

Квантовые алгоритмы:
возможности и ограничения.
Лекция 5: Нижние оценки квантовой
коммуникационной сложности. Другие модели
коммуникации

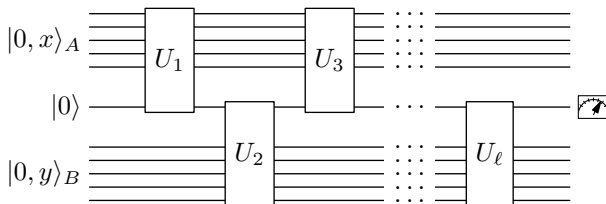
М. Вялый

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

Санкт-Петербург, 2011

- 1 Нижние оценки квантовой коммуникационной сложности
- 2 Нижняя оценка для функции пересечения множеств
- 3 Модель коммуникации SMP
- 4 Квантовая (псевдо-)телепатия

Разложение Яо – Кремера



Теорема

Состояние квантовой памяти после ℓ раундов общения с передачей по одному кубиту представляется в виде

$$|\psi\rangle = \sum_{m \in \{0,1\}^\ell} |\alpha_m\rangle_A \otimes |m_\ell\rangle \otimes |\beta_m\rangle_B,$$

где $|\alpha_m| \leq 1$, $|\beta_m| \leq 1$, а m_ℓ — последний бит двоичной строки m .

Разложение Яо – Кремера: доказательство

Индукция по длине протокола.

Начальное состояние $|x, 0\rangle_A \otimes |0\rangle \otimes |0, y\rangle_B$ разложимо.

Пусть после ℓ раундов состояние имеет вид

$$|\psi\rangle = \sum_{m \in \{0,1\}^\ell} |\alpha_m\rangle_A \otimes |m_\ell\rangle \otimes |\beta_m\rangle_B.$$

Рассмотрим случай четного ℓ (следующий ход Алисы). Получаем:

$$U_{\ell+1} |\alpha_m\rangle_A \otimes |m_\ell\rangle = |\alpha'_{m0}\rangle \otimes |0\rangle + |\alpha'_{m1}\rangle \otimes |1\rangle,$$

$$|\alpha'_{m0}\rangle^2 + |\alpha'_{m1}\rangle^2 = |\alpha_m|^2 \leq 1,$$

$$U_{\ell+1} |\psi\rangle = \sum_{m \in \{0,1\}^{\ell+1}} |\alpha'_m\rangle_A \otimes |m_\ell\rangle \otimes |\beta'_m\rangle_B,$$

$$\text{где } |\beta'_{m0}\rangle = |\beta'_{m1}\rangle = |\beta_m\rangle.$$

Разложение Яо – Кремера: доказательство

Индукция по длине протокола.

Начальное состояние $|x, 0\rangle_A \otimes |0\rangle \otimes |0, y\rangle_B$ разложимо.

Пусть после ℓ раундов состояние имеет вид

$$|\psi\rangle = \sum_{m \in \{0,1\}^\ell} |\alpha_m\rangle_A \otimes |m_\ell\rangle \otimes |\beta_m\rangle_B.$$

Рассмотрим случай четного ℓ (следующий ход Алисы). Получаем:

$$U_{\ell+1}|\alpha_m\rangle_A \otimes |m_\ell\rangle = |\alpha'_{m0}\rangle \otimes |0\rangle + |\alpha'_{m1}\rangle \otimes |1\rangle,$$

$$|\alpha'_{m0}|^2 + |\alpha'_{m1}|^2 = |\alpha_m|^2 \leq 1,$$

$$U_{\ell+1}|\psi\rangle = \sum_{m \in \{0,1\}^{\ell+1}} |\alpha'_m\rangle_A \otimes |m_\ell\rangle \otimes |\beta'_m\rangle_B,$$

$$\text{где } |\beta'_{m0}\rangle = |\beta'_{m1}\rangle = |\beta_m\rangle.$$

Разложение Яо – Кремера: доказательство

Индукция по длине протокола.

Начальное состояние $|x, 0\rangle_A \otimes |0\rangle \otimes |0, y\rangle_B$ разложимо.

Пусть после ℓ раундов состояние имеет вид

$$|\psi\rangle = \sum_{m \in \{0,1\}^\ell} |\alpha_m\rangle_A \otimes |m_\ell\rangle \otimes |\beta_m\rangle_B.$$

Рассмотрим случай четного ℓ (следующий ход Алисы). Получаем:

$$U_{\ell+1} |\alpha_m\rangle_A \otimes |m_\ell\rangle = |\alpha'_{m0}\rangle \otimes |0\rangle + |\alpha'_{m1}\rangle \otimes |1\rangle,$$

$$|\alpha'_{m0}|^2 + |\alpha'_{m1}|^2 = |\alpha_m|^2 \leq 1,$$

$$U_{\ell+1} |\psi\rangle = \sum_{m \in \{0,1\}^{\ell+1}} |\alpha'_m\rangle_A \otimes |m_\ell\rangle \otimes |\beta'_m\rangle_B,$$

$$\text{где } |\beta'_{m0}\rangle = |\beta'_{m1}\rangle = |\beta_m\rangle.$$

Разложение Яо – Кремера: доказательство

Индукция по длине протокола.

Начальное состояние $|x, 0\rangle_A \otimes |0\rangle \otimes |0, y\rangle_B$ разложимо.

Пусть после ℓ раундов состояние имеет вид

$$|\psi\rangle = \sum_{m \in \{0,1\}^\ell} |\alpha_m\rangle_A \otimes |m_\ell\rangle \otimes |\beta_m\rangle_B.$$

Рассмотрим случай четного ℓ (следующий ход Алисы). Получаем:

$$U_{\ell+1} |\alpha_m\rangle_A \otimes |m_\ell\rangle = |\alpha'_{m0}\rangle \otimes |0\rangle + |\alpha'_{m1}\rangle \otimes |1\rangle,$$

$$|\alpha'_{m0}|^2 + |\alpha'_{m1}|^2 = |\alpha_m|^2 \leq 1,$$

$$U_{\ell+1} |\psi\rangle = \sum_{m \in \{0,1\}^{\ell+1}} |\alpha'_m\rangle_A \otimes |m_\ell\rangle \otimes |\beta'_m\rangle_B,$$

$$\text{где } |\beta'_{m0}\rangle = |\beta'_{m1}\rangle = |\beta_m\rangle.$$

Разложение Яо – Кремера: доказательство

Индукция по длине протокола.

Начальное состояние $|x, 0\rangle_A \otimes |0\rangle \otimes |0, y\rangle_B$ разложимо.

Пусть после ℓ раундов состояние имеет вид

$$|\psi\rangle = \sum_{m \in \{0,1\}^\ell} |\alpha_m\rangle_A \otimes |m_\ell\rangle \otimes |\beta_m\rangle_B.$$

Рассмотрим случай четного ℓ (следующий ход Алисы). Получаем:

$$U_{\ell+1}|\alpha_m\rangle_A \otimes |m_\ell\rangle = |\alpha'_{m0}\rangle \otimes |0\rangle + |\alpha'_{m1}\rangle \otimes |1\rangle,$$

$$|\alpha'_{m0}|^2 + |\alpha'_{m1}|^2 = |\alpha_m|^2 \leq 1,$$

$$U_{\ell+1}|\psi\rangle = \sum_{m \in \{0,1\}^{\ell+1}} |\alpha'_m\rangle_A \otimes |m_\ell\rangle \otimes |\beta'_m\rangle_B,$$

$$\text{где } |\beta'_{m0}\rangle = |\beta'_{m1}\rangle = |\beta_m\rangle.$$

Разложение Яо – Кремера: доказательство

Индукция по длине протокола.

Начальное состояние $|x, 0\rangle_A \otimes |0\rangle \otimes |0, y\rangle_B$ разложимо.

Пусть после ℓ раундов состояние имеет вид

$$|\psi\rangle = \sum_{m \in \{0,1\}^\ell} |\alpha_m\rangle_A \otimes |m_\ell\rangle \otimes |\beta_m\rangle_B.$$

Рассмотрим случай четного ℓ (следующий ход Алисы). Получаем:

$$U_{\ell+1}|\alpha_m\rangle_A \otimes |m_\ell\rangle = |\alpha'_{m0}\rangle \otimes |0\rangle + |\alpha'_{m1}\rangle \otimes |1\rangle,$$

$$|\alpha'_{m0}|^2 + |\alpha'_{m1}|^2 = |\alpha_m|^2 \leq 1,$$

$$U_{\ell+1}|\psi\rangle = \sum_{m \in \{0,1\}^{\ell+1}} |\alpha'_m\rangle_A \otimes |m_\ell\rangle \otimes |\beta'_m\rangle_B,$$

$$\text{где } |\beta'_{m0}\rangle = |\beta'_{m1}\rangle = |\beta_m\rangle.$$

Разложение Яо – Кремера: доказательство

Индукция по длине протокола.

Начальное состояние $|x, 0\rangle_A \otimes |0\rangle \otimes |0, y\rangle_B$ разложимо.

Пусть после ℓ раундов состояние имеет вид

$$|\psi\rangle = \sum_{m \in \{0,1\}^\ell} |\alpha_m\rangle_A \otimes |m_\ell\rangle \otimes |\beta_m\rangle_B.$$

Рассмотрим случай четного ℓ (следующий ход Алисы). Получаем:

$$U_{\ell+1}|\alpha_m\rangle_A \otimes |m_\ell\rangle = |\alpha'_{m0}\rangle \otimes |0\rangle + |\alpha'_{m1}\rangle \otimes |1\rangle,$$

$$|\alpha'_{m0}|^2 + |\alpha'_{m1}|^2 = |\alpha_m|^2 \leq 1,$$

$$U_{\ell+1}|\psi\rangle = \sum_{m \in \{0,1\}^{\ell+1}} |\alpha'_m\rangle_A \otimes |m_\ell\rangle \otimes |\beta'_m\rangle_B,$$

$$\text{где } |\beta'_{m0}\rangle = |\beta'_{m1}\rangle = |\beta_m\rangle.$$

Разложение Яо – Кремера: доказательство

Индукция по длине протокола.

Начальное состояние $|x, 0\rangle_A \otimes |0\rangle \otimes |0, y\rangle_B$ разложимо.

Пусть после ℓ раундов состояние имеет вид

$$|\psi\rangle = \sum_{m \in \{0,1\}^\ell} |\alpha_m\rangle_A \otimes |m_\ell\rangle \otimes |\beta_m\rangle_B.$$

Рассмотрим случай четного ℓ (следующий ход Алисы). Получаем:

$$U_{\ell+1}|\alpha_m\rangle_A \otimes |m_\ell\rangle = |\alpha'_{m0}\rangle \otimes |0\rangle + |\alpha'_{m1}\rangle \otimes |1\rangle,$$

$$|\alpha'_{m0}|^2 + |\alpha'_{m1}|^2 = |\alpha_m|^2 \leq 1,$$

$$U_{\ell+1}|\psi\rangle = \sum_{m \in \{0,1\}^{\ell+1}} |\alpha'_m\rangle_A \otimes |m_\ell\rangle \otimes |\beta'_m\rangle_B,$$

$$\text{где } |\beta'_{m0}\rangle = |\beta'_{m1}\rangle = |\beta_m\rangle.$$

Матрица положительных ответов

p_{xy} — вероятность ответа 1 на входе x, y ; $x \in X, y \in Y$.

Лемма

Для протокола длины ℓ выполняется

$$p_{xy} = \sum_{k=0}^{2^{2\ell-2}-1} a_{x,k} \cdot b_{y,k}, \quad |a_{x,k}| \leq 1, \quad |b_{y,k}| \leq 1.$$

Доказательство

Из (*) вероятность наблюдения исхода 1

$$p_{xy} = \sum_{m', m''} \langle \alpha_{m'1} | \alpha_{m''1} \rangle \cdot \langle \beta_{m'1} | \beta_{m''1} \rangle$$

Матрица положительных ответов

p_{xy} — вероятность ответа 1 на входе x, y ; $x \in X, y \in Y$.

$P = (p_{xy})$ — матрица положительных ответов.

Лемма

Для протокола длины ℓ выполняется

$$p_{xy} = \sum_{k=0}^{2^{2\ell-2}-1} a_{x,k} \cdot b_{y,k}, \quad |a_{x,k}| \leq 1, \quad |b_{x,k}| \leq 1.$$

Доказательство

Из (*) вероятность наблюдения исхода 1

$$p_{xy} = \sum_{m', m''} \langle \alpha_{m'1} | \alpha_{m''1} \rangle \cdot \langle \beta_{m'1} | \beta_{m''1} \rangle$$

Матрица положительных ответов

p_{xy} — вероятность ответа 1 на входе x, y ; $x \in X, y \in Y$.

$P = (p_{xy})$ — матрица положительных ответов.

