Квантовые алгоритмы: возможности и ограничения. Лекция 7: Конечные базисы.

М. Вялый

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

Санкт-Петербург, 2011

План

Приближение унитарного оператора

Определение

Оператор $\tilde{U}$ представляет оператор U с точностью δ, если

$$\|\tilde{U} - U\| < \delta.$$

Здесь используется операторная норма $\|A\| = \max_{x:|x|=1} |Ax|$.

Утверждение 1.

Если унитарный оператор $\tilde{U}$ приближает U с точностью δ, то $\tilde{U}^{-1}$ приближает U^{-1} с такой же точностью δ.

Утверждение 2. Линейное накопление ошибки

Если $\|\tilde{U}_k - U_k\| < \delta_k$, то

$$\|\tilde{U}_L \cdot \ldots \cdot \tilde{U}_1 - U_L \cdot \ldots \cdot U_1\| \leq \sum_k \delta_k.$$

Приближение унитарного оператора

Определение

Оператор $\tilde{U}$ представляет оператор U с точностью δ, если

$$\|\tilde{U} - U\| < \delta.$$

Здесь используется операторная норма $\|A\| = \max_{x:|x|=1} |Ax|$.

Утверждение 1.

Если унитарный оператор $\tilde{U}$ приближает U с точностью δ, то $\tilde{U}^{-1}$ приближает U^{-1} с такой же точностью δ.

Утверждение 2. Линейное накопление ошибки

Если $\|\tilde{U}_k - U_k\| < \delta_k$, то

$$\|\tilde{U}_L \cdot \ldots \cdot \tilde{U}_1 - U_L \cdot \ldots \cdot U_1\| \le \sum_k \delta_k.$$

Приближение унитарного оператора

Определение

Оператор $\tilde{U}$ представляет оператор U с точностью δ, если

$$\|\tilde{U} - U\| < \delta.$$

Здесь используется операторная норма $\|A\| = \max_{x:|x|=1} |Ax|$.

Утверждение 1.

Если унитарный оператор $\tilde{U}$ приближает U с точностью δ, то $\tilde{U}^{-1}$ приближает U^{-1} с такой же точностью δ.

Утверждение 2. Линейное накопление ошибки

Если $\|\tilde{U}_k - U_k\| < \delta_k$, то

$$\left\|\tilde{U}_L \cdot \ldots \cdot \tilde{U}_1 - U_L \cdot \ldots \cdot U_1\right\| \leq \sum_k \delta_k.$$

Свойства операторной нормы

1. $\|X\|^2 = \max_{x:|x|=1}\langle x|X^\dagger X|x\rangle$ — наибольшее собственное число оператора $X^\dagger X$.
2. $\|XY\| \leqslant \|X\|\,\|Y\|$ (так как $|XYx| \leqslant \|X\|\,|Yx| \leqslant \|X\|\,\|Y\|\,|x|$).
3. $\|X \otimes Y\| = \|X\|\,\|Y\|$ (уже было раньше, следует из 1).
4. Для унитарного оператора $\|U\| = 1$ (из определения).

Доказательство утверждения 1

Пусть $\|\tilde{U} - U\| \leqslant \delta$. Тогда

$$\|U^{-1} - \tilde{U}^{-1}\| = \|\tilde{U}^{-1}(\tilde{U} - U)U^{-1}\| \overset{(2,4)}{\leqslant} \|\tilde{U} - U\| \leqslant \delta.$$

Свойства операторной нормы

1. $\|X\|^2 = \max_{x:|x|=1} \langle x|X^\dagger X|x\rangle$ — наибольшее собственное число оператора $X^\dagger X$.
2. $\|XY\| \leqslant \|X\|\,\|Y\|$ (так как $|XYx| \leqslant \|X\|\,|Yx| \leqslant \|X\|\,\|Y\|\,|x|$).
3. $\|X \otimes Y\| = \|X\|\,\|Y\|$ (уже было раньше, следует из 1).
4. Для унитарного оператора $\|U\| = 1$ (из определения).

Доказательство утверждения 1

Пусть $\|\tilde{U} - U\| \leqslant \delta$. Тогда

$$\|U^{-1} - \tilde{U}^{-1}\| = \|\tilde{U}^{-1}(\tilde{U} - U)U^{-1}\| \overset{(2,4)}{\leqslant} \|\tilde{U} - U\| \leqslant \delta.$$

Свойства операторной нормы

1. $\|X\|^2 = \max_{x:|x|=1} \langle x|X^\dagger X|x\rangle$ — наибольшее собственное число оператора $X^\dagger X$.
2. $\|XY\| \leqslant \|X\|\,\|Y\|$ (так как $|XYx| \leqslant \|X\|\,|Yx| \leqslant \|X\|\,\|Y\|\,|x|$).
3. $\|X \otimes Y\| = \|X\|\,\|Y\|$ (уже было раньше, следует из 1).
4. Для унитарного оператора $\|U\| = 1$ (из определения).

Доказательство утверждения 1

Пусть $\|\tilde{U} - U\| \leqslant \delta$. Тогда

$$\|U^{-1} - \tilde{U}^{-1}\| = \|\tilde{U}^{-1}(\tilde{U} - U)U^{-1}\| \overset{(2,4)}{\leqslant} \|\tilde{U} - U\| \leqslant \delta.$$

Свойства операторной нормы

1. $\|X\|^2 = \max_{x:|x|=1}\langle x|X^\dagger X|x\rangle$ — наибольшее собственное число оператора $X^\dagger X$.
2. $\|XY\| \leqslant \|X\|\,\|Y\|$ (так как $|XYx| \leqslant \|X\|\,|Yx| \leqslant \|X\|\,\|Y\|\,|x|$).
3. $\|X\otimes Y\| = \|X\|\,\|Y\|$ (уже было раньше, следует из 1).
4. Для унитарного оператора $\|U\| = 1$ (из определения).

Доказательство утверждения 1

Пусть $\|\tilde U - U\| \leqslant \delta$. Тогда

$$\|U^{-1} - \tilde U^{-1}\| = \|\tilde U^{-1}(\tilde U - U)U^{-1}\| \overset{(2,4)}{\leqslant} \|\tilde U - U\| \leqslant \delta.$$

Свойства операторной нормы

1. $\|X\|^2 = \max_{x:|x|=1}\langle x|X^\dagger X|x\rangle$ — наибольшее собственное число оператора $X^\dagger X$.
2. $\|XY\| \leqslant \|X\|\,\|Y\|$ (так как $|XYx| \leqslant \|X\|\,|Yx| \leqslant \|X\|\,\|Y\|\,|x|$).
3. $\|X \otimes Y\| = \|X\|\,\|Y\|$ (уже было раньше, следует из 1).
4. Для унитарного оператора $\|U\| = 1$ (из определения).

Доказательство утверждения 1

Пусть $\|\tilde{U} - U\| \leqslant \delta$. Тогда

$$\|U^{-1} - \tilde{U}^{-1}\| = \|\tilde{U}^{-1}(\tilde{U} - U)U^{-1}\| \overset{(2,4)}{\leqslant} \|\tilde{U} - U\| \leqslant \delta.$$

Линейное накопление ошибок (случай двух операторов)

$$\begin{aligned}\big\|\tilde{U}_2\tilde{U}_1 - U_2U_1\big\| &= \big\|\tilde{U}_2(\tilde{U}_1 - U_1) + (\tilde{U}_2 - U_2)U_1\big\| \leqslant \\ &\leqslant \big\|\tilde{U}_2(\tilde{U}_1 - U_1)\big\| + \big\|(\tilde{U}_2 - U_2)U_1\big\| \leqslant \\ &\leqslant \big\|\tilde{U}_2\big\|\,\big\|\tilde{U}_1 - U_1\big\| + \big\|\tilde{U}_2 - U_2\big\|\,\big\|U_1\big\| = \\ &= \big\|\tilde{U}_1 - U_1\big\| + \big\|\tilde{U}_2 - U_2\big\|.\end{aligned}$$

Существенна унитарность операторов. В общем случае ошибки накапливаются экспоненциально быстро.

Линейное накопление ошибок (случай двух операторов)

$$
\begin{aligned}
\left\|\tilde{U}_2\tilde{U}_1 - U_2U_1\right\| &= \left\|\tilde{U}_2(\tilde{U}_1 - U_1) + (\tilde{U}_2 - U_2)U_1\right\| \leqslant \\
&\leqslant \left\|\tilde{U}_2(\tilde{U}_1 - U_1)\right\| + \left\|(\tilde{U}_2 - U_2)U_1\right\| \leqslant \\
&\leqslant \left\|\tilde{U}_2\right\|\left\|\tilde{U}_1 - U_1\right\| + \left\|\tilde{U}_2 - U_2\right\|\left\|U_1\right\| = \\
&= \left\|\tilde{U}_1 - U_1\right\| + \left\|\tilde{U}_2 - U_2\right\|.
\end{aligned}
$$

Существенна унитарность операторов. В общем случае ошибки накапливаются экспоненциально быстро.

Линейное накопление ошибок (случай двух операторов)

$$
\begin{aligned}
\|\tilde{U}_2\tilde{U}_1 - U_2U_1\| &= \|\tilde{U}_2(\tilde{U}_1 - U_1) + (\tilde{U}_2 - U_2)U_1\| \leqslant \\
&\leqslant \|\tilde{U}_2(\tilde{U}_1 - U_1)\| + \|(\tilde{U}_2 - U_2)U_1\| \leqslant \\
&\leqslant \|\tilde{U}_2\|\,\|\tilde{U}_1 - U_1\| + \|\tilde{U}_2 - U_2\|\,\|U_1\| = \\
&= \|\tilde{U}_1 - U_1\| + \|\tilde{U}_2 - U_2\|.
\end{aligned}
$$

Существенна унитарность операторов. В общем случае ошибки накапливаются экспоненциально быстро.

Линейное накопление ошибок (случай двух операторов)

$$\begin{aligned}\left\|\tilde U_2\tilde U_1 - U_2U_1\right\| &= \left\|\tilde U_2(\tilde U_1 - U_1) + (\tilde U_2 - U_2)U_1\right\| \leqslant \\ &\leqslant \left\|\tilde U_2(\tilde U_1 - U_1)\right\| + \left\|(\tilde U_2 - U_2)U_1\right\| \leqslant \\ &\leqslant \left\|\tilde U_2\right\|\left\|\tilde U_1 - U_1\right\| + \left\|\tilde U_2 - U_2\right\|\left\|U_1\right\| = \\ &= \left\|\tilde U_1 - U_1\right\| + \left\|\tilde U_2 - U_2\right\|.\end{aligned}$$

Существенна унитарность операторов. В общем случае ошибки накапливаются экспоненциально быстро.

