Квантовые алгоритмы: возможности и ограничения. Лекция 6: Квантовые схемы

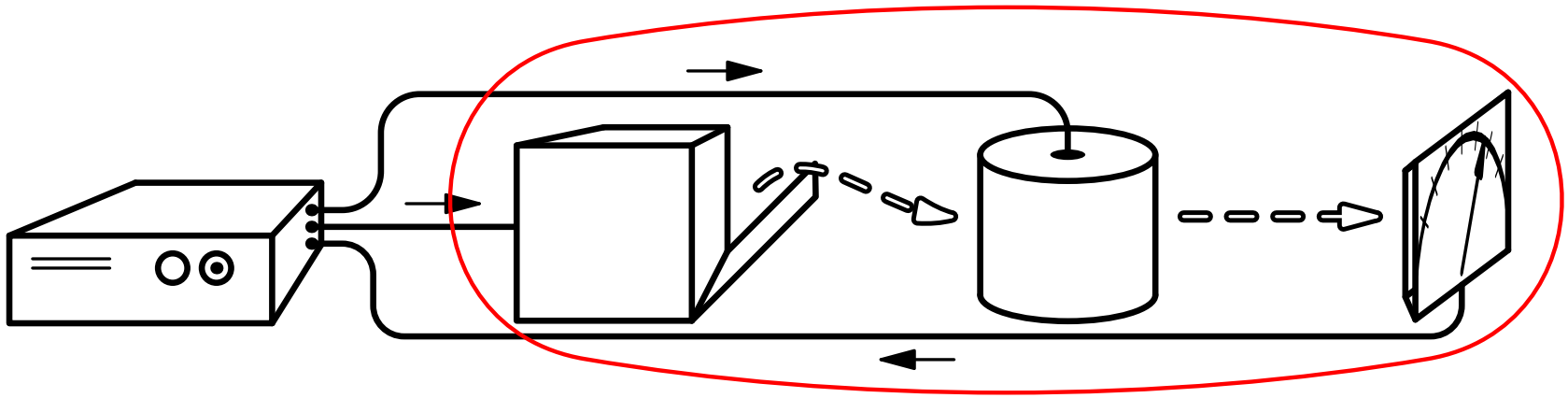
М. Вялый

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

Санкт-Петербург, 2011

План

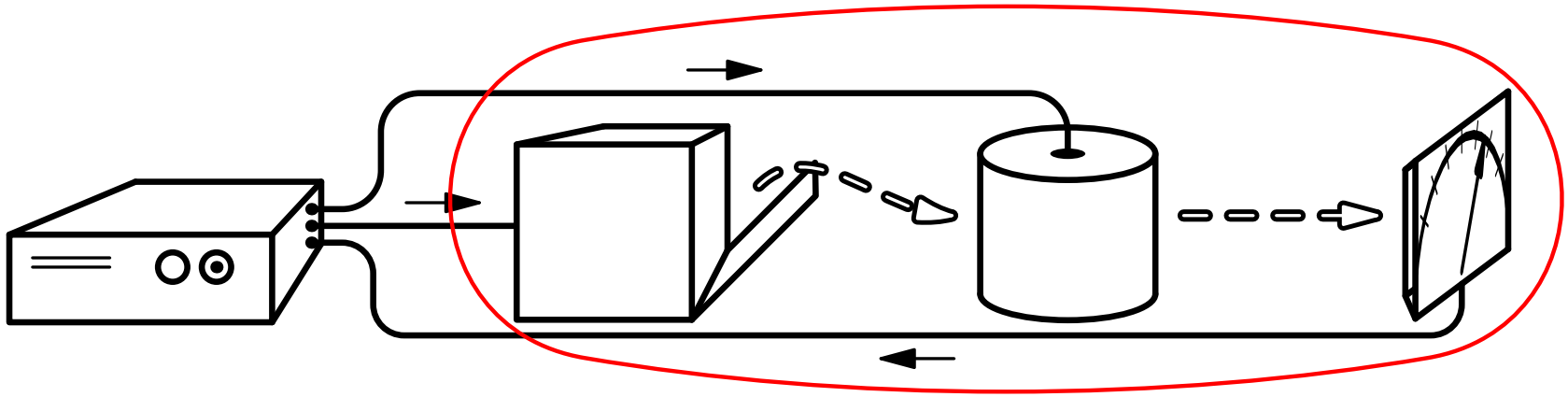
Квантовое устройство с точки зрения классического наблюдателя



Порождает вероятностное распределение на результатах наблюдения.
Два основных вопроса:

1. Как определить ресурсы (например, время) для порождения распределения p квантовым устройством?
2. Насколько сложно породить близкое распределение классическими средствами?

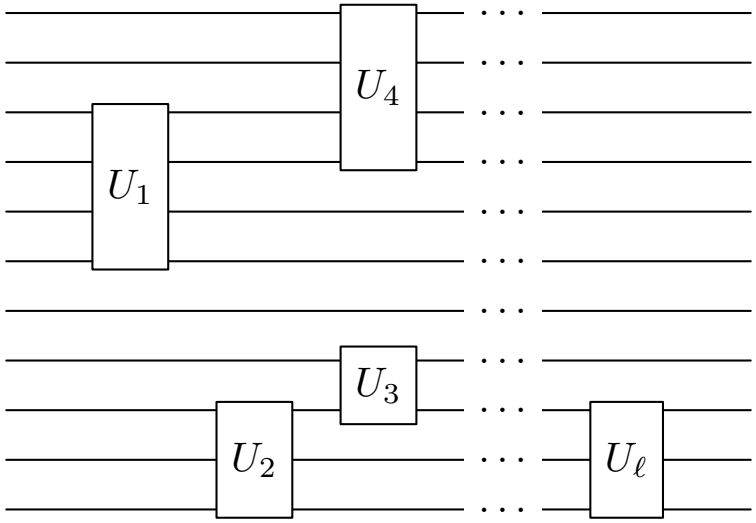
Квантовое устройство с точки зрения классического наблюдателя



Порождает вероятностное распределение на результатах наблюдения.
Два основных вопроса:

1. Как определить ресурсы (например, время) для порождения распределения p квантовым устройством?
2. Насколько сложно породить близкое распределение классическими средствами?