Лемма

Для протокола длины ℓ выполняется

$$p_{xy} = \sum_{k=0}^{2^{2\ell}-1} a_{x,k} \cdot b_{y,k}, \quad |a_{x,k}| \leq 1, \quad |b_{x,k}| \leq 1.$$

Доказательство

Из (*) вероятность наблюдения исхода 1

$$p_{xy} = \sum_{m', m''} \langle \alpha_{m'1} | \alpha_{m''1} \rangle \cdot \langle \beta_{m'1} | \beta_{m''1} \rangle$$

Матрица положительных ответов

$$\begin{aligned} \text{Разложение Яо – Кремера} \quad |\psi\rangle &= \sum_{m \in \{0,1\}^\ell} |\alpha_m\rangle_A \otimes |m_\ell\rangle \otimes |\beta_m\rangle_B = \\ &= \sum_{m \in \{0,1\}^{\ell-1}} |\alpha_{m0}\rangle_A \otimes |0\rangle \otimes |\beta_{m0}\rangle_B + \sum_{m \in \{0,1\}^{\ell-1}} |\alpha_{m1}\rangle_A \otimes |1\rangle \otimes |\beta_{m1}\rangle_B \quad (*) \end{aligned}$$

Лемма

Для протокола длины ℓ выполняется

$$p_{xy} = \sum_{k=0}^{2^{2\ell-2}-1} a_{x,k} \cdot b_{y,k}, \quad |a_{x,k}| \leq 1, \quad |b_{x,k}| \leq 1.$$

Доказательство

Из (*) вероятность наблюдения исхода 1

$$p_{xy} = \sum_{m', m''} \langle \alpha_{m'1} | \alpha_{m''1} \rangle \cdot \langle \beta_{m'1} | \beta_{m''1} \rangle$$

- Скалярное произведение операторов (произведение Фробениуса):

$$\langle A, B \rangle = \text{Tr}(A^\dagger B)$$

- Норма Фробениуса

$$\|A\|_F = \sqrt{\langle A, A \rangle}$$

- Операторная норма

$$\|A\| = \max_{x: |x|=1} |Ax|$$

- Следовая норма

$$\|A\|_{\text{tr}} = \max_{\|X\|=1} |\langle A, X \rangle|$$

Утверждение

Норма Фробениуса, операторная норма и следовая норма удовлетворяют свойствам нормы:

(1) $\|x\| \geq 0$; (2) $\|\lambda x\| = |\lambda| \cdot \|x\|$; (3) $\|x + y\| \leq \|x\| + \|y\|$.

Матричные нормы

- Скалярное произведение операторов (произведение Фробениуса):

$$\langle A, B \rangle = \text{Tr}(A^\dagger B)$$

- Норма Фробениуса

$$\|A\|_F = \sqrt{\langle A, A \rangle}$$

- Операторная норма

$$\|A\| = \max_{x: |x|=1} |Ax|$$

- Следовая норма

$$\|A\|_{\text{tr}} = \max_{\|X\|=1} |\langle A, X \rangle|$$

Утверждение

Норма Фробениуса, операторная норма и следовая норма удовлетворяют свойствам нормы:

(1) $\|x\| \geq 0$; (2) $\|\lambda x\| = |\lambda| \cdot \|x\|$; (3) $\|x + y\| \leq \|x\| + \|y\|$.

Матричные нормы

- Скалярное произведение операторов (произведение Фробениуса):

$$\langle A, B \rangle = \text{Tr}(A^\dagger B)$$

- Норма Фробениуса

$$\|A\|_F = \sqrt{\langle A, A \rangle}$$

- Операторная норма

$$\|A\| = \max_{x: |x|=1} |Ax|$$

- Следовая норма

$$\|A\|_{\text{tr}} = \max_{\|X\|=1} |\langle A, X \rangle|$$

Утверждение

Норма Фробениуса, операторная норма и следовая норма удовлетворяют свойствам нормы:

(1) $\|x\| \geq 0$; (2) $\|\lambda x\| = |\lambda| \cdot \|x\|$; (3) $\|x + y\| \leq \|x\| + \|y\|$.

Матричные нормы

- Скалярное произведение операторов (произведение Фробениуса):

$$\langle A, B \rangle = \text{Tr}(A^\dagger B)$$

- Норма Фробениуса

$$\|A\|_F = \sqrt{\langle A, A \rangle}$$

- Операторная норма

$$\|A\| = \max_{x: |x|=1} |Ax|$$

- Следовая норма

$$\|A\|_{\text{tr}} = \max_{\|X\|=1} |\langle A, X \rangle|$$

Утверждение

Норма Фробениуса, операторная норма и следовая норма удовлетворяют свойствам нормы:

(1) $\|x\| \geq 0$; (2) $\|\lambda x\| = |\lambda| \cdot \|x\|$; (3) $\|x + y\| \leq \|x\| + \|y\|$.

Матричные нормы

- Скалярное произведение операторов (произведение Фробениуса):

$$\langle A, B \rangle = \text{Tr}(A^\dagger B)$$

- Норма Фробениуса

$$\|A\|_F = \sqrt{\langle A, A \rangle}$$

- Операторная норма

$$\|A\| = \max_{x: |x|=1} |Ax|$$

- Следовая норма

$$\|A\|_{\text{tr}} = \max_{\|X\|=1} |\langle A, X \rangle|$$

Утверждение

Норма Фробениуса, операторная норма и следовая норма удовлетворяют свойствам нормы:

(1) $\|x\| \geq 0$; (2) $\|\lambda x\| = |\lambda| \cdot \|x\|$; (3) $\|x + y\| \leq \|x\| + \|y\|$.

Теорема о сингулярном разложении

Теорема

Любой оператор представляется в виде

$$A = \sum_{k=1}^r s_k |\xi_k\rangle \langle \psi_k| \quad \text{или для матриц} \quad A = UDV,$$

где $\{\xi_k\}$, $\{\psi_k\}$ — ортонормированные системы векторов,

$s_k \geq 0$ — сингулярные числа, r — ранг оператора,

U , V — унитарные, D — неотрицательная диагональная.

Утверждение

Для любого оператора A оператор $A^\dagger A$ — эрмитов.

Упражнение

Выведите теорему о сингулярном разложении из утверждения и теоремы о существовании для эрмитова оператора ортонормированного базиса из собственных векторов.

Теорема о сингулярном разложении

Теорема

Любой оператор представляется в виде

$$A = \sum_{k=1}^r s_k |\xi_k\rangle \langle \psi_k| \quad \text{или для матриц} \quad A = UDV,$$

где $\{\xi_k\}$, $\{\psi_k\}$ — ортонормированные системы векторов,
 $s_k \geq 0$ — **сингулярные числа**, r — **ранг** оператора,
 U , V — унитарные, D — неотрицательная диагональная.

Утверждение

Для любого оператора A оператор $A^\dagger A$ — эрмитов.

Упражнение

Выведите теорему о сингулярном разложении из утверждения и теоремы о существовании для эрмитова оператора ортонормированного базиса из собственных векторов.

Теорема о сингулярном разложении

Теорема

Любой оператор представляется в виде

$$A = \sum_{k=1}^r s_k |\xi_k\rangle \langle \psi_k| \quad \text{или для матриц} \quad A = UDV,$$

где $\{\xi_k\}$, $\{\psi_k\}$ — ортонормированные системы векторов,
 $s_k \geq 0$ — **сингулярные числа**, r — **ранг** оператора,
 U , V — унитарные, D — неотрицательная диагональная.

Утверждение

Для любого оператора A оператор $A^\dagger A$ — эрмитов.

Упражнение

Выведите теорему о сингулярном разложении из утверждения и теоремы о существовании для эрмитова оператора ортонормированного базиса из собственных векторов.

Утверждение

$$\|A\|_{\text{tr}} = \sum_k s_k.$$

Доказательство

Пусть $A = UDV = \sum_{k=1}^r s_k |\xi_k\rangle\langle\psi_k|$. Тогда

$$\langle A, UV \rangle = \text{Tr}(A^\dagger UV) = \text{Tr}(V^\dagger D U^\dagger UV) = \text{Tr}(D) = \sum_k s_k.$$

С другой стороны,

$$\begin{aligned} \langle A, A \rangle &= \sum_k s_k \langle \text{Tr}(|\xi_k\rangle\langle\psi_k|), s_k |\xi_k\rangle\langle\psi_k| \rangle = \sum_k s_k^2 \langle \text{Tr}(|\xi_k\rangle\langle\psi_k|), |\xi_k\rangle\langle\psi_k| \rangle = \\ &= \sum_k s_k^2 \langle \langle \xi_k | \xi_k \rangle, \langle \psi_k | \psi_k \rangle \rangle = \sum_k s_k^2 \langle 1, 1 \rangle = \sum_k s_k^2. \end{aligned}$$

Утверждение

$$\|A\|_{\text{tr}} = \sum_k s_k.$$

Доказательство

Пусть $A = UDV = \sum_{k=1}^r s_k |\xi_k\rangle\langle\psi_k|$. Тогда

$$\langle A, UV \rangle = \text{Tr}(A^\dagger UV) = \text{Tr}(V^\dagger D U^\dagger UV) = \text{Tr}(D) = \sum_k s_k.$$

С другой стороны,

$$\begin{aligned} |\text{Tr}(A^\dagger X)| &\leq \sum_k s_k |\text{Tr}(|\psi_k\rangle\langle\xi_k| X)| = \sum_k s_k |\text{Tr}(\langle\xi_k| X |\psi_k\rangle)| = \\ &= \sum_k s_k |\langle\xi_k| X |\psi_k\rangle| \leq \sum_k s_k |X|\psi_k\rangle| \leq \|X\| \sum_k s_k. \end{aligned}$$

Утверждение

$$\|A\|_{\text{tr}} = \sum_k s_k.$$

Доказательство

Пусть $A = UDV = \sum_{k=1}^r s_k |\xi_k\rangle\langle\psi_k|$. Тогда

$$\langle A, UV \rangle = \text{Tr}(A^\dagger UV) = \text{Tr}(V^\dagger DU^\dagger UV) = \text{Tr}(D) = \sum_k s_k.$$

С другой стороны,

$$\begin{aligned} |\text{Tr}(A^\dagger X)| &\leq \sum_k s_k |\text{Tr}(|\psi_k\rangle\langle\xi_k|X)| = \sum_k s_k |\text{Tr}(\langle\xi_k|X|\psi_k\rangle)| = \\ &= \sum_k s_k |\langle\xi_k|X|\psi_k\rangle| \leq \sum_k s_k |X|\psi_k\rangle| \leq \|X\| \sum_k s_k. \end{aligned}$$

Утверждение

$$\|A\|_{\text{tr}} = \sum_k s_k.$$

Доказательство

Пусть $A = UDV = \sum_{k=1}^r s_k |\xi_k\rangle\langle\psi_k|$. Тогда

$$\langle A, UV \rangle = \text{Tr}(A^\dagger UV) = \text{Tr}(V^\dagger DU^\dagger UV) = \text{Tr}(D) = \sum_k s_k.$$

С другой стороны,

$$\begin{aligned} |\text{Tr}(A^\dagger X)| &\leq \sum_k s_k |\text{Tr}(|\psi_k\rangle\langle\xi_k|X)| = \sum_k s_k |\text{Tr}(\langle\xi_k|X|\psi_k\rangle)| = \\ &= \sum_k s_k |\langle\xi_k|X|\psi_k\rangle| \leq \sum_k s_k |X|\psi_k\rangle| \leq \|X\| \sum_k s_k. \end{aligned}$$

Оценка следовой нормы матрицы P

Лемма

$$\|P\|_{\text{tr}} \leq 2^{2\ell-2} \sqrt{|X| \cdot |Y|}.$$

Доказательство

Из предыдущей леммы

$$p_{xy} = \sum_{k=0}^{2^{2\ell-2}-1} a_{x,k} \cdot b_{y,k}, \quad |a_{x,k}| \leq 1, \quad |b_{y,k}| \leq 1.$$

Рассмотрим $a_x = (a_{x,k})$, $b_y = (b_{y,k})$. Тогда $P = \sum_{x,y} |a_x\rangle\langle b_y|$.

