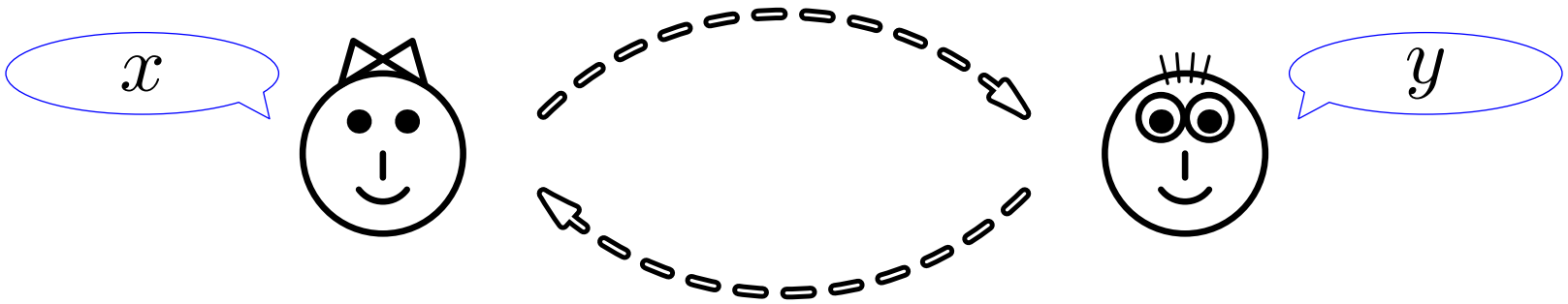
# Основная модель: вероятностная, общий генератор




Изменения к предыдущему:

- Возможности: Алиса и Боб используют один и тот же генератор случайности.
- Вероятностная коммуникационная сложность с общим генератором $R_\varepsilon^{\mathrm{pub}}(f)$: наименьшее количество битов в протоколе, гарантирующем вычисление $f(x, y)$ с ошибкой не более $\varepsilon$ для любых $x$, $y$.

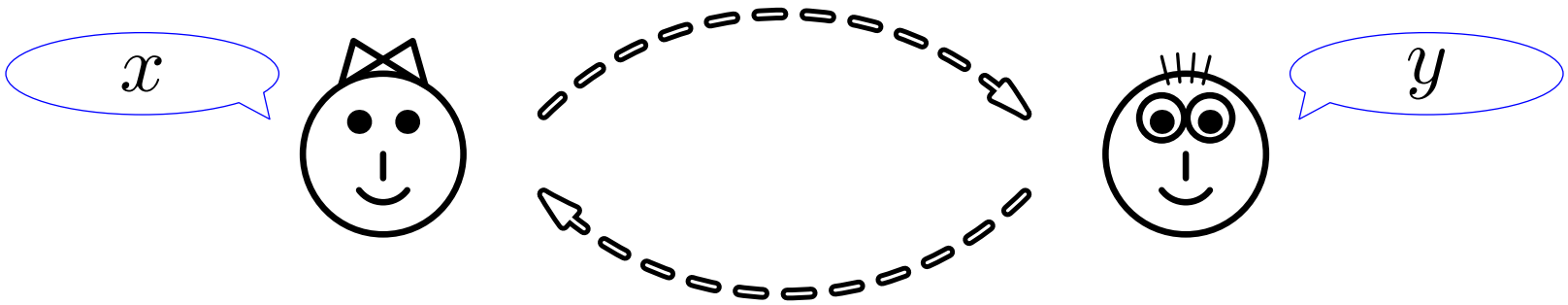
# Основная модель: квантовая




Изменения к предыдущему:

- Возможности: Алиса и Боб используют квантовые носители информации. Обмениваются также квантовыми сообщениями.
- Квантовая коммуникационная сложность $Q_\varepsilon(f)$: наименьшая длина протокола, гарантирующего вычисление $f(x, y)$ с ошибкой не более $\varepsilon$ для любых $x$, $y$.

# Основная модель: квантовая




Изменения к предыдущему:

- Возможности: Алиса и Боб используют квантовые носители информации. Обмениваются также квантовыми сообщениями.
- Квантовая коммуникационная сложность $Q_\varepsilon(f)$: наименьшая длина протокола, гарантирующего вычисление $f(x, y)$ с ошибкой не более $\varepsilon$ для любых $x$, $y$.

# Общий случай: передача нескольких кубитов

- Обозначение: $U[S]$ — оператор $U$, который действует на множестве кубитов $S$, а на остальных как единичный. Если $S$ — первые кубиты, то $U[S]|s,t\rangle = U|s\rangle \otimes |t\rangle$.

**Упражнение**

Напишите в вычислительном базисе матрицу оператора c-NOT$[1,3]$, который действует на трех кубитах. Оператор c-NOT — это оператор обратимого копирования: c-NOT$: |x,y\rangle \mapsto |x, x \oplus y\rangle$.