Элементы квантовых схем



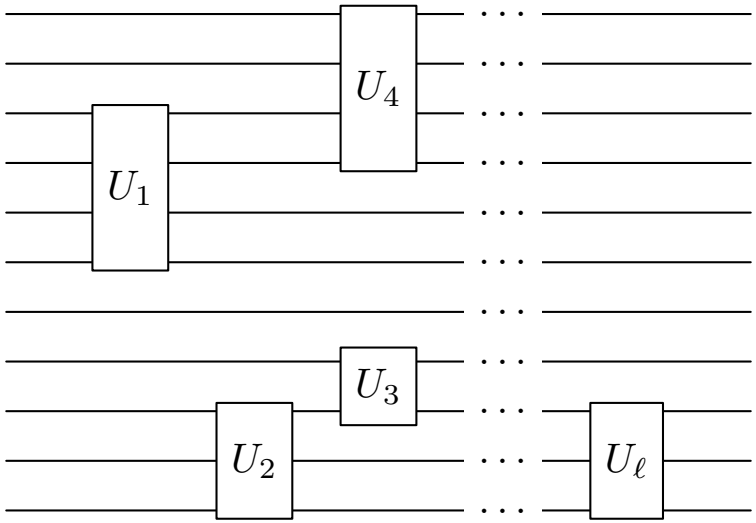
Базис

Набор унитарных операторов $\mathcal{B}$, описывающих элементарные действия.

Физические ограничения

1. Элементарное действие локально: нетривиально действует лишь на небольшое количество кубитов (один, два, три, ..., $O(1)$).
2. Если два элементарных действия совершаются одновременно, то они нетривиально действуют на разных наборах кубитов.

Элементы квантовых схем



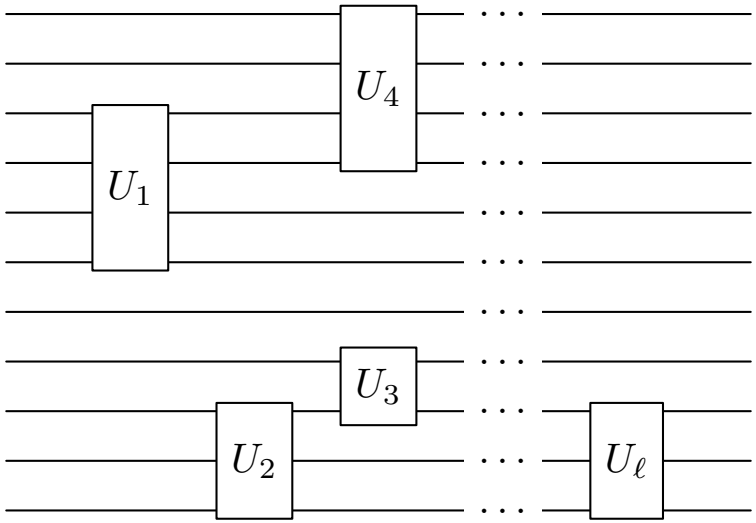
Базис

Набор унитарных операторов $\mathcal{B}$, описывающих элементарные действия.

Физические ограничения

1. Элементарное действие локально: нетривиально действует лишь на небольшое количество кубитов (один, два, три, ..., $O(1)$).
2. Если два элементарных действия совершаются одновременно, то они нетривиально действуют на разных наборах кубитов.

Элементы квантовых схем



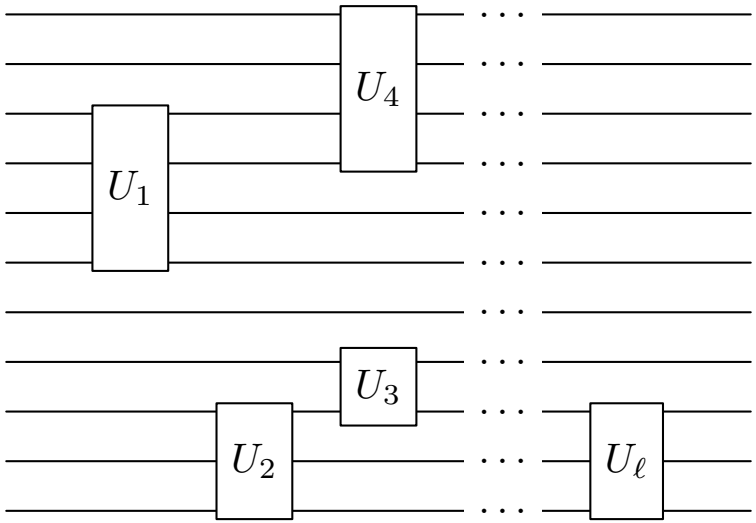
Базис

Набор унитарных операторов $\mathcal{B}$, описывающих элементарные действия.

Физические ограничения

1. Элементарное действие локально: нетривиально действует лишь на небольшое количество кубитов (один, два, три, ..., $O(1)$).
2. Если два элементарных действия совершаются одновременно, то они нетривиально действуют на разных наборах кубитов.

Квантовая схема над базисом $\mathcal{B}$: определение



Квантовая схема

Последовательность операторов

$$U_1[S_1], U_2[S_2], \ldots, U_\ell[S_\ell],$$

где $U_k \in \mathcal{B}$, $S_k \subseteq \{1, \ldots, n\}$, n — количество используемых кубитов.

Матричные элементы $U[S]$

Пусть

$$U = \sum_{x,y \in \{0,1\}^d} u_{x,y} |x\rangle\langle y|,$$

$$S = \{j_1, \ldots, j_d\}.$$

Обозначим $x[S]$ подпоследовательность битов, стоящих на местах из множества S.

Тогда

$$U[S] = \sum_{x,y \in \{0,1\}^n : x[\bar{S}] = y[\bar{S}]} u_{x[S],y[S]} |x\rangle\langle y|.$$

Матричные элементы $U[S]$

Пусть

$$U = \sum_{x,y \in \{0,1\}^d} u_{x,y} |x\rangle\langle y|,$$

$$S = \{j_1, \ldots, j_d\}.$$

Обозначим $x[S]$ подпоследовательность битов, стоящих на местах из множества S.

Тогда

$$U[S] = \sum_{x,y \in \{0,1\}^n : x[\bar{S}] = y[\bar{S}]} u_{x[S],y[S]} |x\rangle\langle y|.$$

Матричные элементы $U[S]$

Пусть

$$U = \sum_{x,y \in \{0,1\}^d} u_{x,y} |x\rangle\langle y|,$$

$$S = \{j_1, \ldots, j_d\}.$$

Обозначим $x[S]$ подпоследовательность битов, стоящих на местах из множества S.

Тогда

$$U[S] = \sum_{x,y \in \{0,1\}^n : x[\bar{S}] = y[\bar{S}]} u_{x[S],y[S]} |x\rangle\langle y|.$$

Меры сложности схемы

Размер схемы

Количество элементов в схеме. Отвечает за время вычисления на последовательном устройстве.