Оценка следовой нормы матрицы P

Лемма

$$\|P\|_{\text{tr}} \leq 2^{2\ell-2} \sqrt{|X| \cdot |Y|}.$$

Доказательство

Из предыдущей леммы

$$p_{xy} = \sum_{k=0}^{2^{2\ell-2}-1} a_{x,k} \cdot b_{y,k}, \quad |a_{x,k}| \leq 1, \quad |b_{x,k}| \leq 1.$$

Введем векторы $\mathbf{a}_k = (a_{x,k})$, $\mathbf{b}_k = (b_{y,k}^*)$. Тогда $P = \sum_k |\mathbf{a}_k\rangle\langle\mathbf{b}_k|$ и

$$\|P\|_{\text{tr}}$$

Оценка следовой нормы матрицы P

Лемма

$$\|P\|_{\text{tr}} \leq 2^{2\ell-2} \sqrt{|X| \cdot |Y|}.$$

Доказательство

Из предыдущей леммы

$$p_{xy} = \sum_{k=0}^{2^{2\ell-2}-1} a_{x,k} \cdot b_{y,k}, \quad |a_{x,k}| \leq 1, \quad |b_{x,k}| \leq 1.$$

Введем векторы $\mathbf{a}_k = (a_{x,k})$, $\mathbf{b}_k = (b_{y,k}^*)$. Тогда $P = \sum_k |\mathbf{a}_k\rangle\langle\mathbf{b}_k|$ и

$$\|P\|_{\text{tr}}$$

Оценка следовой нормы матрицы P

Лемма

$$\|P\|_{\text{tr}} \leq 2^{2\ell-2} \sqrt{|X| \cdot |Y|}.$$

Доказательство

Из предыдущей леммы

$$p_{xy} = \sum_{k=0}^{2^{2\ell-2}-1} a_{x,k} \cdot b_{y,k}, \quad |a_{x,k}| \leq 1, \quad |b_{x,k}| \leq 1.$$

Введем векторы $\mathbf{a}_k = (a_{x,k})$, $\mathbf{b}_k = (b_{y,k}^*)$. Тогда $P = \sum_k |\mathbf{a}_k\rangle\langle\mathbf{b}_k|$ и

$$\|P\|_{\text{tr}} \leq \sum_{k=0}^{2^{2\ell-2}-1} \||\mathbf{a}_k\rangle\langle\mathbf{b}_k|\|_{\text{tr}} = \sum_{k=0}^{2^{2\ell-2}-1} \|\mathbf{a}_k\|_2 \|\mathbf{b}_k\|_2 \leq \sum_{k=0}^{2^{2\ell-2}-1} 1 = 2^{2\ell-2}.$$

Оценка следовой нормы матрицы P

Лемма

$$\|P\|_{\text{tr}} \leq 2^{2\ell-2} \sqrt{|X| \cdot |Y|}.$$

Доказательство

Из предыдущей леммы

$$p_{xy} = \sum_{k=0}^{2^{2\ell-2}-1} a_{x,k} \cdot b_{y,k}, \quad |a_{x,k}| \leq 1, \quad |b_{y,k}| \leq 1.$$

Введем векторы $\mathbf{a}_k = (a_{x,k})$, $\mathbf{b}_k = (b_{y,k}^*)$. Тогда $P = \sum_k |\mathbf{a}_k\rangle\langle\mathbf{b}_k|$ и

$$\|P\|_{\text{tr}} \leq \sum_{k=0}^{2^{2\ell-2}-1} \||\mathbf{a}_k\rangle\langle\mathbf{b}_k|\|_{\text{tr}} \leq \sum_{k=0}^{2^{2\ell-2}-1} |\mathbf{a}_k| \cdot |\mathbf{b}_k| \leq 2^{2\ell-2} \sqrt{|X| \cdot |Y|}.$$

Оценка следовой нормы матрицы P

Лемма

$$\|P\|_{\text{tr}} \leq 2^{2\ell-2} \sqrt{|X| \cdot |Y|}.$$

Доказательство

Из предыдущей леммы

$$p_{xy} = \sum_{k=0}^{2^{2\ell-2}-1} a_{x,k} \cdot b_{y,k}, \quad |a_{x,k}| \leq 1, \quad |b_{x,k}| \leq 1.$$

Введем векторы $\mathbf{a}_k = (a_{x,k})$, $\mathbf{b}_k = (b_{y,k}^*)$. Тогда $P = \sum_k |\mathbf{a}_k\rangle\langle\mathbf{b}_k|$ и

$$\|P\|_{\text{tr}} \leq \sum_{k=0}^{2^{2\ell-2}-1} \left\| |\mathbf{a}_k\rangle\langle\mathbf{b}_k| \right\|_{\text{tr}} \leq \sum_{k=0}^{2^{2\ell-2}-1} |\mathbf{a}_k| \cdot |\mathbf{b}_k| \leq 2^{2\ell-2} \sqrt{|X| \cdot |Y|}.$$

Оценка следовой нормы матрицы P

Лемма

$$\|P\|_{\text{tr}} \leq 2^{2\ell-2} \sqrt{|X| \cdot |Y|}.$$

Доказательство

Из предыдущей леммы

$$p_{xy} = \sum_{k=0}^{2^{2\ell-2}-1} a_{x,k} \cdot b_{y,k}, \quad |a_{x,k}| \leq 1, \quad |b_{x,k}| \leq 1.$$

Введем векторы $\mathbf{a}_k = (a_{x,k})$, $\mathbf{b}_k = (b_{y,k}^*)$. Тогда $P = \sum_k |\mathbf{a}_k\rangle\langle\mathbf{b}_k|$ и

$$\|P\|_{\text{tr}} \leq \sum_{k=0}^{2^{2\ell-2}-1} \||\mathbf{a}_k\rangle\langle\mathbf{b}_k|\|_{\text{tr}} \leq \sum_{k=0}^{2^{2\ell-2}-1} |\mathbf{a}_k| \cdot |\mathbf{b}_k| \leq 2^{2\ell-2} \sqrt{|X| \cdot |Y|}.$$

Оценка следовой нормы матрицы P

Лемма

$$\|P\|_{\text{tr}} \leq 2^{2\ell-2} \sqrt{|X| \cdot |Y|}.$$

Доказательство

Из предыдущей леммы

$$p_{xy} = \sum_{k=0}^{2^{2\ell-2}-1} a_{x,k} \cdot b_{y,k}, \quad |a_{x,k}| \leq 1, \quad |b_{x,k}| \leq 1.$$

Введем векторы $\mathbf{a}_k = (a_{x,k})$, $\mathbf{b}_k = (b_{y,k}^*)$. Тогда $P = \sum_k |\mathbf{a}_k\rangle\langle\mathbf{b}_k|$ и

$$\|P\|_{\text{tr}} \leq \sum_{k=0}^{2^{2\ell-2}-1} \||\mathbf{a}_k\rangle\langle\mathbf{b}_k|\|_{\text{tr}} \leq \sum_{k=0}^{2^{2\ell-2}-1} |\mathbf{a}_k| \cdot |\mathbf{b}_k| \leq 2^{2\ell-2} \sqrt{|X| \cdot |Y|}.$$

Пример: нижняя оценка для скалярного произведения

Функция $IP(x, y) = \bigoplus_{k=1}^n x_k y_k$.

Утверждение

$$Q_{1/3}(IP) = \Omega(n).$$

Эскиз доказательства

Пример: нижняя оценка для скалярного произведения

Функция $IP(x, y) = \bigoplus_{k=1}^n x_k y_k$.

Утверждение

$$Q_{1/3}(IP) = \Omega(n).$$

Эскиз доказательства

Пример: нижняя оценка для скалярного произведения

Функция $IP(x, y) = \bigoplus_{k=1}^n x_k y_k$.

Утверждение

$$Q_{1/3}(IP) = \Omega(n).$$

Эскиз доказательства

Полагаем $X = Y = \{0, 1\}^n$.

Пример: нижняя оценка для скалярного произведения

Функция $IP(x, y) = \bigoplus_{k=1}^n x_k y_k$.

Утверждение

$$Q_{1/3}(IP) = \Omega(n).$$

Эскиз доказательства

Полагаем $X = Y = \{0, 1\}^n$. Матрица скалярных произведений:

$$M = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}^{\otimes n} \quad (\text{проверьте, что } M_{xy} = (-1)^{IP(x,y)}).$$

Пример: нижняя оценка для скалярного произведения

Функция $\text{IP}(x, y) = \bigoplus_{k=1}^n x_k y_k$.

Утверждение

$$Q_{1/3}(\text{IP}) = \Omega(n).$$

Эскиз доказательства

Полагаем $X = Y = \{0, 1\}^n$. Матрица скалярных произведений:

$$M = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}^{\otimes n} \quad (\text{проверьте, что } M_{xy} = (-1)^{\text{IP}(x,y)}).$$

Пусть P — матрица положительных ответов для протокола, вычисляющего IP.

Тогда $M_{xy} = 1 \Rightarrow P_{xy} > 2/3$, $M_{xy} = -1 \Rightarrow P_{xy} < 1/3$.

Пример: нижняя оценка для скалярного произведения

Функция $IP(x, y) = \bigoplus_{k=1}^n x_k y_k$.

Утверждение

$$Q_{1/3}(IP) = \Omega(n).$$

Эскиз доказательства

Тогда $M_{xy} = 1 \Rightarrow P_{xy} > 2/3$, $M_{xy} = -1 \Rightarrow P_{xy} < 1/3$. Поэтому

$$\langle P, M \rangle = \sum_{x,y} P_{xy} M_{xy} \geq 2^{2n}/6.$$

Пример: нижняя оценка для скалярного произведения

Функция $IP(x, y) = \bigoplus_{k=1}^n x_k y_k$.

Утверждение

$$Q_{1/3}(IP) = \Omega(n).$$

Эскиз доказательства

Тогда $M_{xy} = 1 \Rightarrow P_{xy} > 2/3$, $M_{xy} = -1 \Rightarrow P_{xy} < 1/3$. Поэтому

$$\langle P, M \rangle = \sum_{x,y} P_{xy} M_{xy} \geq 2^{2n}/6.$$

Но $\|M\| = 2^{n/2}$ (упражнение) и

$$\langle P, M \rangle \leq \|P\|_{\text{tr}} \|M\| = 2^{n/2} \|P\|_{\text{tr}} \leq 2^{3n/2} 2^{2\ell-2}.$$

Пример: нижняя оценка для скалярного произведения

Функция $IP(x, y) = \bigoplus_{k=1}^n x_k y_k$.

Утверждение

$$Q_{1/3}(IP) = \Omega(n).$$

Эскиз доказательства

Тогда $M_{xy} = 1 \Rightarrow P_{xy} > 2/3$, $M_{xy} = -1 \Rightarrow P_{xy} < 1/3$. Поэтому

$$\langle P, M \rangle = \sum_{x,y} P_{xy} M_{xy} \geq 2^{2n}/6.$$

$$\langle P, M \rangle \leq \|P\|_{\text{tr}} \|M\| = 2^{n/2} \|P\|_{\text{tr}} \leq 2^{3n/2} 2^{2\ell-2}.$$

Окончательно,

$$2^{2\ell-2} \geq \frac{1}{6} 2^{n/2}, \quad \text{т. е. } \ell = \Omega(n).$$

- 1 Нижние оценки квантовой коммуникационной сложности
- 2 Нижняя оценка для функции пересечения множеств
- 3 Модель коммуникации SMP
- 4 Квантовая (псевдо-)телепатия

Оценка Разборова $Q_{1/3}(\text{DISJ}) = \Omega(\sqrt{n})$ (план)

- Выбираем $X = Y = \binom{n}{n/4}$ — множество слов длины n веса $n/4$ (вес — количество единиц).

- Подбираем такие матрицы μ_s , $0 \leq s \leq n/4$, что

$$\langle P, \mu_0 \rangle \in (2/3; 1], \text{ а } \langle P, \mu_s \rangle \in [0; 1/3) \text{ для } s = 1, \dots, n/4;$$

$$\text{и для любых } d \leq n/4 \text{ выполняется неравенство } \langle P, \mu_d \rangle \leq 1/3.$$

$$|p(s) - \langle P, \mu_s \rangle| \leq \frac{\langle P, \mu_0 \rangle}{\binom{n}{n/4}} \text{ для } 0 \leq s \leq n/4.$$

- Для $d = 8\ell + 8$ из леммы о следовой норме матрицы положительных ответов получаем

$$|p(s) - \langle P, \mu_s \rangle| \leq \frac{2^{2\ell-2} \binom{n}{n/4}}{\binom{n}{n/4} 2^{2\ell-2}} = \frac{1}{2^4}.$$

- Поэтому к многочлену p можно применить теорему о нижней оценке степени многочлена.
- Значит, $d = \Omega(\sqrt{n})$ и $\ell = \Omega(\sqrt{n})$.

Оценка Разборова $Q_{1/3}(\text{DISJ}) = \Omega(\sqrt{n})$ (план)

- Выбираем $X = Y = \binom{n}{n/4}$ — множество слов длины n веса $n/4$ (вес — количество единиц).
- Подбираем такие матрицы μ_s , $0 \leq s \leq n/4$, что
 - 1 $\langle P, \mu_0 \rangle \in (2/3; 1]$, а $\langle P, \mu_s \rangle \in [0; 1/3)$ для $s = 1, \dots, n/4$;
 - 2 для любого $d \leq n/4$ существует многочлен p степени d такой, что

$$|p(s) - \langle P, \mu_s \rangle| \leq \frac{\|P\|_{\text{tr}}}{\binom{n}{n/4} 2^{d/4}} \quad \text{для } 0 \leq s \leq n/8.$$

- Для $d = 8\ell + 8$ из леммы о следовой норме матрицы положительных ответов получаем

$$|p(s) - \langle P, \mu_s \rangle| \leq \frac{2^{2\ell-2} \binom{n}{n/4}}{\binom{n}{n/4} 2^{2\ell-2}} = \frac{1}{2^4}.$$

- Поэтому к многочлену p можно применить теорему о нижней оценке степени многочлена.
- Значит, $d = \Omega(\sqrt{n})$ и $\ell = \Omega(\sqrt{n})$.