Линейное накопление ошибок (случай двух операторов)

$$
\begin{aligned}
\|\tilde{U}_2\tilde{U}_1 - U_2U_1\| &= \|\tilde{U}_2(\tilde{U}_1 - U_1) + (\tilde{U}_2 - U_2)U_1\| \leqslant \\
&\leqslant \|\tilde{U}_2(\tilde{U}_1 - U_1)\| + \|(\tilde{U}_2 - U_2)U_1\| \leqslant \\
&\leqslant \|\tilde{U}_2\|\,\|\tilde{U}_1 - U_1\| + \|\tilde{U}_2 - U_2\|\,\|U_1\| = \\
&= \|\tilde{U}_1 - U_1\| + \|\tilde{U}_2 - U_2\|.
\end{aligned}
$$

Существенна унитарность операторов. В общем случае ошибки накапливаются экспоненциально быстро.

Линейное накопление ошибок (случай двух операторов)

$$\begin{aligned}\|\tilde{U}_2\tilde{U}_1 - U_2U_1\| &= \|\tilde{U}_2(\tilde{U}_1 - U_1) + (\tilde{U}_2 - U_2)U_1\| \leqslant \\ &\leqslant \|\tilde{U}_2(\tilde{U}_1 - U_1)\| + \|(\tilde{U}_2 - U_2)U_1\| \leqslant \\ &\leqslant \|\tilde{U}_2\|\,\|\tilde{U}_1 - U_1\| + \|\tilde{U}_2 - U_2\|\,\|U_1\| = \\ &= \|\tilde{U}_1 - U_1\| + \|\tilde{U}_2 - U_2\|.\end{aligned}$$

Существенна унитарность операторов. В общем случае ошибки накапливаются экспоненциально быстро.

Приближенная реализация в расширенном смысле

Определение

Оператор $U\colon (\mathbb{C}^2)^{\otimes n} \to (\mathbb{C}^2)^{\otimes n}$ приближается в расширенном смысле оператором $\tilde{U}\colon (\mathbb{C}^2)^{\otimes N} \to (\mathbb{C}^2)^{\otimes N}$ с точностью δ, если для любого $|\xi\rangle$ из $(\mathbb{C}^2)^{\otimes n}$ выполнено

$$\left|\tilde{U}\left(|\xi\rangle \otimes |0^{N-n}\rangle\right) - U|\xi\rangle \otimes |0^{N-n}\rangle\right| \le \delta\big|\xi\big|.$$

Задача о свойствах приближений в расширенном смысле

Докажите, что если U_1 приближается в расширенном смысле $\tilde{U}_1$ с точностью δ_1, а U_2 приближается в расширенном смысле $\tilde{U}_2$ с точностью δ_2, то U_1^{-1} приближается в расширенном смысле $\tilde{U}_1^{-1}$ с точностью δ_1, а $U_1 U_2$ приближается в расширенном смысле $\tilde{U}_1 \tilde{U}_2$ с точностью $\delta_1 + \delta_2$.

Приближенная реализация в расширенном смысле

Определение

Оператор $U\colon (\mathbb{C}^2)^{\otimes n} \to (\mathbb{C}^2)^{\otimes n}$ приближается в расширенном смысле оператором $\tilde{U}\colon (\mathbb{C}^2)^{\otimes N} \to (\mathbb{C}^2)^{\otimes N}$ с точностью δ, если для любого $|\xi\rangle$ из $(\mathbb{C}^2)^{\otimes n}$ выполнено

$$\left|\tilde{U}\left(|\xi\rangle \otimes |0^{N-n}\rangle\right) - U|\xi\rangle \otimes |0^{N-n}\rangle\right| \le \delta|\xi|.$$

Задача о свойствах приближений в расширенном смысле

Докажите, что если U_1 приближается в расширенном смысле $\tilde{U}_1$ с точностью δ_1, а U_2 приближается в расширенном смысле $\tilde{U}_2$ с точностью δ_2, то U_1^{-1} приближается в расширенном смысле $\tilde{U}_1^{-1}$ с точностью δ_1, а $U_1 U_2$ приближается в расширенном смысле $\tilde{U}_1\tilde{U}_2$ с точностью $\delta_1 + \delta_2$.

О распределении результатов измерения

Нас интересуют насколько близки распределения результатов измерения. Пусть U приближается в расширенном смысле $\tilde{U}$ с точностью δ. Насколько близки вероятности наблюдения различных событий в одном и другом случае?

- Ортонормированный базис $\{|x\rangle\}$.
- Состояние $|\psi\rangle = \sum_x c_x|x\rangle$.
- Вероятность $\mathbf{Pr}(|\psi\rangle, x)$ исхода x равна $|c_x|^2$.
- Вероятность события A:

$$\mathbf{Pr}(|\psi\rangle, A) = \sum_{x\in A} |c_x|^2 = \big|\Pi_A|\psi\rangle\big|^2,$$

где Π_A — оператор ортогонального проектирования на подпространство, порожденное векторами $|x\rangle$, $x \in A$.

О распределении результатов измерения

Нас интересуют насколько близки распределения результатов измерения. Пусть U приближается в расширенном смысле $\tilde{U}$ с точностью δ. Насколько близки вероятности наблюдения различных событий в одном и другом случае?

- Ортонормированный базис $\{|x\rangle\}$.
- Состояние $|\psi\rangle = \sum_x c_x|x\rangle$.
- Вероятность $\mathbf{Pr}(|\psi\rangle, x)$ исхода x равна $|c_x|^2$.
- Вероятность события A:

$$\mathbf{Pr}(|\psi\rangle, A) = \sum_{x \in A} |c_x|^2 = \left|\Pi_A|\psi\rangle\right|^2,$$

где Π_A — оператор ортогонального проектирования на подпространство, порожденное векторами $|x\rangle$, $x \in A$.

О распределении результатов измерения

Нас интересуют насколько близки распределения результатов измерения. Пусть U приближается в расширенном смысле $\tilde{U}$ с точностью δ. Насколько близки вероятности наблюдения различных событий в одном и другом случае?

- Ортонормированный базис $\{|x\rangle\}$.
- Состояние $|\psi\rangle = \sum_x c_x |x\rangle$.
- Вероятность $\mathbf{Pr}(|\psi\rangle, x)$ исхода x равна $|c_x|^2$.
- Вероятность события A:

$$\mathbf{Pr}(|\psi\rangle, A) = \sum_{x \in A} |c_x|^2 = \big|\Pi_A |\psi\rangle\big|^2,$$

где Π_A — оператор ортогонального проектирования на подпространство, порожденное векторами $|x\rangle$, $x \in A$.

О распределении результатов измерения

Нас интересуют насколько близки распределения результатов измерения. Пусть U приближается в расширенном смысле $\tilde{U}$ с точностью δ. Насколько близки вероятности наблюдения различных событий в одном и другом случае?

- Ортонормированный базис $\{|x\rangle\}$.
- Состояние $|\psi\rangle = \sum_x c_x|x\rangle$.
- Вероятность $\mathbf{Pr}(|\psi\rangle, x)$ исхода x равна $|c_x|^2$.
- Вероятность события A:

$$\mathbf{Pr}(|\psi\rangle, A) = \sum_{x\in A} |c_x|^2 = \left|\Pi_A|\psi\rangle\right|^2,$$

где Π_A — оператор ортогонального проектирования на подпространство, порожденное векторами $|x\rangle$, $x \in A$.

О распределении результатов измерения

Нас интересуют насколько близки распределения результатов измерения. Пусть U приближается в расширенном смысле $\tilde{U}$ с точностью δ. Насколько близки вероятности наблюдения различных событий в одном и другом случае?

- Ортонормированный базис $\{|x\rangle\}$.
- Состояние $|\psi\rangle = \sum_x c_x|x\rangle$.
- Вероятность $\mathbf{Pr}(|\psi\rangle, x)$ исхода x равна $|c_x|^2$.
- Вероятность события A:

$$\mathbf{Pr}(|\psi\rangle, A) = \sum_{x\in A} |c_x|^2 = \big|\Pi_A|\psi\rangle\big|^2,$$

где Π_A — оператор ортогонального проектирования на подпространство, порожденное векторами $|x\rangle$, $x \in A$.

О распределении результатов измерения (продолжение)

- Пусть $U|0^n\rangle = |\psi'\rangle_A + |\psi''\rangle_{\bar{A}}$ — ортогональное разложение.
- Аналогичное разложение для приближающего оператора

$$\tilde{U}(|0^n\rangle\otimes|0^N\rangle) = U|0^n\rangle\otimes|0^N\rangle+|\Delta\rangle = |\psi'\rangle_A\otimes|0^N\rangle+|\psi''\rangle_{\bar{A}}\otimes|0^N\rangle+|\Delta\rangle,$$

  здесь $|\Delta| < \delta$.
- Ортогональное разложение для вектора ошибки: $|\Delta\rangle = |\Delta'\rangle_A + |\Delta''\rangle_{\bar{A}}$.
- Вероятности события A в двух случаях:

$$\mathbf{Pr}(U|0^n\rangle, A) = |\psi'|^2$$

$$\mathbf{Pr}(\tilde{U}(|0^n\rangle \otimes |0^N\rangle), A) = \big||\psi'\rangle \otimes |0^N\rangle + |\Delta'\rangle\big|^2$$

О распределении результатов измерения (продолжение)

- Пусть $U|0^n\rangle = |\psi'\rangle_A + |\psi''\rangle_{\bar{A}}$ — ортогональное разложение.
- Аналогичное разложение для приближающего оператора

$$\tilde{U}(|0^n\rangle\otimes|0^N\rangle) = U|0^n\rangle\otimes|0^N\rangle+|\Delta\rangle = |\psi'\rangle_A\otimes|0^N\rangle+|\psi''\rangle_{\bar{A}}\otimes|0^N\rangle+|\Delta\rangle,$$

здесь $|\Delta| < \delta$.