Глубина схемы

Наименьшее количество слоев, в которые можно расположить элементы схемы при соблюдении условий:

1. элементы, которые стоят в схеме после j-го, не попадают в слои, предшествующие слою, в котором находится j-й элемент;
2. элементы из одного слоя действуют на непересекающиеся множества кубитов.

Глубина отвечает за время вычисления на параллельном устройстве.

Меры сложности схемы

Размер схемы

Количество элементов в схеме. Отвечает за время вычисления на последовательном устройстве.

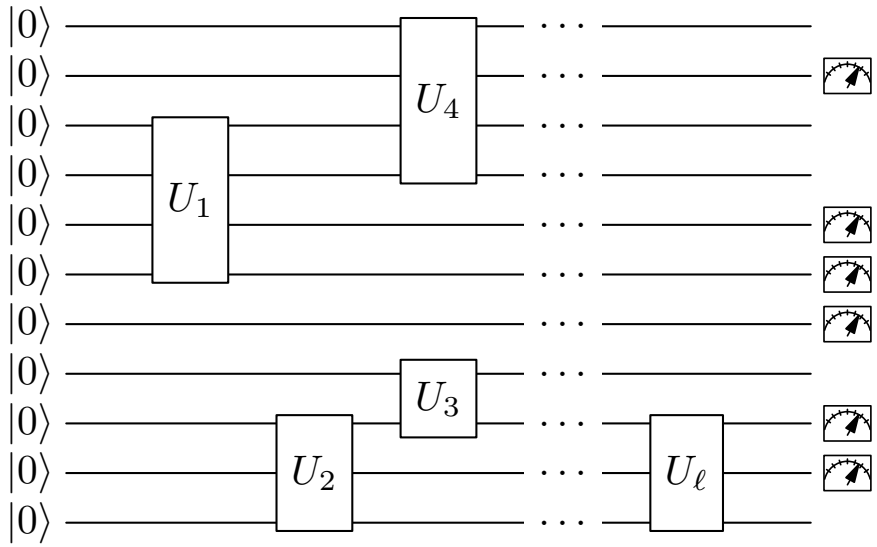
Глубина схемы

Наименьшее количество слоев, в которые можно расположить элементы схемы при соблюдении условий:

1. элементы, которые стоят в схеме после j-го, не попадают в слои, предшествующие слою, в котором находится j-й элемент;
2. элементы из одного слоя действуют на непересекающиеся множества кубитов.

Глубина отвечает за время вычисления на параллельном устройстве.

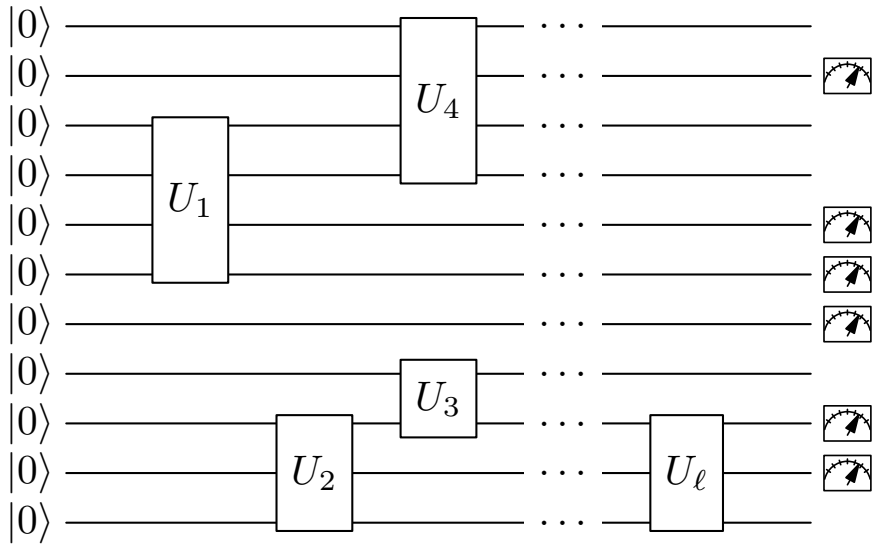
Использование квантового ресурса: уточнение



Вопросы

1. Почему можно использовать начальное состояние $|0^n\rangle$?
2. Какие начальные состояния помимо $|0^n\rangle$ можно использовать?
3. Как зависит трудоемкость от выбора базиса?

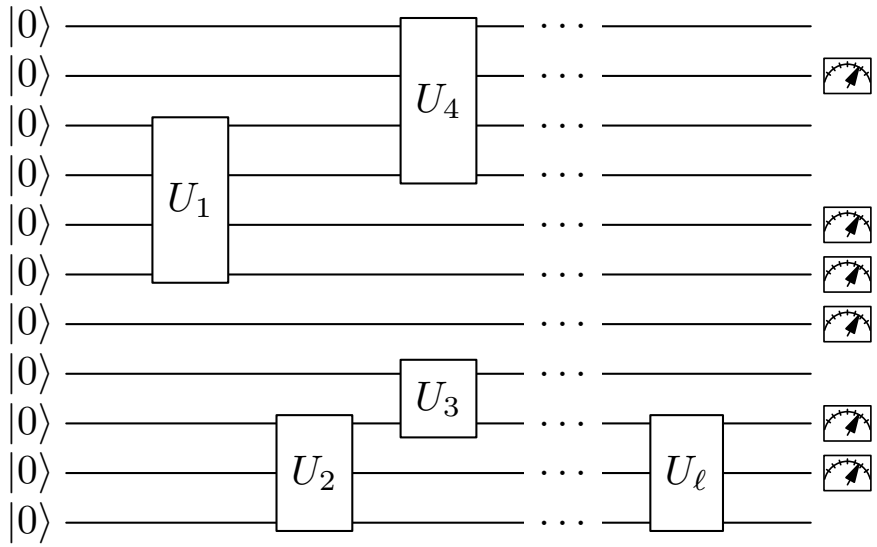
Использование квантового ресурса: уточнение



Вопросы

1. Почему можно использовать начальное состояние $|0^n\rangle$?
2. Какие начальные состояния помимо $|0^n\rangle$ можно использовать?
3. Как зависит трудоемкость от выбора базиса?