Оценка Разборова $Q_{1/3}(\text{DISJ}) = \Omega(\sqrt{n})$ (план)

- Выбираем $X = Y = \binom{n}{n/4}$ — множество слов длины n веса $n/4$ (вес — количество единиц).
- Подбираем такие матрицы μ_s , $0 \leq s \leq n/4$, что
 - 1 $\langle P, \mu_0 \rangle \in (2/3; 1]$, а $\langle P, \mu_s \rangle \in [0; 1/3)$ для $s = 1, \dots, n/4$;
 - 2 для любого $d \leq n/4$ существует многочлен p степени d такой, что

$$|p(s) - \langle P, \mu_s \rangle| \leq \frac{\|P\|_{\text{tr}}}{\binom{n}{n/4} 2^{d/4}} \quad \text{для } 0 \leq s \leq n/8.$$

- Для $d = 8\ell + 8$ из леммы о следовой норме матрицы положительных ответов получаем

$$|p(s) - \langle P, \mu_s \rangle| \leq \frac{2^{2\ell-2} \binom{n}{n/4}}{\binom{n}{n/4} 2^{2\ell-2}} = \frac{1}{2^4}.$$

- Поэтому к многочлену p можно применить теорему о нижней оценке степени многочлена.
- Значит, $d = \Omega(\sqrt{n})$ и $\ell = \Omega(\sqrt{n})$.

Оценка Разборова $Q_{1/3}(\text{DISJ}) = \Omega(\sqrt{n})$ (план)

- Выбираем $X = Y = \binom{n}{n/4}$ — множество слов длины n веса $n/4$ (вес — количество единиц).
- Подбираем такие матрицы μ_s , $0 \leq s \leq n/4$, что
 - 1 $\langle P, \mu_0 \rangle \in (2/3; 1]$, а $\langle P, \mu_s \rangle \in [0; 1/3)$ для $s = 1, \dots, n/4$;
 - 2 для любого $d \leq n/4$ существует многочлен p степени d такой, что

$$|p(s) - \langle P, \mu_s \rangle| \leq \frac{\|P\|_{\text{tr}}}{\binom{n}{n/4} 2^{d/4}} \quad \text{для } 0 \leq s \leq n/8.$$

- Для $d = 8\ell + 8$ из леммы о следовой норме матрицы положительных ответов получаем

$$|p(s) - \langle P, \mu_s \rangle| \leq \frac{2^{2\ell-2} \binom{n}{n/4}}{\binom{n}{n/4} 2^{2\ell-2}} = \frac{1}{2^4}.$$

- Поэтому к многочлену p можно применить теорему о нижней оценке степени многочлена.
- Значит, $d = \Omega(\sqrt{n})$ и $\ell = \Omega(\sqrt{n})$.

Оценка Разборова $Q_{1/3}(\text{DISJ}) = \Omega(\sqrt{n})$ (план)

- Выбираем $X = Y = \binom{n}{n/4}$ — множество слов длины n веса $n/4$ (вес — количество единиц).
- Подбираем такие матрицы μ_s , $0 \leq s \leq n/4$, что
 - 1 $\langle P, \mu_0 \rangle \in (2/3; 1]$, а $\langle P, \mu_s \rangle \in [0; 1/3)$ для $s = 1, \dots, n/4$;
 - 2 для любого $d \leq n/4$ существует многочлен p степени d такой, что

$$|p(s) - \langle P, \mu_s \rangle| \leq \frac{\|P\|_{\text{tr}}}{\binom{n}{n/4} 2^{d/4}} \quad \text{для } 0 \leq s \leq n/8.$$

- Для $d = 8\ell + 8$ из леммы о следовой норме матрицы положительных ответов получаем

$$|p(s) - \langle P, \mu_s \rangle| \leq \frac{2^{2\ell-2} \binom{n}{n/4}}{\binom{n}{n/4} 2^{2\ell-2}} = \frac{1}{2^4}.$$

- Поэтому к многочлену p можно применить теорему о нижней оценке степени многочлена.
- Значит, $d = \Omega(\sqrt{n})$ и $\ell = \Omega(\sqrt{n})$.

Оценка Разборова $Q_{1/3}(\text{DISJ}) = \Omega(\sqrt{n})$ (план)

- Выбираем $X = Y = \binom{n}{n/4}$ — множество слов длины n веса $n/4$ (вес — количество единиц).
- Подбираем такие матрицы μ_s , $0 \leq s \leq n/4$, что
 - 1 $\langle P, \mu_0 \rangle \in (2/3; 1]$, а $\langle P, \mu_s \rangle \in [0; 1/3]$ для $s = 1, \dots, n/4$;
 - 2 для любого $d \leq n/4$ существует многочлен p степени d такой, что

$$|p(s) - \langle P, \mu_s \rangle| \leq \frac{\|P\|_{\text{tr}}}{\binom{n}{n/4} 2^{d/4}} \quad \text{для } 0 \leq s \leq n/8.$$

- Для $d = 8\ell + 8$ из леммы о следовой норме матрицы положительных ответов получаем

$$|p(s) - \langle P, \mu_s \rangle| \leq \frac{2^{2\ell-2} \binom{n}{n/4}}{\binom{n}{n/4} 2^{2\ell-2}} = \frac{1}{2^4}.$$

- Поэтому к многочлену p можно применить теорему о нижней оценке степени многочлена.
- Значит, $d = \Omega(\sqrt{n})$ и $\ell = \Omega(\sqrt{n})$.

Оценка Разборова $Q_{1/3}(\text{DISJ}) = \Omega(\sqrt{n})$ (план)

- Выбираем $X = Y = \binom{n}{n/4}$ — множество слов длины n веса $n/4$ (вес — количество единиц).
- Подбираем такие матрицы μ_s , $0 \leq s \leq n/4$, что
 - 1 $\langle P, \mu_0 \rangle \in (2/3; 1]$, а $\langle P, \mu_s \rangle \in [0; 1/3)$ для $s = 1, \dots, n/4$;
 - 2 для любого $d \leq n/4$ существует многочлен p степени d такой, что

$$|p(s) - \langle P, \mu_s \rangle| \leq \frac{\|P\|_{\text{tr}}}{\binom{n}{n/4} 2^{d/4}} \quad \text{для } 0 \leq s \leq n/8.$$

- Для $d = 8\ell + 8$ из леммы о следовой норме матрицы положительных ответов получаем

$$|p(s) - \langle P, \mu_s \rangle| \leq \frac{2^{2\ell-2} \binom{n}{n/4}}{\binom{n}{n/4} 2^{2\ell-2}} = \frac{1}{2^4}.$$

- Поэтому к многочлену p можно применить теорему о нижней оценке степени многочлена.
- Значит, $d = \Omega(\sqrt{n})$ и $\ell = \Omega(\sqrt{n})$.

Выбор матриц μ_s

$$\mu_s = \frac{1}{\binom{n}{n/4} \binom{n/4}{s} \binom{n-n/4}{n/4-s}} J_{n,n/4,s},$$

где $J_{n,k,s}$ — матрица из схемы отношений Джонсона

$$J_{n,k,s}(x, y) = \begin{cases} 1, & \text{если } |x \cap y| = s, \\ 0, & \text{в противном случае,} \end{cases} \quad x, y \in \{0, 1\}^n; \quad |x| = |y| = k.$$

Матрица μ_s соответствует случайному выбору пары x, y с заданным размером пересечения s .

Поэтому для протокола, вычисляющего $\text{DISJ}(x, y)$, выполняется условие 1:

$$\langle P, \mu_0 \rangle \in (2/3; 1], \quad \langle P, \mu_s \rangle \in [0; 1/3) \text{ для } s = 1, \dots, n/4.$$

Выбор матриц μ_s

$$\mu_s = \frac{1}{\binom{n}{n/4} \binom{n/4}{s} \binom{n-n/4}{n/4-s}} J_{n,n/4,s},$$

где $J_{n,k,s}$ — матрица из схемы отношений Джонсона

$$J_{n,k,s}(x, y) = \begin{cases} 1, & \text{если } |x \cap y| = s, \\ 0, & \text{в противном случае,} \end{cases} \quad x, y \in \{0, 1\}^n; |x| = |y| = k.$$

Матрица μ_s соответствует случайному выбору пары x, y с заданным размером пересечения s .

Поэтому для протокола, вычисляющего $\text{DISJ}(x, y)$, выполняется условие 1:

$$\langle P, \mu_0 \rangle \in (2/3; 1], \quad \langle P, \mu_s \rangle \in [0; 1/3) \text{ для } s = 1, \dots, n/4.$$

Выбор матриц μ_s

$$\mu_s = \frac{1}{\binom{n}{n/4} \binom{n/4}{s} \binom{n-n/4}{n/4-s}} J_{n,n/4,s},$$

где $J_{n,k,s}$ — матрица из схемы отношений Джонсона

$$J_{n,k,s}(x, y) = \begin{cases} 1, & \text{если } |x \cap y| = s, \\ 0, & \text{в противном случае,} \end{cases} \quad x, y \in \{0, 1\}^n; \quad |x| = |y| = k.$$

Матрица μ_s соответствует случайному выбору пары x, y с заданным размером пересечения s .

Поэтому для протокола, вычисляющего $\text{DISJ}(x, y)$, выполняется условие 1:

$$\langle P, \mu_0 \rangle \in (2/3; 1], \quad \langle P, \mu_s \rangle \in [0; 1/3) \text{ для } s = 1, \dots, n/4.$$

- Матрицы $J_{n,k,s}$ попарно коммутируют.
- Поэтому у них есть общая система собственных пространств $E_0, \dots, E_k$.
- Собственное число $\lambda_{s,t}$, отвечающее матрице $J_{n,k,s}$ и пространству E_t , выражается формулой

$$\lambda_{s,t} = \sum_r (-1)^{t-r} \binom{t}{r} \binom{k-r}{s-r} \binom{n-k-t+r}{k-s-t+r}.$$

- Докажите, что соответствующие собственные числа $\lambda_{s,t}(\mu_s)$ матриц μ_s задаются многочленом от s степени t .
- При $k \leq n/4$ и $s \leq k/2$ выполняется неравенство

$$|\lambda_{s,t}(\mu_s)| \leq \binom{n}{k}^{-1} 2^{-t/4}.$$

- Матрицы $J_{n,k,s}$ попарно коммутируют.
- Поэтому у них есть общая система собственных пространств $E_0, \dots, E_k$.
- Собственное число $\lambda_{s,t}$, отвечающее матрице $J_{n,k,s}$ и пространству E_t , выражается формулой

$$\lambda_{s,t} = \sum_r (-1)^{t-r} \binom{t}{r} \binom{k-r}{s-r} \binom{n-k-t+r}{k-s-t+r}.$$

- Докажите, что соответствующие собственные числа $\lambda_{s,t}(\mu_s)$ матриц μ_s задаются многочленом от s степени t .
- При $k \leq n/4$ и $s \leq k/2$ выполняется неравенство

$$|\lambda_{s,t}(\mu_s)| \leq \binom{n}{k}^{-1} 2^{-t/4}.$$

- Матрицы $J_{n,k,s}$ попарно коммутируют.
- Поэтому у них есть общая система собственных пространств $E_0, \dots, E_k$.
- Собственное число $\lambda_{s,t}$, отвечающее матрице $J_{n,k,s}$ и пространству E_t , выражается формулой

$$\lambda_{s,t} = \sum_r (-1)^{t-r} \binom{t}{r} \binom{k-r}{s-r} \binom{n-k-t+r}{k-s-t+r}.$$

- Докажите, что соответствующие собственные числа $\lambda_{s,t}(\mu_s)$ матриц μ_s задаются многочленом от s степени t .
- При $k \leq n/4$ и $s \leq k/2$ выполняется неравенство

$$|\lambda_{s,t}(\mu_s)| \leq \binom{n}{k}^{-1} 2^{-t/4}.$$

- Матрицы $J_{n,k,s}$ попарно коммутируют.
- Поэтому у них есть общая система собственных пространств $E_0, \dots, E_k$.
- Собственное число $\lambda_{s,t}$, отвечающее матрице $J_{n,k,s}$ и пространству E_t , выражается формулой

$$\lambda_{s,t} = \sum_r (-1)^{t-r} \binom{t}{r} \binom{k-r}{s-r} \binom{n-k-t+r}{k-s-t+r}.$$

- Докажите, что соответствующие собственные числа $\lambda_{s,t}(\mu_s)$ матриц μ_s задаются многочленом от s степени t .
- При $k \leq n/4$ и $s \leq k/2$ выполняется неравенство

$$|\lambda_{s,t}(\mu_s)| \leq \binom{n}{k}^{-1} 2^{-t/4}.$$

- Матрицы $J_{n,k,s}$ попарно коммутируют.
- Поэтому у них есть общая система собственных пространств $E_0, \dots, E_k$.
- Собственное число $\lambda_{s,t}$, отвечающее матрице $J_{n,k,s}$ и пространству E_t , выражается формулой

$$\lambda_{s,t} = \sum_r (-1)^{t-r} \binom{t}{r} \binom{k-r}{s-r} \binom{n-k-t+r}{k-s-t+r}.$$

- Докажите, что соответствующие собственные числа $\lambda_{s,t}(\mu_s)$ матриц μ_s задаются многочленом от s степени t .
- При $k \leq n/4$ и $s \leq k/2$ выполняется неравенство

$$|\lambda_{s,t}(\mu_s)| \leq \binom{n}{k}^{-1} 2^{-t/4}.$$

Задача

Выведите из этих свойств условие 2:

для любого $d \leq n/4$ существует многочлен p степени d такой, что

$$|p(s) - \langle P, \mu_s \rangle| \leq \frac{\|P\|_{\text{tr}}}{\binom{n}{n/4} 2^{d/4}} \quad \text{для } 0 \leq s \leq n/8.$$

Указание: перейдите к базису, в котором матрицы $J_{n,k,s}$ диагонализуются.