- Ортогональное разложение для вектора ошибки: $|\Delta\rangle = |\Delta'\rangle_A + |\Delta''\rangle_{\bar{A}}$.
- Вероятности события A в двух случаях:

$$\mathbf{Pr}(U|0^n\rangle, A) = |\psi'|^2$$

$$\mathbf{Pr}(\tilde{U}(|0^n\rangle \otimes |0^N\rangle), A) = \big||\psi'\rangle \otimes |0^N\rangle + |\Delta'\rangle\big|^2$$

О распределении результатов измерения (продолжение)

- Пусть $U|0^n\rangle = |\psi'\rangle_A + |\psi''\rangle_{\bar{A}}$ — ортогональное разложение.
- Аналогичное разложение для приближающего оператора

$$\tilde{U}(|0^n\rangle\otimes|0^N\rangle) = U|0^n\rangle\otimes|0^N\rangle+|\Delta\rangle = |\psi'\rangle_A\otimes|0^N\rangle+|\psi''\rangle_{\bar{A}}\otimes|0^N\rangle+|\Delta\rangle,$$

  здесь $|\Delta| < \delta$.
- Ортогональное разложение для вектора ошибки:
  $|\Delta\rangle = |\Delta'\rangle_A + |\Delta''\rangle_{\bar{A}}$.
- Вероятности события A в двух случаях:

$$\mathbf{Pr}(U|0^n\rangle, A) = |\psi'|^2$$
$$\mathbf{Pr}(\tilde{U}(|0^n\rangle\otimes|0^N\rangle), A) = \left||\psi'\rangle\otimes|0^N\rangle + |\Delta'\rangle\right|^2$$

О распределении результатов измерения (продолжение)

- Пусть $U|0^n\rangle = |\psi'\rangle_A + |\psi''\rangle_{\bar{A}}$ — ортогональное разложение.
- Аналогичное разложение для приближающего оператора

$$\tilde{U}(|0^n\rangle \otimes |0^N\rangle) = U|0^n\rangle \otimes |0^N\rangle + |\Delta\rangle = |\psi'\rangle_A \otimes |0^N\rangle + |\psi''\rangle_{\bar{A}} \otimes |0^N\rangle + |\Delta\rangle,$$

  здесь $|\Delta| < \delta$.
- Ортогональное разложение для вектора ошибки: $|\Delta\rangle = |\Delta'\rangle_A + |\Delta''\rangle_{\bar{A}}$.
- Вероятности события A в двух случаях:

$$\mathbf{Pr}(U|0^n\rangle, A) = |\psi'|^2$$
$$\mathbf{Pr}(\tilde{U}(|0^n\rangle \otimes |0^N\rangle), A) = \big||\psi'\rangle \otimes |0^N\rangle + |\Delta'\rangle\big|^2$$

О распределении результатов измерения (продолжение)

- Имеем
$$|\psi'| - \delta < \big||\psi'\rangle \otimes |0^N\rangle + |\Delta'\rangle\big| < |\psi'| + \delta.$$
- Поэтому при $|\psi'| \geqslant \delta$ имеем
$$\mathbf{Pr}(U|0^n\rangle, A) - 2\delta|\psi'| + \delta^2 < \\ < \mathbf{Pr}(\tilde{U}(|0^n\rangle \otimes |0^N\rangle), A) < \\ < \mathbf{Pr}(U|0^n\rangle, A) + 2\delta|\psi'| + \delta^2.$$
- Значит,
$$|\mathbf{Pr}(U|0^n\rangle, A) - \mathbf{Pr}(\tilde{U}(|0^n\rangle \otimes |0^N\rangle), A)| < 2\delta|\psi'| + \delta^2 \leqslant 2\delta(1+\delta/2) \leqslant 4\delta.$$
(Норма разности унитарных операторов не превосходит 2.)
- Упражнение. Проверьте, что при $|\psi'| < \delta$ выполнено
$$|\mathbf{Pr}(U|0^n\rangle, A) - \mathbf{Pr}(\tilde{U}(|0^n\rangle \otimes |0^N\rangle), A)| < 3\delta^2 < 6\delta.$$

О распределении результатов измерения (продолжение)

- Имеем
$$|\psi'| - \delta < \big||\psi'\rangle \otimes |0^N\rangle + |\Delta'\rangle\big| < |\psi'| + \delta.$$
- Поэтому при $|\psi'| \geqslant \delta$ имеем
$$\mathbf{Pr}(U|0^n\rangle, A) - 2\delta|\psi'| + \delta^2 < \\ < \mathbf{Pr}(\tilde{U}(|0^n\rangle \otimes |0^N\rangle), A) < \\ < \mathbf{Pr}(U|0^n\rangle, A) + 2\delta|\psi'| + \delta^2.$$
- Значит,
$$|\mathbf{Pr}(U|0^n\rangle, A) - \mathbf{Pr}(\tilde{U}(|0^n\rangle \otimes |0^N\rangle), A)| < 2\delta|\psi'| + \delta^2 \leqslant 2\delta(1+\delta/2) \leqslant 4\delta.$$
(Норма разности унитарных операторов не превосходит 2.)
- Упражнение. Проверьте, что при $|\psi'| < \delta$ выполнено
$$|\mathbf{Pr}(U|0^n\rangle, A) - \mathbf{Pr}(\tilde{U}(|0^n\rangle \otimes |0^N\rangle), A)| < 3\delta^2 < 6\delta.$$

О распределении результатов измерения (продолжение)

- Имеем
$$|\psi'| - \delta < \big||\psi'\rangle \otimes |0^N\rangle + |\Delta'\rangle\big| < |\psi'| + \delta.$$
- Поэтому при $|\psi'| \geqslant \delta$ имеем
$$\mathbf{Pr}(U|0^n\rangle, A) - 2\delta|\psi'| + \delta^2 < \\ < \mathbf{Pr}(\tilde{U}(|0^n\rangle \otimes |0^N\rangle), A) < \\ < \mathbf{Pr}(U|0^n\rangle, A) + 2\delta|\psi'| + \delta^2.$$
- Значит,
$$|\,\mathbf{Pr}(U|0^n\rangle, A) - \mathbf{Pr}(\tilde{U}(|0^n\rangle \otimes |0^N\rangle), A)| < 2\delta|\psi'| + \delta^2 \leqslant 2\delta(1+\delta/2) \leqslant 4\delta.$$
(Норма разности унитарных операторов не превосходит 2.)
- Упражнение. Проверьте, что при $|\psi'| < \delta$ выполнено
$$|\,\mathbf{Pr}(U|0^n\rangle, A) - \mathbf{Pr}(\tilde{U}(|0^n\rangle \otimes |0^N\rangle), A)| < 3\delta^2 < 6\delta.$$

О распределении результатов измерения (продолжение)

- Имеем
$$|\psi'| - \delta < \big||\psi'\rangle \otimes |0^N\rangle + |\Delta'\rangle\big| < |\psi'| + \delta.$$
- Поэтому при $|\psi'| \geqslant \delta$ имеем
$$\begin{aligned}\mathbf{Pr}(U|0^n\rangle, A) - 2\delta|\psi'| + \delta^2 <\\ < \mathbf{Pr}(\tilde{U}(|0^n\rangle \otimes |0^N\rangle), A) <\\ < \mathbf{Pr}(U|0^n\rangle, A) + 2\delta|\psi'| + \delta^2.\end{aligned}$$
- Значит,
$$|\,\mathbf{Pr}(U|0^n\rangle, A) - \mathbf{Pr}(\tilde{U}(|0^n\rangle \otimes |0^N\rangle), A)| < 2\delta|\psi'| + \delta^2 \leqslant 2\delta(1+\delta/2) \leqslant 4\delta.$$
(Норма разности унитарных операторов не превосходит 2.)
- Упражнение. Проверьте, что при $|\psi'| < \delta$ выполнено
$$|\,\mathbf{Pr}(U|0^n\rangle, A) - \mathbf{Pr}(\tilde{U}(|0^n\rangle \otimes |0^N\rangle), A)| < 3\delta^2 < 6\delta.$$

О распределении результатов измерения (итог)

Утверждение

Если унитарный оператор U приближается в расширенном смысле унитарным оператором $\tilde{U}$ с точностью δ, то для любого события A выполняется неравенство

$$|\,\mathbf{Pr}(U|0^n\rangle, A) - \mathbf{Pr}(\tilde{U}(|0^n\rangle \otimes |0^N\rangle), A)| < 6\delta.$$

Другими словами операторы U и $\tilde{U}$ порождают статистически близкие распределения.

План

1. Приближенная реализация унитарных операторов
2. Конечные универсальные базисы
3. Эффективные приближения
4. Окончательное определение квантового алгоритма

Приближенная реализация конечным набором операторов

Определение

Конечный базис $\mathcal{B}$ называется универсальным, если любой унитарный оператор U с точностью до скалярного множителя приближается в расширенном смысле с любой точностью ε схемами в базисе $\mathcal{B}$.

Замечание

Поскольку в конечном счете интересны порождаемые операторами распределения, скалярный множитель несущественен.

Приближенная реализация конечным набором операторов

Определение

Конечный базис $\mathcal{B}$ называется универсальным, если любой унитарный оператор U с точностью до скалярного множителя приближается в расширенном смысле с любой точностью ε схемами в базисе $\mathcal{B}$.

Замечание

Поскольку в конечном счете интересны порождаемые операторами распределения, скалярный множитель несущественен.

Пример универсального базиса

Теорема об универсальном конечном базисе

Базис $\{\text{c-NOT}, H, K(\pi/4)\}$ — универсальный. Здесь

$$\text{c-NOT}: |x, y\rangle \mapsto |x, y \oplus x\rangle, \quad H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad K(\frac{\pi}{4}) = \begin{pmatrix} 1 & 0 \\ 0 & e^{\pi i/4} \end{pmatrix}.$$

- Поскольку любой оператор выражается в базисе из однокубитовых операторов и c-NOT, достаточно приближать любой однокубитовый (с точностью до фазового множителя) произведениями H и K.
- Поскольку фазовый множитель несущественен, достаточно приближать элементы $\mathbf{SU}(2) \cong \mathbf{SO}(3)$.

Пример универсального базиса

Теорема об универсальном конечном базисе

Базис $\{\text{c-NOT}, H, K(\pi/4)\}$ — универсальный. Здесь

$$\text{c-NOT}: |x, y\rangle \mapsto |x, y \oplus x\rangle, \quad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad K(\frac{\pi}{4}) = \begin{pmatrix} 1 & 0 \\ 0 & e^{\pi i/4} \end{pmatrix}.$$

- Поскольку любой оператор выражается в базисе из однокубитовых операторов и c-NOT, достаточно приближать любой однокубитовый (с точностью до фазового множителя) произведениями H и K.
- Поскольку фазовый множитель несущественен, достаточно приближать элементы $\mathbf{SU}(2) \cong \mathbf{SO}(3)$.