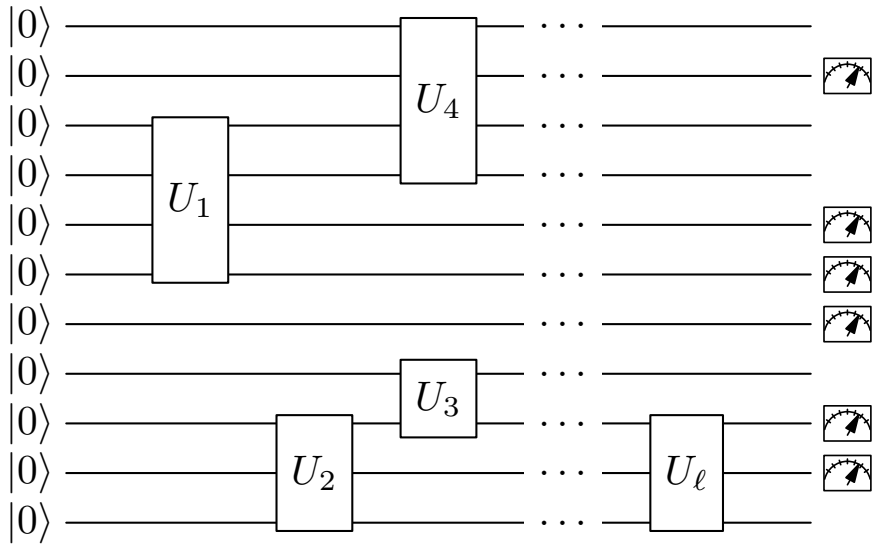
Использование квантового ресурса: уточнение



Вопросы

1. Почему можно использовать начальное состояние $|0^n\rangle$?
2. Какие начальные состояния помимо $|0^n\rangle$ можно использовать?
3. Как зависит трудоемкость от выбора базиса?

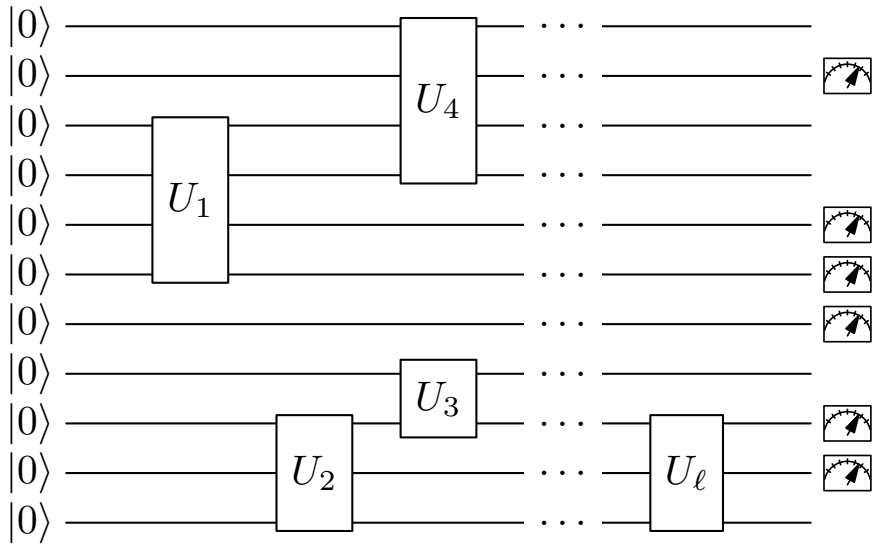
Использование квантового ресурса: уточнение



Вопросы

1. Почему можно использовать начальное состояние $|0^n\rangle$?
2. Какие начальные состояния помимо $|0^n\rangle$ можно использовать?
3. Как зависит трудоемкость от выбора базиса?

Использование квантового ресурса: уточнение



Вопросы

1. Почему можно использовать начальное состояние $|0^n\rangle$?
2. Какие начальные состояния помимо $|0^n\rangle$ можно использовать?
3. Как зависит трудоемкость от выбора базиса?

Ответ на первый вопрос

Утверждение

Если есть прибор, измеряющий в вычислительном базисе, то можно приготавливать состояния из вычислительного базиса.

Порядок действий при изготовлении состояния $|0\rangle$:

1. Берем случайное состояние.
2. Измеряем его в вычислительном базисе.
3. Если наблюдаем исход 0, то кубит находится в состоянии $|0\rangle$. Готово.
4. В противном случае повторяем процедуру.

Ответ на первый вопрос

Утверждение

Если есть прибор, измеряющий в вычислительном базисе, то можно приготавливать состояния из вычислительного базиса.

Порядок действий при изготовлении состояния $|0\rangle$:

1. Берем случайное состояние.
2. Измеряем его в вычислительном базисе.
3. Если наблюдаем исход 0, то кубит находится в состоянии $|0\rangle$: готово.
4. В противном случае повторяем процедуру.

Ответ на первый вопрос

Утверждение

Если есть прибор, измеряющий в вычислительном базисе, то можно приготавливать состояния из вычислительного базиса.

Порядок действий при изготовлении состояния $|0\rangle$:

1. Берем случайное состояние.
2. Измеряем его в вычислительном базисе.
3. Если наблюдаем исход 0, то кубит находится в состоянии $|0\rangle$: готово.
4. В противном случае повторяем процедуру.

Ответ на первый вопрос

Утверждение

Если есть прибор, измеряющий в вычислительном базисе, то можно приготавливать состояния из вычислительного базиса.

Порядок действий при изготовлении состояния $|0\rangle$:

1. Берем случайное состояние.
2. Измеряем его в вычислительном базисе.
3. Если наблюдаем исход 0, то кубит находится в состоянии $|0\rangle$: готово.
4. В противном случае повторяем процедуру.

Ответ на первый вопрос

Утверждение

Если есть прибор, измеряющий в вычислительном базисе, то можно приготавливать состояния из вычислительного базиса.

Порядок действий при изготовлении состояния $|0\rangle$:

1. Берем случайное состояние.
2. Измеряем его в вычислительном базисе.
3. Если наблюдаем исход 0, то кубит находится в состоянии $|0\rangle$: готово.
4. В противном случае повторяем процедуру.

Ответ на первый вопрос

Утверждение

Если есть прибор, измеряющий в вычислительном базисе, то можно приготавливать состояния из вычислительного базиса.

Порядок действий при изготовлении состояния $|0\rangle$:

1. Берем случайное состояние.
2. Измеряем его в вычислительном базисе.
3. Если наблюдаем исход 0, то кубит находится в состоянии $|0\rangle$: готово.
4. В противном случае повторяем процедуру.

Ответ на второй вопрос

Зависит от законов физики. Но вряд ли есть еще какие-нибудь интересные варианты.

Ясно, что начальное состояние нужно уметь приготавливать достаточно быстро.

Годятся любые состояния из вычислительного базиса

А также те, которые получаются из них действием достаточно коротких схем.

Но это неинтересно, поскольку схему приготовления состояния можно включить в основную схему.