- Квантовый протокол — разбиение $\{1,2,\ldots,N\} = A \dot\cup B$; последовательность операторов $U_1[S_1]$, $U_2[S_2]$, …, $U_\ell[S_\ell]$, причем $S_1 \subseteq A$. В начале $A$ — $|0,x\rangle$; $B$ — $|0,y\rangle$.
- Множества $S_j$ определяют, какие кубиты пересылаются: чтобы Алиса могла подействовать на кубит, который у Боба, нужно этот кубит ей переслать, и наоборот.
- Длина протокола — количество пересланных кубитов.
- Результат измеряется в одном заранее указанном кубите.

# Общий случай: передача нескольких кубитов

- Обозначение: $U[S]$ — оператор $U$, который действует на множестве кубитов $S$, а на остальных как единичный. Если $S$ — первые кубиты, то $U[S]|s,t\rangle = U|s\rangle \otimes |t\rangle$.

**Упражнение**

Напишите в вычислительном базисе матрицу оператора c-NOT$[1,3]$, который действует на трех кубитах. Оператор c-NOT — это оператор обратимого копирования: c-NOT$: |x,y\rangle \mapsto |x, x \oplus y\rangle$.

- Квантовый протокол — разбиение $\{1,2,\ldots,N\} = A \dot\cup B$; последовательность операторов $U_1[S_1]$, $U_2[S_2]$, …, $U_\ell[S_\ell]$, причем $S_1 \subseteq A$. В начале $A$ — $|0,x\rangle$; $B$ — $|0,y\rangle$.
- Множества $S_j$ определяют, какие кубиты пересылаются: чтобы Алиса могла подействовать на кубит, который у Боба, нужно этот кубит ей переслать, и наоборот.
- Длина протокола — количество пересланных кубитов.
- Результат измеряется в одном заранее указанном кубите.

# Общий случай: передача нескольких кубитов

- Обозначение: $U[S]$ — оператор $U$, который действует на множестве кубитов $S$, а на остальных как единичный. Если $S$ — первые кубиты, то $U[S]|s,t\rangle = U|s\rangle \otimes |t\rangle$.

**Упражнение**

Напишите в вычислительном базисе матрицу оператора c-NOT$[1,3]$, который действует на трех кубитах. Оператор c-NOT — это оператор обратимого копирования: c-NOT$: |x,y\rangle \mapsto |x, x \oplus y\rangle$.

- Квантовый протокол — разбиение $\{1,2,\ldots,N\} = A \dot\cup B$; последовательность операторов $U_1[S_1]$, $U_2[S_2]$, …, $U_\ell[S_\ell]$, причем $S_1 \subseteq A$. В начале $A$ — $|0,x\rangle$; $B$ — $|0,y\rangle$.
- Множества $S_j$ определяют, какие кубиты пересылаются: чтобы Алиса могла подействовать на кубит, который у Боба, нужно этот кубит ей переслать, и наоборот.
- Длина протокола — количество пересланных кубитов.
- Результат измеряется в одном заранее указанном кубите.

# Общий случай: передача нескольких кубитов

- Обозначение: $U[S]$ — оператор $U$, который действует на множестве кубитов $S$, а на остальных как единичный. Если $S$ — первые кубиты, то $U[S]|s,t\rangle = U|s\rangle \otimes |t\rangle$.

**Упражнение**

Напишите в вычислительном базисе матрицу оператора c-NOT$[1,3]$, который действует на трех кубитах. Оператор c-NOT — это оператор обратимого копирования: c-NOT$: |x,y\rangle \mapsto |x, x \oplus y\rangle$.

- Квантовый протокол — разбиение $\{1,2,\ldots,N\} = A \dot\cup B$; последовательность операторов $U_1[S_1]$, $U_2[S_2]$, …, $U_\ell[S_\ell]$, причем $S_1 \subseteq A$. В начале $A$ — $|0,x\rangle$; $B$ — $|0,y\rangle$.
- Множества $S_j$ определяют, какие кубиты пересылаются: чтобы Алиса могла подействовать на кубит, который у Боба, нужно этот кубит ей переслать, и наоборот.
- Длина протокола — количество пересланных кубитов.
- Результат измеряется в одном заранее указанном кубите.

# Общий случай: передача нескольких кубитов

- Обозначение: $U[S]$ — оператор $U$, который действует на множестве кубитов $S$, а на остальных как единичный. Если $S$ — первые кубиты, то $U[S]|s,t\rangle = U|s\rangle \otimes |t\rangle$.

**Упражнение**

Напишите в вычислительном базисе матрицу оператора c-NOT$[1,3]$, который действует на трех кубитах. Оператор c-NOT — это оператор обратимого копирования: c-NOT$: |x,y\rangle \mapsto |x, x \oplus y\rangle$.

