# Квантовые алгоритмы: возможности и ограничения. Лекция 10: Моделирование квантовых схем классическими средствами. О реализации квантового компьютера

М. Вялый

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

Санкт-Петербург, 2011

# План

# Случай симплектического базиса

Симплектический базис — это базис из операторов $\{\text{c-NOT}, H, K(\pi/2)\}$.

Симплектический базис не является универсальным: операторы из этого базиса образуют конечную подгруппу $\mathbf{U}((\mathbb{C}^2)^{\otimes n})$.

**Теорема Готтесмана – Нилла**

Вероятность наблюдения 1 в первом кубите при измерении состояния, которое получено применением схемы в симплектическом базисе, вычисляется классическим алгоритмом за полиномиальное время.

**Следствие**

Матричные элементы оператора, заданного схемой в симплектическом базисе, можно вычислять классическим алгоритмом за полиномиальное время.

# Случай симплектического базиса

Симплектический базис — это базис из операторов $\{\text{c-NOT}, H, K(\pi/2)\}$.
Симплектический базис не является универсальным: операторы из этого базиса образуют конечную подгруппу $\mathbf{U}((\mathbb{C}^2)^{\otimes n})$.

**Теорема Готтесмана – Нилла**

Вероятность наблюдения 1 в первом кубите при измерении состояния, которое получено применением схемы в симплектическом базисе, вычисляется классическим алгоритмом за полиномиальное время.

**Следствие**

Матричные элементы оператора, заданного схемой в симплектическом базисе, можно вычислять классическим алгоритмом за полиномиальное время.

# Случай симплектического базиса

Симплектический базис — это базис из операторов $\{\text{c-NOT}, H, K(\pi/2)\}$.
Симплектический базис не является универсальным: операторы из этого базиса образуют конечную подгруппу $\mathbf{U}((\mathbb{C}^2)^{\otimes n})$.

## Теорема Готтесмана – Нилла

Вероятность наблюдения 1 в первом кубите при измерении состояния, которое получено применением схемы в симплектическом базисе, вычисляется классическим алгоритмом за полиномиальное время.

## Следствие

Матричные элементы оператора, заданного схемой в симплектическом базисе, можно вычислять классическим алгоритмом за полиномиальное время.

# Случай симплектического базиса

Симплектический базис — это базис из операторов $\{\text{c-NOT}, H, K(\pi/2)\}$.
Симплектический базис не является универсальным: операторы из этого базиса образуют конечную подгруппу $\mathbf{U}((\mathbb{C}^2)^{\otimes n})$.

## Теорема Готтесмана – Нилла

Вероятность наблюдения 1 в первом кубите при измерении состояния, которое получено применением схемы в симплектическом базисе, вычисляется классическим алгоритмом за полиномиальное время.

## Следствие

Матричные элементы оператора, заданного схемой в симплектическом базисе, можно вычислять классическим алгоритмом за полиномиальное время.

# О сцепленности как квантовом ресурсе

Сцепленность как явление означает существование в тензорном произведении пространств неразложимых в вычислительном базисе состояний, например ЭПР пара

$$|\text{ЭПР}\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle.$$

В квантовой теории информации вводятся разнообразные меры сцепленности и количество сцепленности (скажем, ЭПР-пар) является важным информационным ресурсом.
Теорема Готтесмана – Нилла показывает сомнительность пользы от понятия сцепленности для квантовых вычислений. Сцепленность порождается операторами из симплектического базиса

$$|\text{ЭПР}\rangle = \text{c-NOT}[1,2]H[1]|00\rangle,$$

а тот моделируется классически.

# О сцепленности как квантовом ресурсе

Сцепленность как явление означает существование в тензорном произведении пространств неразложимых в вычислительном базисе состояний, например ЭПР пара

$$|\text{ЭПР}\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle.$$

В квантовой теории информации вводятся разнообразные меры сцепленности и количество сцепленности (скажем, ЭПР-пар) является важным информационным ресурсом.

Теорема Готтесмана – Нилла показывает сомнительность пользы от понятия сцепленности для квантовых вычислений. Сцепленность порождается операторами из симплектического базиса

$$|\text{ЭПР}\rangle = \text{c-NOT}[1,2]H[1]|00\rangle,$$

а тот моделируется классически.

# О сцепленности как квантовом ресурсе

Сцепленность как явление означает существование в тензорном произведении пространств неразложимых в вычислительном базисе состояний, например ЭПР пара

$$|\text{ЭПР}\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle.$$

В квантовой теории информации вводятся разнообразные меры сцепленности и количество сцепленности (скажем, ЭПР-пар) является важным информационным ресурсом.
Теорема Готтесмана – Нилла показывает сомнительность пользы от понятия сцепленности для квантовых вычислений. Сцепленность порождается операторами из симплектического базиса

$$|\text{ЭПР}\rangle = \text{c-NOT}[1,2]H[1]|00\rangle,$$

а тот моделируется классически.

# Еще раз о матрицах Паули

$$\sigma_{00} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; \qquad \sigma_{01} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \sigma_z;$$

$$\sigma_{10} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \sigma_x; \quad \sigma_{11} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = \sigma_y.$$

## Утверждение

Матрицы Паули $\frac{1}{\sqrt{2}}\sigma_{\alpha\beta}$ образуют ортонормированный базис в (вещественном) пространстве эрмитовых операторов на $\mathbb{C}^2$.

## Следствие

Тензорные произведения

$$\sigma(f) = \sigma(\alpha_1, \beta_1, \alpha_2, \beta_2, \ldots, \alpha_n, \beta_n) \stackrel{\text{def}}{=} \sigma_{\alpha_1,\beta_1} \otimes \sigma_{\alpha_2,\beta_2} \otimes \cdots \otimes \sigma_{\alpha_n,\beta_n}$$

образуют ортогональный базис в пространстве эрмитовых операторов на $(\mathbb{C}^2)^{\otimes n}$. Здесь $f \in \mathbb{F}_2^{2n}$.

# Еще раз о матрицах Паули

$$\sigma_{00} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; \qquad \sigma_{01} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \sigma_z;$$

$$\sigma_{10} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \sigma_x; \quad \sigma_{11} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = \sigma_y.$$

## Утверждение

Матрицы Паули $\frac{1}{\sqrt{2}}\sigma_{\alpha\beta}$ образуют ортонормированный базис в (вещественном) пространстве эрмитовых операторов на $\mathbb{C}^2$.

## Следствие

Тензорные произведения

$$\sigma(f) = \sigma(\alpha_1, \beta_1, \alpha_2, \beta_2, \ldots, \alpha_n, \beta_n) \stackrel{\text{def}}{=} \sigma_{\alpha_1,\beta_1} \otimes \sigma_{\alpha_2,\beta_2} \otimes \cdots \otimes \sigma_{\alpha_n,\beta_n}$$

образуют ортогональный базис в пространстве эрмитовых операторов на $(\mathbb{C}^2)^{\otimes n}$. Здесь $f \in \mathbb{F}_2^{2n}$.

# Еще раз о матрицах Паули

$$\sigma_{00} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; \qquad \sigma_{01} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \sigma_z;$$

$$\sigma_{10} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \sigma_x; \quad \sigma_{11} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = \sigma_y.$$

## Утверждение

Матрицы Паули $\frac{1}{\sqrt{2}}\sigma_{\alpha\beta}$ образуют ортонормированный базис в (вещественном) пространстве эрмитовых операторов на $\mathbb{C}^2$.

## Следствие

Тензорные произведения

$$\sigma(f) = \sigma(\alpha_1, \beta_1, \alpha_2, \beta_2, \ldots, \alpha_n, \beta_n) \stackrel{\text{def}}{=} \sigma_{\alpha_1,\beta_1} \otimes \sigma_{\alpha_2,\beta_2} \otimes \cdots \otimes \sigma_{\alpha_n,\beta_n}$$

образуют ортогональный базис в пространстве эрмитовых операторов на $(\mathbb{C}^2)^{\otimes n}$. Здесь $f \in \mathbb{F}_2^{2n}$.

# Умножение матриц Паули

$$\sigma(\alpha,\beta)^2 = I; \quad \sigma(\alpha_1,\beta_1)\sigma(\alpha_2,\beta_2) = i^{\tilde{\omega}}\sigma(\alpha_1 \oplus \alpha_2, \beta_1 \oplus \beta_2)$$

$$\tilde{\omega}(\alpha_1,\beta_1;\alpha_2,\beta_2) = \alpha_1^2\beta_1^2 + (\alpha_2)^2(\beta_2)^2 - (\alpha_1+\alpha_2)^2(\beta_1+\beta_2)^2 + 2\alpha_2\beta_1 \text{ mod } 4.$$

# Действие симплектических операторов

## Лемма

Действие симплектических операторов $X \mapsto UXU^\dagger$ на пространстве эрмитовых операторов сохраняет базис $\sigma$-операторов (с точностью до фазового множителя $i^a$).

## Доказательство

Проверка для действия одного оператора. Для одного кубита выполняются следующие соотношения.

# Действие симплектических операторов

## Лемма

Действие симплектических операторов $X \mapsto UXU^\dagger$ на пространстве эрмитовых операторов сохраняет базис $\sigma$-операторов (с точностью до фазового множителя $i^a$).

