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

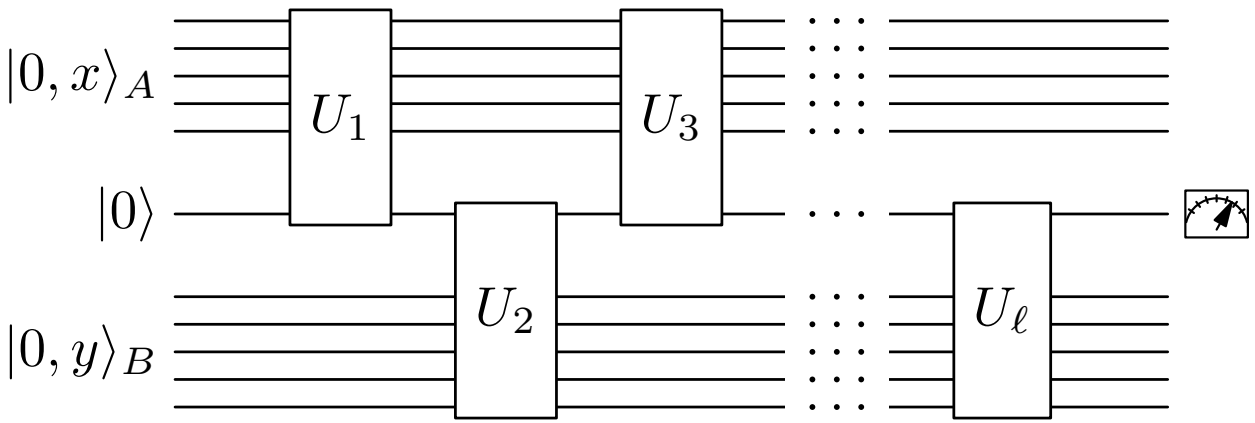
М. Вялый

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

Санкт-Петербург, 2011

План

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 $|\alpha_m| \leqslant 1$, $|\beta_m| \leqslant 1$, 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:

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

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

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

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:

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

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

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

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:

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

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

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

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:

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

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

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

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:

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

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

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

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:

$$U_{\ell+1}|\alpha_m\rangle_A \otimes |m_\ell\rangle = |\alpha'_{m0}\rangle \otimes |0\rangle + |\alpha'_{m1}\rangle \otimes |1\rangle,$$
$$|\alpha'_{m0}|^2 + |\alpha'_{m1}|^2 = |\alpha_m|^2 \leqslant 1,$$
$$U_{\ell+1}|\psi\rangle = \sum_{m\in\{0,1\}^{\ell+1}} |\alpha'_m\rangle_A \otimes |m_{\ell+1}\rangle \otimes |\beta'_m\rangle_B,$$

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:

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

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

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

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:

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

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

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

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

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

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

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

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; $x \in X$, $y \in Y$.

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

Лемма

Для протокола длины ℓ выполняется

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

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

Разложение Яо – Кремера $|\psi\rangle = \sum\limits_{m\in\{0,1\}^\ell} |\alpha_m\rangle_A \otimes |m_\ell\rangle \otimes |\beta_m\rangle_B =$

$$= \sum_{m\in\{0,1\}^{\ell-1}} |\alpha_{m0}\rangle_A \otimes |0\rangle \otimes |\beta_{m0}\rangle_B + \sum_{m\in\{0,1\}^{\ell-1}} |\alpha_{m1}\rangle_A \otimes |1\rangle \otimes |\beta_{m1}\rangle_B \quad (*)$$

Лемма

Для протокола длины ℓ выполняется

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

Доказательство

Из $(*)$ вероятность наблюдения исхода 1

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

Матричные нормы

- Скалярное произведение операторов (произведение Фробениуса):
$$\langle A, B \rangle = \mathrm{Tr}(A^\dagger B)$$
- Норма Фробениуса
$$\|A\|_F = \sqrt{\langle A, A \rangle}$$
- Операторная норма
$$\|A\| = \max_{x:|x|=1} |Ax|$$
- Следовая норма
$$\|A\|_{\mathrm{tr}} = \max_{\|X\|=1} \left|\langle A, X \rangle\right|$$

Утверждение

Норма Фробениуса, операторная норма и следовая норма удовлетворяют свойствам нормы:
(1) $\|x\| \geqslant 0$; (2) $\|\lambda x\| = |\lambda| \cdot \|x\|$; (3) $\|x + y\| \leqslant \|x\| + \|y\|$.

Матричные нормы

- Скалярное произведение операторов (произведение Фробениуса):
$$\langle A, B\rangle = \mathrm{Tr}(A^\dagger B)$$
- Норма Фробениуса
$$\|A\|_F = \sqrt{\langle A, A\rangle}$$
- Операторная норма
$$\|A\| = \max_{x:|x|=1} |Ax|$$
- Следовая норма
$$\|A\|_{\mathrm{tr}} = \max_{\|X\|=1} \left|\langle A, X\rangle\right|$$

Утверждение

Норма Фробениуса, операторная норма и следовая норма удовлетворяют свойствам нормы:
(1) $\|x\| \geqslant 0$; (2) $\|\lambda x\| = |\lambda| \cdot \|x\|$; (3) $\|x + y\| \leqslant \|x\| + \|y\|$.

Матричные нормы

- Скалярное произведение операторов (произведение Фробениуса):
$$\langle A, B\rangle = \mathrm{Tr}(A^\dagger B)$$
- Норма Фробениуса
$$\|A\|_F = \sqrt{\langle A, A\rangle}$$
- Операторная норма
$$\|A\| = \max_{x:|x|=1} |Ax|$$
- Следовая норма
$$\|A\|_{\mathrm{tr}} = \max_{\|X\|=1} \left|\langle A, X\rangle\right|$$

Утверждение

Норма Фробениуса, операторная норма и следовая норма удовлетворяют свойствам нормы:
(1) $\|x\| \geqslant 0$; (2) $\|\lambda x\| = |\lambda| \cdot \|x\|$; (3) $\|x + y\| \leqslant \|x\| + \|y\|$.

Матричные нормы

- Скалярное произведение операторов (произведение Фробениуса):
$$\langle A, B\rangle = \mathrm{Tr}(A^\dagger B)$$
- Норма Фробениуса
$$\|A\|_F = \sqrt{\langle A, A\rangle}$$
- Операторная норма
$$\|A\| = \max_{x:|x|=1} |Ax|$$
- Следовая норма
$$\|A\|_{\mathrm{tr}} = \max_{\|X\|=1} \left|\langle A, X\rangle\right|$$

Утверждение

Норма Фробениуса, операторная норма и следовая норма удовлетворяют свойствам нормы:
(1) $\|x\| \geqslant 0$; (2) $\|\lambda x\| = |\lambda| \cdot \|x\|$; (3) $\|x + y\| \leqslant \|x\| + \|y\|$.