- Квантовый протокол — разбиение $\{1,2,\ldots,N\} = A \dot\cup B$; последовательность операторов $U_1[S_1]$, $U_2[S_2]$, …, $U_\ell[S_\ell]$, причем $S_1 \subseteq A$. В начале $A$ — $|0,x\rangle$; $B$ — $|0,y\rangle$.
- Множества $S_j$ определяют, какие кубиты пересылаются: чтобы Алиса могла подействовать на кубит, который у Боба, нужно этот кубит ей переслать, и наоборот.
- Длина протокола — количество пересланных кубитов.
- Результат измеряется в одном заранее указанном кубите.

# Общий случай: передача нескольких кубитов

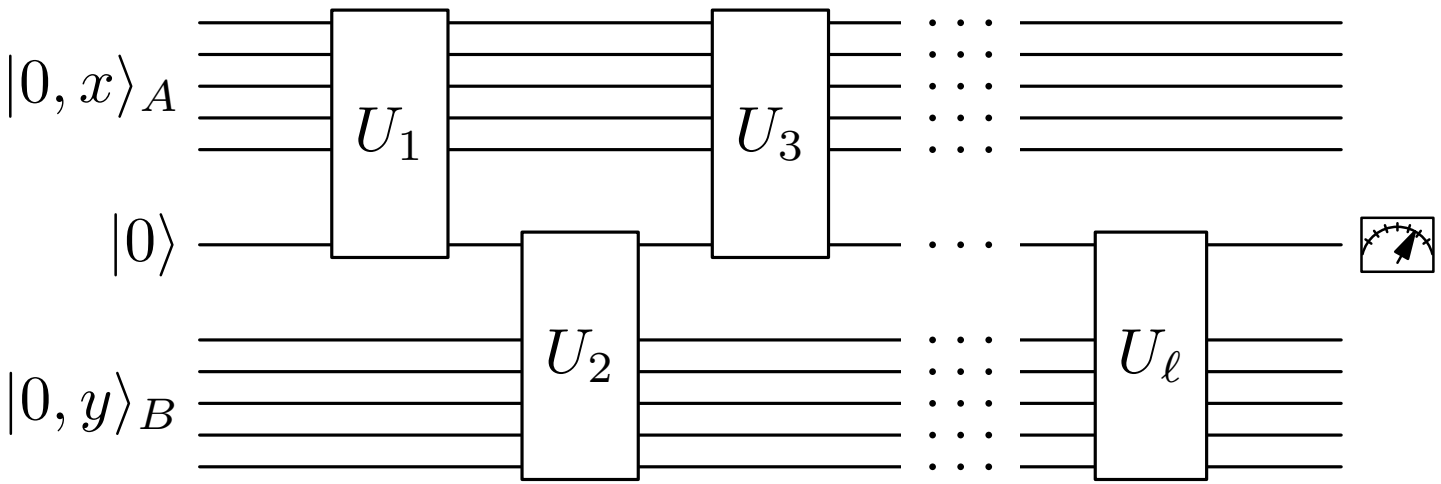
- Обозначение: $U[S]$ — оператор $U$, который действует на множестве кубитов $S$, а на остальных как единичный. Если $S$ — первые кубиты, то $U[S]|s,t\rangle = U|s\rangle \otimes |t\rangle$.

**Упражнение**

Напишите в вычислительном базисе матрицу оператора c-NOT$[1,3]$, который действует на трех кубитах. Оператор c-NOT — это оператор обратимого копирования: c-NOT$: |x,y\rangle \mapsto |x, x \oplus y\rangle$.

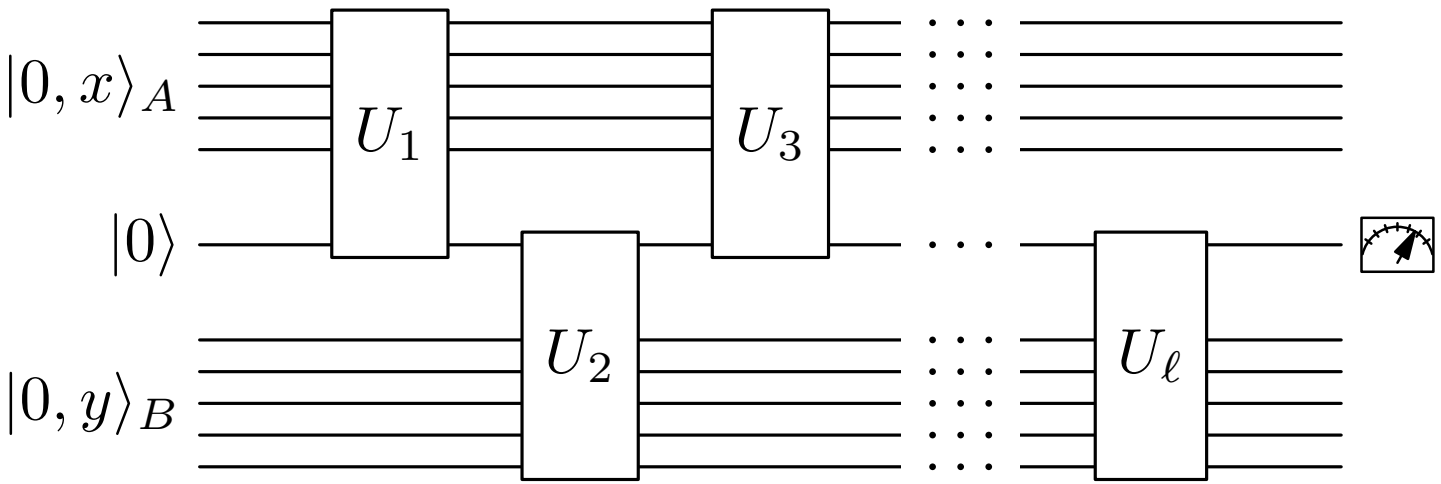
- Квантовый протокол — разбиение $\{1,2,\ldots,N\} = A \dot\cup B$; последовательность операторов $U_1[S_1]$, $U_2[S_2]$, …, $U_\ell[S_\ell]$, причем $S_1 \subseteq A$. В начале $A$ — $|0,x\rangle$; $B$ — $|0,y\rangle$.
- Множества $S_j$ определяют, какие кубиты пересылаются: чтобы Алиса могла подействовать на кубит, который у Боба, нужно этот кубит ей переслать, и наоборот.
- Длина протокола — количество пересланных кубитов.
- Результат измеряется в одном заранее указанном кубите.