Пример универсального базиса

Теорема об универсальном конечном базисе

Базис $\{\text{c-NOT}, H, K(\pi/4)\}$ — универсальный. Здесь

$$\text{c-NOT}\colon |x, y\rangle \mapsto |x, y \oplus x\rangle, \quad H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad K(\tfrac{\pi}{4}) = \begin{pmatrix} 1 & 0 \\ 0 & e^{\pi i/4} \end{pmatrix}.$$

- Поскольку любой оператор выражается в базисе из однокубитовых операторов и c-NOT, достаточно приближать любой однокубитовый (с точностью до фазового множителя) произведениями H и K.
- Поскольку фазовый множитель несущественен, достаточно приближать элементы $\mathbf{SU}(2) \cong \mathbf{SO}(3)$.

О поворотах

Утверждение

Группа $\mathbf{SO}(3)$ поворотов трехмерного пространства порождается поворотами относительно любых двух неколлинеарных осей.

Если $U : a \mapsto a_0$, то
$R_\varphi(a) = U^{-1} R_\varphi(a_0) U$.
Значит, достаточно показать, что любой вектор можно перевести в a_0.

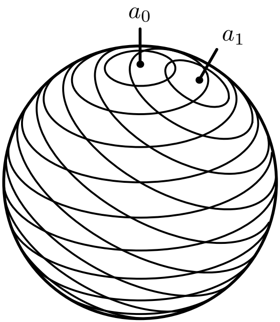
Задача

Докажите, что для перевода любого вектора в a_0 достаточно $O(1/\vartheta)$ поворотов вокруг a_0, a_1, где ϑ — угол между a_0 и a_1.

О поворотах

Утверждение

Группа **SO**(3) поворотов трехмерного пространства порождается поворотами относительно любых двух неколлинеарных осей.



Если $U\colon a \mapsto a_0$, то $R_\varphi(a) = U^{-1}R_\varphi(a_0)U$.
Значит, достаточно показать, что любой вектор можно перевести в a_0.

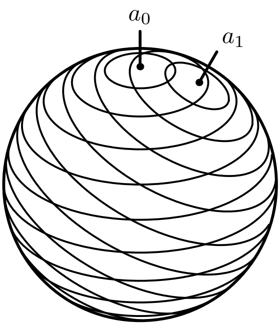
Задача

Докажите, что для перевода любого вектора в a_0 достаточно $O(1/\vartheta)$ поворотов вокруг a_0, a_1, где ϑ — угол между a_0 и a_1.

О поворотах

Утверждение

Группа $\mathbf{SO}(3)$ поворотов трехмерного пространства порождается поворотами относительно любых двух неколлинеарных осей.



Если $U\colon a \mapsto a_0$, то
$R_\varphi(a) = U^{-1} R_\varphi(a_0) U$.

Значит, достаточно показать, что любой вектор можно перевести в a_0.

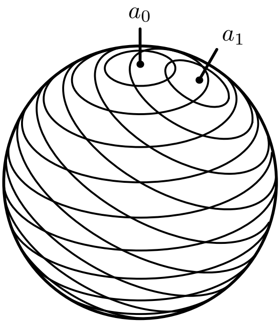
Задача

Докажите, что для перевода любого вектора в a_0 достаточно $O(1/\vartheta)$ поворотов вокруг a_0, a_1, где ϑ — угол между a_0 и a_1.

О поворотах

Утверждение

Группа $\mathbf{SO}(3)$ поворотов трехмерного пространства порождается поворотами относительно любых двух неколлинеарных осей.



Если $U\colon a \mapsto a_0$, то
$R_\varphi(a) = U^{-1} R_\varphi(a_0) U$.
Значит, достаточно показать, что любой вектор можно перевести в a_0.

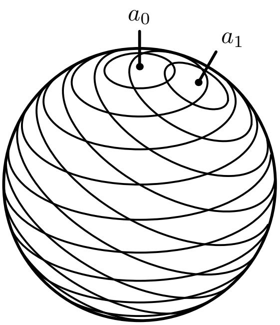
Задача

Докажите, что для перевода любого вектора в a_0 достаточно $O(1/\vartheta)$ поворотов вокруг a_0, a_1, где ϑ — угол между a_0 и a_1.

О поворотах

Утверждение

Группа $\mathbf{SO}(3)$ поворотов трехмерного пространства порождается поворотами относительно любых двух неколлинеарных осей.



Если $U\colon a \mapsto a_0$, то
$R_\varphi(a) = U^{-1}R_\varphi(a_0)U$.
Значит, достаточно показать, что любой вектор можно перевести в a_0.

Задача

Докажите, что для перевода любого вектора в a_0 достаточно $O(1/\vartheta)$ поворотов вокруг a_0, a_1, где ϑ — угол между a_0 и a_1.

Повороты на иррациональный угол

Утверждение

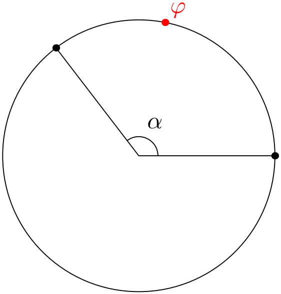
Если угол α несоизмерим с π, то любой поворот R_φ приближается некоторым кратным R_α^n с точностью ε.

Если $m > 2\pi/\varepsilon$, то найдутся $0 < m', m'' \leqslant m$ такие, что $|R_\alpha^{m'}(0) - R_\alpha^{m''}(0)| < \varepsilon$, т. е. $R_\alpha^{m''-m'}$ — поворот на угол $< \varepsilon$.

Повороты на иррациональный угол

Утверждение

Если угол α несоизмерим с π, то любой поворот R_φ приближается некоторым кратным R_α^n с точностью ε.

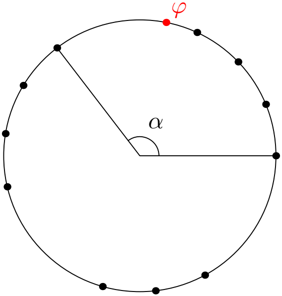


Если $m > 2\pi/\varepsilon$, то найдутся $0 < m', m'' \leqslant m$ такие, что $|R_\alpha^{m'}(0) - R_\alpha^{m''}(0)| < \varepsilon$, т. е. $R_\alpha^{m''-m'}$ — поворот на угол $< \varepsilon$.

Повороты на иррациональный угол

Утверждение

Если угол α несоизмерим с π, то любой поворот R_φ приближается некоторым кратным R_α^n с точностью ε.

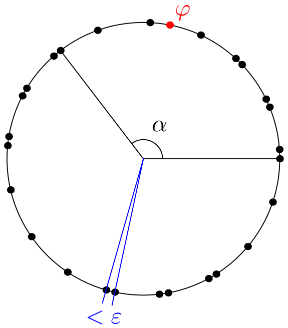


Если $m > 2\pi/\varepsilon$, то найдутся $0 < m', m'' \leqslant m$ такие, что $|R_\alpha^{m'}(0) - R_\alpha^{m''}(0)| < \varepsilon$, т. е. $R_\alpha^{m''-m'}$ — поворот на угол $< \varepsilon$.

Повороты на иррациональный угол

Утверждение

Если угол α несоизмерим с π, то любой поворот R_φ приближается некоторым кратным R_α^n с точностью ε.



Если $m > 2\pi/\varepsilon$, то найдутся $0 < m', m'' \leqslant m$ такие, что $|R_\alpha^{m'}(0) - R_\alpha^{m''}(0)| < \varepsilon$, т. е. $R_\alpha^{m''-m'}$ — поворот на угол $< \varepsilon$.

Упражнение

Проверьте, что

$$H\sigma_x H^\dagger = \sigma_z; \qquad K(\frac{\pi}{4})\sigma_x K(\frac{\pi}{4})^\dagger = \cos\frac{\pi}{4}\sigma_x + \sin\frac{\pi}{4}\sigma_y$$

$$H\sigma_y H^\dagger = -\sigma_y; \qquad K(\frac{\pi}{4})\sigma_y K(\frac{\pi}{4})^\dagger = -\sin\frac{\pi}{4}\sigma_x + \cos\frac{\pi}{4}\sigma_y$$

$$H\sigma_z H^\dagger = \sigma_x; \qquad K(\frac{\pi}{4})\sigma_z K(\frac{\pi}{4})^\dagger = \sigma_z$$

Таким образом, H действует как поворот на π вокруг оси $(1,0,1)$, а $K(\frac{\pi}{4})$ — как поворот на $-\pi/4$ вокруг оси σ_z.
Действие композиции $K(\frac{\pi}{4})H$:

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} \xmapsto{H} \begin{pmatrix} z \\ -y \\ x \end{pmatrix} \xmapsto{K(\frac{\pi}{4})} \begin{pmatrix} z\cos\frac{\pi}{4} - y\sin\frac{\pi}{4} \\ -z\sin\frac{\pi}{4} - y\cos\frac{\pi}{4} \\ x \end{pmatrix}$$

Вычисления

Упражнение

Проверьте, что

$$H\sigma_x H^\dagger = \sigma_z; \qquad K(\frac{\pi}{4})\sigma_x K(\frac{\pi}{4})^\dagger = \cos\frac{\pi}{4}\sigma_x + \sin\frac{\pi}{4}\sigma_y$$

$$H\sigma_y H^\dagger = -\sigma_y; \qquad K(\frac{\pi}{4})\sigma_y K(\frac{\pi}{4})^\dagger = -\sin\frac{\pi}{4}\sigma_x + \cos\frac{\pi}{4}\sigma_y$$

$$H\sigma_z H^\dagger = \sigma_x; \qquad K(\frac{\pi}{4})\sigma_z K(\frac{\pi}{4})^\dagger = \sigma_z$$

Таким образом, H действует как поворот на π вокруг оси $(1,0,1)$, а $K(\frac{\pi}{4})$ — как поворот на $-\pi/4$ вокруг оси σ_z.