Матричные нормы

- Скалярное произведение операторов (произведение Фробениуса):
$$\langle A, B\rangle = \mathrm{Tr}(A^\dagger B)$$
- Норма Фробениуса
$$\|A\|_F = \sqrt{\langle A, A\rangle}$$
- Операторная норма
$$\|A\| = \max_{x:|x|=1} |Ax|$$
- Следовая норма
$$\|A\|_{\mathrm{tr}} = \max_{\|X\|=1} \left|\langle A, X\rangle\right|$$

Утверждение

Норма Фробениуса, операторная норма и следовая норма удовлетворяют свойствам нормы:
(1) $\|x\| \geqslant 0$; (2) $\|\lambda x\| = |\lambda| \cdot \|x\|$; (3) $\|x + y\| \leqslant \|x\| + \|y\|$.

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,
$s_k \geqslant 0$ — 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,
$s_k \geqslant 0$ — 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,
$s_k \geqslant 0$ — 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.

Свойства следовой нормы

Утверждение

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

Доказательство

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

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

С другой стороны,

$$|\mathrm{Tr}(A^\dagger X)| \leqslant \sum_k s_k |\mathrm{Tr}(|\psi_k\rangle\langle\xi_k| X)| = \sum_k s_k |\mathrm{Tr}(\xi_k X \psi_k)| =$$

$$= \sum_k s_k |(\xi_k, X\psi_k)| \leqslant \sum_k s_k \|\xi_k\| \cdot \|X\psi_k\| \leqslant$$

Свойства следовой нормы

Утверждение

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

Доказательство

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

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

С другой стороны,

$$\left|\mathrm{Tr}(A^\dagger X)\right| \leqslant \sum_k s_k \left|\mathrm{Tr}(|\psi_k\rangle\langle\xi_k|X)\right| = \sum_k s_k \left|\mathrm{Tr}(\langle\xi_k|X|\psi_k\rangle)\right| =$$

$$= \sum_k s_k \left|\langle\xi_k|X|\psi_k\rangle\right| \leqslant \sum_k s_k |X|\psi_k\rangle| \leqslant \|X\| \sum_k s_k.$$

Свойства следовой нормы

Утверждение

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

Доказательство

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

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

С другой стороны,

$$\left|\mathrm{Tr}(A^\dagger X)\right| \leqslant \sum_k s_k \left|\mathrm{Tr}(|\psi_k\rangle\langle\xi_k|X)\right| = \sum_k s_k \left|\mathrm{Tr}(\langle\xi_k|X|\psi_k\rangle)\right| =$$

$$= \sum_k s_k \left|\langle\xi_k|X|\psi_k\rangle\right| \leqslant \sum_k s_k |X|\psi_k\rangle| \leqslant \|X\| \sum_k s_k.$$

Свойства следовой нормы

Утверждение

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

Доказательство

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

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

С другой стороны,

$$\left|\mathrm{Tr}(A^\dagger X)\right| \leqslant \sum_k s_k \left|\mathrm{Tr}(|\psi_k\rangle\langle\xi_k|X)\right| = \sum_k s_k \left|\mathrm{Tr}(\langle\xi_k|X|\psi_k\rangle)\right| =$$

$$= \sum_k s_k \left|\langle\xi_k|X|\psi_k\rangle\right| \leqslant \sum_k s_k \left|X|\psi_k\rangle\right| \leqslant \|X\| \sum_k s_k.$$

Оценка следовой нормы матрицы P

Лемма

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

Доказательство

Из предыдущей леммы

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

Введем векторы $a_x = (a_{x,k})$, $b_y = (b_{y,k})$. Тогда $P = \sum_k$ [illegible]

$\|P\|_{\mathrm{tr}}$ [illegible]

Оценка следовой нормы матрицы P

Лемма

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

Доказательство

Из предыдущей леммы

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

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

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

Оценка следовой нормы матрицы P

Лемма

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

Доказательство

Из предыдущей леммы

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

Введем векторы $a_k = (a_{x,k})$, $b_k = (b^*_{y,k})$. Тогда $P = \sum_k |a_k\rangle\langle b_k|$ и

$$\|P\|_{\mathrm{tr}} \leqslant \sum_{k=0}^{2^{2\ell-2}-1} \||a_k\rangle\langle b_k|\|_{\mathrm{tr}} = \sum_{k=0}^{2^{2\ell-2}-1} \|a_k\|\cdot\|b_k\|$$

Оценка следовой нормы матрицы P

Лемма

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

Доказательство

Из предыдущей леммы

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

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

$$\|P\|_{\mathrm{tr}} \leqslant \sum_{k=0}^{2^{2\ell-2}-1} \||a_k\rangle\langle b_k|\|_{\mathrm{tr}} = \sum_{k=0}^{2^{2\ell-2}-1} \|a_k\|\cdot\|b_k\| \leqslant 2^{2\ell-2}\sqrt{|X|\cdot|Y|}.$$

Оценка следовой нормы матрицы P

Лемма

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

Доказательство

Из предыдущей леммы

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

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

$$\|P\|_{\mathrm{tr}} \leqslant \sum_{k=0}^{2^{2\ell-2}-1} \big\||\boldsymbol{a}_k\rangle\langle\boldsymbol{b}_k|\big\|_{\mathrm{tr}} = \sum_{k=0}^{2^{2\ell-2}-1} |\boldsymbol{a}_k|\cdot|\boldsymbol{b}_k| \leqslant 2^{2\ell-2}\sqrt{|X|\cdot|Y|}.$$

Оценка следовой нормы матрицы P

Лемма

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

Доказательство

Из предыдущей леммы

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

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

$$\|P\|_{\mathrm{tr}} \leqslant \sum_{k=0}^{2^{2\ell-2}-1} \big\||\boldsymbol{a}_k\rangle\langle\boldsymbol{b}_k|\big\|_{\mathrm{tr}} = \sum_{k=0}^{2^{2\ell-2}-1} |\boldsymbol{a}_k|\cdot|\boldsymbol{b}_k| \leqslant 2^{2\ell-2}\sqrt{|X|\cdot|Y|}.$$

Оценка следовой нормы матрицы P

Лемма

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

Доказательство

Из предыдущей леммы

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

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

$$\|P\|_{\mathrm{tr}} \leqslant \sum_{k=0}^{2^{2\ell-2}-1} \big\||\boldsymbol{a}_k\rangle\langle\boldsymbol{b}_k|\big\|_{\mathrm{tr}} = \sum_{k=0}^{2^{2\ell-2}-1} |\boldsymbol{a}_k|\cdot|\boldsymbol{b}_k| \leqslant 2^{2\ell-2}\sqrt{|X|\cdot|Y|}.$$

Оценка следовой нормы матрицы P

Лемма

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

Доказательство

Из предыдущей леммы

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

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

$$\|P\|_{\mathrm{tr}} \leqslant \sum_{k=0}^{2^{2\ell-2}-1} \big\||\boldsymbol{a}_k\rangle\langle\boldsymbol{b}_k|\big\|_{\mathrm{tr}} = \sum_{k=0}^{2^{2\ell-2}-1} |\boldsymbol{a}_k|\cdot|\boldsymbol{b}_k| \leqslant 2^{2\ell-2}\sqrt{|X|\cdot|Y|}.$$

Пример: нижняя оценка для скалярного произведения

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

Утверждение

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

Эскиз доказательства

Пример: нижняя оценка для скалярного произведения

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

Утверждение

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

Эскиз доказательства

Пример: нижняя оценка для скалярного произведения

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

Утверждение

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

Эскиз доказательства

Полагаем $X = Y = \{0, 1\}^n$.