## Доказательство

Проверка для действия одного оператора. Для одного кубита выполняются следующие соотношения.

# Действие симплектических операторов

## Лемма

Действие симплектических операторов $X \mapsto UXU^\dagger$ на пространстве эрмитовых операторов сохраняет базис $\sigma$-операторов (с точностью до фазового множителя $i^a$).

## Доказательство

Проверка для действия одного оператора. Для одного кубита выполняются следующие соотношения.
Повороты сферы Блоха

$$H\sigma_x H^\dagger = \sigma_z, \qquad H\sigma_y H^\dagger = -\sigma_y, \qquad H\sigma_z H^\dagger = \sigma_x;$$
$$K\sigma_x K^\dagger = \sigma_y, \qquad K\sigma_y K^\dagger = -\sigma_x, \qquad K\sigma_z K^\dagger = \sigma_z.$$

# Действие симплектических операторов

## Лемма

Действие симплектических операторов $X \mapsto UXU^\dagger$ на пространстве эрмитовых операторов сохраняет базис $\sigma$-операторов (с точностью до фазового множителя $i^a$).

## Доказательство

Проверка для действия одного оператора. Для одного кубита выполняются следующие соотношения.
Пусть $U = \text{c-NOT}[1,2]$. Тогда (проверьте!)

$$U\sigma_z[1]U^\dagger = \sigma_z[1], \qquad U\sigma_x[1]U^\dagger = \sigma_x[1]\sigma_x[2],$$
$$U\sigma_z[2]U^\dagger = \sigma_z[1]\sigma_z[2], \qquad U\sigma_x[2]U^\dagger = \sigma_x[2].$$

# Действие симплектической схемы

## Следствие

Симплектические схемы порождают конечную группу унитарных матриц.

## Лемма

Если оператор $U$ задается симплектической схемой, то $U^\dagger \sigma(f) U = i^{U_a(f)} \sigma(\tilde{U} f)$, причем $U_a$ и $\tilde{U} f$ вычисляются за полиномиальное время классическим алгоритмом.

## Доказательство

Из формул умножения операторов Паули и формул действия для образующих симплектической группы следует, что $\tilde{U}$ — линейное преобразование на $\mathbb{F}^{2n}$.
Фазовый множитель вычисляется эффективно по тем же формулам.

# Действие симплектической схемы

## Следствие

Симплектические схемы порождают конечную группу унитарных матриц.

## Лемма

Если оператор $U$ задается симплектической схемой, то $U^\dagger \sigma(f) U = i^{U_a(f)} \sigma(\tilde{U} f)$, причем $U_a$ и $\tilde{U} f$ вычисляются за полиномиальное время классическим алгоритмом.

## Доказательство

Из формул умножения операторов Паули и формул действия для образующих симплектической группы следует, что $\tilde{U}$ — линейное преобразование на $\mathbb{F}^{2n}$.

Фазовый множитель вычисляется эффективно по тем же формулам.

# Действие симплектической схемы

## Следствие

Симплектические схемы порождают конечную группу унитарных матриц.

## Лемма

Если оператор $U$ задается симплектической схемой, то $U^\dagger \sigma(f) U = i^{U_a(f)} \sigma(\tilde{U} f)$, причем $U_a$ и $\tilde{U} f$ вычисляются за полиномиальное время классическим алгоритмом.

## Доказательство

Из формул умножения операторов Паули и формул действия для образующих симплектической группы следует, что $\tilde{U}$ — линейное преобразование на $\mathbb{F}^{2n}$.
Фазовый множитель вычисляется эффективно по тем же формулам.

# Еще одна формула для вероятности наблюдения 1

Вероятность наблюдения единицы в первом кубите при измерении состояния $|\psi\rangle = \sum_x c_x |x\rangle$

$$\mathbf{Pr}(|\psi\rangle, 1) = \sum_{x:x_1=1} |c_x|^2 = \langle\psi|\Pi_1[1]|\psi\rangle = \langle\psi|\frac{1}{2}(\sigma_{00} - \sigma_{11}) \otimes I^{\otimes n-1}|\psi\rangle =$$

$$= \frac{1}{2}(\langle\psi|\sigma(f_0)|\psi\rangle - \langle\psi|\sigma(f_1)|\psi\rangle) = \frac{1}{2}(1 - \langle\psi|\sigma(f_1)|\psi\rangle)$$

# Еще одна формула для вероятности наблюдения 1

Вероятность наблюдения единицы в первом кубите при измерении состояния $|\psi\rangle = \sum_x c_x |x\rangle$

$$\mathbf{Pr}(|\psi\rangle, 1) = \sum_{x:x_1=1} |c_x|^2 = \langle\psi|\Pi_1[1]|\psi\rangle = \langle\psi|\frac{1}{2}(\sigma_{00} - \sigma_{11}) \otimes I^{\otimes n-1}|\psi\rangle =$$

$$= \frac{1}{2}\left(\langle\psi|\sigma(f_0)|\psi\rangle - \langle\psi|\sigma(f_1)|\psi\rangle\right) = \frac{1}{2}\left(1 - \langle\psi|\sigma(f_1)|\psi\rangle\right)$$

# Еще одна формула для вероятности наблюдения 1

Вероятность наблюдения единицы в первом кубите при измерении состояния $|\psi\rangle = \sum_x c_x |x\rangle$

$$\mathbf{Pr}(|\psi\rangle, 1) = \sum_{x:x_1=1} |c_x|^2 = \langle\psi|\Pi_1[1]|\psi\rangle = \langle\psi|\frac{1}{2}(\sigma_{00} - \sigma_{11}) \otimes I^{\otimes n-1}|\psi\rangle =$$

$$= \frac{1}{2}\left(\langle\psi|\sigma(f_0)|\psi\rangle - \langle\psi|\sigma(f_1)|\psi\rangle\right) = \frac{1}{2}\left(1 - \langle\psi|\sigma(f_1)|\psi\rangle\right)$$

# Еще одна формула для вероятности наблюдения 1

Вероятность наблюдения единицы в первом кубите при измерении состояния $|\psi\rangle = \sum_x c_x |x\rangle$

$$\mathbf{Pr}(|\psi\rangle, 1) = \sum_{x:x_1=1} |c_x|^2 = \langle\psi|\Pi_1[1]|\psi\rangle = \langle\psi|\frac{1}{2}(\sigma_{00} - \sigma_{11}) \otimes I^{\otimes n-1}|\psi\rangle =$$

$$= \frac{1}{2}\left(\langle\psi|\sigma(f_0)|\psi\rangle - \langle\psi|\sigma(f_1)|\psi\rangle\right) = \frac{1}{2}\left(1 - \langle\psi|\sigma(f_1)|\psi\rangle\right)$$

# Еще одна формула для вероятности наблюдения 1

Вероятность наблюдения единицы в первом кубите при измерении состояния $|\psi\rangle = \sum_x c_x |x\rangle$

$$\mathbf{Pr}(|\psi\rangle, 1) = \sum_{x:x_1=1} |c_x|^2 = \langle\psi|\Pi_1[1]|\psi\rangle = \langle\psi|\frac{1}{2}(\sigma_{00} - \sigma_{11}) \otimes I^{\otimes n-1}|\psi\rangle =$$

$$= \frac{1}{2}\left(\langle\psi|\sigma(f_0)|\psi\rangle - \langle\psi|\sigma(f_1)|\psi\rangle\right) = \frac{1}{2}\left(1 - \langle\psi|\sigma(f_1)|\psi\rangle\right)$$

# Доказательство теоремы Готтесмана – Нилла

- Пусть оператор $U$ задается симплектической схемой.
- По формуле для вероятности наблюдения единицы

$$\mathbf{Pr}(U|0^n\rangle, 1) = \frac{1}{2}\left(1 - \langle 0^n|U^\dagger \sigma(f_1) U|0^n\rangle\right) =$$

$$= \frac{1}{2}(1 - i^{U_a(f_1)}\langle 0^n|\sigma(\tilde{U}f_1)|0^n\rangle)$$

- $\sigma(\tilde{U}f_1) = \bigotimes_k \sigma(\alpha_k, \beta_k)$ — разложимый.
- Поэтому

$$\mathbf{Pr}(U|0^n\rangle, 1) = \frac{1}{2} - \frac{i^{U_a(f_1)}}{2}\prod_k \langle 0|\sigma(\alpha_k, \beta_k)|0\rangle$$

вычисляется за полиномиальное время.

# Доказательство теоремы Готтесмана – Нилла

- Пусть оператор $U$ задается симплектической схемой.
- По формуле для вероятности наблюдения единицы

$$\mathbf{Pr}(U|0^n\rangle, 1) = \frac{1}{2}\left(1 - \langle 0^n|U^\dagger \sigma(f_1) U|0^n\rangle\right) =$$

$$= \frac{1}{2}\left(1 - i^{U_a(f_1)}\langle 0^n|\sigma(\tilde{U}f_1)|0^n\rangle\right)$$

- $\sigma(\tilde{U}f_1) = \bigotimes_k \sigma(\alpha_k, \beta_k)$ — разложимый.
- Поэтому

$$\mathbf{Pr}(U|0^n\rangle, 1) = \frac{1}{2} - \frac{i^{U_a(f_1)}}{2}\prod_k \langle 0|\sigma(\alpha_k, \beta_k)|0\rangle$$

вычисляется за полиномиальное время.