Есть ли в природе другие возможности?

Ответ на второй вопрос

Зависит от законов физики. Но вряд ли есть еще какие-нибудь интересные варианты.

Ясно, что начальное состояние нужно уметь приготавливать достаточно быстро.

Годятся любые состояния из вычислительного базиса

А также те, которые получаются из них действием достаточно коротких схем.

Но это неинтересно, поскольку схему приготовления состояния можно включить в основную схему.

Есть ли в природе другие возможности?

Ответ на второй вопрос

Зависит от законов физики. Но вряд ли есть еще какие-нибудь интересные варианты.
Ясно, что начальное состояние нужно уметь приготавливать достаточно быстро.
Годятся любые состояния из вычислительного базиса
А также те, которые получаются из них действием достаточно коротких схем.
Но это неинтересно, поскольку схему приготовления состояния можно включить в основную схему.
Есть ли в природе другие возможности?

Ответ на второй вопрос

Зависит от законов физики. Но вряд ли есть еще какие-нибудь интересные варианты.
Ясно, что начальное состояние нужно уметь приготавливать достаточно быстро.
Годятся любые состояния из вычислительного базиса
А также те, которые получаются из них действием достаточно коротких схем.
Но это неинтересно, поскольку схему приготовления состояния можно включить в основную схему.
Есть ли в природе другие возможности?

Ответ на второй вопрос

Зависит от законов физики. Но вряд ли есть еще какие-нибудь интересные варианты.
Ясно, что начальное состояние нужно уметь приготавливать достаточно быстро.
Годятся любые состояния из вычислительного базиса
А также те, которые получаются из них действием достаточно коротких схем.
Но это неинтересно, поскольку схему приготовления состояния можно включить в основную схему.
Есть ли в природе другие возможности?

Ответ на второй вопрос

Зависит от законов физики. Но вряд ли есть еще какие-нибудь интересные варианты.
Ясно, что начальное состояние нужно уметь приготавливать достаточно быстро.
Годятся любые состояния из вычислительного базиса
А также те, которые получаются из них действием достаточно коротких схем.
Но это неинтересно, поскольку схему приготовления состояния можно включить в основную схему.
Есть ли в природе другие возможности?

Ответы на третий вопрос

- Базис из операторов, действующих на одном кубите, неинтересен (моделируется классически).
- Базисы из операторов, действующих на k кубитах, эффективно эквивалентны для всех k.
- Более того, существует конечный базис из операторов, действующих не более чем на двух кубитах, который им всем эффективно эквивалентен (при разумных предположениях).

Ответы на третий вопрос

- Базис из операторов, действующих на одном кубите, неинтересен (моделируется классически).
- Базисы из операторов, действующих на k кубитах, эффективно эквивалентны для всех k.
- Более того, существует конечный базис из операторов, действующих не более чем на двух кубитах, который им всем эффективно эквивалентен (при разумных предположениях).

Ответы на третий вопрос

- Базис из операторов, действующих на одном кубите, неинтересен (моделируется классически).
- Базисы из операторов, действующих на k кубитах, эффективно эквивалентны для всех k.
- Более того, существует конечный базис из операторов, действующих не более чем на двух кубитах, который им всем эффективно эквивалентен (при разумных предположениях).

План

1. Трудоемкость квантового вычисления

2. Точная реализация унитарных операторов квантовыми схемами
   - Обратимые вычисления: мостик между классическими и квантовыми
   - Базис из операторов, действующих на одном кубите
   - Базис из операторов, действующих на двух кубитах

3. Об унитарных преобразованиях одного кубита

Определения

Схема $U_1[S_1], U_2[S_2], \ldots, U_\ell[S_\ell]$ реализует оператор

$$U = U_\ell[S_\ell] \ldots U_2[S_2] U_1[S_1]$$

(обратите внимание на порядок).

Схема $U_1[S_1], U_2[S_2], \ldots, U_\ell[S_\ell]$ реализует оператор U в расширенном смысле, если

$$U_\ell[S_\ell] \ldots U_2[S_2] U_1[S_1] \colon |\psi\rangle \otimes |0^N\rangle \mapsto U|\psi\rangle \otimes |0^N\rangle$$

для всех $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$.

Сложностью реализации оператора U (в расширенном смысле) в базисе $\mathcal{B}$ называется наименьший размер схемы в базисе $\mathcal{B}$, реализующей U (в расширенном смысле).

Сложность бесконечна, если реализации не существует.

Определения

Схема $U_1[S_1], U_2[S_2], \ldots, U_\ell[S_\ell]$ реализует оператор

$$U = U_\ell[S_\ell] \ldots U_2[S_2] U_1[S_1]$$

(обратите внимание на порядок).
Схема $U_1[S_1], U_2[S_2], \ldots, U_\ell[S_\ell]$ реализует оператор U в расширенном смысле, если

$$U_\ell[S_\ell] \ldots U_2[S_2] U_1[S_1] \colon |\psi\rangle \otimes |0^N\rangle \mapsto U|\psi\rangle \otimes |0^N\rangle$$

для всех $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$.
Сложностью реализации оператора U (в расширенном смысле) в базисе $\mathcal{B}$ называется наименьший размер схемы в базисе $\mathcal{B}$, реализующей U (в расширенном смысле).
Сложность бесконечна, если реализации не существует.

Определения

Схема $U_1[S_1], U_2[S_2], \ldots, U_\ell[S_\ell]$ реализует оператор

$$U = U_\ell[S_\ell] \ldots U_2[S_2] U_1[S_1]$$

(обратите внимание на порядок).
Схема $U_1[S_1], U_2[S_2], \ldots, U_\ell[S_\ell]$ реализует оператор U в расширенном смысле, если

$$U_\ell[S_\ell] \ldots U_2[S_2] U_1[S_1] \colon |\psi\rangle \otimes |0^N\rangle \mapsto U|\psi\rangle \otimes |0^N\rangle$$

для всех $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$.
Сложностью реализации оператора U (в расширенном смысле) в базисе $\mathcal{B}$ называется наименьший размер схемы в базисе $\mathcal{B}$, реализующей U (в расширенном смысле).
Сложность бесконечна, если реализации не существует.

О реализации в расширенном смысле

Основная цель — моделировать вероятностные распределения, порождаемые унитарными операторами.
Условие реализации в расширенном смысле гарантирует, что при измерении состояния $U_\ell[S_\ell] \dots U_2[S_2] U_1[S_1](|\psi\rangle \otimes |0^N\rangle)$ значения кубитов первого регистра распределены также, как при измерении состояния $U|\psi\rangle$.
Достаточны и более слабые условия, например,

$$U_\ell[S_\ell] \dots U_2[S_2] U_1[S_1] \colon |\psi\rangle \otimes |0^N\rangle \mapsto U|\psi\rangle \otimes V|\psi\rangle. \qquad (*)$$

Однако, это условие не слишком добавляет общности.