Пример: нижняя оценка для скалярного произведения

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

Утверждение

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

Эскиз доказательства

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

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

Пример: нижняя оценка для скалярного произведения

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

Утверждение

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

Эскиз доказательства

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

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

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

Утверждение

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

Эскиз доказательства

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

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

Пример: нижняя оценка для скалярного произведения

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

Утверждение

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

Эскиз доказательства

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

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

Но $\|M\| = 2^{n/2}$ (упражнение) и

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

Пример: нижняя оценка для скалярного произведения

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

Утверждение

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

Эскиз доказательства

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

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

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

Окончательно,

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

План

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

- Выбираем $X = Y = \binom{n}{n/4}$ — множество слов длины n веса $n/4$ (вес — количество единиц).
- Подбираем такие матрицы μ_s, $0 \leqslant s \leqslant n/4$, что
  1. $\langle P, \mu_0 \rangle \in (2/3; 1]$, а $\langle P, \mu_s \rangle \in [0; 1/3)$ для $s = 1, \ldots, n/4$;
  2. для любого $d < n/4$ существует многочлен p степени d такой, что
$$|p(s) - \langle P, \mu_s \rangle| \leqslant \frac{\|P\|_\infty}{\binom{n}{n/4} 2^{2d/4}} \quad \text{для } 0 \leqslant s \leqslant n/4.$$
- Для $d = 8\ell + 8$ из леммы о следовой норме матрицы положительных ответов получаем
$$|p(s) - \langle P, \mu_s \rangle| \leqslant \frac{2^{2\ell-2}\binom{n}{n/4}}{\binom{n}{n/4} 2^{2\ell-2}} = \frac{1}{2^4}.$$
- Поэтому к многочлену p можно применить теорему о нижней оценке степени многочлена.
- Значит, $d = \Omega(\sqrt{n})$ и $\ell = \Omega(\sqrt{n})$.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- 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

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

Матрица μ_s соответствует случайному выбору пары x, y с заданным размером пересечения s.
Поэтому для протокола, вычисляющего $\mathrm{DISJ}(x,y)$, выполняется условие 1:

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

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

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

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

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

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

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

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

Матрица μ_s соответствует случайному выбору пары x, y с заданным размером пересечения s.
Поэтому для протокола, вычисляющего $\mathrm{DISJ}(x,y)$, выполняется условие 1:

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

Алгебраическая комбинаторика

- 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 $k \leqslant n/4$ и $s \leqslant k/2$ выполняется неравенство

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

Алгебраическая комбинаторика

- Матрицы $J_{n,k,s}$ попарно коммутируют.
- Поэтому у них есть общая система собственных пространств $E_0, \ldots, E_k$.
- 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 $k \leqslant n/4$ и $s \leqslant k/2$ выполняется неравенство

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

Алгебраическая комбинаторика

- Матрицы $J_{n,k,s}$ попарно коммутируют.
- Поэтому у них есть общая система собственных пространств $E_0, \ldots, E_k$.
- 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 $k \leqslant n/4$ и $s \leqslant k/2$ выполняется неравенство

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

Алгебраическая комбинаторика

- 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 $k \leqslant n/4$ и $s \leqslant k/2$ выполняется неравенство

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

Алгебраическая комбинаторика

- 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 $k \leqslant n/4$ и $s \leqslant k/2$ выполняется неравенство

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

Алгебраическая комбинаторика (окончание)

Задача

Выведите из этих свойств условие 2:
для любого $d \leqslant n/4$ существует многочлен p степени d такой, что

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

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

План

Коммуникационная сложность проверки равенства

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

Коммуникационная сложность в основной модели

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

Коммуникационная сложность в модели SMP

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

Коммуникационная сложность проверки равенства

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

Коммуникационная сложность в основной модели

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

Коммуникационная сложность в модели SMP

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

Коммуникационная сложность проверки равенства

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

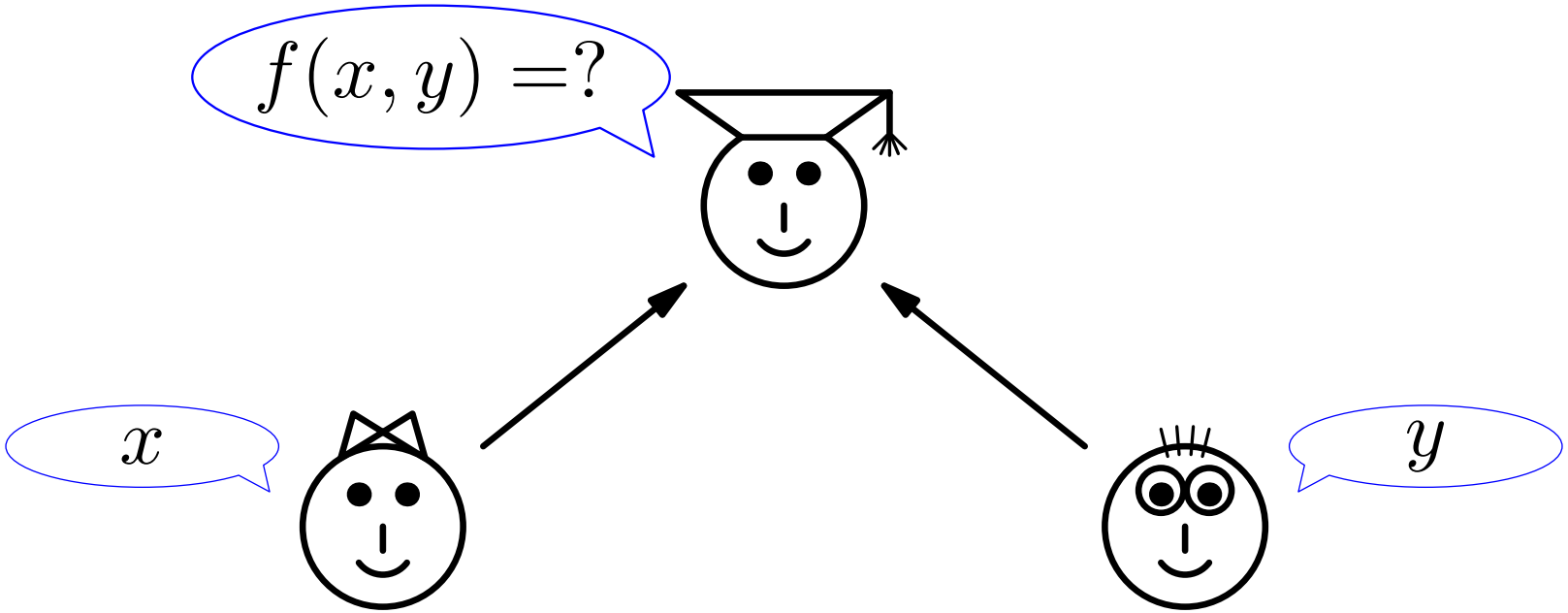
Коммуникационная сложность в основной модели

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

Коммуникационная сложность в модели SMP

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

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).