Действие композиции $K(\frac{\pi}{4})H$:

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} \xmapsto{H} \begin{pmatrix} z \\ -y \\ x \end{pmatrix} \xmapsto{K(\frac{\pi}{4})} \begin{pmatrix} z\cos\frac{\pi}{4} - y\sin\frac{\pi}{4} \\ -z\sin\frac{\pi}{4} - y\cos\frac{\pi}{4} \\ x \end{pmatrix}$$

Вычисления

Упражнение

Проверьте, что

$$H\sigma_x H^\dagger = \sigma_z; \qquad K(\frac{\pi}{4})\sigma_x K(\frac{\pi}{4})^\dagger = \cos\frac{\pi}{4}\sigma_x + \sin\frac{\pi}{4}\sigma_y$$
$$H\sigma_y H^\dagger = -\sigma_y; \qquad K(\frac{\pi}{4})\sigma_y K(\frac{\pi}{4})^\dagger = -\sin\frac{\pi}{4}\sigma_x + \cos\frac{\pi}{4}\sigma_y$$
$$H\sigma_z H^\dagger = \sigma_x; \qquad K(\frac{\pi}{4})\sigma_z K(\frac{\pi}{4})^\dagger = \sigma_z$$

Таким образом, H действует как поворот на π вокруг оси $(1,0,1)$, а $K(\frac{\pi}{4})$ — как поворот на $-\pi/4$ вокруг оси σ_z.
Действие композиции $K(\frac{\pi}{4})H$:

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} \xmapsto{H} \begin{pmatrix} z \\ -y \\ x \end{pmatrix} \xmapsto{K(\frac{\pi}{4})} \begin{pmatrix} z\cos\frac{\pi}{4} - y\sin\frac{\pi}{4} \\ -z\sin\frac{\pi}{4} - y\cos\frac{\pi}{4} \\ x \end{pmatrix}$$

Вычисления (продолжение)

Композиция $K(\frac{\pi}{4})H$ действует как поворот.
Находим ось поворота из системы уравнений

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} z\cos\frac{\pi}{4} - y\sin\frac{\pi}{4} \\ -z\sin\frac{\pi}{4} - y\cos\frac{\pi}{4} \\ x \end{pmatrix}, \qquad \text{ось поворота} \begin{pmatrix} 1 \\ -\sqrt{2}+1 \\ 1 \end{pmatrix}.$$

Чтобы найти угол поворота, подействуем на вектор, перпендикулярный оси поворота:

$$K(\frac{\pi}{4})H \colon \vec{v} = \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix} \mapsto \begin{pmatrix} -\cos\frac{\pi}{4} \\ \sin\frac{\pi}{4} \\ 1 \end{pmatrix} = \vec{u}.$$

Для угла поворота α получаем соотношение

$$\cos\alpha = \frac{1}{2}(\vec{v},\vec{u}) = -\frac{1+\cos(\pi/4)}{2} = -\cos^2\frac{\pi}{8}.$$

Вычисления (продолжение)

Композиция $K(\frac{\pi}{4})H$ действует как поворот.
Находим ось поворота из системы уравнений

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} z\cos\frac{\pi}{4} - y\sin\frac{\pi}{4} \\ -z\sin\frac{\pi}{4} - y\cos\frac{\pi}{4} \\ x \end{pmatrix}, \qquad \text{ось поворота} \quad \begin{pmatrix} 1 \\ -\sqrt{2}+1 \\ 1 \end{pmatrix}.$$

Чтобы найти угол поворота, подействуем на вектор, перпендикулярный оси поворота:

$$K(\frac{\pi}{4})H\colon \vec{v} = \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix} \mapsto \begin{pmatrix} -\cos\frac{\pi}{4} \\ \sin\frac{\pi}{4} \\ 1 \end{pmatrix} = \vec{u}.$$

Для угла поворота α получаем соотношение

$$\cos\alpha = \frac{1}{2}(\vec{v}, \vec{u}) = -\frac{1+\cos(\pi/4)}{2} = -\cos^2\frac{\pi}{8}.$$

Вычисления (продолжение)

Композиция $K(\frac{\pi}{4})H$ действует как поворот.
Находим ось поворота из системы уравнений

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} z\cos\frac{\pi}{4} - y\sin\frac{\pi}{4} \\ -z\sin\frac{\pi}{4} - y\cos\frac{\pi}{4} \\ x \end{pmatrix}, \qquad \text{ось поворота} \quad \begin{pmatrix} 1 \\ -\sqrt{2}+1 \\ 1 \end{pmatrix}.$$

Чтобы найти угол поворота, подействуем на вектор, перпендикулярный оси поворота:

$$K(\frac{\pi}{4})H\colon \vec{v} = \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix} \mapsto \begin{pmatrix} -\cos\frac{\pi}{4} \\ \sin\frac{\pi}{4} \\ 1 \end{pmatrix} = \vec{u}.$$

Для угла поворота α получаем соотношение

$$\cos\alpha = \frac{1}{2}(\vec{v},\vec{u}) = -\frac{1+\cos(\pi/4)}{2} = -\cos^2\frac{\pi}{8}.$$

Вычисления (окончание)

Задача

Докажите, что если $\cos\alpha = -\cos^2\frac{\pi}{8} = -\frac{1}{2} - \frac{1}{4}\sqrt{2}$, то α несоизмерим с π.

Теорема Влодарского

Если β не является целым кратным $\pi/4$ и $\cos\alpha = \cos^2\beta$, то хотя бы один из углов α, β несоизмерим с π.

Завершение доказательства теоремы об универсальном базисе

- $K(\frac{\pi}{4})H$ действует как поворот на угол, несоизмеримый с π, вокруг оси $(1, -\sqrt{2}+1, 1)^T$.
- $HK(\frac{\pi}{4}) = H(K(\frac{\pi}{4})H)H$ — как поворот на тот же угол вокруг другой оси.
- Значит, композиции $K(\frac{\pi}{4})$ и H порождают всюду плотное множество в $SU(2)$.

Вычисления (окончание)

Задача

Докажите, что если $\cos\alpha = -\cos^2\frac{\pi}{8} = -\frac{1}{2} - \frac{1}{4}\sqrt{2}$, то α несоизмерим с π.

Теорема Влодарского

Если β не является целым кратным $\pi/4$ и $\cos\alpha = \cos^2\beta$, то хотя бы один из углов α, β несоизмерим с π.

Завершение доказательства теоремы об универсальном базисе

- $K(\frac{\pi}{4})H$ действует как поворот на угол, несоизмеримый с π, вокруг оси $(1, -\sqrt{2}+1, 1)^T$.
- $HK(\frac{\pi}{4}) = H(K(\frac{\pi}{4})H)H$ — как поворот на тот же угол вокруг другой оси.
- Значит, композиции $K(\frac{\pi}{4})$ и H порождают всюду плотное множество в $SU(2)$.

Вычисления (окончание)

Задача

Докажите, что если $\cos\alpha = -\cos^2\frac{\pi}{8} = -\frac{1}{2} - \frac{1}{4}\sqrt{2}$, то α несоизмерим с π.

Теорема Влодарского

Если β не является целым кратным $\pi/4$ и $\cos\alpha = \cos^2\beta$, то хотя бы один из углов α, β несоизмерим с π.

Завершение доказательства теоремы об универсальном базисе

- $K(\frac{\pi}{4})H$ действует как поворот на угол, несоизмеримый с π, вокруг оси $(1, -\sqrt{2}+1, 1)^T$.
- $HK(\frac{\pi}{4}) = H(K(\frac{\pi}{4})H)H$ — как поворот на тот же угол вокруг другой оси.
- Значит, композиции $K(\frac{\pi}{4})$ и H порождают всюду плотное множество в $\mathrm{SU}(2)$.

Вычисления (окончание)

Задача

Докажите, что если $\cos\alpha = -\cos^2\frac{\pi}{8} = -\frac{1}{2} - \frac{1}{4}\sqrt{2}$, то α несоизмерим с π.

Теорема Влодарского

Если β не является целым кратным $\pi/4$ и $\cos\alpha = \cos^2\beta$, то хотя бы один из углов α, β несоизмерим с π.

Завершение доказательства теоремы об универсальном базисе

- $K(\frac{\pi}{4})H$ действует как поворот на угол, несоизмеримый с π, вокруг оси $(1, -\sqrt{2}+1, 1)^T$.
- $HK(\frac{\pi}{4}) = H(K(\frac{\pi}{4})H)H$ — как поворот на тот же угол вокруг другой оси.
- Значит, композиции $K(\frac{\pi}{4})$ и H порождают всюду плотное множество в $\mathrm{SU}(2)$.

Вычисления (окончание)

Задача

Докажите, что если $\cos\alpha = -\cos^2\frac{\pi}{8} = -\frac{1}{2} - \frac{1}{4}\sqrt{2}$, то α несоизмерим с π.

Теорема Влодарского

Если β не является целым кратным $\pi/4$ и $\cos\alpha = \cos^2\beta$, то хотя бы один из углов α, β несоизмерим с π.

Завершение доказательства теоремы об универсальном базисе

- $K(\frac{\pi}{4})H$ действует как поворот на угол, несоизмеримый с π, вокруг оси $(1, -\sqrt{2}+1, 1)^T$.
- $HK(\frac{\pi}{4}) = H(K(\frac{\pi}{4})H)H$ — как поворот на тот же угол вокруг другой оси.
- Значит, композиции $K(\frac{\pi}{4})$ и H порождают всюду плотное множество в $\mathbf{SU}(2)$.

Другие универсальные базисы

Базис Китаева

Базис $\{\text{cc-NOT}, \text{c-NOT}, H, K(\pi/2)\}$ — универсальный.

Лемма

Для вектора $|\xi\rangle \neq 0$ в унитарном пространстве размерности $\geqslant 3$ через H обозначим подгруппу унитарных операторов, сохраняющих $\mathbb{C}(\xi)$. Пусть V — произвольный унитарный оператор, не сохраняющий подпространство $\mathbb{C}(\xi)$. Тогда $H \cup V^{-1}HV$ порождает всю группу унитарных операторов на этом пространстве.

Теоремы Ши (Y. Shi, 2002)

1. cc-NOT и любой однокубитовый оператор, не сохраняющий вычислительный базис, образуют универсальный базис.
2. c-NOT и любой однокубитовый T такой, что T^2 не сохраняет вычислительный базис, образуют универсальный базис.

Другие универсальные базисы

Базис Китаева

Базис $\{\text{cc-NOT}, \text{c-NOT}, H, K(\pi/2)\}$ — универсальный.

Лемма

Для вектора $|\xi\rangle \neq 0$ в унитарном пространстве размерности $\geqslant 3$ через H обозначим подгруппу унитарных операторов, сохраняющих $\mathbb{C}(\xi)$. Пусть V — произвольный унитарный оператор, не сохраняющий подпространство $\mathbb{C}(\xi)$. Тогда $H \cup V^{-1}HV$ порождает всю группу унитарных операторов на этом пространстве.

Теоремы Ши (Y. Shi, 2002)

1. cc-NOT и любой однокубитовый оператор, не сохраняющий вычислительный базис, образуют универсальный базис.
2. c-NOT и любой однокубитовый T такой, что T^2 не сохраняет вычислительный базис, образуют универсальный базис.