- 1 Нижние оценки квантовой коммуникационной сложности
- 2 Нижняя оценка для функции пересечения множеств
- 3 Модель коммуникации SMP
- 4 Квантовая (псевдо-)телепатия

Коммуникационная сложность проверки равенства

$$\text{EQ}(x, y) = \begin{cases} 1, & \text{если } x = y, \\ 0, & \text{иначе.} \end{cases}$$

Коммуникационная сложность в основной модели

$$D(\text{EQ}) = n; \quad R_\epsilon(\text{EQ}) = O(\log n).$$

Коммуникационная сложность в модели SMP

$$R_\epsilon^{\text{SMP}}(\text{EQ}) = \Omega(\sqrt{n}); \quad Q_\epsilon^{\text{SMP}}(\text{EQ}) = O(\log n).$$

Коммуникационная сложность проверки равенства

$$\text{EQ}(x, y) = \begin{cases} 1, & \text{если } x = y, \\ 0, & \text{иначе.} \end{cases}$$

Коммуникационная сложность в основной модели

$$D(\text{EQ}) = n; \quad R_\epsilon(\text{EQ}) = O(\log n).$$

Коммуникационная сложность в модели SMP

$$R_\epsilon^{\text{SMP}}(\text{EQ}) = \Omega(\sqrt{n}); \quad Q_\epsilon^{\text{SMP}}(\text{EQ}) = O(\log n).$$

$$\text{EQ}(x, y) = \begin{cases} 1, & \text{если } x = y, \\ 0, & \text{иначе.} \end{cases}$$

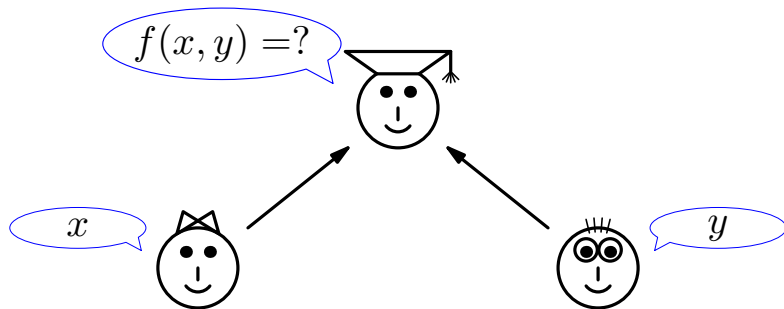
Коммуникационная сложность в основной модели

$$D(\text{EQ}) = n; \quad R_\varepsilon(\text{EQ}) = O(\log n).$$

Коммуникационная сложность в модели SMP

$$R_\varepsilon^{\text{SMP}}(\text{EQ}) = \Omega(\sqrt{n}); \quad Q_\varepsilon^{\text{SMP}}(\text{EQ}) = O(\log n).$$

Одновременная передача сообщений (модель SMP)



Алиса (знает x) и Боб (знает y) посылают сообщения Чарли, который должен вычислить $f(x, y)$.

Аналогично предыдущему формулируются вероятностная модель (с частными или общими генераторами) и квантовая (с предварительной сцепленностью или без).

Определение

Семейство подмножеств $C_n \subset \{0, 1\}^n$ называется (асимптотически) **хорошим кодом**, если найдутся такие две константы δ, r , что

- $|C_n| \geq 2^{rn}$;
- $\|x \oplus y\| \geq \delta n$ при $x, y \in C_n, x \neq y$.

r назовем **пропускной способностью**,
 δ — (относительным) **кодовым расстоянием**.

Задача

Докажите, что хорошие коды существуют при $r + H_2(\delta) < 1$, $\delta < 1/2$.
Здесь $H_2 = -\delta \log_2 \delta - (1 - \delta) \log_2 \delta$.

Определение

Семейство подмножеств $C_n \subset \{0, 1\}^n$ называется (асимптотически) **хорошим кодом**, если найдутся такие две константы δ, r , что

- $|C_n| \geq 2^{rn}$;
- $\|x \oplus y\| \geq \delta n$ при $x, y \in C_n, x \neq y$.

r назовем **пропускной способностью**,
 δ — (относительным) **кодовым расстоянием**.

Задача

Докажите, что хорошие коды существуют при $r + H_2(\delta) < 1, \delta < 1/2$.
Здесь $H_2 = -\delta \log_2 \delta - (1 - \delta) \log_2 \delta$.

Определение

Семейство подмножеств $C_n \subset \{0, 1\}^n$ называется (асимптотически) **хорошим кодом**, если найдутся такие две константы δ, r , что

- $|C_n| \geq 2^{rn}$;
- $\|x \oplus y\| \geq \delta n$ при $x, y \in C_n, x \neq y$.

r назовем **пропускной способностью**,
 δ — (относительным) **кодовым расстоянием**.

Задача

Докажите, что хорошие коды существуют при $r + H_2(\delta) < 1, \delta < 1/2$.
Здесь $H_2 = -\delta \log_2 \delta - (1 - \delta) \log_2 \delta$.

Определение

Семейство подмножеств $C_n \subset \{0, 1\}^n$ называется (асимптотически) **хорошим кодом**, если найдутся такие две константы δ, r , что

- $|C_n| \geq 2^{rn}$;
- $\|x \oplus y\| \geq \delta n$ при $x, y \in C_n, x \neq y$.

r назовем **пропускной способностью**,
 δ — (относительным) **кодовым расстоянием**.

Задача

Докажите, что хорошие коды существуют при $r + H_2(\delta) < 1, \delta < 1/2$.
Здесь $H_2 = -\delta \log_2 \delta - (1 - \delta) \log_2 \delta$.

Хорошие коды помогают вычислять EQ

Задача

Докажите, используя хорошие коды, что $R_\epsilon(\text{EQ}) = O(\log n)$.

Задача

Докажите, используя хорошие коды, что $R_\epsilon^{\text{SMP, pub}}(\text{EQ}) = O(\log n)$.

Однако:

$$R_\epsilon^{\text{SMP}}(\text{EQ}) = \Omega(\sqrt{n})$$

Следствие: для задачи SMP не существует эффективной (полиномиальной) коммуникационной схемы с общедоступным каналом. Следовательно, для задачи SMP не существует эффективной схемы с общедоступным каналом.

Квантовые сообщения экспоненциально эффективнее:

$$Q_\epsilon^{\text{SMP}}(\text{EQ}) = O(\log n)$$

Хорошие коды помогают вычислять EQ

Задача

Докажите, используя хорошие коды, что $R_\epsilon(\text{EQ}) = O(\log n)$.

Задача

Докажите, используя хорошие коды, что $R_\epsilon^{\text{SMP, pub}}(\text{EQ}) = O(\log n)$.

Однако:

$$R_\epsilon^{\text{SMP}}(\text{EQ}) = \Omega(\sqrt{n})$$

(Babai, Kimmel, 1996: в SMP модели разрыв между вероятностной и детерминированной коммуникационной сложностью не более чем квадратичный.)

Квантовые сообщения экспоненциально эффективнее:

$$Q_\epsilon^{\text{SMP}}(\text{EQ}) = O(\log n)$$

Хорошие коды помогают вычислять EQ

Задача

Докажите, используя хорошие коды, что $R_\epsilon(\text{EQ}) = O(\log n)$.

Задача

Докажите, используя хорошие коды, что $R_\epsilon^{\text{SMP, pub}}(\text{EQ}) = O(\log n)$.

Однако:

$$R_\epsilon^{\text{SMP}}(\text{EQ}) = \Omega(\sqrt{n})$$

(Babai, Kimmel, 1996: в SMP модели разрыв между вероятностной и детерминированной коммуникационной сложностью не более чем квадратичный.)

Квантовые сообщения экспоненциально эффективнее:

$$Q_\epsilon^{\text{SMP}}(\text{EQ}) = O(\log n)$$

Хорошие коды помогают вычислять EQ

Задача

Докажите, используя хорошие коды, что $R_\epsilon(\text{EQ}) = O(\log n)$.

Задача

Докажите, используя хорошие коды, что $R_\epsilon^{\text{SMP, pub}}(\text{EQ}) = O(\log n)$.

Однако:

$$R_\epsilon^{\text{SMP}}(\text{EQ}) = \Omega(\sqrt{n})$$

(Babai, Kimmel, 1996: в SMP модели разрыв между вероятностной и детерминированной коммуникационной сложностью не более чем квадратичный.)

Квантовые сообщения экспоненциально эффективнее:

$$Q_\epsilon^{\text{SMP}}(\text{EQ}) = O(\log n)$$

Хорошие коды помогают вычислять EQ

Задача

Докажите, используя хорошие коды, что $R_\epsilon(\text{EQ}) = O(\log n)$.

Задача

Докажите, используя хорошие коды, что $R_\epsilon^{\text{SMP, pub}}(\text{EQ}) = O(\log n)$.

Однако:

$$R_\epsilon^{\text{SMP}}(\text{EQ}) = \Omega(\sqrt{n})$$

(Babai, Kimmel, 1996: в SMP модели разрыв между вероятностной и детерминированной коммуникационной сложностью не более чем квадратичный.)

Квантовые сообщения экспоненциально эффективнее:

$$Q_\epsilon^{\text{SMP}}(\text{EQ}) = O(\log n)$$

Вычисление EQ в модели SMP (квантовое хеширование)

Фиксируем хорошее семейство кодов C_m с пропускной способностью r и кодовым расстоянием δ . (Для определенности $\delta = 1/4$, $r = 1/8$.)

Выберем кодирующую функцию (инъективное отображение)

$$c_n: \{0, 1\}^n \rightarrow C_{n/r}.$$

Алиса готовит сообщение (Боб действует аналогично):

- 1 по x находит $u^{(x)} = c_n(x)$, где $n = |x|$;
- 2 строит квантовое состояние

$$|\psi_x\rangle = \frac{1}{\sqrt{m}} \sum_{k=1}^m |k, u_k^{(x)}\rangle, \quad m = n/r, \quad u_k^{(x)} \text{ — } k\text{-й бит } u^{(x)},$$

на $O(\log m)$ кубитах (k представляется двоичной записью).

Вычисление EQ в модели SMP (квантовое хеширование)

Фиксируем хорошее семейство кодов C_m с пропускной способностью r и кодовым расстоянием δ . (Для определенности $\delta = 1/4$, $r = 1/8$.)
Выберем кодирующую функцию (инъективное отображение)

$$c_n: \{0, 1\}^n \rightarrow C_{n/r}.$$

Алиса готовит сообщение (Боб действует аналогично):

- 1 по x находит $u^{(x)} = c_n(x)$, где $n = |x|$;
- 2 строит квантовое состояние

$$|\psi_x\rangle = \frac{1}{\sqrt{m}} \sum_{k=1}^m |k, u_k^{(x)}\rangle, \quad m = n/r, \quad u_k^{(x)} \text{ — } k\text{-й бит } u^{(x)},$$

на $O(\log m)$ кубитах (k представляется двоичной записью).

Вычисление EQ в модели SMP (квантовое хеширование)

Фиксируем хорошее семейство кодов C_m с пропускной способностью r и кодовым расстоянием δ . (Для определенности $\delta = 1/4$, $r = 1/8$.)
Выберем кодирующую функцию (инъективное отображение)

$$c_n: \{0, 1\}^n \rightarrow C_{n/r}.$$

Алиса готовит сообщение (Боб действует аналогично):

- 1 по x находит $u^{(x)} = c_n(x)$, где $n = |x|$;
- 2 строит квантовое состояние

$$|\psi_x\rangle = \frac{1}{\sqrt{m}} \sum_{k=1}^m |k, u_k^{(x)}\rangle, \quad m = n/r, \quad u_k^{(x)} \text{ — } k\text{-й бит } u^{(x)},$$

на $O(\log m)$ кубитах (k представляется двоичной записью).

Вычисление EQ в модели SMP (квантовое хеширование)

Фиксируем хорошее семейство кодов C_m с пропускной способностью r и кодовым расстоянием δ . (Для определенности $\delta = 1/4$, $r = 1/8$.)
Выберем кодирующую функцию (инъективное отображение)

$$c_n: \{0, 1\}^n \rightarrow C_{n/r}.$$

Алиса готовит сообщение (Боб действует аналогично):

- 1 по x находит $u^{(x)} = c_n(x)$, где $n = |x|$;
- 2 строит квантовое состояние

$$|\psi_x\rangle = \frac{1}{\sqrt{m}} \sum_{k=1}^m |k, u_k^{(x)}\rangle, \quad m = n/r, \quad u_k^{(x)} \text{ — } k\text{-й бит } u^{(x)},$$

на $O(\log m)$ кубитах (k представляется двоичной записью).