# Доказательство теоремы Готтесмана – Нилла

- Пусть оператор $U$ задается симплектической схемой.
- По формуле для вероятности наблюдения единицы

$$\mathbf{Pr}(U|0^n\rangle, 1) = \frac{1}{2}\left(1 - \langle 0^n|U^\dagger \sigma(f_1) U|0^n\rangle\right) =$$

$$= \frac{1}{2}\left(1 - i^{U_a(f_1)}\langle 0^n|\sigma(\tilde{U}f_1)|0^n\rangle\right)$$

- $\sigma(\tilde{U}f_1) = \bigotimes_k \sigma(\alpha_k, \beta_k)$ — разложимый.
- Поэтому

$$\mathbf{Pr}(U|0^n\rangle, 1) = \frac{1}{2} - \frac{i^{U_a(f_1)}}{2}\prod_k \langle 0|\sigma(\alpha_k, \beta_k)|0\rangle$$

вычисляется за полиномиальное время.

# Доказательство теоремы Готтесмана – Нилла

- Пусть оператор $U$ задается симплектической схемой.
- По формуле для вероятности наблюдения единицы

$$\mathbf{Pr}(U|0^n\rangle, 1) = \frac{1}{2}\left(1 - \langle 0^n|U^\dagger \sigma(f_1) U|0^n\rangle\right) =$$

$$= \frac{1}{2}\left(1 - i^{U_a(f_1)}\langle 0^n|\sigma(\tilde{U}f_1)|0^n\rangle\right)$$

- $\sigma(\tilde{U}f_1) = \bigotimes_k \sigma(\alpha_k, \beta_k)$ — разложимый.
- Поэтому

$$\mathbf{Pr}(U|0^n\rangle, 1) = \frac{1}{2} - \frac{i^{U_a(f_1)}}{2}\prod_k \langle 0|\sigma(\alpha_k, \beta_k)|0\rangle$$

вычисляется за полиномиальное время.

# Замечания Джоза (Jozsa)

- В доказательстве теоремы Готтесмана – Нилла групповая структура не существенна. Нужны два ингредиента:
- множество $\mathcal{S}_n$ эрмитовых операторов такое, что $\langle 0^n|S|0^n\rangle$ вычисляется эффективно для $S \in \mathcal{S}_n$, нужно также, чтобы это множество содержало $\sigma(f_1)$;
- множество унитарных операторов $\mathcal{K}_n$, сохраняющих $\mathcal{S}_n$, т. е. $K^\dagger SK \in \mathcal{S}_n$ для $K \in \mathcal{K}_n$, $S \in \mathcal{S}_n$.

В случае теоремы Готтесмана – Нилла $\mathcal{S}_n$ — это группа $\sigma$-операторов с фазовыми подкрутками, $\mathcal{K}_n$ — группа симплектических операторов.

# Замечания Джоза (Jozsa)

- В доказательстве теоремы Готтесмана – Нилла групповая структура не существенна. Нужны два ингредиента:
- множество $\mathcal{S}_n$ эрмитовых операторов такое, что $\langle 0^n|S|0^n\rangle$ вычисляется эффективно для $S \in \mathcal{S}_n$, нужно также, чтобы это множество содержало $\sigma(f_1)$;
- множество унитарных операторов $\mathcal{K}_n$, сохраняющих $\mathcal{S}_n$, т. е. $K^\dagger SK \in \mathcal{S}_n$ для $K \in \mathcal{K}_n$, $S \in \mathcal{S}_n$.

В случае теоремы Готтесмана – Нилла $\mathcal{S}_n$ — это группа $\sigma$-операторов с фазовыми подкрутками, $\mathcal{K}_n$ — группа симплектических операторов.

# Замечания Джоза (Jozsa)

- В доказательстве теоремы Готтесмана – Нилла групповая структура не существенна. Нужны два ингредиента:
- множество $\mathcal{S}_n$ эрмитовых операторов такое, что $\langle 0^n|S|0^n\rangle$ вычисляется эффективно для $S \in \mathcal{S}_n$, нужно также, чтобы это множество содержало $\sigma(f_1)$;
- множество унитарных операторов $\mathcal{K}_n$, сохраняющих $\mathcal{S}_n$, т. е. $K^\dagger S K \in \mathcal{S}_n$ для $K \in \mathcal{K}_n$, $S \in \mathcal{S}_n$.

В случае теоремы Готтесмана – Нилла $\mathcal{S}_n$ — это группа $\sigma$-операторов с фазовыми подкрутками, $\mathcal{K}_n$ — группа симплектических операторов.

# Замечания Джоза (Jozsa)

- В доказательстве теоремы Готтесмана – Нилла групповая структура не существенна. Нужны два ингредиента:
- множество $\mathcal{S}_n$ эрмитовых операторов такое, что $\langle 0^n|S|0^n\rangle$ вычисляется эффективно для $S \in \mathcal{S}_n$, нужно также, чтобы это множество содержало $\sigma(f_1)$;
- множество унитарных операторов $\mathcal{K}_n$, сохраняющих $\mathcal{S}_n$, т. е. $K^\dagger SK \in \mathcal{S}_n$ для $K \in \mathcal{K}_n$, $S \in \mathcal{S}_n$.

В случае теоремы Готтесмана – Нилла $\mathcal{S}_n$ — это группа $\sigma$-операторов с фазовыми подкрутками, $\mathcal{K}_n$ — группа симплектических операторов.

# Еще один пример: элементы Вэлианта (matchgates)

## Определение

Двухкубитовый элемент Вэлианта (matchgate) задается матрицей

$$G(A,B) = \begin{pmatrix} p & 0 & 0 & q \\ 0 & w & x & 0 \\ 0 & y & z & 0 \\ r & 0 & 0 & s \end{pmatrix}, \quad \text{где } A = \begin{pmatrix} p & q \\ r & s \end{pmatrix}, \quad B = \begin{pmatrix} w & x \\ y & z \end{pmatrix}$$

две унитарные матрицы с одинаковым детерминантом.

## Плоская схема Вэлианта

В такой схеме кубиты упорядочены и элементы Вэлианта применяются только к соседним кубитам. Предполагается также, что матричные элементы в схеме Вэлианта эффективно вычислимы.

# Еще один пример: элементы Вэлианта (matchgates)

## Определение

Двухкубитовый элемент Вэлианта (matchgate) задается матрицей

$$G(A,B) = \begin{pmatrix} p & 0 & 0 & q \\ 0 & w & x & 0 \\ 0 & y & z & 0 \\ r & 0 & 0 & s \end{pmatrix}, \quad \text{где } A = \begin{pmatrix} p & q \\ r & s \end{pmatrix}, \quad B = \begin{pmatrix} w & x \\ y & z \end{pmatrix}$$

две унитарные матрицы с одинаковым детерминантом.

## Плоская схема Вэлианта

В такой схеме кубиты упорядочены и элементы Вэлианта применяются только к соседним кубитам. Предполагается также, что матричные элементы в схеме Вэлианта эффективно вычислимы.

# Возможности схем Вэлианта

**Теорема (Valiant, 2001)**

Существует алгоритм, который за полиномиальное время вычисляет вероятности наблюдения исходов для состояния, которое получается из $|0^n\rangle$ применением плоской схемы Вэлианта.

**Теорема (Josza, Miyake, 2008)**

Схемы, в которых элементы Вэлианта применяются к кубитам на расстоянии не больше 2, универсальны для квантового вычисления.

# Возможности схем Вэлианта

**Теорема (Valiant, 2001)**

Существует алгоритм, который за полиномиальное время вычисляет вероятности наблюдения исходов для состояния, которое получается из $|0^n\rangle$ применением плоской схемы Вэлианта.

**Теорема (Josza, Miyake, 2008)**

Схемы, в которых элементы Вэлианта применяются к кубитам на расстоянии не больше 2, универсальны для квантового вычисления.

# Доказательства теоремы Вэлианта

- Вэлиант: сводимость к вычислению пфаффиана плоского графа.
- Джоза: выбор подходящего семейства $\mathcal{S}_n$ ($\mathcal{K}_n$ — плоские схемы Вэлианта):

$$\mathcal{S}_n = \mathbb{R}(\sigma_z^{\otimes k} \otimes \sigma_x \otimes I^{\otimes n-k-1}, \sigma_z^{\otimes k} \otimes \sigma_y \otimes I^{\otimes n-k-1}), \quad 1 \leqslant k \leqslant n.$$

- Терхал и Дивинченцо: плоские схемы Вэлианта моделируются системами невзаимодействующих фермионов.

# Доказательства теоремы Вэлианта

- Вэлиант: сводимость к вычислению пфаффиана плоского графа.
- Джоза: выбор подходящего семейства $\mathcal{S}_n$ ($\mathcal{K}_n$ — плоские схемы Вэлианта):

$$\mathcal{S}_n = \mathbb{R}(\sigma_z^{\otimes k} \otimes \sigma_x \otimes I^{\otimes n-k-1}, \sigma_z^{\otimes k} \otimes \sigma_y \otimes I^{\otimes n-k-1}), \quad 1 \leqslant k \leqslant n.$$

- Терхал и Дивинченцо: плоские схемы Вэлианта моделируются системами невзаимодействующих фермионов.