Другие универсальные базисы

Базис Китаева

Базис $\{\text{cc-NOT}, \text{c-NOT}, H, K(\pi/2)\}$ — универсальный.

Лемма

Для вектора $|\xi\rangle \neq 0$ в унитарном пространстве размерности $\geqslant 3$ через H обозначим подгруппу унитарных операторов, сохраняющих $\mathbb{C}(\xi)$. Пусть V — произвольный унитарный оператор, не сохраняющий подпространство $\mathbb{C}(\xi)$. Тогда $H \cup V^{-1}HV$ порождает всю группу унитарных операторов на этом пространстве.

Теоремы Ши (Y. Shi, 2002)

1. cc-NOT и любой однокубитовый оператор, не сохраняющий вычислительный базис, образуют универсальный базис.
2. c-NOT и любой однокубитовый T такой, что T^2 не сохраняет вычислительный базис, образуют универсальный базис.

Комментарии к теоремам Ши

Следствия

1. Базис $\{\text{cc-NOT}, H\}$ — универсальный.
2. Базис $\{\text{c-NOT}, F\}$, где

$$F = \frac{1}{5}\begin{pmatrix} 4 & -3 \\ 3 & 4 \end{pmatrix},$$

является универсальным.

Вопрос

В базисе $\{\text{cc-NOT}, H\}$ все матричные элементы вещественные. В каком смысле этот базис универсальный?

Ответ

В теоремах Ши речь идет о подмножествах ортогональной группы, порождающих всюду плотное подмножество.

Комментарии к теоремам Ши

Следствия

1. Базис $\{\text{cc-NOT}, H\}$ — универсальный.
2. Базис $\{\text{c-NOT}, F\}$, где
$$F = \frac{1}{5}\begin{pmatrix} 4 & -3 \\ 3 & 4 \end{pmatrix},$$
является универсальным.

Вопрос

В базисе $\{\text{cc-NOT}, H\}$ все матричные элементы вещественные.
В каком смысле этот базис универсальный?

Ответ

В теоремах Ши речь идет о подмножествах ортогональной группы, порождающих всюду плотное подмножество.

Комментарии к теоремам Ши

Следствия

1. Базис $\{\text{cc-NOT}, H\}$ — универсальный.
2. Базис $\{\text{c-NOT}, F\}$, где
$$F = \frac{1}{5}\begin{pmatrix} 4 & -3 \\ 3 & 4 \end{pmatrix},$$
является универсальным.

Вопрос

В базисе $\{\text{cc-NOT}, H\}$ все матричные элементы вещественные. В каком смысле этот базис универсальный?

Ответ

В теоремах Ши речь идет о подмножествах ортогональной группы, порождающих всюду плотное подмножество.

Ортогональных преобразований достаточно

Заведем дополнительный кубит 0, который будет представлять действительную и мнимую части амплитуд: вектору $(a+bi)|x\rangle$ будем сопоставлять $(a|0\rangle + b|1\rangle) \otimes |x\rangle$.

Упражнение

- Проверьте, что для любого унитарного оператора U оператор
$$R(U) = \mathrm{Re}(U) - i\sigma_y[0]\,\mathrm{Im}(U)$$
является ортогональным в расширенном пространстве.
- Проверьте, что это соответствие сохраняется при произведении операторов:
$$R(UV) = R(U)R(V).$$
- Проверьте, что U и $R(U)$ порождают одинаковые вероятностные распределения при измерении всех кубитов, кроме нулевого.

Ортогональных преобразований достаточно

Заведем дополнительный кубит 0, который будет представлять действительную и мнимую части амплитуд: вектору $(a+bi)|x\rangle$ будем сопоставлять $(a|0\rangle + b|1\rangle) \otimes |x\rangle$.

Упражнение

- Проверьте, что для любого унитарного оператора U оператор
$$R(U) = \mathrm{Re}(U) - i\sigma_y[0]\,\mathrm{Im}(U)$$
является ортогональным в расширенном пространстве.
- Проверьте, что это соответствие сохраняется при произведении операторов:
$$R(UV) = R(U)R(V).$$
- Проверьте, что U и $R(U)$ порождают одинаковые вероятностные распределения при измерении всех кубитов, кроме нулевого.

Ортогональных преобразований достаточно

Заведем дополнительный кубит 0, который будет представлять действительную и мнимую части амплитуд: вектору $(a+bi)|x\rangle$ будем сопоставлять $(a|0\rangle + b|1\rangle) \otimes |x\rangle$.

Упражнение

- Проверьте, что для любого унитарного оператора U оператор

$$R(U) = \mathrm{Re}(U) - i\sigma_y[0]\,\mathrm{Im}(U)$$

  является ортогональным в расширенном пространстве.
- Проверьте, что это соответствие сохраняется при произведении операторов:

$$R(UV) = R(U)R(V).$$

- Проверьте, что U и $R(U)$ порождают одинаковые вероятностные распределения при измерении всех кубитов, кроме нулевого.

Ортогональных преобразований достаточно

Заведем дополнительный кубит 0, который будет представлять действительную и мнимую части амплитуд: вектору $(a+bi)|x\rangle$ будем сопоставлять $(a|0\rangle + b|1\rangle) \otimes |x\rangle$.

Упражнение

- Проверьте, что для любого унитарного оператора U оператор

$$R(U) = \mathrm{Re}(U) - i\sigma_y[0]\,\mathrm{Im}(U)$$

  является ортогональным в расширенном пространстве.
- Проверьте, что это соответствие сохраняется при произведении операторов:

$$R(UV) = R(U)R(V).$$

- Проверьте, что U и $R(U)$ порождают одинаковые вероятностные распределения при измерении всех кубитов, кроме нулевого.

План

Если нас интересует размер схем, то при использовании приближенных реализаций нужно оценивать увеличение размера схемы при приближении со стремящейся к 0 точностью.

Из свойств приближений следует, что если каждый оператор в схеме размера ℓ приближается (в расширенном смысле) с точностью ε/ℓ, то реализуемый схемой оператор приближается с точностью ε (линейное накопление ошибок).

Посмотрим на предыдущие результаты об универсальности с этой точки зрения. Нужна теорема вида

(теорема?) Оценка скорости приближения

Если угол α несоизмерим с π, то любой поворот R_φ приближается некоторым кратным R_α^n с точностью ε при $n \leqslant ?(\varepsilon)$.

(Устроит $n = O(1/\varepsilon)$, но для произвольного α это неверно.)

Приближения схем

Если нас интересует размер схем, то при использовании приближенных реализаций нужно оценивать увеличение размера схемы при приближении со стремящейся к 0 точностью.

Из свойств приближений следует, что если каждый оператор в схеме размера ℓ приближается (в расширенном смысле) с точностью ε/ℓ, то реализуемый схемой оператор приближается с точностью ε (линейное накопление ошибок).

Посмотрим на предыдущие результаты об универсальности с этой точки зрения. Нужна теорема вида

(теорема?) Оценка скорости приближения

Если угол α несоизмерим с π, то любой поворот R_φ приближается некоторым кратным R_α^n с точностью ε при $n \leqslant ?(\varepsilon)$.

(Устроит $n = O(1/\varepsilon)$, но для произвольного α это неверно.)

Приближения схем

Если нас интересует размер схем, то при использовании приближенных реализаций нужно оценивать увеличение размера схемы при приближении со стремящейся к 0 точностью.

Из свойств приближений следует, что если каждый оператор в схеме размера ℓ приближается (в расширенном смысле) с точностью ε/ℓ, то реализуемый схемой оператор приближается с точностью ε (линейное накопление ошибок).

Посмотрим на предыдущие результаты об универсальности с этой точки зрения. Нужна теорема вида

(теорема?) Оценка скорости приближения

Если угол α несоизмерим с π, то любой поворот R_φ приближается некоторым кратным R_α^n с точностью ε при $n \leqslant ?(\varepsilon)$.

(Устроит $n = O(1/\varepsilon)$, но для произвольного α это неверно.)

Эффективное приближение в базисе $\{\text{c-NOT}, H, K(\pi/4)\}$

Вопрос

Верна ли оценка приближения $n = O(1/\varepsilon)$ при $\cos\alpha = \cos^2(\pi/8)$?
Тогда схема размера ℓ в произвольном конечном базисе будет приближаться схемой в базисе $\{\text{c-NOT}, H, K(\pi/4)\}$ размера $O(\ell^2)$.

Предположительный ответ

Видимо, верна. Дело в том, что $\cos\alpha$ и $\sin\alpha$ — алгебраические числа, которые плохо приближаются рациональными.
В данном случае «плохо» как раз означает «хорошо»: знаменатели цепных дробей для $\cos\alpha$, $\sin\alpha$ растут не слишком быстро.

Задача (неизвестной трудности)

При $\cos\alpha = \cos^2(\pi/8)$ докажите оценку приближения вида $n = \mathrm{poly}(1/\varepsilon)$.

Эффективное приближение в базисе $\{\text{c-NOT}, H, K(\pi/4)\}$

Вопрос

Верна ли оценка приближения $n = O(1/\varepsilon)$ при $\cos\alpha = \cos^2(\pi/8)$?
Тогда схема размера ℓ в произвольном конечном базисе будет приближаться схемой в базисе $\{\text{c-NOT}, H, K(\pi/4)\}$ размера $O(\ell^2)$.

Предположительный ответ

Видимо, верна. Дело в том, что $\cos\alpha$ и $\sin\alpha$ — алгебраические числа, которые плохо приближаются рациональными.
В данном случае «плохо» как раз означает «хорошо»: знаменатели цепных дробей для $\cos\alpha$, $\sin\alpha$ растут не слишком быстро.

Задача (неизвестной трудности)

При $\cos\alpha = \cos^2(\pi/8)$ докажите оценку приближения вида $n = \mathrm{poly}(1/\varepsilon)$.

Эффективное приближение в базисе $\{\text{c-NOT}, H, K(\pi/4)\}$

Вопрос

Верна ли оценка приближения $n = O(1/\varepsilon)$ при $\cos\alpha = \cos^2(\pi/8)$?
Тогда схема размера ℓ в произвольном конечном базисе будет приближаться схемой в базисе $\{\text{c-NOT}, H, K(\pi/4)\}$ размера $O(\ell^2)$.

Предположительный ответ

Видимо, верна. Дело в том, что $\cos\alpha$ и $\sin\alpha$ — алгебраические числа, которые плохо приближаются рациональными.
В данном случае «плохо» как раз означает «хорошо»: знаменатели цепных дробей для $\cos\alpha$, $\sin\alpha$ растут не слишком быстро.