Хорошие коды

Определение

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

- $|C_n| \geqslant 2^{rn}$;
- $\|x \oplus y\| \geqslant \delta n$ 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

Определение

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

- $|C_n| \geqslant 2^{rn}$;
- $\|x \oplus y\| \geqslant \delta n$ 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

Определение

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

- $|C_n| \geqslant 2^{rn}$;
- $\|x \oplus y\| \geqslant \delta n$ 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

Определение

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

- $|C_n| \geqslant 2^{rn}$;
- $\|x \oplus y\| \geqslant \delta n$ 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 $R_\varepsilon(\mathrm{EQ}) = O(\log n)$.

Задача

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

Однако:

$R_\varepsilon^{\mathrm{SMP}}(\mathrm{EQ}) = \Omega(\sqrt{n})$

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

Квантовые сообщения экспоненциально эффективнее:

$Q_\varepsilon^{\mathrm{SMP}}(\mathrm{EQ}) = O(\log n)$

Хорошие коды помогают вычислять EQ

Задача

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

Задача

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

Однако:

$R_\varepsilon^{\mathrm{SMP}}(\mathrm{EQ}) = \Omega(\sqrt{n})$

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

Квантовые сообщения экспоненциально эффективнее:

$Q_\varepsilon^{\mathrm{SMP}}(\mathrm{EQ}) = O(\log n)$

Хорошие коды помогают вычислять EQ

Задача

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

Задача

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

Однако:

$R_\varepsilon^{\mathrm{SMP}}(\mathrm{EQ}) = \Omega(\sqrt{n})$

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

Квантовые сообщения экспоненциально эффективнее:

$Q_\varepsilon^{\mathrm{SMP}}(\mathrm{EQ}) = O(\log n)$

Хорошие коды помогают вычислять EQ

Задача

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

Задача

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

Однако:

$R_\varepsilon^{\mathrm{SMP}}(\mathrm{EQ}) = \Omega(\sqrt{n})$
(Babai, Kimmel, 1996: в SMP модели разрыв между вероятностной и детерминированной коммуникационной сложностью не более чем квадратичный.)

Квантовые сообщения экспоненциально эффективнее:

$Q_\varepsilon^{\mathrm{SMP}}(\mathrm{EQ}) = O(\log n)$

Хорошие коды помогают вычислять EQ

Задача

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

Задача

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

Однако:

$R_\varepsilon^{\mathrm{SMP}}(\mathrm{EQ}) = \Omega(\sqrt{n})$
(Babai, Kimmel, 1996: в SMP модели разрыв между вероятностной и детерминированной коммуникационной сложностью не более чем квадратичный.)

Квантовые сообщения экспоненциально эффективнее:

$Q_\varepsilon^{\mathrm{SMP}}(\mathrm{EQ}) = O(\log n)$

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)

$$c_n \colon \{0,1\}^n \to C_{n/r}.$$

Алиса готовит сообщение (Боб действует аналогично):

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

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

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)

$$c_n \colon \{0,1\}^n \to C_{n/r}.$$

Алиса готовит сообщение (Боб действует аналогично):

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

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

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)

$$c_n \colon \{0,1\}^n \to C_{n/r}.$$

Алиса готовит сообщение (Боб действует аналогично):

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

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

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)

$$c_n \colon \{0,1\}^n \to C_{n/r}.$$

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)

$$c_n \colon \{0,1\}^n \to C_{n/r}.$$

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).

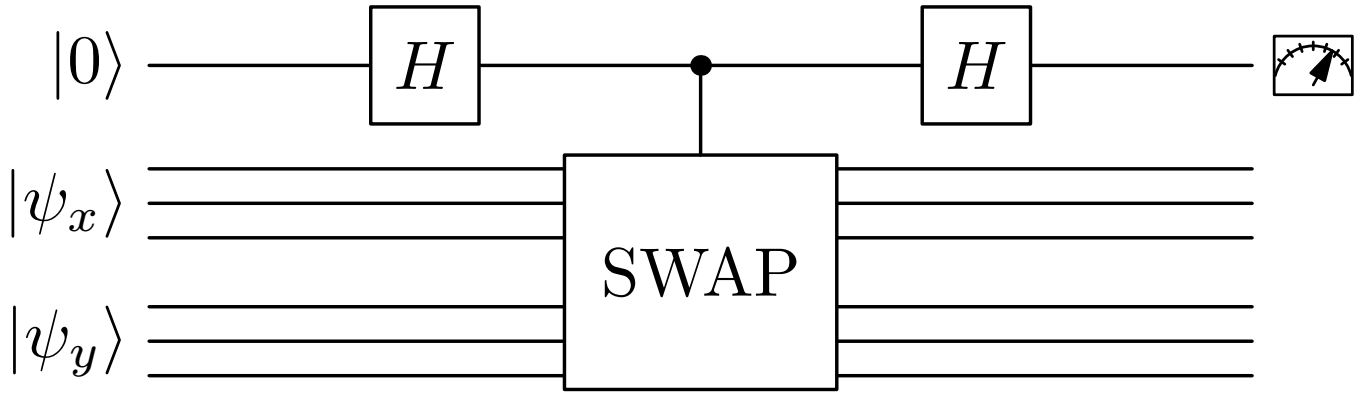
Вычисление EQ в модели SMP: действия Чарли

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

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

Вычисление EQ в модели SMP: действия Чарли

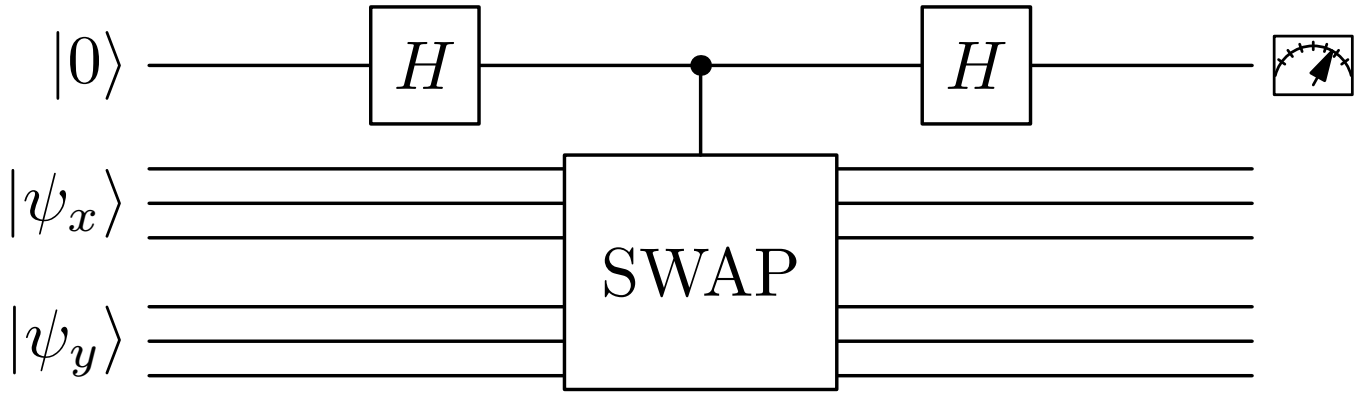
Чарли получает два сообщения $|\psi_x\rangle$, $|\psi_y\rangle$ и должен ответить, справедливо ли равенство $x = y$. Его действия описываются схемой:



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

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:

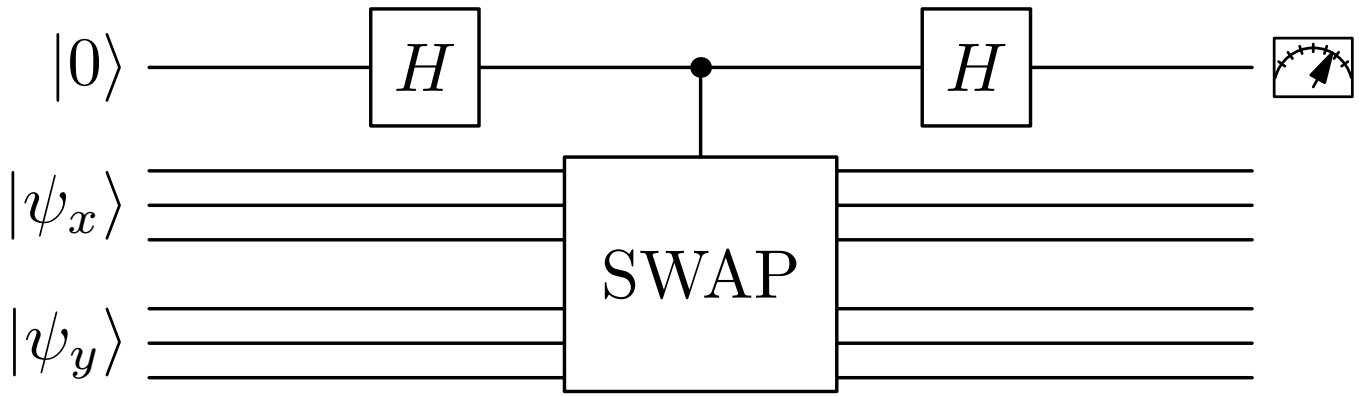


$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

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

Вычисление EQ в модели SMP: действия Чарли

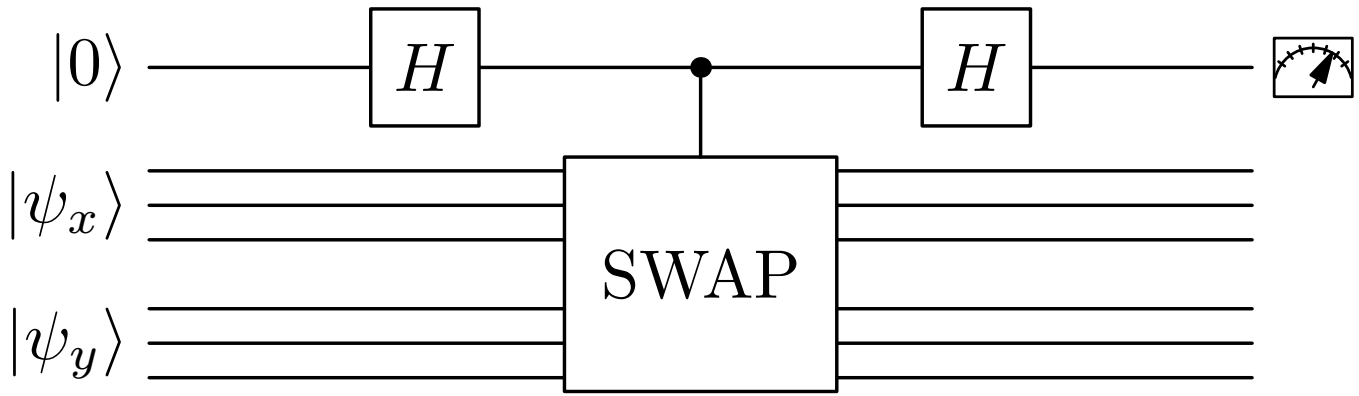
Чарли получает два сообщения $|\psi_x\rangle$, $|\psi_y\rangle$ и должен ответить, справедливо ли равенство $x = y$. Его действия описываются схемой:



$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad \mathrm{SWAP}\colon |u\rangle \otimes |v\rangle \mapsto |v\rangle \otimes |u\rangle$$

Вычисление EQ в модели SMP: действия Чарли

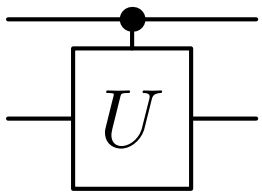
Чарли получает два сообщения $|\psi_x\rangle$, $|\psi_y\rangle$ и должен ответить, справедливо ли равенство $x = y$. Его действия описываются схемой:



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

$$\mathrm{SWAP}\colon |u\rangle \otimes |v\rangle \mapsto |v\rangle \otimes |u\rangle$$

c-U =



$$\text{c-}U\colon |0\rangle \otimes |\psi\rangle \to |0\rangle \otimes |\psi\rangle$$
$$\text{c-}U\colon |1\rangle \otimes |\psi\rangle \to |1\rangle \otimes U|\psi\rangle$$

Анализ протокола

- 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

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

$$\langle \psi_x | \psi_x \rangle = 1 \quad \text{(для любого состояния)}.$$

Анализ протокола

- 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

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

$$\langle\psi_x|\psi_x\rangle = 1 \quad \text{(для любого состояния)}.$$

Анализ протокола (продолжение)

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

$$|0\rangle \otimes |\psi_x\rangle \otimes |\psi_y\rangle \stackrel{H}{\longmapsto} \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big) \otimes |\psi_x\rangle \otimes |\psi_y\rangle$$

$$\stackrel{\text{c-SWAP}}{\longmapsto} \frac{1}{\sqrt{2}}|0\rangle \otimes |\psi_x\rangle \otimes |\psi_y\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes |\psi_y\rangle \otimes |\psi_x\rangle$$

$$\stackrel{H}{\longmapsto} \frac{1}{2}\big(|0\rangle + |1\rangle\big) \otimes |\psi_x\rangle \otimes |\psi_y\rangle + \frac{1}{2}\big(|0\rangle - |1\rangle\big) \otimes |\psi_y\rangle \otimes |\psi_x\rangle =$$

$$= \frac{1}{2}|0\rangle \otimes \big(|\psi_x\rangle \otimes |\psi_y\rangle + |\psi_y\rangle \otimes |\psi_x\rangle\big) + \frac{1}{2}|1\rangle \otimes \big(|\psi_x\rangle \otimes |\psi_y\rangle - |\psi_y\rangle \otimes |\psi_x\rangle\big)$$

$$\mathbf{Pr}(1) = \frac{1}{4}\big(\langle\psi_x| \otimes \langle\psi_y| - \langle\psi_y| \otimes \langle\psi_x|\big)\big(|\psi_x\rangle \otimes |\psi_y\rangle - |\psi_y\rangle \otimes |\psi_x\rangle\big) =$$

$$= \frac{1}{4}\big(2 - \langle\psi_x|\psi_y\rangle\langle\psi_y|\psi_x\rangle - \langle\psi_y|\psi_x\rangle\langle\psi_x|\psi_y\rangle\big) = \frac{1}{2} - \frac{1}{2}|\langle\psi_x|\psi_y\rangle|^2.$$

Анализ протокола (продолжение)