Вычисление EQ в модели SMP (квантовое хеширование)

Фиксируем хорошее семейство кодов C_m с пропускной способностью r и кодовым расстоянием δ . (Для определенности $\delta = 1/4$, $r = 1/8$.)
Выберем кодирующую функцию (инъективное отображение)

$$c_n: \{0, 1\}^n \rightarrow C_{n/r}.$$

Алиса готовит сообщение (Боб действует аналогично):

- 1 по x находит $u^{(x)} = c_n(x)$, где $n = |x|$;
- 2 строит квантовое состояние

$$|\psi_x\rangle = \frac{1}{\sqrt{m}} \sum_{k=1}^m |k, u_k^{(x)}\rangle, \quad m = n/r, \quad u_k^{(x)} \text{ — } k\text{-й бит } u^{(x)},$$

на $O(\log m)$ кубитах (k представляется двоичной записью).

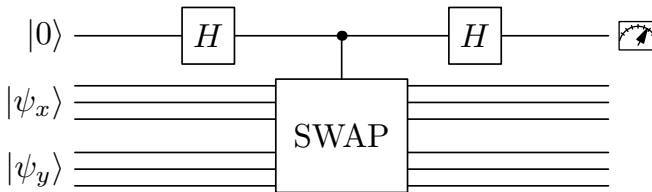
Вычисление EQ в модели SMP: действия Чарли

Чарли получает два сообщения $|\psi_x\rangle$, $|\psi_y\rangle$ и должен ответить, справедливо ли равенство $x = y$. Его действия описываются схемой:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad \text{SWAP: } |u\rangle \otimes |v\rangle \mapsto |v\rangle \otimes |u\rangle$$

Вычисление EQ в модели SMP: действия Чарли

Чарли получает два сообщения $|\psi_x\rangle$, $|\psi_y\rangle$ и должен ответить, справедливо ли равенство $x = y$. Его действия описываются схемой:

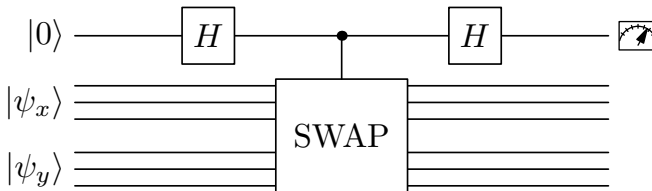


$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$\text{SWAP: } |u\rangle \otimes |v\rangle \mapsto |v\rangle \otimes |u\rangle$$

Вычисление EQ в модели SMP: действия Чарли

Чарли получает два сообщения $|\psi_x\rangle$, $|\psi_y\rangle$ и должен ответить, справедливо ли равенство $x = y$. Его действия описываются схемой:

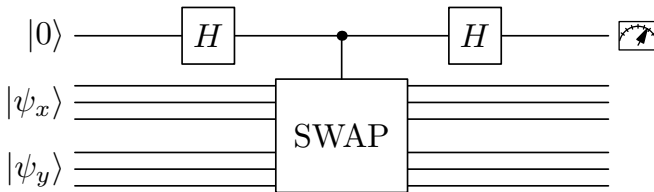


$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$\text{SWAP: } |u\rangle \otimes |v\rangle \mapsto |v\rangle \otimes |u\rangle$$

Вычисление EQ в модели SMP: действия Чарли

Чарли получает два сообщения $|\psi_x\rangle$, $|\psi_y\rangle$ и должен ответить, справедливо ли равенство $x = y$. Его действия описываются схемой:

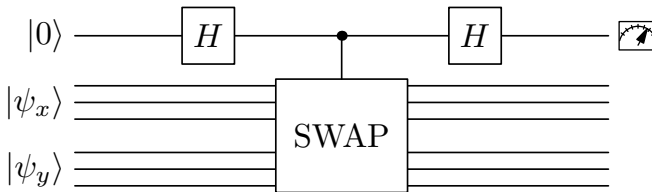


$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$\text{SWAP: } |u\rangle \otimes |v\rangle \mapsto |v\rangle \otimes |u\rangle$$

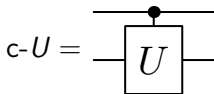
Вычисление EQ в модели SMP: действия Чарли

Чарли получает два сообщения $|\psi_x\rangle$, $|\psi_y\rangle$ и должен ответить, справедливо ли равенство $x = y$. Его действия описываются схемой:



$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$\text{SWAP}: |u\rangle \otimes |v\rangle \mapsto |v\rangle \otimes |u\rangle$$



$$c-U: |0\rangle \otimes |\psi\rangle \rightarrow |0\rangle \otimes |\psi\rangle$$

$$c-U: |1\rangle \otimes |\psi\rangle \rightarrow |1\rangle \otimes U|\psi\rangle$$

- Сообщения Алисы и Боба:

$$|\psi_x\rangle = \frac{1}{\sqrt{m}} \sum_{k=1}^m |k, u_k^{(x)}\rangle, \quad |\psi_y\rangle = \frac{1}{\sqrt{m}} \sum_{k=1}^m |k, u_k^{(y)}\rangle.$$

- Из свойств кода

$$\langle \psi_x | \psi_y \rangle = \frac{1}{m} \#(k : u_k^{(x)} = u_k^{(y)}) \leq 1 - \delta, \quad \text{если } x \neq y,$$
$$\langle \psi_x | \psi_x \rangle = 1 \quad (\text{для любого состояния}).$$

- Сообщения Алисы и Боба:

$$|\psi_x\rangle = \frac{1}{\sqrt{m}} \sum_{k=1}^m |k, u_k^{(x)}\rangle, \quad |\psi_y\rangle = \frac{1}{\sqrt{m}} \sum_{k=1}^m |k, u_k^{(y)}\rangle.$$

- Из свойств кода

$$\langle \psi_x | \psi_y \rangle = \frac{1}{m} \#(k : u_k^{(x)} = u_k^{(y)}) \leq 1 - \delta, \quad \text{если } x \neq y,$$
$$\langle \psi_x | \psi_x \rangle = 1 \quad (\text{для любого состояния}).$$

Анализ протокола (продолжение)

Действия Чарли с заметной вероятностью обнаружат разницу в случае $x \neq y$. Вычисления:

$$\begin{aligned} |0\rangle \otimes |\psi_x\rangle \otimes |\psi_y\rangle &\xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |\psi_x\rangle \otimes |\psi_y\rangle \\ &\xrightarrow{\text{c-SWAP}} \frac{1}{\sqrt{2}}|0\rangle \otimes |\psi_x\rangle \otimes |\psi_y\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes |\psi_y\rangle \otimes |\psi_x\rangle \\ &\xrightarrow{H} \frac{1}{2}(|0\rangle + |1\rangle) \otimes |\psi_x\rangle \otimes |\psi_y\rangle + \frac{1}{2}(|0\rangle - |1\rangle) \otimes |\psi_y\rangle \otimes |\psi_x\rangle = \\ &= \frac{1}{2}|0\rangle \otimes (|\psi_x\rangle \otimes |\psi_y\rangle + |\psi_y\rangle \otimes |\psi_x\rangle) + \frac{1}{2}|1\rangle \otimes (|\psi_x\rangle \otimes |\psi_y\rangle - |\psi_y\rangle \otimes |\psi_x\rangle) \end{aligned}$$

$$\begin{aligned} \Pr(1) &= \frac{1}{4}(\langle\psi_x| \otimes \langle\psi_y| - \langle\psi_y| \otimes \langle\psi_x|)(|\psi_x\rangle \otimes |\psi_y\rangle - |\psi_y\rangle \otimes |\psi_x\rangle) = \\ &= \frac{1}{4}(2 - \langle\psi_x|\psi_y\rangle\langle\psi_y|\psi_x\rangle - \langle\psi_y|\psi_x\rangle\langle\psi_x|\psi_y\rangle) = \frac{1}{2} - \frac{1}{2}|\langle\psi_x|\psi_y\rangle|^2. \end{aligned}$$

Анализ протокола (продолжение)

Действия Чарли с заметной вероятностью обнаружат разницу в случае $x \neq y$. Вычисления:

$$\begin{aligned} |0\rangle \otimes |\psi_x\rangle \otimes |\psi_y\rangle &\xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |\psi_x\rangle \otimes |\psi_y\rangle \\ &\xrightarrow{\text{c-SWAP}} \frac{1}{\sqrt{2}}|0\rangle \otimes |\psi_x\rangle \otimes |\psi_y\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes |\psi_y\rangle \otimes |\psi_x\rangle \\ &\xrightarrow{H} \frac{1}{2}(|0\rangle + |1\rangle) \otimes |\psi_x\rangle \otimes |\psi_y\rangle + \frac{1}{2}(|0\rangle - |1\rangle) \otimes |\psi_y\rangle \otimes |\psi_x\rangle = \\ &= \frac{1}{2}|0\rangle \otimes (|\psi_x\rangle \otimes |\psi_y\rangle + |\psi_y\rangle \otimes |\psi_x\rangle) + \frac{1}{2}|1\rangle \otimes (|\psi_x\rangle \otimes |\psi_y\rangle - |\psi_y\rangle \otimes |\psi_x\rangle) \end{aligned}$$

$$\begin{aligned} \Pr(1) &= \frac{1}{4}(\langle\psi_x| \otimes \langle\psi_y| - \langle\psi_y| \otimes \langle\psi_x|)(|\psi_x\rangle \otimes |\psi_y\rangle - |\psi_y\rangle \otimes |\psi_x\rangle) = \\ &= \frac{1}{4}(2 - \langle\psi_x|\psi_y\rangle\langle\psi_y|\psi_x\rangle - \langle\psi_y|\psi_x\rangle\langle\psi_x|\psi_y\rangle) = \frac{1}{2} - \frac{1}{2}|\langle\psi_x|\psi_y\rangle|^2. \end{aligned}$$

Анализ протокола (продолжение)

Действия Чарли с заметной вероятностью обнаружат разницу в случае $x \neq y$. Вычисления:

$$\begin{aligned} |0\rangle \otimes |\psi_x\rangle \otimes |\psi_y\rangle &\xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |\psi_x\rangle \otimes |\psi_y\rangle \\ &\xrightarrow{\text{c-SWAP}} \frac{1}{\sqrt{2}}|0\rangle \otimes |\psi_x\rangle \otimes |\psi_y\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes |\psi_y\rangle \otimes |\psi_x\rangle \\ &\xrightarrow{H} \frac{1}{2}(|0\rangle + |1\rangle) \otimes |\psi_x\rangle \otimes |\psi_y\rangle + \frac{1}{2}(|0\rangle - |1\rangle) \otimes |\psi_y\rangle \otimes |\psi_x\rangle = \\ &= \frac{1}{2}|0\rangle \otimes (|\psi_x\rangle \otimes |\psi_y\rangle + |\psi_y\rangle \otimes |\psi_x\rangle) + \frac{1}{2}|1\rangle \otimes (|\psi_x\rangle \otimes |\psi_y\rangle - |\psi_y\rangle \otimes |\psi_x\rangle) \end{aligned}$$

$$\begin{aligned} \Pr(1) &= \frac{1}{4}(\langle\psi_x| \otimes \langle\psi_y| - \langle\psi_y| \otimes \langle\psi_x|)(|\psi_x\rangle \otimes |\psi_y\rangle - |\psi_y\rangle \otimes |\psi_x\rangle) = \\ &= \frac{1}{4}(2 - \langle\psi_x|\psi_y\rangle\langle\psi_y|\psi_x\rangle - \langle\psi_y|\psi_x\rangle\langle\psi_x|\psi_y\rangle) = \frac{1}{2} - \frac{1}{2}|\langle\psi_x|\psi_y\rangle|^2. \end{aligned}$$

Анализ протокола (продолжение)

Действия Чарли с заметной вероятностью обнаружат разницу в случае $x \neq y$. Вычисления:

$$\begin{aligned} |0\rangle \otimes |\psi_x\rangle \otimes |\psi_y\rangle &\xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |\psi_x\rangle \otimes |\psi_y\rangle \\ &\xrightarrow{\text{c-SWAP}} \frac{1}{\sqrt{2}}|0\rangle \otimes |\psi_x\rangle \otimes |\psi_y\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes |\psi_y\rangle \otimes |\psi_x\rangle \\ &\xrightarrow{H} \frac{1}{2}(|0\rangle + |1\rangle) \otimes |\psi_x\rangle \otimes |\psi_y\rangle + \frac{1}{2}(|0\rangle - |1\rangle) \otimes |\psi_y\rangle \otimes |\psi_x\rangle = \\ &= \frac{1}{2}|0\rangle \otimes (|\psi_x\rangle \otimes |\psi_y\rangle + |\psi_y\rangle \otimes |\psi_x\rangle) + \frac{1}{2}|1\rangle \otimes (|\psi_x\rangle \otimes |\psi_y\rangle - |\psi_y\rangle \otimes |\psi_x\rangle) \end{aligned}$$

$$\begin{aligned} \Pr(1) &= \frac{1}{4}(\langle\psi_x| \otimes \langle\psi_y| - \langle\psi_y| \otimes \langle\psi_x|)(|\psi_x\rangle \otimes |\psi_y\rangle - |\psi_y\rangle \otimes |\psi_x\rangle) = \\ &= \frac{1}{4}(2 - \langle\psi_x|\psi_y\rangle\langle\psi_y|\psi_x\rangle - \langle\psi_y|\psi_x\rangle\langle\psi_x|\psi_y\rangle) = \frac{1}{2} - \frac{1}{2}|\langle\psi_x|\psi_y\rangle|^2. \end{aligned}$$