# Квантовый коммуникационный протокол с передачей по одному кубиту



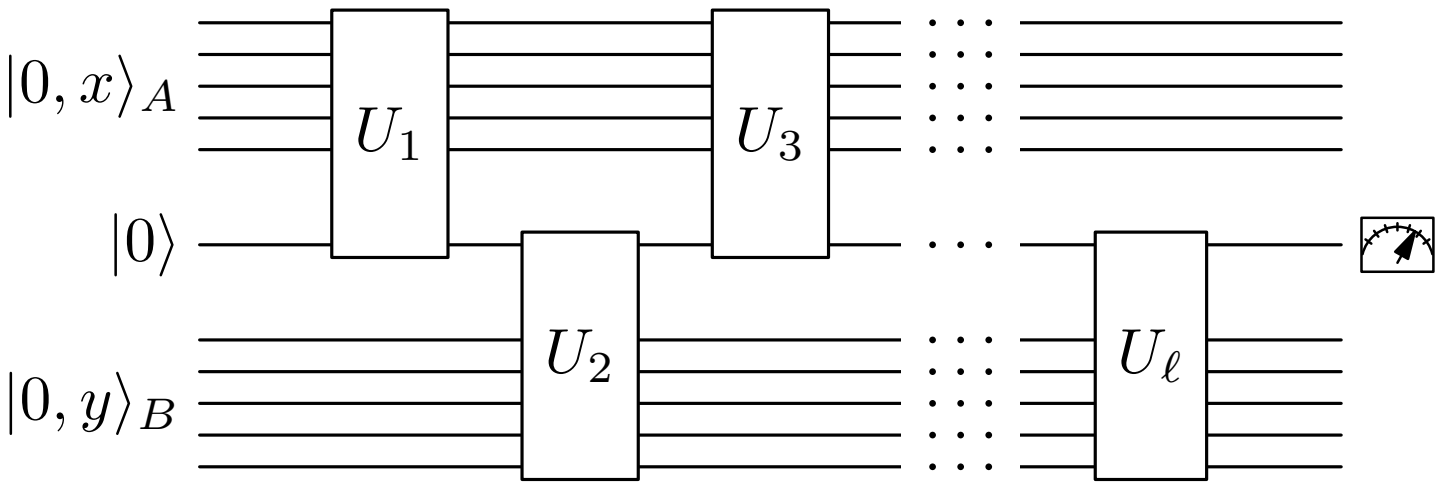

- Начальное состояние $|x,0\rangle_A \otimes |0\rangle \otimes |0,y\rangle_B$.
- $U_{2k+1}$ действует на кубиты Алисы и кубит сообщения.
- $U_{2k}$ действует на кубиты Боба и кубит сообщения.
- Результат определяется измерением кубита сообщения.
- Длина протокола $\ell$.