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

$$|0\rangle \otimes |\psi_x\rangle \otimes |\psi_y\rangle \stackrel{H}{\longmapsto} \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big) \otimes |\psi_x\rangle \otimes |\psi_y\rangle$$

$$\stackrel{\text{c-SWAP}}{\longmapsto} \frac{1}{\sqrt{2}}|0\rangle \otimes |\psi_x\rangle \otimes |\psi_y\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes |\psi_y\rangle \otimes |\psi_x\rangle$$

$$\stackrel{H}{\longmapsto} \frac{1}{2}\big(|0\rangle + |1\rangle\big) \otimes |\psi_x\rangle \otimes |\psi_y\rangle + \frac{1}{2}\big(|0\rangle - |1\rangle\big) \otimes |\psi_y\rangle \otimes |\psi_x\rangle =$$

$$= \frac{1}{2}|0\rangle \otimes \big(|\psi_x\rangle \otimes |\psi_y\rangle + |\psi_y\rangle \otimes |\psi_x\rangle\big) + \frac{1}{2}|1\rangle \otimes \big(|\psi_x\rangle \otimes |\psi_y\rangle - |\psi_y\rangle \otimes |\psi_x\rangle\big)$$

$$\mathbf{Pr}(1) = \frac{1}{4}\big(\langle\psi_x| \otimes \langle\psi_y| - \langle\psi_y| \otimes \langle\psi_x|\big)\big(|\psi_x\rangle \otimes |\psi_y\rangle - |\psi_y\rangle \otimes |\psi_x\rangle\big) =$$

$$= \frac{1}{4}\big(2 - \langle\psi_x|\psi_y\rangle\langle\psi_y|\psi_x\rangle - \langle\psi_y|\psi_x\rangle\langle\psi_x|\psi_y\rangle\big) = \frac{1}{2} - \frac{1}{2}|\langle\psi_x|\psi_y\rangle|^2.$$

Анализ протокола (продолжение)

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

$$|0\rangle \otimes |\psi_x\rangle \otimes |\psi_y\rangle \xmapsto{H} \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big) \otimes |\psi_x\rangle \otimes |\psi_y\rangle$$

$$\xmapsto{\text{c-SWAP}} \frac{1}{\sqrt{2}}|0\rangle \otimes |\psi_x\rangle \otimes |\psi_y\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes |\psi_y\rangle \otimes |\psi_x\rangle$$

$$\xmapsto{H} \frac{1}{2}\big(|0\rangle + |1\rangle\big) \otimes |\psi_x\rangle \otimes |\psi_y\rangle + \frac{1}{2}\big(|0\rangle - |1\rangle\big) \otimes |\psi_y\rangle \otimes |\psi_x\rangle =$$

$$= \frac{1}{2}|0\rangle \otimes \big(|\psi_x\rangle \otimes |\psi_y\rangle + |\psi_y\rangle \otimes |\psi_x\rangle\big) + \frac{1}{2}|1\rangle \otimes \big(|\psi_x\rangle \otimes |\psi_y\rangle - |\psi_y\rangle \otimes |\psi_x\rangle\big)$$

$$\Pr(1) = \frac{1}{4}\big(\langle\psi_x| \otimes \langle\psi_y| - \langle\psi_y| \otimes \langle\psi_x|\big)\big(|\psi_x\rangle \otimes |\psi_y\rangle - |\psi_y\rangle \otimes |\psi_x\rangle\big) =$$

$$= \frac{1}{4}\big(2 - \langle\psi_x|\psi_y\rangle\langle\psi_y|\psi_x\rangle - \langle\psi_y|\psi_x\rangle\langle\psi_x|\psi_y\rangle\big) = \frac{1}{2} - \frac{1}{2}|\langle\psi_x|\psi_y\rangle|^2.$$

Анализ протокола (продолжение)

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

$$|0\rangle \otimes |\psi_x\rangle \otimes |\psi_y\rangle \stackrel{H}{\longmapsto} \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big) \otimes |\psi_x\rangle \otimes |\psi_y\rangle$$

$$\stackrel{\text{c-SWAP}}{\longmapsto} \frac{1}{\sqrt{2}}|0\rangle \otimes |\psi_x\rangle \otimes |\psi_y\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes |\psi_y\rangle \otimes |\psi_x\rangle$$

$$\stackrel{H}{\longmapsto} \frac{1}{2}\big(|0\rangle + |1\rangle\big) \otimes |\psi_x\rangle \otimes |\psi_y\rangle + \frac{1}{2}\big(|0\rangle - |1\rangle\big) \otimes |\psi_y\rangle \otimes |\psi_x\rangle =$$

$$= \frac{1}{2}|0\rangle \otimes \big(|\psi_x\rangle \otimes |\psi_y\rangle + |\psi_y\rangle \otimes |\psi_x\rangle\big) + \frac{1}{2}|1\rangle \otimes \big(|\psi_x\rangle \otimes |\psi_y\rangle - |\psi_y\rangle \otimes |\psi_x\rangle\big)$$

$$\mathbf{Pr}(1) = \frac{1}{4}\big(\langle\psi_x| \otimes \langle\psi_y| - \langle\psi_y| \otimes \langle\psi_x|\big)\big(|\psi_x\rangle \otimes |\psi_y\rangle - |\psi_y\rangle \otimes |\psi_x\rangle\big) =$$

$$= \frac{1}{4}\big(2 - \langle\psi_x|\psi_y\rangle\langle\psi_y|\psi_x\rangle - \langle\psi_y|\psi_x\rangle\langle\psi_x|\psi_y\rangle\big) = \frac{1}{2} - \frac{1}{2}|\langle\psi_x|\psi_y\rangle|^2.$$

Анализ протокола (продолжение)

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

$$|0\rangle \otimes |\psi_x\rangle \otimes |\psi_y\rangle \xmapsto{H} \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big) \otimes |\psi_x\rangle \otimes |\psi_y\rangle$$

$$\xmapsto{\text{c-SWAP}} \frac{1}{\sqrt{2}}|0\rangle \otimes |\psi_x\rangle \otimes |\psi_y\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes |\psi_y\rangle \otimes |\psi_x\rangle$$

$$\xmapsto{H} \frac{1}{2}\big(|0\rangle + |1\rangle\big) \otimes |\psi_x\rangle \otimes |\psi_y\rangle + \frac{1}{2}\big(|0\rangle - |1\rangle\big) \otimes |\psi_y\rangle \otimes |\psi_x\rangle =$$

$$= \frac{1}{2}|0\rangle \otimes \big(|\psi_x\rangle \otimes |\psi_y\rangle + |\psi_y\rangle \otimes |\psi_x\rangle\big) + \frac{1}{2}|1\rangle \otimes \big(|\psi_x\rangle \otimes |\psi_y\rangle - |\psi_y\rangle \otimes |\psi_x\rangle\big)$$

$$\mathbf{Pr}(1) = \frac{1}{4}\big(\langle\psi_x| \otimes \langle\psi_y| - \langle\psi_y| \otimes \langle\psi_x|\big)\big(|\psi_x\rangle \otimes |\psi_y\rangle - |\psi_y\rangle \otimes |\psi_x\rangle\big) =$$

$$= \frac{1}{4}\big(2 - \langle\psi_x|\psi_y\rangle\langle\psi_y|\psi_x\rangle - \langle\psi_y|\psi_x\rangle\langle\psi_x|\psi_y\rangle\big) = \frac{1}{2} - \frac{1}{2}|\langle\psi_x|\psi_y\rangle|^2.$$