Анализ протокола (продолжение)

Действия Чарли с заметной вероятностью обнаружат разницу в случае $x \neq y$. Вычисления:

$$\begin{aligned} |0\rangle \otimes |\psi_x\rangle \otimes |\psi_y\rangle &\xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |\psi_x\rangle \otimes |\psi_y\rangle \\ &\xrightarrow{\text{c-SWAP}} \frac{1}{\sqrt{2}}|0\rangle \otimes |\psi_x\rangle \otimes |\psi_y\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes |\psi_y\rangle \otimes |\psi_x\rangle \\ &\xrightarrow{H} \frac{1}{2}(|0\rangle + |1\rangle) \otimes |\psi_x\rangle \otimes |\psi_y\rangle + \frac{1}{2}(|0\rangle - |1\rangle) \otimes |\psi_y\rangle \otimes |\psi_x\rangle = \\ &= \frac{1}{2}|0\rangle \otimes (|\psi_x\rangle \otimes |\psi_y\rangle + |\psi_y\rangle \otimes |\psi_x\rangle) + \frac{1}{2}|1\rangle \otimes (|\psi_x\rangle \otimes |\psi_y\rangle - |\psi_y\rangle \otimes |\psi_x\rangle) \end{aligned}$$

$$\begin{aligned} \Pr(1) &= \frac{1}{4}(\langle\psi_x| \otimes \langle\psi_y| - \langle\psi_y| \otimes \langle\psi_x|)(|\psi_x\rangle \otimes |\psi_y\rangle - |\psi_y\rangle \otimes |\psi_x\rangle) = \\ &= \frac{1}{4}(2 - \langle\psi_x|\psi_y\rangle\langle\psi_y|\psi_x\rangle - \langle\psi_y|\psi_x\rangle\langle\psi_x|\psi_y\rangle) = \frac{1}{2} - \frac{1}{2}|\langle\psi_x|\psi_y\rangle|^2. \end{aligned}$$

Анализ протокола (продолжение)

Действия Чарли с заметной вероятностью обнаружат разницу в случае $x \neq y$. Вычисления:

$$\begin{aligned} & |0\rangle \otimes |\psi_x\rangle \otimes |\psi_y\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |\psi_x\rangle \otimes |\psi_y\rangle \\ & \xrightarrow{\text{c-SWAP}} \frac{1}{\sqrt{2}}|0\rangle \otimes |\psi_x\rangle \otimes |\psi_y\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes |\psi_y\rangle \otimes |\psi_x\rangle \\ & \xrightarrow{H} \frac{1}{2}(|0\rangle + |1\rangle) \otimes |\psi_x\rangle \otimes |\psi_y\rangle + \frac{1}{2}(|0\rangle - |1\rangle) \otimes |\psi_y\rangle \otimes |\psi_x\rangle = \\ & = \frac{1}{2}|0\rangle \otimes (|\psi_x\rangle \otimes |\psi_y\rangle + |\psi_y\rangle \otimes |\psi_x\rangle) + \frac{1}{2}|1\rangle \otimes (|\psi_x\rangle \otimes |\psi_y\rangle - |\psi_y\rangle \otimes |\psi_x\rangle) \end{aligned}$$

$$\begin{aligned} \text{Pr}(1) &= \frac{1}{4}(\langle\psi_x| \otimes \langle\psi_y| - \langle\psi_y| \otimes \langle\psi_x|)(|\psi_x\rangle \otimes |\psi_y\rangle - |\psi_y\rangle \otimes |\psi_x\rangle) = \\ &= \frac{1}{4}(2 - \langle\psi_x|\psi_y\rangle\langle\psi_y|\psi_x\rangle - \langle\psi_y|\psi_x\rangle\langle\psi_x|\psi_y\rangle) = \frac{1}{2} - \frac{1}{2}|\langle\psi_x|\psi_y\rangle|^2. \end{aligned}$$

Анализ протокола (продолжение)

Действия Чарли с заметной вероятностью обнаружат разницу в случае $x \neq y$. Вычисления:

$$\begin{aligned} &|0\rangle \otimes |\psi_x\rangle \otimes |\psi_y\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |\psi_x\rangle \otimes |\psi_y\rangle \\ &\xrightarrow{\text{c-SWAP}} \frac{1}{\sqrt{2}}|0\rangle \otimes |\psi_x\rangle \otimes |\psi_y\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes |\psi_y\rangle \otimes |\psi_x\rangle \\ &\xrightarrow{H} \frac{1}{2}(|0\rangle + |1\rangle) \otimes |\psi_x\rangle \otimes |\psi_y\rangle + \frac{1}{2}(|0\rangle - |1\rangle) \otimes |\psi_y\rangle \otimes |\psi_x\rangle = \\ &= \frac{1}{2}|0\rangle \otimes (|\psi_x\rangle \otimes |\psi_y\rangle + |\psi_y\rangle \otimes |\psi_x\rangle) + \frac{1}{2}|1\rangle \otimes (|\psi_x\rangle \otimes |\psi_y\rangle - |\psi_y\rangle \otimes |\psi_x\rangle) \end{aligned}$$

$$\begin{aligned} \Pr(1) &= \frac{1}{4}(\langle\psi_x| \otimes \langle\psi_y| - \langle\psi_y| \otimes \langle\psi_x|)(|\psi_x\rangle \otimes |\psi_y\rangle - |\psi_y\rangle \otimes |\psi_x\rangle) = \\ &= \frac{1}{4}(2 - \langle\psi_x|\psi_y\rangle\langle\psi_y|\psi_x\rangle - \langle\psi_y|\psi_x\rangle\langle\psi_x|\psi_y\rangle) = \frac{1}{2} - \frac{1}{2}|\langle\psi_x|\psi_y\rangle|^2. \end{aligned}$$

Анализ протокола (продолжение)

Действия Чарли с заметной вероятностью обнаружат разницу в случае $x \neq y$. Вычисления:

$$\begin{aligned} |0\rangle \otimes |\psi_x\rangle \otimes |\psi_y\rangle &\xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |\psi_x\rangle \otimes |\psi_y\rangle \\ &\xrightarrow{\text{c-SWAP}} \frac{1}{\sqrt{2}}|0\rangle \otimes |\psi_x\rangle \otimes |\psi_y\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes |\psi_y\rangle \otimes |\psi_x\rangle \\ &\xrightarrow{H} \frac{1}{2}(|0\rangle + |1\rangle) \otimes |\psi_x\rangle \otimes |\psi_y\rangle + \frac{1}{2}(|0\rangle - |1\rangle) \otimes |\psi_y\rangle \otimes |\psi_x\rangle = \\ &= \frac{1}{2}|0\rangle \otimes (|\psi_x\rangle \otimes |\psi_y\rangle + |\psi_y\rangle \otimes |\psi_x\rangle) + \frac{1}{2}|1\rangle \otimes (|\psi_x\rangle \otimes |\psi_y\rangle - |\psi_y\rangle \otimes |\psi_x\rangle) \end{aligned}$$

$$\begin{aligned} \Pr(1) &= \frac{1}{4}(\langle\psi_x| \otimes \langle\psi_y| - \langle\psi_y| \otimes \langle\psi_x|)(|\psi_x\rangle \otimes |\psi_y\rangle - |\psi_y\rangle \otimes |\psi_x\rangle) = \\ &= \frac{1}{4}(2 - \langle\psi_x|\psi_y\rangle\langle\psi_y|\psi_x\rangle - \langle\psi_y|\psi_x\rangle\langle\psi_x|\psi_y\rangle) = \frac{1}{2} - \frac{1}{2}|\langle\psi_x|\psi_y\rangle|^2. \end{aligned}$$

Анализ протокола (продолжение)

Действия Чарли с заметной вероятностью обнаружат разницу в случае $x \neq y$. Вычисления:

$$\begin{aligned} & |0\rangle \otimes |\psi_x\rangle \otimes |\psi_y\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |\psi_x\rangle \otimes |\psi_y\rangle \\ & \xrightarrow{\text{c-SWAP}} \frac{1}{\sqrt{2}}|0\rangle \otimes |\psi_x\rangle \otimes |\psi_y\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes |\psi_y\rangle \otimes |\psi_x\rangle \\ & \xrightarrow{H} \frac{1}{2}(|0\rangle + |1\rangle) \otimes |\psi_x\rangle \otimes |\psi_y\rangle + \frac{1}{2}(|0\rangle - |1\rangle) \otimes |\psi_y\rangle \otimes |\psi_x\rangle = \\ & = \frac{1}{2}|0\rangle \otimes (|\psi_x\rangle \otimes |\psi_y\rangle + |\psi_y\rangle \otimes |\psi_x\rangle) + \frac{1}{2}|1\rangle \otimes (|\psi_x\rangle \otimes |\psi_y\rangle - |\psi_y\rangle \otimes |\psi_x\rangle) \end{aligned}$$

$$\begin{aligned} \Pr(1) &= \frac{1}{4}(\langle\psi_x| \otimes \langle\psi_y| - \langle\psi_y| \otimes \langle\psi_x|)(|\psi_x\rangle \otimes |\psi_y\rangle - |\psi_y\rangle \otimes |\psi_x\rangle) = \\ &= \frac{1}{4}(2 - \langle\psi_x|\psi_y\rangle\langle\psi_y|\psi_x\rangle - \langle\psi_y|\psi_x\rangle\langle\psi_x|\psi_y\rangle) = \frac{1}{2} - \frac{1}{2}|\langle\psi_x|\psi_y\rangle|^2. \end{aligned}$$

Анализ протокола (продолжение)

Действия Чарли с заметной вероятностью обнаружат разницу в случае $x \neq y$. Вычисления:

$$\begin{aligned} & |0\rangle \otimes |\psi_x\rangle \otimes |\psi_y\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |\psi_x\rangle \otimes |\psi_y\rangle \\ & \xrightarrow{\text{c-SWAP}} \frac{1}{\sqrt{2}}|0\rangle \otimes |\psi_x\rangle \otimes |\psi_y\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes |\psi_y\rangle \otimes |\psi_x\rangle \\ & \xrightarrow{H} \frac{1}{2}(|0\rangle + |1\rangle) \otimes |\psi_x\rangle \otimes |\psi_y\rangle + \frac{1}{2}(|0\rangle - |1\rangle) \otimes |\psi_y\rangle \otimes |\psi_x\rangle = \\ & = \frac{1}{2}|0\rangle \otimes (|\psi_x\rangle \otimes |\psi_y\rangle + |\psi_y\rangle \otimes |\psi_x\rangle) + \frac{1}{2}|1\rangle \otimes (|\psi_x\rangle \otimes |\psi_y\rangle - |\psi_y\rangle \otimes |\psi_x\rangle) \end{aligned}$$

$$\begin{aligned} \Pr(1) &= \frac{1}{4}(\langle\psi_x| \otimes \langle\psi_y| - \langle\psi_y| \otimes \langle\psi_x|)(|\psi_x\rangle \otimes |\psi_y\rangle - |\psi_y\rangle \otimes |\psi_x\rangle) = \\ &= \frac{1}{4}(2 - \langle\psi_x|\psi_y\rangle\langle\psi_y|\psi_x\rangle - \langle\psi_y|\psi_x\rangle\langle\psi_x|\psi_y\rangle) = \frac{1}{2} - \frac{1}{2}|\langle\psi_x|\psi_y\rangle|^2. \end{aligned}$$

Анализ протокола (продолжение)