# Доказательства теоремы Вэлианта

- Вэлиант: сводимость к вычислению пфаффиана плоского графа.
- Джоза: выбор подходящего семейства $\mathcal{S}_n$ ($\mathcal{K}_n$ — плоские схемы Вэлианта):

$$\mathcal{S}_n = \mathbb{R}(\sigma_z^{\otimes k} \otimes \sigma_x \otimes I^{\otimes n-k-1}, \sigma_z^{\otimes k} \otimes \sigma_y \otimes I^{\otimes n-k-1}), \quad 1 \leqslant k \leqslant n.$$

- Терхал и Дивинченцо: плоские схемы Вэлианта моделируются системами невзаимодействующих фермионов.

# План

# Проблема шума

## Наблюдение фон Неймана

Аналоговые системы более чувствительны к шуму, чем дискретные. Вероятность неправильного изменения бита невелика и может быть быстро и эффективно уменьшена применением корректирующих кодов.

- Квантовые системы, описываемые стандартной моделью, — аналоговые.
- За счет линейного накопления ошибок для ограниченной ошибки на выходе схемы необходима точность реализации операторов, обратно пропорциональная размеру схемы. Уже это плохо.
- Что еще хуже: помимо неточностей в реализации элементов схем, в реальных системах имеется шум: случайные сбои в работе. Для классических компьютеров проблема шума не слишком тяжела (см. наблюдение фон Неймана).
- Квантовые алгоритмы подвержены шуму в большей степени.

# Проблема шума

## Наблюдение фон Неймана

Аналоговые системы более чувствительны к шуму, чем дискретные. Вероятность неправильного изменения бита невелика и может быть быстро и эффективно уменьшена применением корректирующих кодов.

- Квантовые системы, описываемые стандартной моделью, — аналоговые.
- За счет линейного накопления ошибок для ограниченной ошибки на выходе схемы необходима точность реализации операторов, обратно пропорциональная размеру схемы. Уже это плохо.
- Что еще хуже: помимо неточностей в реализации элементов схем, в реальных системах имеется шум: случайные сбои в работе. Для классических компьютеров проблема шума не слишком тяжела (см. наблюдение фон Неймана).
- Квантовые алгоритмы подвержены шуму в большей степени.

# Проблема шума

## Наблюдение фон Неймана

Аналоговые системы более чувствительны к шуму, чем дискретные. Вероятность неправильного изменения бита невелика и может быть быстро и эффективно уменьшена применением корректирующих кодов.

- Квантовые системы, описываемые стандартной моделью, — аналоговые.
- За счет линейного накопления ошибок для ограниченной ошибки на выходе схемы необходима точность реализации операторов, обратно пропорциональная размеру схемы. Уже это плохо.
- Что еще хуже: помимо неточностей в реализации элементов схем, в реальных системах имеется шум: случайные сбои в работе. Для классических компьютеров проблема шума не слишком тяжела (см. наблюдение фон Неймана).
- Квантовые алгоритмы подвержены шуму в большей степени.

# Проблема шума

## Наблюдение фон Неймана

Аналоговые системы более чувствительны к шуму, чем дискретные. Вероятность неправильного изменения бита невелика и может быть быстро и эффективно уменьшена применением корректирующих кодов.

- Квантовые системы, описываемые стандартной моделью, — аналоговые.
- За счет линейного накопления ошибок для ограниченной ошибки на выходе схемы необходима точность реализации операторов, обратно пропорциональная размеру схемы. Уже это плохо.
- Что еще хуже: помимо неточностей в реализации элементов схем, в реальных системах имеется шум: случайные сбои в работе. Для классических компьютеров проблема шума не слишком тяжела (см. наблюдение фон Неймана).
- Квантовые алгоритмы подвержены шуму в большей степени.

# Проблема шума

## Наблюдение фон Неймана

Аналоговые системы более чувствительны к шуму, чем дискретные. Вероятность неправильного изменения бита невелика и может быть быстро и эффективно уменьшена применением корректирующих кодов.

- Квантовые системы, описываемые стандартной моделью, — аналоговые.
- За счет линейного накопления ошибок для ограниченной ошибки на выходе схемы необходима точность реализации операторов, обратно пропорциональная размеру схемы. Уже это плохо.
- Что еще хуже: помимо неточностей в реализации элементов схем, в реальных системах имеется шум: случайные сбои в работе. Для классических компьютеров проблема шума не слишком тяжела (см. наблюдение фон Неймана).
- Квантовые алгоритмы подвержены шуму в большей степени.

# Основной вопрос

Предположим, что при реализации элемента квантовой схемы возникает ошибка, причем вероятность ошибки мала (но не сколь угодно мала) и каждая ошибка влияет только на небольшое количество кубитов.

Можно ли, используя такие элементы строить сколь угодно большие схемы, которые дают ответ с небольшой вероятностью ошибки?

**Вопрос**

Какова модель ошибки в квантовом случае?

# Основной вопрос

Предположим, что при реализации элемента квантовой схемы возникает ошибка, причем вероятность ошибки мала (но не сколь угодно мала) и каждая ошибка влияет только на небольшое количество кубитов.
Можно ли, используя такие элементы строить сколь угодно большие схемы, которые дают ответ с небольшой вероятностью ошибки?

**Вопрос**

Какова модель ошибки в квантовом случае?

# Основной вопрос

Предположим, что при реализации элемента квантовой схемы возникает ошибка, причем вероятность ошибки мала (но не сколь угодно мала) и каждая ошибка влияет только на небольшое количество кубитов.
Можно ли, используя такие элементы строить сколь угодно большие схемы, которые дают ответ с небольшой вероятностью ошибки?

**Вопрос**

Какова модель ошибки в квантовом случае?

# Открытые квантовые системы

Ошибка возникает из-за взаимодействия с окружающей средой.
Поэтому наша модель (унитарные операторы) недостаточна.

**Пример**

Возьмем ЭПР пару

$$|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle.$$

Предположим, что ошибка состоит в том, что потерялся второй кубит.
В каком состоянии оказывается первый кубит?
Ответ: Первый кубит с вероятностью $1/2$ находится в состоянии $|0\rangle$ и с вероятностью $1/2$ в состоянии $|1\rangle$.
Не существует чистого квантового состояния, которое давало бы такие вероятности наблюдения исходов.

# Открытые квантовые системы

Ошибка возникает из-за взаимодействия с окружающей средой.
Поэтому наша модель (унитарные операторы) недостаточна.

## Пример

Возьмем ЭПР пару

$$|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle.$$

Предположим, что ошибка состоит в том, что потерялся второй кубит.
В каком состоянии оказывается первый кубит?
Ответ: Первый кубит с вероятностью $1/2$ находится в состоянии $|0\rangle$ и с вероятностью $1/2$ в состоянии $|1\rangle$.
Не существует чистого квантового состояния, которое давало бы такие вероятности наблюдения исходов.

# Открытые квантовые системы

Ошибка возникает из-за взаимодействия с окружающей средой.
Поэтому наша модель (унитарные операторы) недостаточна.

## Пример

Возьмем ЭПР пару

$$|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle.$$

Предположим, что ошибка состоит в том, что потерялся второй кубит.
В каком состоянии оказывается первый кубит?
Ответ: Первый кубит с вероятностью $1/2$ находится в состоянии $|0\rangle$ и с вероятностью $1/2$ в состоянии $|1\rangle$.
Не существует чистого квантового состояния, которое давало бы такие вероятности наблюдения исходов.

# Смешанные состояния

## Определение

Два вероятностных распределения на чистых состояниях неразличимы, если они дают одинаковые распределения исходов при одинаковом наблюдении.
Класс неразличимых распределений на чистых состояниях называется смешанным состоянием.

## Теорема

Смешанное состояние однозначно описывается оператором плотности $\rho$, удовлетворящим условиям:

$$\rho^\dagger = \rho; \quad \langle\psi|\rho|\psi\rangle \geqslant 0; \quad \operatorname{Tr}\rho = 1.$$

Вероятность наблюдения исхода $x$ в состоянии $\rho$ равна

$$\mathbf{Pr}(\rho, x) = \operatorname{Tr}(\rho\Pi_x) = \langle x|\rho|x\rangle.$$

# Чистые состояния

Чистое состояние — это оператор плотности ранга 1, т. е. $\Pi_\psi = |\psi\rangle\langle\psi|$.

Вероятностные распределения на чистых состояниях

$$\rho = \sum_j p_j \Pi_{\psi_j}, \quad p_j \geqslant 0, \ \sum_j p_j = 1$$

дают все операторы плотности.

Вероятности исходов в чистом состоянии

$$\mathbf{Pr}(|\psi\rangle, x) = |c_x|^2 = \langle x|\psi\rangle\langle\psi|x\rangle = \langle x|\Pi_\psi|x\rangle = \mathrm{Tr}(\Pi_\psi \Pi_x).$$

В последнем равенстве использовано циклическое свойство следа

$$\mathrm{Tr}(ABC) = \sum_{j,k,l} a_{jk} b_{kl} c_{lj} = \mathrm{Tr}(BCA).$$

Для смешанного состояния получаем

$$\mathbf{Pr}(\sum_j p_j \Pi_{\psi_j}, x) = \sum_j p_j \,\mathrm{Tr}(\Pi_\psi \Pi_x) = \mathrm{Tr}(\rho \Pi_x).$$

# Чистые состояния

Чистое состояние — это оператор плотности ранга 1, т. е. $\Pi_\psi = |\psi\rangle\langle\psi|$.
Вероятностные распределения на чистых состояниях

$$\rho = \sum_j p_j \Pi_{\psi_j}, \quad p_j \geqslant 0, \ \sum_j p_j = 1$$

дают все операторы плотности.