Задача

Докажите, что из выполнения $(*)$ следует $V|\psi\rangle = |\xi\rangle$ для любого ψ.

Дополнительным преимуществом условия реализации в расширенном смысле является сохранение этого свойства при композициях.

Перестановочные операторы

Определение

Унитарный оператор назовем перестановочным, если он сохраняет множество базисных векторов.

Перестановочный оператор действует классически. Если ограничить базис только перестановочными операторами, то предыдущие определения дают понятие обратимого вычисления.

Перестановочные операторы

Определение

Унитарный оператор назовем перестановочным, если он сохраняет множество базисных векторов.

Перестановочный оператор действует классически. Если ограничить базис только перестановочными операторами, то предыдущие определения дают понятие обратимого вычисления.

Необратимое вычисление: моделирование обратимым

- Если разрешить вместо перестановок базисных векторов любые отображения, получим обычные классические схемы.
- Базис из отображений на двух битах полный (проверьте, что достаточно использовать в базисе булевы функции от двух переменных).
- По классическому базису $\mathcal{B} = \{f_1, \ldots, f_m\}$ из функций $f_k : \{0,1\}^{d_k} \to \{0,1\}$ построим обратимый базис $\mathcal{B}_\oplus = \{f_k^\oplus, \text{c-NOT}\}$, где

$$f_k^\oplus : (x, y) \mapsto (x, y \oplus f_k(x)), \quad \text{c-NOT} : (x, y) \mapsto (x, x \oplus y).$$

Теорема (реализация в расширенном смысле)

Если отображение $F : \{0,1\}^n \to \{0,1\}^m$ реализуется булевой схемой размера L в базисе $\mathcal{B}$, то существует схема размера $O(L + m)$ в базисе $\mathcal{B}_\oplus$, которая реализует отображение

$$F^\oplus : (x, y, 0^L) \mapsto (x, y \oplus F(x), 0^L).$$

Необратимое вычисление: моделирование обратимым

- Если разрешить вместо перестановок базисных векторов любые отображения, получим обычные классические схемы.
- Базис из отображений на двух битах полный (проверьте, что достаточно использовать в базисе булевы функции от двух переменных).
- По классическому базису $\mathcal{B} = \{f_1, \ldots, f_m\}$ из функций $f_k : \{0,1\}^{d_k} \to \{0,1\}$ построим обратимый базис $\mathcal{B}_\oplus = \{f_k^\oplus, \text{c-NOT}\}$, где

$$f_k^\oplus : (x, y) \mapsto (x, y \oplus f_k(x)), \quad \text{c-NOT} : (x, y) \mapsto (x, x \oplus y).$$

Теорема (реализация в расширенном смысле)

Если отображение $F : \{0,1\}^n \to \{0,1\}^m$ реализуется булевой схемой размера L в базисе $\mathcal{B}$, то существует схема размера $O(L + m)$ в базисе $\mathcal{B}_\oplus$, которая реализует отображение

$$F^\oplus : (x, y, 0^L) \mapsto (x, y \oplus F(x), 0^L).$$

Необратимое вычисление: моделирование обратимым

- Если разрешить вместо перестановок базисных векторов любые отображения, получим обычные классические схемы.
- Базис из отображений на двух битах полный (проверьте, что достаточно использовать в базисе булевы функции от двух переменных).
- По классическому базису $\mathcal{B} = \{f_1, \ldots, f_m\}$ из функций $f_k : \{0,1\}^{d_k} \to \{0,1\}$ построим обратимый базис $\mathcal{B}_\oplus = \{f_k^\oplus, \text{c-NOT}\}$, где

$$f_k^\oplus : (x, y) \mapsto (x, y \oplus f_k(x)), \quad \text{c-NOT} : (x, y) \mapsto (x, x \oplus y).$$

Теорема (реализация в расширенном смысле)

Если отображение $F : \{0,1\}^n \to \{0,1\}^m$ реализуется булевой схемой размера L в базисе $\mathcal{B}$, то существует схема размера $O(L+m)$ в базисе $\mathcal{B}_\oplus$, которая реализует отображение

$$F^\oplus : (x, y, 0^L) \mapsto (x, y \oplus F(x), 0^L).$$

Необратимое вычисление: моделирование обратимым

- Если разрешить вместо перестановок базисных векторов любые отображения, получим обычные классические схемы.
- Базис из отображений на двух битах полный (проверьте, что достаточно использовать в базисе булевы функции от двух переменных).
- По классическому базису $\mathcal{B} = \{f_1, \ldots, f_m\}$ из функций $f_k : \{0,1\}^{d_k} \to \{0,1\}$ построим обратимый базис $\mathcal{B}_\oplus = \{f_k^\oplus, \text{c-NOT}\}$, где

$$f_k^\oplus : (x, y) \mapsto (x, y \oplus f_k(x)), \quad \text{c-NOT} : (x, y) \mapsto (x, x \oplus y).$$

Теорема (реализация в расширенном смысле)

Если отображение $F : \{0,1\}^n \to \{0,1\}^m$ реализуется булевой схемой размера L в базисе $\mathcal{B}$, то существует схема размера $O(L + m)$ в базисе $\mathcal{B}_\oplus$, которая реализует отображение

$$F^\oplus : (x, y, 0^L) \mapsto (x, y \oplus F(x), 0^L).$$

Набросок доказательства

- Представим схему как последовательность присваиваний

$$z_j := f_{k_j}(\text{предыдущие значения и входные переменные}).$$

- Сопоставим битам из третьего регистра вспомогательные переменные схемы z_j (результаты присваиваний).
- Заменим каждое присваивание на применение соответствующего $f_{k_j}^{\oplus}$ к соответствующим битам. Получим состояние

x	y	$z_1\ z_2 \cdots z_L$

- Скопируем, используя c-NOT, биты ответа во второй регистр.
- Откатим все шаги, кроме последнего (в порядке, обратном первоначальному).