Действия Чарли с заметной вероятностью обнаружат разницу в случае $x \neq y$. Вычисления:

$$\begin{aligned} &|0\rangle \otimes |\psi_x\rangle \otimes |\psi_y\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |\psi_x\rangle \otimes |\psi_y\rangle \\ &\xrightarrow{\text{c-SWAP}} \frac{1}{\sqrt{2}}|0\rangle \otimes |\psi_x\rangle \otimes |\psi_y\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes |\psi_y\rangle \otimes |\psi_x\rangle \\ &\xrightarrow{H} \frac{1}{2}(|0\rangle + |1\rangle) \otimes |\psi_x\rangle \otimes |\psi_y\rangle + \frac{1}{2}(|0\rangle - |1\rangle) \otimes |\psi_y\rangle \otimes |\psi_x\rangle = \\ &= \frac{1}{2}|0\rangle \otimes (|\psi_x\rangle \otimes |\psi_y\rangle + |\psi_y\rangle \otimes |\psi_x\rangle) + \frac{1}{2}|1\rangle \otimes (|\psi_x\rangle \otimes |\psi_y\rangle - |\psi_y\rangle \otimes |\psi_x\rangle) \end{aligned}$$

$$\begin{aligned} \Pr(1) &= \frac{1}{4}(\langle\psi_x| \otimes \langle\psi_y| - \langle\psi_y| \otimes \langle\psi_x|)(|\psi_x\rangle \otimes |\psi_y\rangle - |\psi_y\rangle \otimes |\psi_x\rangle) = \\ &= \frac{1}{4}(2 - \langle\psi_x|\psi_y\rangle\langle\psi_y|\psi_x\rangle - \langle\psi_y|\psi_x\rangle\langle\psi_x|\psi_y\rangle) = \frac{1}{2} - \frac{1}{2}|\langle\psi_x|\psi_y\rangle|^2. \end{aligned}$$

Анализ протокола (продолжение)

Действия Чарли с заметной вероятностью обнаружат разницу в случае $x \neq y$. Вычисления:

$$\begin{aligned} &|0\rangle \otimes |\psi_x\rangle \otimes |\psi_y\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |\psi_x\rangle \otimes |\psi_y\rangle \\ &\xrightarrow{\text{c-SWAP}} \frac{1}{\sqrt{2}}|0\rangle \otimes |\psi_x\rangle \otimes |\psi_y\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes |\psi_y\rangle \otimes |\psi_x\rangle \\ &\xrightarrow{H} \frac{1}{2}(|0\rangle + |1\rangle) \otimes |\psi_x\rangle \otimes |\psi_y\rangle + \frac{1}{2}(|0\rangle - |1\rangle) \otimes |\psi_y\rangle \otimes |\psi_x\rangle = \\ &= \frac{1}{2}|0\rangle \otimes (|\psi_x\rangle \otimes |\psi_y\rangle + |\psi_y\rangle \otimes |\psi_x\rangle) + \frac{1}{2}|1\rangle \otimes (|\psi_x\rangle \otimes |\psi_y\rangle - |\psi_y\rangle \otimes |\psi_x\rangle) \end{aligned}$$

$$\begin{aligned} \Pr(1) &= \frac{1}{4}(\langle\psi_x| \otimes \langle\psi_y| - \langle\psi_y| \otimes \langle\psi_x|)(|\psi_x\rangle \otimes |\psi_y\rangle - |\psi_y\rangle \otimes |\psi_x\rangle) = \\ &= \frac{1}{4}(2 - \langle\psi_x|\psi_y\rangle\langle\psi_y|\psi_x\rangle - \langle\psi_y|\psi_x\rangle\langle\psi_x|\psi_y\rangle) = \frac{1}{2} - \frac{1}{2}|\langle\psi_x|\psi_y\rangle|^2. \end{aligned}$$

- Итак, вероятность наблюдения 1 равна

$$\Pr(1) = \frac{1}{2} - \frac{1}{2} |\langle \psi_x | \psi_y \rangle|^2$$

- Если $x = y$, то вероятность измерения 1 равна 0.
- Если $x \neq y$ то вероятность измерения 1 больше $\frac{1}{2} - \frac{1}{2}(1 - \delta)^2 = \delta - \delta^2/2 > 1/5$.
- Чтобы достичь сколь угодно малой ошибки, Алиса и Боб должны приготовить несколько сообщений такого вида, а Чарли должен их обработать независимо и сказать « $x \neq y$ », если хотя бы один из наблюдаемых исходов равен 1.

Анализ протокола (окончание)

- Итак, вероятность наблюдения 1 равна

$$\Pr(1) = \frac{1}{2} - \frac{1}{2} |\langle \psi_x | \psi_y \rangle|^2$$

- Если $x = y$, то вероятность измерения 1 равна 0.
- Если $x \neq y$ то вероятность измерения 1 больше $\frac{1}{2} - \frac{1}{2}(1 - \delta)^2 = \delta - \delta^2/2 > 1/5$.
- Чтобы достичь сколь угодно малой ошибки, Алиса и Боб должны приготовить несколько сообщений такого вида, а Чарли должен их обработать независимо и сказать « $x \neq y$ », если хотя бы один из наблюдаемых исходов равен 1.

- Итак, вероятность наблюдения 1 равна

$$\Pr(1) = \frac{1}{2} - \frac{1}{2} |\langle \psi_x | \psi_y \rangle|^2$$

- Если $x = y$, то вероятность измерения 1 равна 0.
- Если $x \neq y$ то вероятность измерения 1 больше $\frac{1}{2} - \frac{1}{2}(1 - \delta)^2 = \delta - \delta^2/2 > 1/5$.
- Чтобы достичь сколь угодно малой ошибки, Алиса и Боб должны приготовить несколько сообщений такого вида, а Чарли должен их обработать независимо и сказать « $x \neq y$ », если хотя бы один из наблюдаемых исходов равен 1.

- Итак, вероятность наблюдения 1 равна

$$\Pr(1) = \frac{1}{2} - \frac{1}{2} |\langle \psi_x | \psi_y \rangle|^2$$

- Если $x = y$, то вероятность измерения 1 равна 0.
- Если $x \neq y$ то вероятность измерения 1 больше $\frac{1}{2} - \frac{1}{2}(1 - \delta)^2 = \delta - \delta^2/2 > 1/5$.
- Чтобы достичь сколь угодно малой ошибки, Алиса и Боб должны приготовить несколько сообщений такого вида, а Чарли должен их обработать независимо и сказать « $x \neq y$ », если хотя бы один из наблюдаемых исходов равен 1.

- 1 Нижние оценки квантовой коммуникационной сложности
- 2 Нижняя оценка для функции пересечения множеств
- 3 Модель коммуникации SMP
- 4 Квантовая (псевдо-)телепатия

Игра Мермина

УСЛОВИЯ: Алиса, Боб и Чарли рассаживаются по хорошо изолированным камерам. Каждый из них получает один бит: x_a , x_b , x_c . Им заранее известно, что либо ровно два значения из выданных битов равны 1, либо все биты равны 0. Другими словами,

$$x_a + x_b + x_c \equiv 0 \pmod{2}.$$

Каждый из игроков должен сообщить один бит: y_a , y_b , y_c .

ЦЕЛЬ: Игроки выигрывают, если

$$y_a + y_b + y_c \equiv (x_a + x_b + x_c)/2 \pmod{2}.$$

Задача

- (i) Докажите, что не существует вероятностной стратегии в игре Мермина, которая гарантировала бы (с вероятностью 1) победу игроков, даже если они используют общий генератор случайности.
- (ii) Постройте стратегию с общим генератором случайности, при которой вероятность выигрыша $3/4$.

Игра Мермина

УСЛОВИЯ: Алиса, Боб и Чарли рассаживаются по хорошо изолированным камерам. Каждый из них получает один бит: x_a , x_b , x_c . Им заранее известно, что либо ровно два значения из выданных битов равны 1, либо все биты равны 0. Другими словами,

$$x_a + x_b + x_c \equiv 0 \pmod{2}.$$

Каждый из игроков должен сообщить один бит: y_a , y_b , y_c .

ЦЕЛЬ: Игроки выигрывают, если

$$y_a + y_b + y_c \equiv (x_a + x_b + x_c)/2 \pmod{2}.$$

Задача

- (i) Докажите, что не существует вероятностной стратегии в игре Мермина, которая гарантировала бы (с вероятностью 1) победу игроков, даже если они используют общий генератор случайности.
- (ii) Постройте стратегию с общим генератором случайности, при которой вероятность выигрыша $3/4$.

Игра Мермина

УСЛОВИЯ: Алиса, Боб и Чарли рассаживаются по хорошо изолированным камерам. Каждый из них получает один бит: x_a , x_b , x_c . Им заранее известно, что либо ровно два значения из выданных битов равны 1, либо все биты равны 0. Другими словами,

$$x_a + x_b + x_c \equiv 0 \pmod{2}.$$

Каждый из игроков должен сообщить один бит: y_a , y_b , y_c .

ЦЕЛЬ: Игроки выигрывают, если

$$y_a + y_b + y_c \equiv (x_a + x_b + x_c)/2 \pmod{2}.$$

Задача

- (i) Докажите, что не существует вероятностной стратегии в игре Мермина, которая гарантировала бы (с вероятностью 1) победу игроков, даже если они используют общий генератор случайности.
- (ii) Постройте стратегию с общим генератором случайности, при которой вероятность выигрыша $3/4$.

Как победить в игре Мермина

- 1 Используется предварительная сцепленность. До того, как игроков рассадили по камерам, они готовят состояние GHZ

$$\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$

и забирают с собой в камеру по одному из кубитов.

- 2 Получив бит x , игрок применяет условный фазовый сдвиг к своему кубиту:

$$S: |0\rangle \mapsto |0\rangle, \quad S: |1\rangle \mapsto i^x |1\rangle,$$

- 3 затем применяет преобразование Адамара H ,
- 4 после чего производит измерение своего кубита и сообщает наблюдаемый исход.

Как победить в игре Мермина

- 1 Используется предварительная сцепленность. До того, как игроков рассадили по камерам, они готовят состояние GHZ

$$\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$

и забирают с собой в камеру по одному из кубитов.

- 2 Получив бит x , игрок применяет условный фазовый сдвиг к своему кубиту:

$$S: |0\rangle \mapsto |0\rangle, \quad S: |1\rangle \mapsto i^x |1\rangle,$$

- 3 затем применяет преобразование Адамара H ,
- 4 после чего производит измерение своего кубита и сообщает наблюдаемый исход.

Как победить в игре Мермина

- 1 Используется предварительная сцепленность. До того, как игроков рассадили по камерам, они готовят состояние GHZ

$$\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$

и забирают с собой в камеру по одному из кубитов.

- 2 Получив бит x , игрок применяет условный фазовый сдвиг к своему кубиту:

$$S: |0\rangle \mapsto |0\rangle, \quad S: |1\rangle \mapsto i^x |1\rangle,$$

- 3 затем применяет преобразование Адамара H ,
- 4 после чего производит измерение своего кубита и сообщает наблюдаемый исход.

Как победить в игре Мермина

- 1 Используется предварительная сцепленность. До того, как игроков рассадили по камерам, они готовят состояние GHZ

$$\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$

и забирают с собой в камеру по одному из кубитов.

- 2 Получив бит x , игрок применяет условный фазовый сдвиг к своему кубиту:

$$S: |0\rangle \mapsto |0\rangle, \quad S: |1\rangle \mapsto i^x |1\rangle,$$

- 3 затем применяет преобразование Адамара H ,
- 4 после чего производит измерение своего кубита и сообщает наблюдаемый исход.

Почему это работает?

Перед условным фазовым сдвигом состояние трех кубитов:

$$\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle).$$

После условного фазового сдвига оно изменяется на

$$\begin{aligned} \frac{1}{\sqrt{2}}(|000\rangle + i^{x_a+x_b+x_c}|111\rangle) = \\ = \begin{cases} \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle), & \text{если } x_a + x_b + x_c = 0 \text{ (случай (ч))}; \\ \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle), & \text{если } x_a + x_b + x_c = 2 \text{ (случай (н))}. \end{cases} \end{aligned}$$

Задача

Проверьте, что после применения преобразования Адамара к каждому из кубитов в случае (ч) получается сумма базисных состояний с четным числом единиц, а в случае (н) — с нечетным числом единиц.

Почему это работает?

Перед условным фазовым сдвигом состояние трех кубитов:

$$\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle).$$

После условного фазового сдвига оно изменяется на

$$\begin{aligned} \frac{1}{\sqrt{2}}(|000\rangle + i^{x_a+x_b+x_c}|111\rangle) = \\ = \begin{cases} \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle), & \text{если } x_a + x_b + x_c = 0 \text{ (случай (ч))}; \\ \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle), & \text{если } x_a + x_b + x_c = 2 \text{ (случай (н))}. \end{cases} \end{aligned}$$

Задача

Проверьте, что после применения преобразования Адамара к каждому из кубитов в случае (ч) получается сумма базисных состояний с четным числом единиц, а в случае (н) — с нечетным числом единиц.

Почему это работает?

Перед условным фазовым сдвигом состояние трех кубитов:

$$\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle).$$

После условного фазового сдвига оно изменяется на

$$\begin{aligned} \frac{1}{\sqrt{2}}(|000\rangle + i^{x_a+x_b+x_c}|111\rangle) = \\ = \begin{cases} \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle), & \text{если } x_a + x_b + x_c = 0 \text{ (случай (ч))}; \\ \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle), & \text{если } x_a + x_b + x_c = 2 \text{ (случай (н))}. \end{cases} \end{aligned}$$

Задача

Проверьте, что после применения преобразования Адамара к каждому из кубитов в случае (ч) получается сумма базисных состояний с четным числом единиц, а в случае (н) — с нечетным числом единиц.