Вероятности исходов в чистом состоянии

$$\mathbf{Pr}(|\psi\rangle, x) = |c_x|^2 = \langle x|\psi\rangle\langle\psi|x\rangle = \langle x|\Pi_\psi|x\rangle = \operatorname{Tr}(\Pi_\psi \Pi_x).$$

В последнем равенстве использовано циклическое свойство следа

$$\operatorname{Tr}(ABC) = \sum_{j,k,l} a_{jk} b_{kl} c_{lj} = \operatorname{Tr}(BCA).$$

Для смешанного состояния получаем

$$\mathbf{Pr}(\sum_j p_j \Pi_{\psi_j}, x) = \sum_j p_j \operatorname{Tr}(\Pi_\psi \Pi_x) = \operatorname{Tr}(\rho \Pi_x).$$

# Чистые состояния

Чистое состояние — это оператор плотности ранга 1, т. е. $\Pi_\psi = |\psi\rangle\langle\psi|$.
Вероятностные распределения на чистых состояниях

$$\rho = \sum_j p_j \Pi_{\psi_j}, \quad p_j \geqslant 0, \ \sum_j p_j = 1$$

дают все операторы плотности.
Вероятности исходов в чистом состоянии

$$\mathbf{Pr}(|\psi\rangle, x) = |c_x|^2 = \langle x|\psi\rangle\langle\psi|x\rangle = \langle x|\Pi_\psi|x\rangle = \mathrm{Tr}(\Pi_\psi \Pi_x).$$

В последнем равенстве использовано циклическое свойство следа

$$\mathrm{Tr}(ABC) = \sum_{j,k,l} a_{jk} b_{kl} c_{lj} = \mathrm{Tr}(BCA).$$

Для смешанного состояния получаем

$$\mathbf{Pr}(\sum_j p_j \Pi_{\psi_j}, x) = \sum_j p_j \,\mathrm{Tr}(\Pi_\psi \Pi_x) = \mathrm{Tr}(\rho \Pi_x).$$

# Чистые состояния

Чистое состояние — это оператор плотности ранга 1, т. е. $\Pi_\psi = |\psi\rangle\langle\psi|$.
Вероятностные распределения на чистых состояниях

$$\rho = \sum_j p_j \Pi_{\psi_j}, \quad p_j \geqslant 0, \ \sum_j p_j = 1$$

дают все операторы плотности.
Вероятности исходов в чистом состоянии

$$\mathbf{Pr}(|\psi\rangle, x) = |c_x|^2 = \langle x|\psi\rangle\langle\psi|x\rangle = \langle x|\Pi_\psi|x\rangle = \mathrm{Tr}(\Pi_\psi \Pi_x).$$

В последнем равенстве использовано циклическое свойство следа

$$\mathrm{Tr}(ABC) = \sum_{j,k,l} a_{jk} b_{kl} c_{lj} = \mathrm{Tr}(BCA).$$

Для смешанного состояния получаем

$$\mathbf{Pr}(\sum_j p_j \Pi_{\psi_j}, x) = \sum_j p_j \,\mathrm{Tr}(\Pi_\psi \Pi_x) = \mathrm{Tr}(\rho \Pi_x).$$

# Состояние части квантового системы

- Пусть мы имеем $\rho$ — смешанное в общем случае состояние составной системы $AB$, где возможные результаты наблюдения системы $A$ — это $\{a_1, \ldots, a_n\}$, а системы $B$ — это $\{b_1, \ldots, b_m\}$.
- Как определить состояние подсистемы $A$?
- Для этого нужно посчитать вероятность наблюдения результата $a_j$ в составной системе и выразить ее с помощью подходящего оператора плотности:

$$\mathbf{Pr}(\rho, a_j) = \sum_k \mathbf{Pr}(\rho, a_j b_k) = \mathbf{Pr}(\mathrm{Tr}_B\, \rho, a_j).$$

- Здесь $\mathrm{Tr}_B\, \rho$ обозначает искомый ответ, который называется частичным следом оператора.

# Состояние части квантового системы

- Пусть мы имеем $\rho$ — смешанное в общем случае состояние составной системы $AB$, где возможные результаты наблюдения системы $A$ — это $\{a_1, \ldots, a_n\}$, а системы $B$ — это $\{b_1, \ldots, b_m\}$.
- Как определить состояние подсистемы $A$?
- Для этого нужно посчитать вероятность наблюдения результата $a_j$ в составной системе и выразить ее с помощью подходящего оператора плотности:

$$\mathbf{Pr}(\rho, a_j) = \sum_k \mathbf{Pr}(\rho, a_j b_k) = \mathbf{Pr}(\mathrm{Tr}_B\, \rho, a_j).$$

- Здесь $\mathrm{Tr}_B\, \rho$ обозначает искомый ответ, который называется частичным следом оператора.

# Состояние части квантового системы

- Пусть мы имеем $\rho$ — смешанное в общем случае состояние составной системы $AB$, где возможные результаты наблюдения системы $A$ — это $\{a_1, \ldots, a_n\}$, а системы $B$ — это $\{b_1, \ldots, b_m\}$.
- Как определить состояние подсистемы $A$?
- Для этого нужно посчитать вероятность наблюдения результата $a_i$ в составной системе и выразить ее с помощью подходящего оператора плотности:

$$\mathbf{Pr}(\rho, a_j) = \sum_k \mathbf{Pr}(\rho, a_j b_k) = \mathbf{Pr}(\mathrm{Tr}_B\, \rho, a_j).$$

- Здесь $\mathrm{Tr}_B\, \rho$ обозначает искомый ответ, который называется частичным следом оператора.

# Состояние части квантового системы

- Пусть мы имеем $\rho$ — смешанное в общем случае состояние составной системы $AB$, где возможные результаты наблюдения системы $A$ — это $\{a_1, \ldots, a_n\}$, а системы $B$ — это $\{b_1, \ldots, b_m\}$.
- Как определить состояние подсистемы $A$?
- Для этого нужно посчитать вероятность наблюдения результата $a_i$ в составной системе и выразить ее с помощью подходящего оператора плотности:

$$\mathbf{Pr}(\rho, a_j) = \sum_k \mathbf{Pr}(\rho, a_j b_k) = \mathbf{Pr}(\mathrm{Tr}_B\, \rho, a_j).$$

- Здесь $\mathrm{Tr}_B\, \rho$ обозначает искомый ответ, который называется частичным следом оператора.

# Частичный след

## Определение

Частичный след — это линейное отображение операторов на пространстве $\mathcal{A} \otimes \mathcal{B}$ в операторы на пространстве $\mathcal{A}$, которое на разложимых операторах задается формулой

$$\mathrm{Tr}_B(X \otimes Y) = X \,\mathrm{Tr}\, Y,$$

а на остальные операторы продолжается по линейности.

## Упражнение

Докажите корректность определения частичного следа (значение не зависит от представления оператора в виде суммы разложимых).

## Упражнение

Проверьте, что для разложимых чистых состояний $\rho = \rho_1 \otimes \rho_2$

$$\mathbf{Pr}(\rho, a_j) = \mathbf{Pr}(\mathrm{Tr}_B\, \rho, a_j).$$

# Частичный след

## Определение

Частичный след — это линейное отображение операторов на пространстве $\mathcal{A} \otimes \mathcal{B}$ в операторы на пространстве $\mathcal{A}$, которое на разложимых операторах задается формулой

$$\mathrm{Tr}_B(X \otimes Y) = X \,\mathrm{Tr}\, Y,$$

а на остальные операторы продолжается по линейности.

## Упражнение

Докажите корректность определения частичного следа (значение не зависит от представления оператора в виде суммы разложимых).

## Упражнение

Проверьте, что для разложимых чистых состояний $\rho = \rho_1 \otimes \rho_2$

$$\mathbf{Pr}(\rho, a_j) = \mathbf{Pr}(\mathrm{Tr}_B\, \rho, a_j).$$

# Частичный след

## Определение

Частичный след — это линейное отображение операторов на пространстве $\mathcal{A} \otimes \mathcal{B}$ в операторы на пространстве $\mathcal{A}$, которое на разложимых операторах задается формулой

$$\mathrm{Tr}_B(X \otimes Y) = X \,\mathrm{Tr}\, Y,$$

а на остальные операторы продолжается по линейности.

## Упражнение

Докажите корректность определения частичного следа (значение не зависит от представления оператора в виде суммы разложимых).