# Квантовый коммуникационный протокол с передачей по одному кубиту



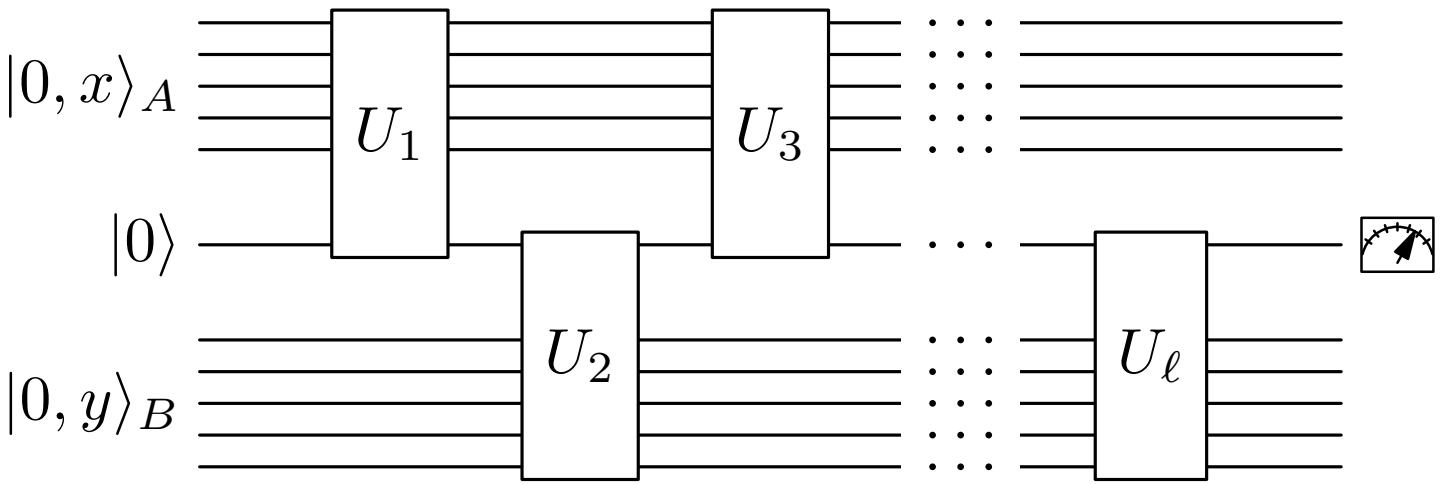

- Начальное состояние $|x,0\rangle_A \otimes |0\rangle \otimes |0,y\rangle_B$.
- $U_{2k+1}$ действует на кубиты Алисы и кубит сообщения.
- $U_{2k}$ действует на кубиты Боба и кубит сообщения.
- Результат определяется измерением кубита сообщения.
- Длина протокола $\ell$.

# Квантовый коммуникационный протокол с передачей по одному кубиту



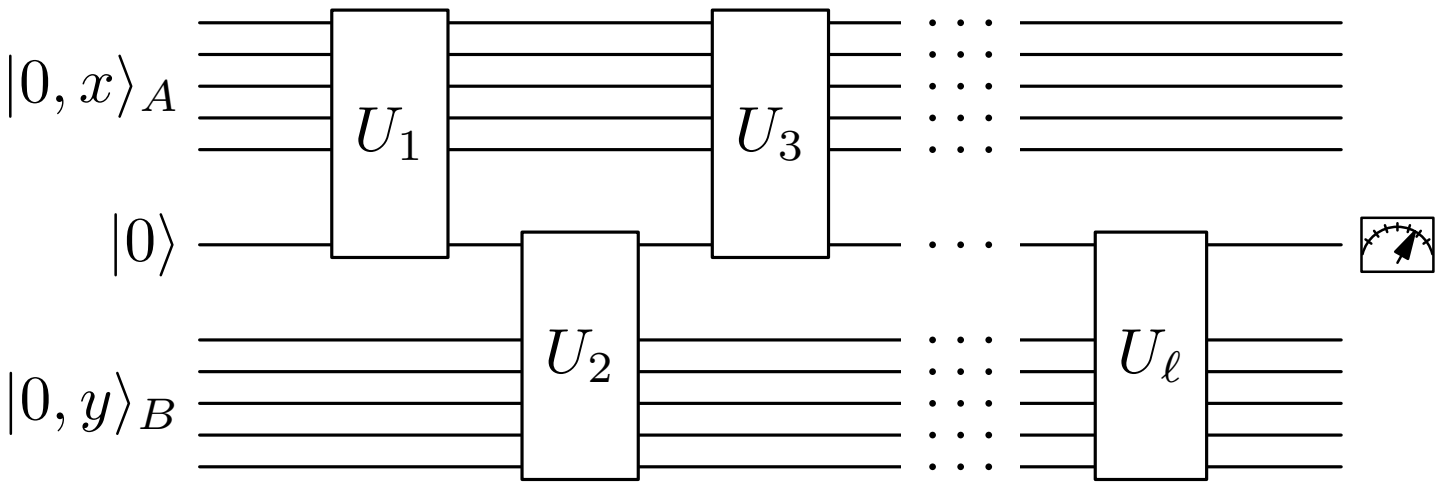

- Начальное состояние $|x,0\rangle_A \otimes |0\rangle \otimes |0,y\rangle_B$.
- $U_{2k+1}$ действует на кубиты Алисы и кубит сообщения.
- $U_{2k}$ действует на кубиты Боба и кубит сообщения.
- Результат определяется измерением кубита сообщения.
- Длина протокола $\ell$.

# Квантовый коммуникационный протокол с передачей по одному кубиту




- Начальное состояние $|x,0\rangle_A \otimes |0\rangle \otimes |0,y\rangle_B$.
- $U_{2k+1}$ действует на кубиты Алисы и кубит сообщения.
- $U_{2k}$ действует на кубиты Боба и кубит сообщения.
- Результат определяется измерением кубита сообщения.
- Длина протокола $\ell$.