Набросок доказательства

- Представим схему как последовательность присваиваний

$$z_j := f_{k_j}(\text{предыдущие значения и входные переменные}).$$

- Сопоставим битам из третьего регистра вспомогательные переменные схемы z_j (результаты присваиваний).
- Заменим каждое присваивание на применение соответствующего $f_{k_j}^{\oplus}$ к соответствующим битам. Получим состояние

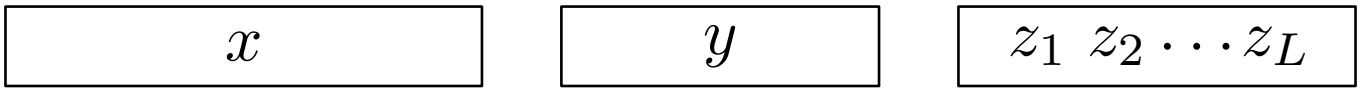
- Скопируем, используя c-NOT, биты ответа во второй регистр.
- Откатим все шаги, кроме последнего (в порядке, обратном первоначальному).

Набросок доказательства

- Представим схему как последовательность присваиваний

$$z_j := f_{k_j}(\text{предыдущие значения и входные переменные}).$$

- Сопоставим битам из третьего регистра вспомогательные переменные схемы z_j (результаты присваиваний).
- Заменим каждое присваивание на применение соответствующего $f_{k_j}^{\oplus}$ к соответствующим битам. Получим состояние



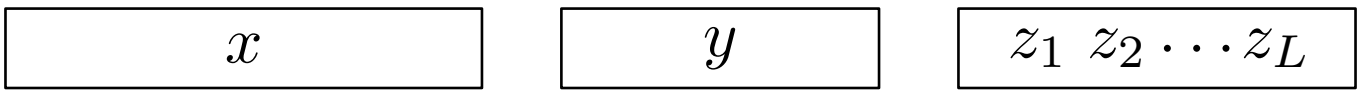
- Скопируем, используя c-NOT, биты ответа во второй регистр.
- Откатим все шаги, кроме последнего (в порядке, обратном первоначальному).

Набросок доказательства

- Представим схему как последовательность присваиваний

$$z_j := f_{k_j}(\text{предыдущие значения и входные переменные}).$$

- Сопоставим битам из третьего регистра вспомогательные переменные схемы z_j (результаты присваиваний).
- Заменим каждое присваивание на применение соответствующего $f_{k_j}^{\oplus}$ к соответствующим битам. Получим состояние



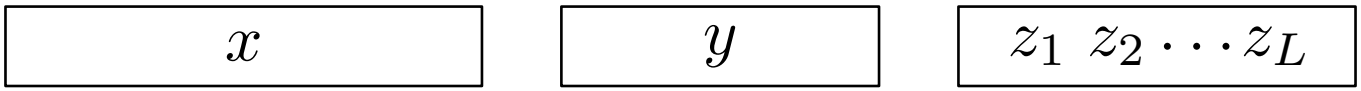
- Скопируем, используя c-NOT, биты ответа во второй регистр.
- Откатим все шаги, кроме последнего (в порядке, обратном первоначальному).

Набросок доказательства

- Представим схему как последовательность присваиваний

$$z_j := f_{k_j}(\text{предыдущие значения и входные переменные}).$$

- Сопоставим битам из третьего регистра вспомогательные переменные схемы z_j (результаты присваиваний).
- Заменим каждое присваивание на применение соответствующего $f_{k_j}^{\oplus}$ к соответствующим битам. Получим состояние



- Скопируем, используя c-NOT, биты ответа во второй регистр.
- Откатим все шаги, кроме последнего (в порядке, обратном первоначальному).

Откатка (uncompute)

В общем случае для откатки нужно применять обратные операторы.
Но $f^{\oplus}$ инволютивна:

$$(x, y) \overset{f^{\oplus}}{\longmapsto} (x, y \oplus f(x)) \overset{f^{\oplus}}{\longmapsto} (x, y \oplus f(x) \oplus f(x)) = (x, y)$$

Комментарии

Теорема

Любая булева функция реализуется схемами в базисе (конъюнкция, отрицание).

Следствие (NOT-базис)

Любое отображение $F\colon \{0,1\}^n \to \{0,1\}^m$ реализуется в расширенном смысле (с использованием вспомогательных битов, не меняющих своего значения после вычисления) в базисе

$$\sigma_x = \mathrm{NOT}\colon x \mapsto 1 \oplus x; \quad \text{c-NOT}\colon (x,y) \mapsto (x, x \oplus y);$$
$$\text{cc-NOT}\colon (x,y,z) \mapsto (x,y,z \oplus xy) \text{ (элемент Тоффоли).}$$

Задача

Докажите, что в базисе из перестановок двух битов не все отображения реализуемы в расширенном смысле.

Комментарии

Теорема

Любая булева функция реализуется схемами в базисе (конъюнкция, отрицание).

Следствие (NOT-базис)

Любое отображение $F\colon \{0,1\}^n \to \{0,1\}^m$ реализуется в расширенном смысле (с использованием вспомогательных битов, не меняющих своего значения после вычисления) в базисе

$$\sigma_x = \mathrm{NOT}\colon x \mapsto 1 \oplus x; \quad \text{c-NOT}\colon (x,y) \mapsto (x, x \oplus y);$$
$$\text{cc-NOT}\colon (x,y,z) \mapsto (x,y,z \oplus xy) \text{ (элемент Тоффоли).}$$

Задача

Докажите, что в базисе из перестановок двух битов не все отображения реализуемы в расширенном смысле.

Комментарии

Теорема

Любая булева функция реализуется схемами в базисе (конъюнкция, отрицание).

Следствие (NOT-базис)

Любое отображение $F\colon \{0,1\}^n \to \{0,1\}^m$ реализуется в расширенном смысле (с использованием вспомогательных битов, не меняющих своего значения после вычисления) в базисе

$$\sigma_x = \mathrm{NOT}\colon x \mapsto 1 \oplus x; \quad \text{c-NOT}\colon (x,y) \mapsto (x, x \oplus y);$$
$$\text{cc-NOT}\colon (x,y,z) \mapsto (x,y,z \oplus xy) \text{ (элемент Тоффоли).}$$

Задача

Докажите, что в базисе из перестановок двух битов не все отображения реализуемы в расширенном смысле.

Комментарии (продолжение)

Задача

Докажите, что без использования вспомогательных битов невозможно реализовать отображение

$$\mathrm{c}^{(n)}\text{-NOT}\colon (x_1, \ldots, x_n, y) \mapsto (x_1, \ldots, x_n, y \oplus x_1 x_2 \ldots x_n)$$

в базисе из перестановок n битов.

Базис из операторов, действующих на одном кубите

$$(U_1 \otimes I)(I \otimes U_2) = U_1 \otimes U_2 = (I \otimes U_2)(U_1 \otimes I)$$

Поэтому в таком базисе реализуются лишь операторы вида

$$U_1 \otimes U_2 \otimes \cdots \otimes U_n,$$

а исходы при наблюдении распределены независимо для каждого кубита.