## Упражнение

Проверьте, что для разложимых чистых состояний $\rho = \rho_1 \otimes \rho_2$

$$\mathbf{Pr}(\rho, a_j) = \mathbf{Pr}(\mathrm{Tr}_B\, \rho, a_j).$$

# Физически возможные преобразования смешанных состояний

Всего три вида преобразований:

- Действие унитарного оператора на операторах плотности:

$$\rho \mapsto U\rho U^\dagger$$

(Для чистых состояний согласовано с предыдущим определением $|\psi\rangle\langle\psi| \mapsto U|\psi\rangle\langle\psi|U^\dagger = |U\psi\rangle\langle U\psi|$.)

- Добавление в систему новой части в известном состоянии $\gamma$:

$$\rho \mapsto \rho \otimes \gamma;$$

- Отбрасывание части составной системы (взятие частичного следа):

$$\rho \mapsto \mathrm{Tr}_B\, \rho.$$

# Физически возможные преобразования смешанных состояний

Всего три вида преобразований:

- Действие унитарного оператора на операторах плотности:

$$\rho \mapsto U\rho U^\dagger$$

(Для чистых состояний согласовано с предыдущим определением $|\psi\rangle\langle\psi| \mapsto U|\psi\rangle\langle\psi|U^\dagger = |U\psi\rangle\langle U\psi|$.)

- Добавление в систему новой части в известном состоянии $\gamma$:

$$\rho \mapsto \rho \otimes \gamma;$$

- Отбрасывание части составной системы (взятие частичного следа):

$$\rho \mapsto \mathrm{Tr}_B\, \rho.$$

# Физически возможные преобразования смешанных состояний

Всего три вида преобразований:

- Действие унитарного оператора на операторах плотности:

$$\rho \mapsto U\rho U^\dagger$$

(Для чистых состояний согласовано с предыдущим определением $|\psi\rangle\langle\psi| \mapsto U|\psi\rangle\langle\psi|U^\dagger = |U\psi\rangle\langle U\psi|$.)

- Добавление в систему новой части в известном состоянии $\gamma$:

$$\rho \mapsto \rho \otimes \gamma;$$

- Отбрасывание части составной системы (взятие частичного следа):

$$\rho \mapsto \mathrm{Tr}_B\, \rho.$$

# Модель квантовой ошибки

## Определение

Элемент $U$ с ошибкой $\varepsilon$ на $r$ кубитах реализует преобразование операторов плотности

$$\rho \mapsto (1-\varepsilon)U\rho U^\dagger + \varepsilon E(\rho),$$

где $E$ — преобразование матриц плотности, которое является суммой преобразований, нетривиально действующих на $r$ кубитах.

## Теорема (представление операторной суммой)

Любое физически реализуемое преобразование матриц плотности представляется в виде

$$\rho \mapsto \sum_m A_m \rho A_m^\dagger, \quad \text{где} \sum_m A_m^\dagger A_m = I.$$

## Следствие

Множество физически реализуемых преобразований выпукло.

# Модель квантовой ошибки

## Определение

Элемент $U$ с ошибкой $\varepsilon$ на $r$ кубитах реализует преобразование операторов плотности

$$\rho \mapsto (1-\varepsilon)U\rho U^\dagger + \varepsilon E(\rho),$$

где $E$ — преобразование матриц плотности, которое является суммой преобразований, нетривиально действующих на $r$ кубитах.

## Теорема (представление операторной суммой)

Любое физически реализуемое преобразование матриц плотности представляется в виде

$$\rho \mapsto \sum_m A_m \rho A_m^\dagger, \quad \text{где} \ \sum_m A_m^\dagger A_m = I.$$

## Следствие

Множество физически реализуемых преобразований выпукло.

# Модель квантовой ошибки

## Определение

Элемент $U$ с ошибкой $\varepsilon$ на $r$ кубитах реализует преобразование операторов плотности

$$\rho \mapsto (1-\varepsilon)U\rho U^\dagger + \varepsilon E(\rho),$$

где $E$ — преобразование матриц плотности, которое является суммой преобразований, нетривиально действующих на $r$ кубитах.

## Теорема (представление операторной суммой)

Любое физически реализуемое преобразование матриц плотности представляется в виде

$$\rho \mapsto \sum_m A_m \rho A_m^\dagger, \quad \text{где} \ \sum_m A_m^\dagger A_m = I.$$

## Следствие

Множество физически реализуемых преобразований выпукло.

# Почему квантовые ошибки сложнее исправлять

Код повторений: кубит $|0\rangle$ кодируется кубитом $|0^n\rangle$, а кубит $|1\rangle$ — кубитом $|1^n\rangle$.
В классическом случае можно обнаружить и исправить чуть меньше половины ошибок.
В квантовом случае это не так. Уже ошибка на одном кубите, причем унитарная, приводит к совпадению кодовых векторов. Рассмотрим два вектора из кодового пространства:

$$|\psi_1\rangle = |0^n\rangle + |1^n\rangle; \quad |\psi_2\rangle = |0^n\rangle - |1^n\rangle.$$

Пусть ошибка имеет вид $E = \sigma_z[j]$. Тогда $E|\psi_2\rangle = |\psi_1\rangle$. После такой ошибки у нас не остается шансов различить эти два кодовых вектора.

## Определение

Квантовый код, исправляющий ошибки из множества $\mathcal{E}$ — это подпространство $V$ пространства $(\mathbb{C}^2)^{\otimes n}$ такое, что

$$\forall\, |\xi_1\rangle, |\xi_2\rangle \in V\ \forall\, X, Y \in \mathcal{E}\ (\langle\xi_2|\xi_1\rangle = 0) \Rightarrow \Big(\langle\xi_2|Y^\dagger X|\xi_1\rangle = 0\Big). \qquad (*)$$

## Коды, исправляющие $r$ ошибок

В этом случае $\mathcal{E}$ состоит из линейных отображений, которые являются суммами $r$-локальных (действующих только на $r$ кубитах).
В этом случае условие (*) упрощается до

$$\forall\, |\xi_1\rangle, |\xi_2\rangle \in V\ \forall\, f \in \mathbb{F}_2^{2n}(\|f\| \leqslant 2r)\ (\langle\xi_2|\xi_1\rangle = 0) \Rightarrow (\langle\xi_2|\sigma(f)|\xi_1\rangle = 0). \qquad (**)$$

Здесь $\|f\|$ — количество ненулевых пар $(\alpha_k, \beta_k)$ в наборе $f$.

# Квантовые корректирующие коды

## Определение

Квантовый код, исправляющий ошибки из множества $\mathcal{E}$ — это подпространство $V$ пространства $(\mathbb{C}^2)^{\otimes n}$ такое, что

$$\forall\, |\xi_1\rangle, |\xi_2\rangle \in V\ \forall\, X, Y \in \mathcal{E}\ (\langle\xi_2|\xi_1\rangle = 0) \Rightarrow \Big(\langle\xi_2|Y^\dagger X|\xi_1\rangle = 0\Big). \qquad (*)$$

## Коды, исправляющие $r$ ошибок

В этом случае $\mathcal{E}$ состоит из линейных отображений, которые являются суммами $r$-локальных (действующих только на $r$ кубитах).
В этом случае условие (*) упрощается до

$$\forall\, |\xi_1\rangle, |\xi_2\rangle \in V\ \forall\, f \in \mathbb{F}_2^{2n}(\|f\| \leqslant 2r)\ (\langle\xi_2|\xi_1\rangle = 0) \Rightarrow (\langle\xi_2|\sigma(f)|\xi_1\rangle = 0). \qquad (**)$$

Здесь $\|f\|$ — количество ненулевых пар $(\alpha_k, \beta_k)$ в наборе $f$.

# Симплектические коды (stabilizer codes)

## Идея конструкции

В качестве кода выбираются собственные подпространства систем попарно коммутирующих $\sigma$-операторов.

## Задача (правила коммутирования $\sigma$-операторов)

Проверьте, что $\sigma(f)\sigma(g) = (-1)^{\omega(f,g)}\sigma(g)\sigma(f)$, где

$$\omega(f,g) = \sum_k \Big(\alpha_k(f)\beta_k(g) - \alpha_k(g)\beta_k(f)\Big) \bmod 2.$$

Таким образом, симплектический код задается изотропным подпространством $F$ пространства $\mathbb{F}_2^n$, снабженного симплектической формой $\omega$.

# Симплектические коды (stabilizer codes)

## Идея конструкции

В качестве кода выбираются собственные подпространства систем попарно коммутирующих $\sigma$-операторов.

## Задача (правила коммутирования $\sigma$-операторов)

Проверьте, что $\sigma(f)\sigma(g) = (-1)^{\omega(f,g)}\sigma(g)\sigma(f)$, где

$$\omega(f,g) = \sum_k \Big(\alpha_k(f)\beta_k(g) - \alpha_k(g)\beta_k(f)\Big) \bmod 2.$$

Таким образом, симплектический код задается изотропным подпространством $F$ пространства $\mathbb{F}_2^n$, снабженного симплектической формой $\omega$.

# Симплектические коды (stabilizer codes)

## Идея конструкции

В качестве кода выбираются собственные подпространства систем попарно коммутирующих $\sigma$-операторов.

## Задача (правила коммутирования $\sigma$-операторов)

Проверьте, что $\sigma(f)\sigma(g) = (-1)^{\omega(f,g)}\sigma(g)\sigma(f)$, где

$$\omega(f,g) = \sum_k \Big(\alpha_k(f)\beta_k(g) - \alpha_k(g)\beta_k(f)\Big) \bmod 2.$$

Таким образом, симплектический код задается изотропным подпространством $F$ пространства $\mathbb{F}_2^n$, снабженного симплектической формой $\omega$.