# Квантовый коммуникационный протокол с передачей по одному кубиту




- Начальное состояние $|x,0\rangle_A \otimes |0\rangle \otimes |0,y\rangle_B$.
- $U_{2k+1}$ действует на кубиты Алисы и кубит сообщения.
- $U_{2k}$ действует на кубиты Боба и кубит сообщения.
- Результат определяется измерением кубита сообщения.
- Длина протокола $\ell$.

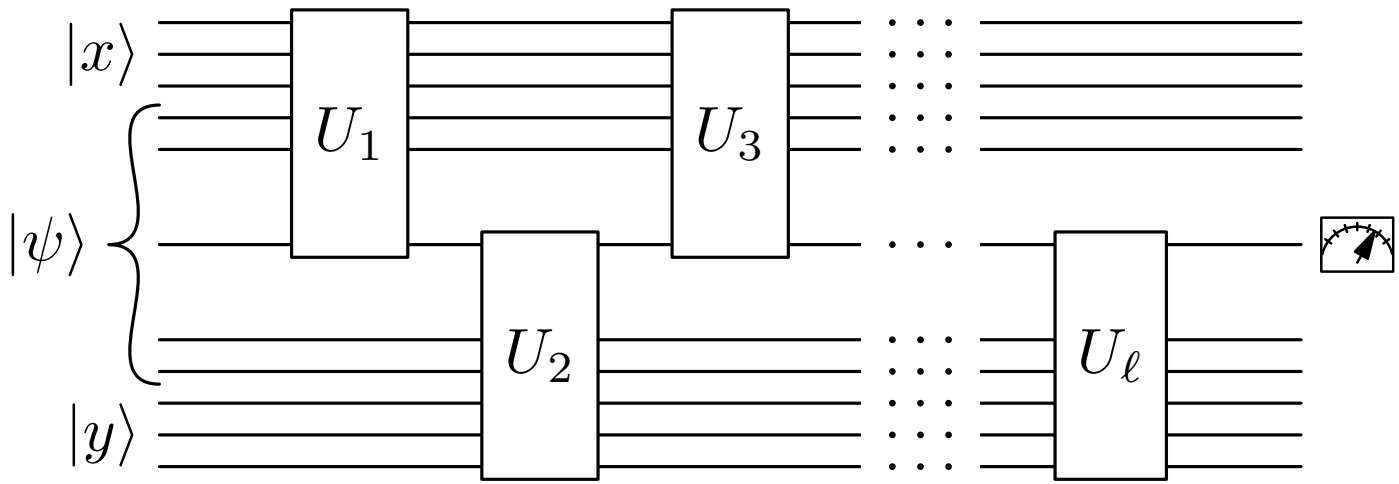
# Передача нескольких кубитов моделируется передачей одного и того же кубита

## Задача

Докажите, что общий протокол можно моделировать протоколом с передачей лишь одного кубита.

Указание: перестановка кубитов (тензорных сомножителей) — унитарный оператор.

# Квантовая коммуникация с предварительной сцепленностью




- Начальное состояние $|x\rangle \otimes |\psi\rangle \otimes |y\rangle$.
- Длина протокола $\ell$.
- Коммуникационная сложность с предварительной сцепленностью $Q_\varepsilon^{\mathrm{ent}}(f)$ — длина наименьшего протокола вычисления $f$.
- Обычно $|\psi\rangle = \left(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\right)^{\otimes m} \otimes |0\rangle$ (ЭПР-пары), где первый кубит в сомножителе идет Алисе, а второй — Бобу (последний — кубит сообщения).

# Соотношения между коммуникационными сложностями

## Упражнение

Докажите, что для любой $f$

$$Q_\varepsilon^{\mathrm{ent}}(f) \leqslant R_\varepsilon^{\mathrm{pub}}(f) \leqslant R_\varepsilon(f) \leqslant D(f) \leqslant n,$$
$$Q_\varepsilon^{\mathrm{ent}}(f) \leqslant Q_\varepsilon(f) \leqslant R_\varepsilon(f).$$

## Вопрос (открытый?)

Верно ли, что для любой $f$

$$Q_\varepsilon(f) \leqslant R_\varepsilon^{\mathrm{pub}}(f)?$$

(Неверно для модели одновременной передачи сообщений.)

## Открытая проблема

Возможен ли экспоненциальный разрыв между вероятностной и квантовой коммуникационными сложностями в основной модели?

# Соотношения между коммуникационными сложностями

## Упражнение

Докажите, что для любой $f$

$$Q_\varepsilon^{\mathrm{ent}}(f) \leqslant R_\varepsilon^{\mathrm{pub}}(f) \leqslant R_\varepsilon(f) \leqslant D(f) \leqslant n,$$
$$Q_\varepsilon^{\mathrm{ent}}(f) \leqslant Q_\varepsilon(f) \leqslant R_\varepsilon(f).$$

## Вопрос (открытый?)

Верно ли, что для любой $f$

$$Q_\varepsilon(f) \leqslant R_\varepsilon^{\mathrm{pub}}(f)?$$

(Неверно для модели одновременной передачи сообщений.)