Анализ протокола (продолжение)

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

$$|0\rangle \otimes |\psi_x\rangle \otimes |\psi_y\rangle \stackrel{H}{\mapsto} \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big) \otimes |\psi_x\rangle \otimes |\psi_y\rangle$$

$$\stackrel{\text{c-SWAP}}{\longmapsto} \frac{1}{\sqrt{2}}|0\rangle \otimes |\psi_x\rangle \otimes |\psi_y\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes |\psi_y\rangle \otimes |\psi_x\rangle$$

$$\stackrel{H}{\mapsto} \frac{1}{2}\big(|0\rangle + |1\rangle\big) \otimes |\psi_x\rangle \otimes |\psi_y\rangle + \frac{1}{2}\big(|0\rangle - |1\rangle\big) \otimes |\psi_y\rangle \otimes |\psi_x\rangle =$$

$$= \frac{1}{2}|0\rangle \otimes \big(|\psi_x\rangle \otimes |\psi_y\rangle + |\psi_y\rangle \otimes |\psi_x\rangle\big) + \frac{1}{2}|1\rangle \otimes \big(|\psi_x\rangle \otimes |\psi_y\rangle - |\psi_y\rangle \otimes |\psi_x\rangle\big)$$

$$\mathbf{Pr}(1) = \frac{1}{4}\big(\langle\psi_x| \otimes \langle\psi_y| - \langle\psi_y| \otimes \langle\psi_x|\big)\big(|\psi_x\rangle \otimes |\psi_y\rangle - |\psi_y\rangle \otimes |\psi_x\rangle\big) =$$

$$= \frac{1}{4}\big(2 - \langle\psi_x|\psi_y\rangle\langle\psi_y|\psi_x\rangle - \langle\psi_y|\psi_x\rangle\langle\psi_x|\psi_y\rangle\big) = \frac{1}{2} - \frac{1}{2}|\langle\psi_x|\psi_y\rangle|^2.$$

Анализ протокола (продолжение)

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

$$|0\rangle \otimes |\psi_x\rangle \otimes |\psi_y\rangle \stackrel{H}{\mapsto} \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big) \otimes |\psi_x\rangle \otimes |\psi_y\rangle$$

$$\stackrel{\text{c-SWAP}}{\longmapsto} \frac{1}{\sqrt{2}}|0\rangle \otimes |\psi_x\rangle \otimes |\psi_y\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes |\psi_y\rangle \otimes |\psi_x\rangle$$

$$\stackrel{H}{\mapsto} \frac{1}{2}\big(|0\rangle + |1\rangle\big) \otimes |\psi_x\rangle \otimes |\psi_y\rangle + \frac{1}{2}\big(|0\rangle - |1\rangle\big) \otimes |\psi_y\rangle \otimes |\psi_x\rangle =$$

$$= \frac{1}{2}|0\rangle \otimes \big(|\psi_x\rangle \otimes |\psi_y\rangle + |\psi_y\rangle \otimes |\psi_x\rangle\big) + \frac{1}{2}|1\rangle \otimes \big(|\psi_x\rangle \otimes |\psi_y\rangle - |\psi_y\rangle \otimes |\psi_x\rangle\big)$$

$$\mathbf{Pr}(1) = \frac{1}{4}\big(\langle\psi_x| \otimes \langle\psi_y| - \langle\psi_y| \otimes \langle\psi_x|\big)\big(|\psi_x\rangle \otimes |\psi_y\rangle - |\psi_y\rangle \otimes |\psi_x\rangle\big) =$$

$$= \frac{1}{4}\big(2 - \langle\psi_x|\psi_y\rangle\langle\psi_y|\psi_x\rangle - \langle\psi_y|\psi_x\rangle\langle\psi_x|\psi_y\rangle\big) = \frac{1}{2} - \frac{1}{2}|\langle\psi_x|\psi_y\rangle|^2.$$

Анализ протокола (продолжение)

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

$$|0\rangle \otimes |\psi_x\rangle \otimes |\psi_y\rangle \stackrel{H}{\mapsto} \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big) \otimes |\psi_x\rangle \otimes |\psi_y\rangle$$

$$\stackrel{\text{c-SWAP}}{\longmapsto} \frac{1}{\sqrt{2}}|0\rangle \otimes |\psi_x\rangle \otimes |\psi_y\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes |\psi_y\rangle \otimes |\psi_x\rangle$$

$$\stackrel{H}{\mapsto} \frac{1}{2}\big(|0\rangle + |1\rangle\big) \otimes |\psi_x\rangle \otimes |\psi_y\rangle + \frac{1}{2}\big(|0\rangle - |1\rangle\big) \otimes |\psi_y\rangle \otimes |\psi_x\rangle =$$

$$= \frac{1}{2}|0\rangle \otimes \big(|\psi_x\rangle \otimes |\psi_y\rangle + |\psi_y\rangle \otimes |\psi_x\rangle\big) + \frac{1}{2}|1\rangle \otimes \big(|\psi_x\rangle \otimes |\psi_y\rangle - |\psi_y\rangle \otimes |\psi_x\rangle\big)$$

$$\mathbf{Pr}(1) = \frac{1}{4}\big(\langle\psi_x| \otimes \langle\psi_y| - \langle\psi_y| \otimes \langle\psi_x|\big)\big(|\psi_x\rangle \otimes |\psi_y\rangle - |\psi_y\rangle \otimes |\psi_x\rangle\big) =$$

$$= \frac{1}{4}\big(2 - \langle\psi_x|\psi_y\rangle\langle\psi_y|\psi_x\rangle - \langle\psi_y|\psi_x\rangle\langle\psi_x|\psi_y\rangle\big) = \frac{1}{2} - \frac{1}{2}|\langle\psi_x|\psi_y\rangle|^2.$$

Анализ протокола (продолжение)

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

$$|0\rangle \otimes |\psi_x\rangle \otimes |\psi_y\rangle \xmapsto{H} \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big) \otimes |\psi_x\rangle \otimes |\psi_y\rangle$$

$$\xmapsto{\text{c-SWAP}} \frac{1}{\sqrt{2}}|0\rangle \otimes |\psi_x\rangle \otimes |\psi_y\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes |\psi_y\rangle \otimes |\psi_x\rangle$$

$$\xmapsto{H} \frac{1}{2}\big(|0\rangle + |1\rangle\big) \otimes |\psi_x\rangle \otimes |\psi_y\rangle + \frac{1}{2}\big(|0\rangle - |1\rangle\big) \otimes |\psi_y\rangle \otimes |\psi_x\rangle =$$

$$= \frac{1}{2}|0\rangle \otimes \big(|\psi_x\rangle \otimes |\psi_y\rangle + |\psi_y\rangle \otimes |\psi_x\rangle\big) + \frac{1}{2}|1\rangle \otimes \big(|\psi_x\rangle \otimes |\psi_y\rangle - |\psi_y\rangle \otimes |\psi_x\rangle\big)$$

$$\mathbf{Pr}(1) = \frac{1}{4}\big(\langle\psi_x| \otimes \langle\psi_y| - \langle\psi_y| \otimes \langle\psi_x|\big)\big(|\psi_x\rangle \otimes |\psi_y\rangle - |\psi_y\rangle \otimes |\psi_x\rangle\big) =$$

$$= \frac{1}{4}\big(2 - \langle\psi_x|\psi_y\rangle\langle\psi_y|\psi_x\rangle - \langle\psi_y|\psi_x\rangle\langle\psi_x|\psi_y\rangle\big) = \frac{1}{2} - \frac{1}{2}|\langle\psi_x|\psi_y\rangle|^2.$$