# Кодовое расстояние симплектического кода

## Теорема

Кодовое расстояние кода, задаваемого подпространством $F$, равно

$$\min(\|f\| : f \in F^{\perp} \setminus F), \quad \text{где } F^{\perp} = \{g : \forall f \in F\ \omega(f,g) = 0\}.$$

Эта теорема позволяет применять конструкции классических корректирующих кодов (с дополнительными условиями) для построения квантовых кодов.

## Неформальная аннотация теории квантовых корректирующих кодов

Всё хорошо. Есть конструкции кодов, исправляющих любое заданное количество ошибок. Есть асимптотически хорошие квантовые коды. Возможны каскадные конструкции. Есть процедуры декодирования (причем реализуются в симплектическом базисе).

# Кодовое расстояние симплектического кода

**Теорема**

Кодовое расстояние кода, задаваемого подпространством $F$, равно

$$\min(\|f\| : f \in F^{\perp} \setminus F), \quad \text{где } F^{\perp} = \{g : \forall f \in F\ \omega(f,g) = 0\}.$$

Эта теорема позволяет применять конструкции классических корректирующих кодов (с дополнительными условиями) для построения квантовых кодов.

**Неформальная аннотация теории квантовых корректирующих кодов**

Всё хорошо. Есть конструкции кодов, исправляющих любое заданное количество ошибок. Есть асимптотически хорошие квантовые коды. Возможны каскадные конструкции. Есть процедуры декодирования (причем реализуются в симплектическом базисе).

# Кодовое расстояние симплектического кода

## Теорема

Кодовое расстояние кода, задаваемого подпространством $F$, равно

$$\min(\|f\| : f \in F^{\perp} \setminus F), \quad \text{где } F^{\perp} = \{g : \forall f \in F\ \omega(f,g) = 0\}.$$

Эта теорема позволяет применять конструкции классических корректирующих кодов (с дополнительными условиями) для построения квантовых кодов.

## Неформальная аннотация теории квантовых корректирующих кодов

Всё хорошо. Есть конструкции кодов, исправляющих любое заданное количество ошибок. Есть асимптотически хорошие квантовые коды. Возможны каскадные конструкции. Есть процедуры декодирования (причем реализуются в симплектическом базисе).

# Основные идеи квантового вычисления, устойчивого к ошибкам

- Кубиты кодируются корректирующим кодом, после чего применяется каскадная конструкция для уменьшения вероятности ошибки (глубина каскада — логарифм от размера схемы, которую нужно реализовать).
- Действия над закодированными кубитами выполняются без раскодирования: строятся преобразования кодовых слов, отвечающие действию унитарного оператора на исходных кубитах.

# Основные идеи квантового вычисления, устойчивого к ошибкам

- Кубиты кодируются корректирующим кодом, после чего применяется каскадная конструкция для уменьшения вероятности ошибки (глубина каскада — логарифм от размера схемы, которую нужно реализовать).
- Действия над закодированными кубитами выполняются без раскодирования: строятся преобразования кодовых слов, отвечающие действию унитарного оператора на исходных кубитах.

# Пороговая теорема

## Формулировка

Существует такое число $p_0$, что любая квантовая схема размера $\ell$ может быть реализована с вероятностью ошибки не более $\varepsilon$ схемой размера $O(\mathrm{poly}(\log \ell/\varepsilon)\ell)$ из неточных элементов, вероятность ошибки каждого из которых не превосходит $p_0$.

Важные уточнения.

- Пороговая теорема доказана лишь при очень малых значениях порога: $p_0 \sim 10^{-5}$. Один из критических вопросов в области квантовых вычислений: определить точную величину порога.
- Неизбежность высокого параллелизма. Схемы из неточных элементов, в которых одновременно преобразуются лишь $O(1)$ кубитов, при любой ненулевой величине порога ошибки моделируются вероятностными алгоритмами.

# Пороговая теорема

## Формулировка

Существует такое число $p_0$, что любая квантовая схема размера $\ell$ может быть реализована с вероятностью ошибки не более $\varepsilon$ схемой размера $O(\mathrm{poly}(\log \ell/\varepsilon)\ell)$ из неточных элементов, вероятность ошибки каждого из которых не превосходит $p_0$.

Важные уточнения.

- Пороговая теорема доказана лишь при очень малых значениях порога: $p_0 \sim 10^{-5}$. Один из критических вопросов в области квантовых вычислений: определить точную величину порога.
- Неизбежность высокого параллелизма. Схемы из неточных элементов, в которых одновременно преобразуются лишь $O(1)$ кубитов, при любой ненулевой величине порога ошибки моделируются вероятностными алгоритмами.

# Пороговая теорема

## Формулировка

Существует такое число $p_0$, что любая квантовая схема размера $\ell$ может быть реализована с вероятностью ошибки не более $\varepsilon$ схемой размера $O(\mathrm{poly}(\log \ell/\varepsilon)\ell)$ из неточных элементов, вероятность ошибки каждого из которых не превосходит $p_0$.

Важные уточнения.

- Пороговая теорема доказана лишь при очень малых значениях порога: $p_0 \sim 10^{-5}$. Один из критических вопросов в области квантовых вычислений: определить точную величину порога.
- Неизбежность высокого параллелизма. Схемы из неточных элементов, в которых одновременно преобразуются лишь $O(1)$ кубитов, при любой ненулевой величине порога ошибки моделируются вероятностными алгоритмами.

# План

# Шкала оптимизма

Квантовые компьютеры

1. никогда не будут созданы, потому что их вычислительные возможности не стоят усилий по их созданию.
2. никогда не будут созданы из-за непреодолимых технологических трудностей.
3. невозможны, поскольку противоречат (еще не открытым) законам природы.
4. будут построены, но будут реализовывать более слабую, чем стандартная, модель квантового вычисления.
5. на основе известных законов квантовой механики возможны и будут построены в обозримом будущем.
6. могут быть гораздо мощнее, чем нам сейчас кажется из-за неполноты знаний законов квантового мира. Когда они будут созданы, квантовые компьютеры смогут решать алгоритмически неразрешимые задачи.

# Шкала оптимизма

Квантовые компьютеры

1. никогда не будут созданы, потому что их вычислительные возможности не стоят усилий по их созданию.
2. никогда не будут созданы из-за непреодолимых технологических трудностей.
3. невозможны, поскольку противоречат (еще не открытым) законам природы.
4. будут построены, но будут реализовывать более слабую, чем стандартная, модель квантового вычисления.
5. на основе известных законов квантовой механики возможны и будут построены в обозримом будущем.
6. могут быть гораздо мощнее, чем нам сейчас кажется из-за неполноты знаний законов квантового мира. Когда они будут созданы, квантовые компьютеры смогут решать алгоритмически неразрешимые задачи.

# Шкала оптимизма

Квантовые компьютеры

1. никогда не будут созданы, потому что их вычислительные возможности не стоят усилий по их созданию.
2. никогда не будут созданы из-за непреодолимых технологических трудностей.
3. невозможны, поскольку противоречат (еще не открытым) законам природы.
4. будут построены, но будут реализовывать более слабую, чем стандартная, модель квантового вычисления.
5. на основе известных законов квантовой механики возможны и будут построены в обозримом будущем.
6. могут быть гораздо мощнее, чем нам сейчас кажется из-за неполноты знаний законов квантового мира. Когда они будут созданы, квантовые компьютеры смогут решать алгоритмически неразрешимые задачи.

# Шкала оптимизма

Квантовые компьютеры

1. никогда не будут созданы, потому что их вычислительные возможности не стоят усилий по их созданию.
2. никогда не будут созданы из-за непреодолимых технологических трудностей.
3. невозможны, поскольку противоречат (еще не открытым) законам природы.
4. будут построены, но будут реализовывать более слабую, чем стандартная, модель квантового вычисления.
5. на основе известных законов квантовой механики возможны и будут построены в обозримом будущем.
6. могут быть гораздо мощнее, чем нам сейчас кажется из-за неполноты знаний законов квантового мира. Когда они будут созданы, квантовые компьютеры смогут решать алгоритмически неразрешимые задачи.

# Шкала оптимизма

Квантовые компьютеры

1. никогда не будут созданы, потому что их вычислительные возможности не стоят усилий по их созданию.
2. никогда не будут созданы из-за непреодолимых технологических трудностей.
3. невозможны, поскольку противоречат (еще не открытым) законам природы.
4. будут построены, но будут реализовывать более слабую, чем стандартная, модель квантового вычисления.
5. на основе известных законов квантовой механики возможны и будут построены в обозримом будущем.
6. могут быть гораздо мощнее, чем нам сейчас кажется из-за неполноты знаний законов квантового мира. Когда они будут созданы, квантовые компьютеры смогут решать алгоритмически неразрешимые задачи.