## Открытая проблема

Возможен ли экспоненциальный разрыв между вероятностной и квантовой коммуникационными сложностями в основной модели?

# Соотношения между коммуникационными сложностями

## Упражнение

Докажите, что для любой $f$

$$Q_\varepsilon^{\mathrm{ent}}(f) \leqslant R_\varepsilon^{\mathrm{pub}}(f) \leqslant R_\varepsilon(f) \leqslant D(f) \leqslant n,$$
$$Q_\varepsilon^{\mathrm{ent}}(f) \leqslant Q_\varepsilon(f) \leqslant R_\varepsilon(f).$$

## Вопрос (открытый?)

Верно ли, что для любой $f$

$$Q_\varepsilon(f) \leqslant R_\varepsilon^{\mathrm{pub}}(f)?$$

(Неверно для модели одновременной передачи сообщений.)

## Открытая проблема

Возможен ли экспоненциальный разрыв между вероятностной и квантовой коммуникационными сложностями в основной модели?

# Соотношения между коммуникационными сложностями

## Упражнение

Докажите, что для любой $f$

$$Q_\varepsilon^{\mathrm{ent}}(f) \leqslant R_\varepsilon^{\mathrm{pub}}(f) \leqslant R_\varepsilon(f) \leqslant D(f) \leqslant n,$$
$$Q_\varepsilon^{\mathrm{ent}}(f) \leqslant Q_\varepsilon(f) \leqslant R_\varepsilon(f).$$

## Вопрос (открытый?)

Верно ли, что для любой $f$

$$Q_\varepsilon(f) \leqslant R_\varepsilon^{\mathrm{pub}}(f)?$$

(Неверно для модели одновременной передачи сообщений.)

## Открытая проблема

Возможен ли экспоненциальный разрыв между вероятностной и квантовой коммуникационными сложностями в основной модели?

# План

# Функция DISJ: квадратичный разрыв

**Определение**

$\mathrm{DISJ}(x, y) = 1 \quad \Leftrightarrow \quad x \cap y = \varnothing$ (т. е. $x_j y_j = 0$ для любого $j$).

**Теорема 1 (Razborov, '92)**

$R_\varepsilon(\mathrm{DISJ}) = \Omega(n)$.

**Теорема 3 (Razborov, '02)**

$Q_\varepsilon(\mathrm{DISJ}) = \Omega(\sqrt{n})$.

# Функция DISJ: квадратичный разрыв

**Определение**

$\mathrm{DISJ}(x, y) = 1 \quad \Leftrightarrow \quad x \cap y = \varnothing$ (т. е. $x_j y_j = 0$ для любого $j$).

**Теорема 1 (Razborov, '92)**

$R_\varepsilon(\mathrm{DISJ}) = \Omega(n)$.

**Теорема 3 (Razborov, '02)**

$Q_\varepsilon(\mathrm{DISJ}) = \Omega(\sqrt{n})$.

# Функция DISJ: квадратичный разрыв

**Определение**

$\mathrm{DISJ}(x, y) = 1 \quad \Leftrightarrow \quad x \cap y = \varnothing$ (т. е. $x_j y_j = 0$ для любого $j$).

**Теорема 1 (Razborov, '92)**

$R_\varepsilon(\mathrm{DISJ}) = \Omega(n)$.

**Теорема 2 (Buhrman, Cleve, Wigderson '98)**

$Q_\varepsilon(\mathrm{DISJ}) = O(\sqrt{n} \log n)$.

**Теорема 3 (Razborov, '02)**

$Q_\varepsilon(\mathrm{DISJ}) = \Omega(\sqrt{n})$.

# Функция DISJ: квадратичный разрыв

**Определение**

$\mathrm{DISJ}(x, y) = 1 \quad \Leftrightarrow \quad x \cap y = \varnothing$ (т. е. $x_j y_j = 0$ для любого $j$).

**Теорема 1 (Razborov, '92)**

$R_\varepsilon(\mathrm{DISJ}) = \Omega(n)$.

**Теорема 2′ (Aaronson, Ambainis '05)**

$Q_\varepsilon(\mathrm{DISJ}) = O(\sqrt{n})$.

**Теорема 3 (Razborov, '02)**

$Q_\varepsilon(\mathrm{DISJ}) = \Omega(\sqrt{n})$.

# Функция DISJ: квадратичный разрыв

**Определение**

$\mathrm{DISJ}(x, y) = 1 \quad \Leftrightarrow \quad x \cap y = \varnothing$ (т. е. $x_j y_j = 0$ для любого $j$).

**Теорема 1 (Razborov, '92)**

$R_\varepsilon(\mathrm{DISJ}) = \Omega(n)$.

**Теорема 2′ (Aaronson, Ambainis '05)**

$Q_\varepsilon(\mathrm{DISJ}) = O(\sqrt{n})$.