Анализ протокола (продолжение)

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

$$|0\rangle \otimes |\psi_x\rangle \otimes |\psi_y\rangle \xmapsto{H} \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big) \otimes |\psi_x\rangle \otimes |\psi_y\rangle$$

$$\xmapsto{\text{c-SWAP}} \frac{1}{\sqrt{2}}|0\rangle \otimes |\psi_x\rangle \otimes |\psi_y\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes |\psi_y\rangle \otimes |\psi_x\rangle$$

$$\xmapsto{H} \frac{1}{2}\big(|0\rangle + |1\rangle\big) \otimes |\psi_x\rangle \otimes |\psi_y\rangle + \frac{1}{2}\big(|0\rangle - |1\rangle\big) \otimes |\psi_y\rangle \otimes |\psi_x\rangle =$$

$$= \frac{1}{2}|0\rangle \otimes \big(|\psi_x\rangle \otimes |\psi_y\rangle + |\psi_y\rangle \otimes |\psi_x\rangle\big) + \frac{1}{2}|1\rangle \otimes \big(|\psi_x\rangle \otimes |\psi_y\rangle - |\psi_y\rangle \otimes |\psi_x\rangle\big)$$

$$\mathbf{Pr}(1) = \frac{1}{4}\big(\langle\psi_x| \otimes \langle\psi_y| - \langle\psi_y| \otimes \langle\psi_x|\big)\big(|\psi_x\rangle \otimes |\psi_y\rangle - |\psi_y\rangle \otimes |\psi_x\rangle\big) =$$

$$= \frac{1}{4}\big(2 - \langle\psi_x|\psi_y\rangle\langle\psi_y|\psi_x\rangle - \langle\psi_y|\psi_x\rangle\langle\psi_x|\psi_y\rangle\big) = \frac{1}{2} - \frac{1}{2}|\langle\psi_x|\psi_y\rangle|^2.$$

Анализ протокола (продолжение)

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

$$|0\rangle \otimes |\psi_x\rangle \otimes |\psi_y\rangle \stackrel{H}{\mapsto} \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big) \otimes |\psi_x\rangle \otimes |\psi_y\rangle$$

$$\stackrel{\text{c-SWAP}}{\longmapsto} \frac{1}{\sqrt{2}}|0\rangle \otimes |\psi_x\rangle \otimes |\psi_y\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes |\psi_y\rangle \otimes |\psi_x\rangle$$

$$\stackrel{H}{\mapsto} \frac{1}{2}\big(|0\rangle + |1\rangle\big) \otimes |\psi_x\rangle \otimes |\psi_y\rangle + \frac{1}{2}\big(|0\rangle - |1\rangle\big) \otimes |\psi_y\rangle \otimes |\psi_x\rangle =$$

$$= \frac{1}{2}|0\rangle \otimes \big(|\psi_x\rangle \otimes |\psi_y\rangle + |\psi_y\rangle \otimes |\psi_x\rangle\big) + \frac{1}{2}|1\rangle \otimes \big(|\psi_x\rangle \otimes |\psi_y\rangle - |\psi_y\rangle \otimes |\psi_x\rangle\big)$$

$$\mathbf{Pr}(1) = \frac{1}{4}\big(\langle\psi_x| \otimes \langle\psi_y| - \langle\psi_y| \otimes \langle\psi_x|\big)\big(|\psi_x\rangle \otimes |\psi_y\rangle - |\psi_y\rangle \otimes |\psi_x\rangle\big) =$$

$$= \frac{1}{4}\big(2 - \langle\psi_x|\psi_y\rangle\langle\psi_y|\psi_x\rangle - \langle\psi_y|\psi_x\rangle\langle\psi_x|\psi_y\rangle\big) = \frac{1}{2} - \frac{1}{2}|\langle\psi_x|\psi_y\rangle|^2.$$

Анализ протокола (продолжение)

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

$$|0\rangle \otimes |\psi_x\rangle \otimes |\psi_y\rangle \xmapsto{H} \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big) \otimes |\psi_x\rangle \otimes |\psi_y\rangle$$

$$\xmapsto{\text{c-SWAP}} \frac{1}{\sqrt{2}}|0\rangle \otimes |\psi_x\rangle \otimes |\psi_y\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes |\psi_y\rangle \otimes |\psi_x\rangle$$

$$\xmapsto{H} \frac{1}{2}\big(|0\rangle + |1\rangle\big) \otimes |\psi_x\rangle \otimes |\psi_y\rangle + \frac{1}{2}\big(|0\rangle - |1\rangle\big) \otimes |\psi_y\rangle \otimes |\psi_x\rangle =$$

$$= \frac{1}{2}|0\rangle \otimes \big(|\psi_x\rangle \otimes |\psi_y\rangle + |\psi_y\rangle \otimes |\psi_x\rangle\big) + \frac{1}{2}|1\rangle \otimes \big(|\psi_x\rangle \otimes |\psi_y\rangle - |\psi_y\rangle \otimes |\psi_x\rangle\big)$$

$$\mathbf{Pr}(1) = \frac{1}{4}\big(\langle\psi_x| \otimes \langle\psi_y| - \langle\psi_y| \otimes \langle\psi_x|\big)\big(|\psi_x\rangle \otimes |\psi_y\rangle - |\psi_y\rangle \otimes |\psi_x\rangle\big) =$$

$$= \frac{1}{4}\big(2 - \langle\psi_x|\psi_y\rangle\langle\psi_y|\psi_x\rangle - \langle\psi_y|\psi_x\rangle\langle\psi_x|\psi_y\rangle\big) = \frac{1}{2} - \frac{1}{2}|\langle\psi_x|\psi_y\rangle|^2.$$

Анализ протокола (окончание)

- Итак, вероятность наблюдения 1 равна

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

- 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

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

- 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

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

- 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

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

- 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.

План

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

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

и забирают с собой в камеру по одному из кубитов.

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

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

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

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

   и забирают с собой в камеру по одному из кубитов.
2. Получив бит x, игрок применяет условный фазовый сдвиг к своему кубиту:

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

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

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

   и забирают с собой в камеру по одному из кубитов.
2. Получив бит x, игрок применяет условный фазовый сдвиг к своему кубиту:

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

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

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

   и забирают с собой в камеру по одному из кубитов.
2. Получив бит x, игрок применяет условный фазовый сдвиг к своему кубиту:

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

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

$$\frac{1}{\sqrt{2}}(|000\rangle + i^{x_a+x_b+x_c}|111\rangle) =$$

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

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:

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

После условного фазового сдвига оно изменяется на

$$\frac{1}{\sqrt{2}}\big(|000\rangle + i^{x_a+x_b+x_c}|111\rangle\big) =$$

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

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:

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

После условного фазового сдвига оно изменяется на

$$\frac{1}{\sqrt{2}}\big(|000\rangle + i^{x_a+x_b+x_c}|111\rangle\big) =$$

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

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.