Задача (неизвестной трудности)

При $\cos\alpha = \cos^2(\pi/8)$ докажите оценку приближения вида $n = \mathrm{poly}(1/\varepsilon)$.

Эффективное приближение в базисе $\{\text{c-NOT}, H, K(\pi/4)\}$

Вопрос

Верна ли оценка приближения $n = O(1/\varepsilon)$ при $\cos\alpha = \cos^2(\pi/8)$?
Тогда схема размера ℓ в произвольном конечном базисе будет приближаться схемой в базисе $\{\text{c-NOT}, H, K(\pi/4)\}$ размера $O(\ell^2)$.

Предположительный ответ

Видимо, верна. Дело в том, что $\cos\alpha$ и $\sin\alpha$ — алгебраические числа, которые плохо приближаются рациональными.
В данном случае «плохо» как раз означает «хорошо»: знаменатели цепных дробей для $\cos\alpha$, $\sin\alpha$ растут не слишком быстро.

Задача (неизвестной трудности)

При $\cos\alpha = \cos^2(\pi/8)$ докажите оценку приближения вида $n = \mathrm{poly}(1/\varepsilon)$.

Изучать особенности каждого базиса необязательно!

Теорема Китаева – Соловея

Для любого $\nu > 0$ справедливо следующее.
Пусть имеется конечный базис $\mathcal{B}$, замкнутый относительно взятия обратного оператора, операторы которого порождают всюду плотное подмножество $\mathbf{SU}(M)$, $M \geqslant 2$.
Тогда любой оператор из $\mathbf{SU}(M)$ приближается с точностью δ схемой в базисе $\mathcal{B}$ размера $L = O(\exp(O(M^2)) \log(1/\delta)^{3+\nu})$.
Более того, существует алгоритм, который порождает описание приближающей схемы за время $O(L)$.

Следствие

Операторы любого конечного универсального базиса приближаются в любом другом конечном универсальном базисе схемами полилогарифмического размера от точности. (В данном случае $M = O(1)$.)

Изучать особенности каждого базиса необязательно!

Теорема Китаева – Соловея

Для любого $\nu > 0$ справедливо следующее.
Пусть имеется конечный базис $\mathcal{B}$, замкнутый относительно взятия обратного оператора, операторы которого порождают всюду плотное подмножество $\mathbf{SU}(M)$, $M \geqslant 2$.
Тогда любой оператор из $\mathbf{SU}(M)$ приближается с точностью δ схемой в базисе $\mathcal{B}$ размера $L = O(\exp(O(M^2))\log(1/\delta)^{3+\nu})$.
Более того, существует алгоритм, который порождает описание приближающей схемы за время $O(L)$.

Следствие

Операторы любого конечного универсального базиса приближаются в любом другом конечном универсальном базисе схемами полилогарифмического размера от точности. (В данном случае $M = O(1)$.)

Изучать особенности каждого базиса необязательно!

Теорема Китаева – Соловея

Для любого $\nu > 0$ справедливо следующее.
Пусть имеется конечный базис $\mathcal{B}$, замкнутый относительно взятия обратного оператора, операторы которого порождают всюду плотное подмножество $\mathbf{SU}(M)$, $M \geqslant 2$.
Тогда любой оператор из $\mathbf{SU}(M)$ приближается с точностью δ схемой в базисе $\mathcal{B}$ размера $L = O(\exp(O(M^2))\log(1/\delta)^{3+\nu})$.
Более того, существует алгоритм, который порождает описание приближающей схемы за время $O(L)$.

Следствие

Операторы любого конечного универсального базиса приближаются в любом другом конечном универсальном базисе схемами полилогарифмического размера от точности. (В данном случае $M = O(1)$.)

Изучать особенности каждого базиса необязательно!

Теорема Китаева – Соловея

Для любого $\nu > 0$ справедливо следующее.
Пусть имеется конечный базис $\mathcal{B}$, замкнутый относительно взятия обратного оператора, операторы которого порождают всюду плотное подмножество $\mathbf{SU}(M)$, $M \geqslant 2$.
Тогда любой оператор из $\mathbf{SU}(M)$ приближается с точностью δ схемой в базисе $\mathcal{B}$ размера $L = O(\exp(O(M^2))\log(1/\delta)^{3+\nu})$.
Более того, существует алгоритм, который порождает описание приближающей схемы за время $O(L)$.

Следствие

Операторы любого конечного универсального базиса приближаются в любом другом конечном универсальном базисе схемами полилогарифмического размера от точности. (В данном случае $M = O(1)$.)

- Куда прячется неэффективность (и зависимость от базиса)?
- Ответ: в неявные константы $O(\cdot)$.
- Первый (неконструктивный) шаг в доказательстве теоремы — построение из операторов универсального базиса ε-сети на $\mathbf{SU}(M)$ при достаточно малом ε. Причем эта сеть должна быть достаточно разреженной и содержать $O(\varepsilon^{-M^2})$ элементов.
- Порождение такой сети может занять очень большое время, оценка которого как раз зависит от базиса.

Комментарии к теореме Китаева – Соловея

- Куда прячется неэффективность (и зависимость от базиса)?
- Ответ: в неявные константы $O(\cdot)$.
- Первый (неконструктивный) шаг в доказательстве теоремы — построение из операторов универсального базиса ε-сети на $\mathbf{SU}(M)$ при достаточно малом ε. Причем эта сеть должна быть достаточно разреженной и содержать $O(\varepsilon^{-M^2})$ элементов.
- Порождение такой сети может занять очень большое время, оценка которого как раз зависит от базиса.

Комментарии к теореме Китаева – Соловея

- Куда прячется неэффективность (и зависимость от базиса)?
- Ответ: в неявные константы $O(\cdot)$.
- Первый (неконструктивный) шаг в доказательстве теоремы — построение из операторов универсального базиса ε-сети на $\mathbf{SU}(M)$ при достаточно малом ε. Причем эта сеть должна быть достаточно разреженной и содержать $O(\varepsilon^{-M^2})$ элементов.
- Порождение такой сети может занять очень большое время, оценка которого как раз зависит от базиса.

Комментарии к теореме Китаева – Соловея

- Куда прячется неэффективность (и зависимость от базиса)?
- Ответ: в неявные константы $O(\cdot)$.
- Первый (неконструктивный) шаг в доказательстве теоремы — построение из операторов универсального базиса ε-сети на $\mathbf{SU}(M)$ при достаточно малом ε. Причем эта сеть должна быть достаточно разреженной и содержать $O(\varepsilon^{-M^2})$ элементов.
- Порождение такой сети может занять очень большое время, оценка которого как раз зависит от базиса.

Три идеи для доказательства теоремы

- Иерархическое приближение. Строится последовательность ε_k-сетей и приближение строится последовательно: оператор U приближается в самой грубой ε-сети оператором V_1, затем $V_1^{-1}U$ приближается в следующей по мелкости и т. д.
- Коммутаторы для построения очень мелких сетей. По сетям Γ_1, Γ_2 строится коммутатор

$$[\Gamma_1, \Gamma_2] = \{W : W = UVU^{-1}V^{-1},\ U \in \Gamma_1,\ V \in \Gamma_2\},$$

  который дает сеть очень высокого разрешения в очень малой окрестности единичного оператора.
- «Телескопирование». Из подходящих сетей окрестностей единичного оператора взятием произведения сетей $\Gamma_1\Gamma_2$ конструируется сеть одновременно и достаточно мелкая, и покрывающая достаточно большую окрестность единицы.

Три идеи для доказательства теоремы

- Иерархическое приближение. Строится последовательность ε_k-сетей и приближение строится последовательно: оператор U приближается в самой грубой ε-сети оператором V_1, затем $V_1^{-1}U$ приближается в следующей по мелкости и т. д.
- Коммутаторы для построения очень мелких сетей. По сетям Γ_1, Γ_2 строится коммутатор

$$[\Gamma_1, \Gamma_2] = \{W\colon W = UVU^{-1}V^{-1},\ U \in \Gamma_1,\ V \in \Gamma_2\},$$

  который дает сеть очень высокого разрешения в очень малой окрестности единичного оператора.
- «Телескопирование». Из подходящих сетей окрестностей единичного оператора взятием произведения сетей $\Gamma_1\Gamma_2$ конструируется сеть одновременно и достаточно мелкая, и покрывающая достаточно большую окрестность единицы.

Три идеи для доказательства теоремы

- Иерархическое приближение. Строится последовательность ε_k-сетей и приближение строится последовательно: оператор U приближается в самой грубой ε-сети оператором V_1, затем $V_1^{-1}U$ приближается в следующей по мелкости и т. д.
- Коммутаторы для построения очень мелких сетей. По сетям Γ_1, Γ_2 строится коммутатор

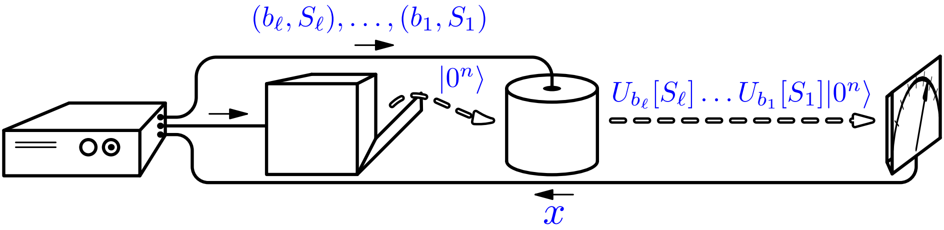
$$[\Gamma_1, \Gamma_2] = \{W : W = UVU^{-1}V^{-1},\ U \in \Gamma_1,\ V \in \Gamma_2\},$$

  который дает сеть очень высокого разрешения в очень малой окрестности единичного оператора.
- «Телескопирование». Из подходящих сетей окрестностей единичного оператора взятием произведения сетей $\Gamma_1\Gamma_2$ конструируется сеть одновременно и достаточно мелкая, и покрывающая достаточно большую окрестность единицы.