**Теорема 3 (Razborov, '02)**

$Q_\varepsilon(\mathrm{DISJ}) = \Omega(\sqrt{n})$.

# Квантовый коммуникационный протокол для DISJ

Идея: использовать алгоритм Гровера.

- Алиса выполняет шаги алгоритма вычисления дизъюнкции $\bigvee_{x_j=1} y_j$.
- Вместо запроса к «черному ящику» она общается с Бобом:
  1. Алиса посылает регистр адреса Бобу;
  2. Боб применяет оператор фазового запроса $Q_{y_1,\ldots,y_n} : |k\rangle \mapsto (-1)^{y_k}|k\rangle$ и возвращает регистр Алисе.
- Моделирование одного запроса требует передачи $O(\log n)$ кубитов.
- Всего запросов нужно $O(\sqrt{n})$.
- Теорема 2 доказана.

# Квантовый коммуникационный протокол для DISJ

Идея: использовать алгоритм Гровера.

- Алиса выполняет шаги алгоритма вычисления дизъюнкции $\bigvee_{x_j=1} y_j$.
- Вместо запроса к «черному ящику» она общается с Бобом:
  1. Алиса посылает регистр адреса Бобу;
  2. Боб применяет оператор фазового запроса $O_y : |k\rangle \mapsto (-1)^{y_k}|k\rangle$ и возвращает регистр Алисе.
- Моделирование одного запроса требует передачи $O(\log n)$ кубитов.
- Всего запросов нужно $O(\sqrt{n})$.
- Теорема 2 доказана.

# Квантовый коммуникационный протокол для DISJ

Идея: использовать алгоритм Гровера.

- Алиса выполняет шаги алгоритма вычисления дизъюнкции $\bigvee_{x_j=1} y_j$.
- Вместо запроса к «черному ящику» она общается с Бобом:
  1. Алиса посылает регистр адреса Бобу;
  2. Боб применяет оператор фазового запроса $O_y : |k\rangle \mapsto (-1)^{y_k}|k\rangle$ и возвращает регистр Алисе.
- Моделирование одного запроса требует передачи $O(\log n)$ кубитов.
- Всего запросов нужно $O(\sqrt{n})$.
- Теорема 2 доказана.

# Квантовый коммуникационный протокол для DISJ

Идея: использовать алгоритм Гровера.

- Алиса выполняет шаги алгоритма вычисления дизъюнкции $\bigvee_{x_j=1} y_j$.
- Вместо запроса к «черному ящику» она общается с Бобом:
  1. Алиса посылает регистр адреса Бобу;
  2. Боб применяет оператор фазового запроса $O_y : |k\rangle \mapsto (-1)^{y_k}|k\rangle$ и возвращает регистр Алисе.
- Моделирование одного запроса требует передачи $O(\log n)$ кубитов.
- Всего запросов нужно $O(\sqrt{n})$.
- Теорема 2 доказана.

# Квантовый коммуникационный протокол для DISJ

Идея: использовать алгоритм Гровера.

- Алиса выполняет шаги алгоритма вычисления дизъюнкции $\bigvee_{x_j=1} y_j$.
- Вместо запроса к «черному ящику» она общается с Бобом:
  1. Алиса посылает регистр адреса Бобу;
  2. Боб применяет оператор фазового запроса $O_y : |k\rangle \mapsto (-1)^{y_k}|k\rangle$ и возвращает регистр Алисе.
- Моделирование одного запроса требует передачи $O(\log n)$ кубитов.
- Всего запросов нужно $O(\sqrt{n})$.
- Теорема 2 доказана.

# Квантовый коммуникационный протокол для DISJ

Идея: использовать алгоритм Гровера.

- Алиса выполняет шаги алгоритма вычисления дизъюнкции $\bigvee_{x_j=1} y_j$.
- Вместо запроса к «черному ящику» она общается с Бобом:
  1. Алиса посылает регистр адреса Бобу;
  2. Боб применяет оператор фазового запроса $O_y : |k\rangle \mapsto (-1)^{y_k}|k\rangle$ и возвращает регистр Алисе.
- Моделирование одного запроса требует передачи $O(\log n)$ кубитов.
- Всего запросов нужно $O(\sqrt{n})$.
- Теорема 2 доказана.

# Квантовый коммуникационный протокол для DISJ

Идея: использовать алгоритм Гровера.

- Алиса выполняет шаги алгоритма вычисления дизъюнкции $\bigvee_{x_j=1} y_j$.
- Вместо запроса к «черному ящику» она общается с Бобом:
  1. Алиса посылает регистр адреса Бобу;
  2. Боб применяет оператор фазового запроса $O_y : |k\rangle \mapsto (-1)^{y_k}|k\rangle$ и возвращает регистр Алисе.
- Моделирование одного запроса требует передачи $O(\log n)$ кубитов.
- Всего запросов нужно $O(\sqrt{n})$.
- Теорема 2 доказана.