# Шкала оптимизма

Квантовые компьютеры

1. никогда не будут созданы, потому что их вычислительные возможности не стоят усилий по их созданию.
2. никогда не будут созданы из-за непреодолимых технологических трудностей.
3. невозможны, поскольку противоречат (еще не открытым) законам природы.
4. будут построены, но будут реализовывать более слабую, чем стандартная, модель квантового вычисления.
5. на основе известных законов квантовой механики возможны и будут построены в обозримом будущем.
6. могут быть гораздо мощнее, чем нам сейчас кажется из-за неполноты знаний законов квантового мира. Когда они будут созданы, квантовые компьютеры смогут решать алгоритмически неразрешимые задачи.

# Подходы к построению квантового компьютера

- Фотоны.
- Ионные ловушки.
- ЯМР.
- Ядерные спины в полупроводниках.
- Экзотические физические системы. Пример: топологические квазичастицы — анионы. К сожалению, анионов нужного сорта пока открыть не удалось.

# Подходы к построению квантового компьютера

- Фотоны.
- Ионные ловушки.
- ЯМР.
- Ядерные спины в полупроводниках.
- Экзотические физические системы. Пример: топологические квазичастицы — анионы. К сожалению, анионов нужного сорта пока открыть не удалось.

# Подходы к построению квантового компьютера

- Фотоны.
- Ионные ловушки.
- ЯМР.
- Ядерные спины в полупроводниках.
- Экзотические физические системы. Пример: топологические квазичастицы — анионы. К сожалению, анионов нужного сорта пока открыть не удалось.

# Подходы к построению квантового компьютера

- Фотоны.
- Ионные ловушки.
- ЯМР.
- Ядерные спины в полупроводниках.
- Экзотические физические системы. Пример: топологические квазичастицы — анионы. К сожалению, анионов нужного сорта пока открыть не удалось.

# Подходы к построению квантового компьютера

- Фотоны.
- Ионные ловушки.
- ЯМР.
- Ядерные спины в полупроводниках.
- Экзотические физические системы. Пример: топологические квазичастицы — анионы. К сожалению, анионов нужного сорта пока открыть не удалось.

# Линейная оптика

- Чтобы реализовать универсальное квантовое вычисление, нужны нелинейные оптические элементы.
- Это плохо из-за большого затухания в таких элементах.
- Если ограничиться только линейными элементами (светоделители и фазовращатели — почти то же самое, что полупрозрачные пластинки и поляризационные фильтры), то получается интересная ограниченная модель квантового вычисления.

# Линейная оптика

- Чтобы реализовать универсальное квантовое вычисление, нужны нелинейные оптические элементы.
- Это плохо из-за большого затухания в таких элементах.
- Если ограничиться только линейными элементами (светоделители и фазовращатели — почти то же самое, что полупрозрачные пластинки и поляризационные фильтры), то получается интересная ограниченная модель квантового вычисления.

# Линейная оптика

- Чтобы реализовать универсальное квантовое вычисление, нужны нелинейные оптические элементы.
- Это плохо из-за большого затухания в таких элементах.
- Если ограничиться только линейными элементами (светоделители и фазовращатели — почти то же самое, что полупрозрачные пластинки и поляризационные фильтры), то получается интересная ограниченная модель квантового вычисления.

# Линейная оптика на полиномах

- Состояния вычислительной системы — многочлены из $\mathbb{C}[x_1, \ldots, x_m]$ степени $n$, здесь $m \geqslant n$.
- Начальное состояние $f_0 = x_1 x_2 \ldots x_n$.
- Вычисление: применение унитарного преобразования $U$ к переменным:

$$f_{\text{final}}(x) = f_0(Ux).$$

- Измерение в состоянии

$$\sum_{S=(s_1,\ldots,s_n)} \alpha_S x_1^{s_1} \ldots x_m^{s_m}$$

дает $S$ с вероятностью $\mathbf{Pr}[S] = |\alpha_S|^2 s_1! \ldots s_m!$.

# Линейная оптика на полиномах

- Состояния вычислительной системы — многочлены из $\mathbb{C}[x_1, \ldots, x_m]$ степени $n$, здесь $m \geqslant n$.
- Начальное состояние $f_0 = x_1 x_2 \ldots x_n$.
- Вычисление: применение унитарного преобразования $U$ к переменным:

$$f_{\text{final}}(x) = f_0(Ux).$$

- Измерение в состоянии

$$\sum_{S=(s_1,\ldots,s_n)} \alpha_S x_1^{s_1} \ldots x_m^{s_m}$$

дает $S$ с вероятностью $\mathbf{Pr}[S] = |\alpha_S|^2 s_1! \ldots s_m!$.

# Линейная оптика на полиномах

- Состояния вычислительной системы — многочлены из $\mathbb{C}[x_1, \ldots, x_m]$ степени $n$, здесь $m \geqslant n$.
- Начальное состояние $f_0 = x_1 x_2 \ldots x_n$.
- Вычисление: применение унитарного преобразования $U$ к переменным:

$$f_{\text{final}}(x) = f_0(Ux).$$

- Измерение в состоянии

$$\sum_{S=(s_1,\ldots,s_n)} \alpha_S x_1^{s_1} \ldots x_m^{s_m}$$

дает $S$ с вероятностью $\mathbf{Pr}[S] = |\alpha_S|^2 s_1! \ldots s_m!$.

# Линейная оптика на полиномах

- Состояния вычислительной системы — многочлены из $\mathbb{C}[x_1, \ldots, x_m]$ степени $n$, здесь $m \geqslant n$.
- Начальное состояние $f_0 = x_1 x_2 \ldots x_n$.
- Вычисление: применение унитарного преобразования $U$ к переменным:

$$f_{\text{final}}(x) = f_0(Ux).$$

- Измерение в состоянии

$$\sum_{S=(s_1,\ldots,s_n)} \alpha_S x_1^{s_1} \ldots x_m^{s_m}$$

дает $S$ с вероятностью $\mathbf{Pr}[S] = |\alpha_S|^2 s_1! \ldots s_m!$.

# Недавние результаты

## Оценка квадрата перманента (ОКП)

Оценить квадрат модуля перманента $|\mathrm{perm}(X)|^2$ с аддитивной точностью $\pm\varepsilon n!$ и вероятностью ошибки $\delta$ за время $\mathrm{poly}(n, 1/\varepsilon, 1/\delta)$ в предположении, что входом является матрица, выбранная из вероятностного распределения $N(0,1)^{n\times n}$, при котором значения всех матричных элементов независимы и каждый распределен по Гауссу (плотность вероятности $\exp(-t^2/2)$).

## Теорема (Aaronson, Arkhipov, 2010)

Если существует классический алгоритм, который приближает распределение, порождаемое схемой в модели невзаимодействующих бозонов, то задача оценки квадрата перманента принадлежит классу $\mathrm{BPP}^{\mathrm{NP}}$ (вероятностные вычисления с оракулами из $\mathrm{NP}$).

# Недавние результаты

## Оценка квадрата перманента (ОКП)

Оценить квадрат модуля перманента $|\mathrm{perm}(X)|^2$ с аддитивной точностью $\pm\varepsilon n!$ и вероятностью ошибки $\delta$ за время $\mathrm{poly}(n, 1/\varepsilon, 1/\delta)$ в предположении, что входом является матрица, выбранная из вероятностного распределения $N(0,1)^{n\times n}$, при котором значения всех матричных элементов независимы и каждый распределен по Гауссу (плотность вероятности $\exp(-t^2/2)$).

## Теорема (Aaronson, Arkhipov, 2010)

Если существует классический алгоритм, который приближает распределение, порождаемое схемой в модели невзаимодействующих бозонов, то задача оценки квадрата перманента принадлежит классу $\mathrm{BPP}^{\mathrm{NP}}$ (вероятностные вычисления с оракулами из $\mathrm{NP}$).

# Надежды

Аронсон надеется, что из принадлежности ОКП классу $\mathrm{BPP}^{\mathrm{NP}}$ удастся получить коллапс полиномиальной иерархии (что почти столь же сомнительно как $\mathrm{P} = \mathrm{NP}$).
Успех этой программы даст первое по-настоящему сильное свидетельство в пользу трудности задач, которые решаются квантовыми устройствами.

**Задача для оптимистов**

Реализовать программу Аронсона.

**Задача для пессимистов**

Построить вероятностный алгоритм решения задачи оценки квадрата перманента.

# Надежды

Аронсон надеется, что из принадлежности ОКП классу $\mathrm{BPP}^{\mathrm{NP}}$ удастся получить коллапс полиномиальной иерархии (что почти столь же сомнительно как $\mathrm{P} = \mathrm{NP}$).
Успех этой программы даст первое по-настоящему сильное свидетельство в пользу трудности задач, которые решаются квантовыми устройствами.

**Задача для оптимистов**

Реализовать программу Аронсона.

**Задача для пессимистов**

Построить вероятностный алгоритм решения задачи оценки квадрата перманента.

# Надежды

Ааронсон надеется, что из принадлежности ОКП классу $\mathrm{BPP}^{\mathrm{NP}}$ удастся получить коллапс полиномиальной иерархии (что почти столь же сомнительно как $\mathrm{P} = \mathrm{NP}$).
Успех этой программы даст первое по-настоящему сильное свидетельство в пользу трудности задач, которые решаются квантовыми устройствами.

**Задача для оптимистов**

Реализовать программу Ааронсона.

**Задача для пессимистов**

Построить вероятностный алгоритм решения задачи оценки квадрата перманента.