План

1. Приближенная реализация унитарных операторов
2. Конечные универсальные базисы
3. Эффективные приближения
4. Окончательное определение квантового алгоритма

Уточнение первоначальной картины квантового вычисления

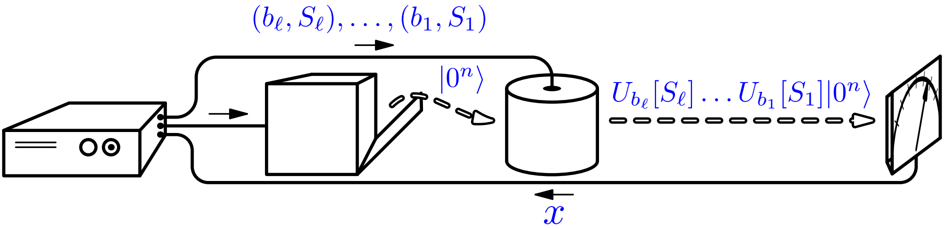


U_{b_k} — операторы из конечного универсального базиса.
S_k — множество кубитов, на которые действует k-й оператор.
x — результат измерения, вероятность наблюдения x

$$\mathbf{Pr}(U_{b_\ell}[S_\ell] \ldots U_{b_1}[S_1]|0^n\rangle, x) = \left|\langle x| U_{b_\ell}[S_\ell] \ldots U_{b_1}[S_1]|0^n\rangle\right|^2.$$

Время выполнения отмеченного на рисунке цикла действий: $O(\ell)$.

Уточнение первоначальной картины квантового вычисления

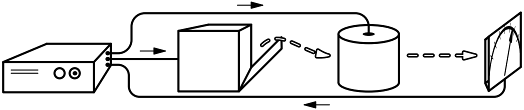


U_{b_k} — операторы из конечного универсального базиса.
S_k — множество кубитов, на которые действует k-й оператор.
x — результат измерения, вероятность наблюдения x

$$\mathbf{Pr}(U_{b_\ell}[S_\ell]\ldots U_{b_1}[S_1]|0^n\rangle, x) = \left|\langle x|U_{b_\ell}[S_\ell]\ldots U_{b_1}[S_1]|0^n\rangle\right|^2.$$

Время выполнения отмеченного на рисунке цикла действий: $O(\ell)$.

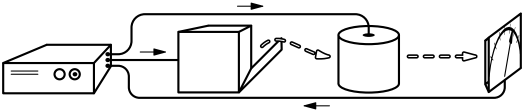
Упрощения



Достаточно одного обращения к квантовому устройству:

- Все классические вычисления моделируются подходящими квантовыми схемами.
- Все промежуточные измерения можно моделировать подходящими квантовыми схемами.
  А именно, после измерения кубита применяются лишь операторы вида
  $$U : |b\rangle \otimes |\psi\rangle \mapsto |b\rangle \otimes U_b|\psi\rangle.$$
  (при необходимости такие операторы приближаются в используемом базисе).

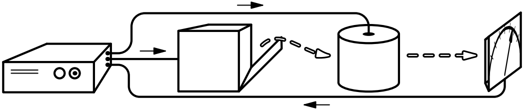
Упрощения



Достаточно одного обращения к квантовому устройству:

- Все классические вычисления моделируются подходящими квантовыми схемами.
- Все промежуточные измерения можно моделировать подходящими квантовыми схемами.
  А именно, после измерения кубита применяются лишь операторы вида
  $$U : |b\rangle \otimes |\psi\rangle \mapsto |b\rangle \otimes U_b|\psi\rangle.$$
  (при необходимости такие операторы приближаются в используемом базисе).

Упрощения



Достаточно одного обращения к квантовому устройству:

- Все классические вычисления моделируются подходящими квантовыми схемами.
- Все промежуточные измерения можно моделировать подходящими квантовыми схемами.
  А именно, после измерения кубита применяются лишь операторы вида
  $$U\colon |b\rangle \otimes |\psi\rangle \mapsto |b\rangle \otimes U_b|\psi\rangle.$$
  (при необходимости такие операторы приближаются в используемом базисе).

Квантовый алгоритм

Определения

Квантовый алгоритм Q: это классический алгоритм A, который по входу x строит описание квантовой схемы C_x в универсальном конечном базисе, реализующей оператор U_x на n_x кубитах, и описание регистра результата S_x.

Время работы алгоритма на входе x: время работы A плюс размер схемы C_x.

Вероятность результата y на входе x:

$$\mathbf{Pr}(y \mid x) = \sum_{z:z[S_x]=y} \left|\langle x|U_x|0^{n_x}\rangle\right|^2.$$

Алгоритм вычисляет функцию $f(x)$ с вероятностью ошибки ε, если

$$\mathbf{Pr}(y \neq f(x) \mid x) < \varepsilon.$$

Квантовый алгоритм

Определения

Квантовый алгоритм Q: это классический алгоритм A, который по входу x строит описание квантовой схемы C_x в универсальном конечном базисе, реализующей оператор U_x на n_x кубитах, и описание регистра результата S_x.

Время работы алгоритма на входе x: время работы A плюс размер схемы C_x.

Вероятность результата y на входе x:

$$\Pr(y \mid x) = \sum_{z:z[S_x]=y} \left| \langle x | U_x | 0^{n_x} \rangle \right|^2.$$

Алгоритм вычисляет функцию $f(x)$ с вероятностью ошибки ε, если

$$\Pr(y \neq f(x) \mid x) < \varepsilon.$$

Квантовый алгоритм

Определения

Квантовый алгоритм Q: это классический алгоритм A, который по входу x строит описание квантовой схемы C_x в универсальном конечном базисе, реализующей оператор U_x на n_x кубитах, и описание регистра результата S_x.

Время работы алгоритма на входе x: время работы A плюс размер схемы C_x.

Вероятность результата y на входе x:

$$\mathbf{Pr}(y \mid x) = \sum_{z:z[S_x]=y} \left| \langle x | U_x | 0^{n_x} \rangle \right|^2.$$

Алгоритм вычисляет функцию $f(x)$ с вероятностью ошибки ε, если

$$\mathbf{Pr}(y \neq f(x) \mid x) < \varepsilon.$$

Квантовый алгоритм

Определения

Квантовый алгоритм Q: это классический алгоритм A, который по входу x строит описание квантовой схемы C_x в универсальном конечном базисе, реализующей оператор U_x на n_x кубитах, и описание регистра результата S_x.

Время работы алгоритма на входе x: время работы A плюс размер схемы C_x.

Вероятность результата y на входе x:

$$\mathbf{Pr}(y \mid x) = \sum_{z:z[S_x]=y} \left| \langle x | U_x | 0^{n_x} \rangle \right|^2.$$

Алгоритм вычисляет функцию $f(x)$ с вероятностью ошибки ε, если

$$\mathbf{Pr}(y \neq f(x) \mid x) < \varepsilon.$$

- Более распространено определение, в котором алгоритм строит описание единой схемы для всех входов длины n и на вход квантовой схемы вместо $|0^n\rangle$ подается $|x\rangle$. Эти определения эквивалентны (упражнение).
- Вероятность ошибки можно довольно быстро понизить.

Задача

Пусть квантовый алгоритм Q вычисляет $f(x)$ с вероятностью ошибки $\varepsilon < 1/2$.
Алгоритм Q'_ε работает следующим образом:

Комментарии к определению квантового алгоритма

- Более распространено определение, в котором алгоритм строит описание единой схемы для всех входов длины n и на вход квантовой схемы вместо $|0^n\rangle$ подается $|x\rangle$. Эти определения эквивалентны (упражнение).
- Вероятность ошибки можно довольно быстро понизить.

Задача

Пусть квантовый алгоритм Q вычисляет $f(x)$ с вероятностью ошибки $\varepsilon < 1/2$.
Алгоритм Q'_s работает следующим образом:

1. s раз независимо повторить алгоритм Q;
2. выдать результатом то значение y, которое встретилось чаще всего.

Докажите, что Q'_s вычисляет $f(x)$ с вероятностью ошибки $< \left(2\sqrt{\varepsilon(1-\varepsilon)}\right)^s$.

Комментарии к определению квантового алгоритма

- Более распространено определение, в котором алгоритм строит описание единой схемы для всех входов длины n и на вход квантовой схемы вместо $|0^n\rangle$ подается $|x\rangle$. Эти определения эквивалентны (упражнение).
- Вероятность ошибки можно довольно быстро понизить.

Задача

Пусть квантовый алгоритм Q вычисляет $f(x)$ с вероятностью ошибки $\varepsilon < 1/2$.
Алгоритм Q'_s работает следующим образом:

1. s раз независимо повторить алгоритм Q;
2. выдать результатом то значение y, которое встретилось чаще всего.

Докажите, что Q'_s вычисляет $f(x)$ с вероятностью ошибки $< (2\sqrt{\varepsilon(1-\varepsilon)})^s$.

Комментарии к определению квантового алгоритма

- Более распространено определение, в котором алгоритм строит описание единой схемы для всех входов длины n и на вход квантовой схемы вместо $|0^n\rangle$ подается $|x\rangle$. Эти определения эквивалентны (упражнение).
- Вероятность ошибки можно довольно быстро понизить.

Задача

Пусть квантовый алгоритм Q вычисляет $f(x)$ с вероятностью ошибки $\varepsilon < 1/2$.
Алгоритм Q'_s работает следующим образом:

1. s раз независимо повторить алгоритм Q;
2. выдать результатом то значение y, которое встретилось чаще всего.

Докажите, что Q'_s вычисляет $f(x)$ с вероятностью ошибки $< (2\sqrt{\varepsilon(1-\varepsilon)})^s$.

Комментарии к определению квантового алгоритма

- Более распространено определение, в котором алгоритм строит описание единой схемы для всех входов длины n и на вход квантовой схемы вместо $|0^n\rangle$ подается $|x\rangle$. Эти определения эквивалентны (упражнение).
- Вероятность ошибки можно довольно быстро понизить.

Задача

Пусть квантовый алгоритм Q вычисляет $f(x)$ с вероятностью ошибки $\varepsilon < 1/2$.
Алгоритм Q'_s работает следующим образом:

1. s раз независимо повторить алгоритм Q;
2. выдать результатом то значение y, которое встретилось чаще всего.

Докажите, что Q'_s вычисляет $f(x)$ с вероятностью ошибки $< (2\sqrt{\varepsilon(1-\varepsilon)})^s$.

Комментарии к определению квантового алгоритма

- Более распространено определение, в котором алгоритм строит описание единой схемы для всех входов длины n и на вход квантовой схемы вместо $|0^n\rangle$ подается $|x\rangle$. Эти определения эквивалентны (упражнение).
- Вероятность ошибки можно довольно быстро понизить.

Задача

Пусть квантовый алгоритм Q вычисляет $f(x)$ с вероятностью ошибки $\varepsilon < 1/2$.
Алгоритм Q'_s работает следующим образом:

1. s раз независимо повторить алгоритм Q;
2. выдать результатом то значение y, которое встретилось чаще всего.

Докажите, что Q'_s вычисляет $f(x)$ с вероятностью ошибки $< (2\sqrt{\varepsilon(1-\varepsilon)})^s$.