Такое распределение моделируется классически.

Но!

Базис из операторов, действующих на одном кубите

$$(U_1 \otimes I)(I \otimes U_2) = U_1 \otimes U_2 = (I \otimes U_2)(U_1 \otimes I)$$

Поэтому в таком базисе реализуются лишь операторы вида

$$U_1 \otimes U_2 \otimes \cdots \otimes U_n,$$

а исходы при наблюдении распределены независимо для каждого кубита.

Такое распределение моделируется классически.

Но!

Базис из операторов, действующих на одном кубите

$$(U_1 \otimes I)(I \otimes U_2) = U_1 \otimes U_2 = (I \otimes U_2)(U_1 \otimes I)$$

Поэтому в таком базисе реализуются лишь операторы вида

$$U_1 \otimes U_2 \otimes \cdots \otimes U_n,$$

а исходы при наблюдении распределены независимо для каждого кубита.

Такое распределение моделируется классически.

Но!

Использование произвольных распределений на $\{0, 1\}$ делает некоторые невычислимые функции вычислимыми (пусть биты $p(1)$ — вероятности 1 — образуют невычислимую последовательность).

Трудность общая для вероятностных и квантовых вычислений.

Базис из операторов, действующих на одном кубите

$$(U_1 \otimes I)(I \otimes U_2) = U_1 \otimes U_2 = (I \otimes U_2)(U_1 \otimes I)$$

Поэтому в таком базисе реализуются лишь операторы вида

$$U_1 \otimes U_2 \otimes \cdots \otimes U_n,$$

а исходы при наблюдении распределены независимо для каждого кубита.

Такое распределение моделируется классически.

Но!

В случае вероятностных вычислений стандартный выход состоит в использовании равномерного распределения на некотором числе кубитов.

Базис из операторов, действующих на одном кубите

$$(U_1 \otimes I)(I \otimes U_2) = U_1 \otimes U_2 = (I \otimes U_2)(U_1 \otimes I)$$

Поэтому в таком базисе реализуются лишь операторы вида

$$U_1 \otimes U_2 \otimes \cdots \otimes U_n,$$

а исходы при наблюдении распределены независимо для каждого кубита.

Такое распределение моделируется классически.

Но!

В квантовом случае трудность преодолевается, если перейти к конечным базисам и приближенной реализации унитарных операторов.

Операторы, действующие на двух кубитах

Теорема об универсальности двухкубитовых операторов

Любой унитарный оператор точно реализуется в расширенном смысле в базисе $\mathcal{B}_2$, состоящем из всех операторов, действующих на двух кубитах.

План доказательства

1. Любой унитарный оператор — композиция подкрученных транспозиций.
2. Любая подкрученная транспозиция реализуется в базисе, который содержит все операторы, действующие на одном кубите, и NOT-базис (NOT, c-NOT, cc-NOT).
3. Элемент Тоффоли cc-NOT реализуется в базисе $\mathcal{B}_2$.

Операторы, действующие на двух кубитах

Теорема об универсальности двухкубитовых операторов

Любой унитарный оператор точно реализуется в расширенном смысле в базисе $\mathcal{B}_2$, состоящем из всех операторов, действующих на двух кубитах.

План доказательства

1. Любой унитарный оператор — композиция подкрученных транспозиций.
2. Любая подкрученная транспозиция реализуется в базисе, который содержит все операторы, действующие на одном кубите, и NOT-базис (NOT, c-NOT, cc-NOT).
3. Элемент Тоффоли cc-NOT реализуется в базисе $\mathcal{B}_2$.

Операторы, действующие на двух кубитах

Теорема об универсальности двухкубитовых операторов

Любой унитарный оператор точно реализуется в расширенном смысле в базисе $\mathcal{B}_2$, состоящем из всех операторов, действующих на двух кубитах.

План доказательства

1. Любой унитарный оператор — композиция подкрученных транспозиций.
2. Любая подкрученная транспозиция реализуется в базисе, который содержит все операторы, действующие на одном кубите, и NOT-базис (NOT, c-NOT, cc-NOT).
3. Элемент Тоффоли cc-NOT реализуется в базисе $\mathcal{B}_2$.

Операторы, действующие на двух кубитах

Теорема об универсальности двухкубитовых операторов

Любой унитарный оператор точно реализуется в расширенном смысле в базисе $\mathcal{B}_2$, состоящем из всех операторов, действующих на двух кубитах.

План доказательства

1. Любой унитарный оператор — композиция подкрученных транспозиций.
2. Любая подкрученная транспозиция реализуется в базисе, который содержит все операторы, действующие на одном кубите, и NOT-базис (NOT, c-NOT, cc-NOT).
3. Элемент Тоффоли cc-NOT реализуется в базисе $\mathcal{B}_2$.

Подкрученные транспозиции

Определение

Назовем подкрученной транспозицией унитарный оператор $U\colon \mathbb{C}^M \to \mathbb{C}^M$, матрица которого имеет вид:

$$\begin{pmatrix}
1 & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\
\vdots & \ddots & 0 & \cdots & \cdots & \cdots & 0 \\
0 & \cdots & a & 0 & \cdots & b & \cdots & 0 \\
0 & \cdots & 0 & 1 & \cdots & 0 & \cdots & 0 \\
\cdots & \cdots & \cdots & \ddots & \cdots & \cdots & \cdots & \cdots \\
0 & \cdots & 0 & 0 & \cdots & 1 & \cdots & 0 \\
0 & \cdots & c & 0 & \cdots & d & \cdots & 0 \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \ddots & 0 \\
0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 1
\end{pmatrix}.$$

Доказательство теоремы об универсальности: шаг 1

Лемма 1

Любой унитарный оператор $U\colon \mathbb{C}^M \to \mathbb{C}^M$, где $M \geqslant 2$, является композицией подкрученных транспозиций.

Доказываем индукцией по порядку матрицы аналогично тому, как доказывается, что транспозиции порождают все перестановки.

Наблюдение

Для любых c_1, c_2 существует такая унитарная матрица V размера 2×2, что

$$V \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} \sqrt{|c_1|^2 + |c_2|^2} \\ 0 \end{pmatrix}.$$

Упражнение

Докажите справедливость этого наблюдения.

Доказательство теоремы об универсальности: шаг 1

Лемма 1

Любой унитарный оператор $U\colon \mathbb{C}^M \to \mathbb{C}^M$, где $M \geqslant 2$, является композицией подкрученных транспозиций.

Доказываем индукцией по порядку матрицы аналогично тому, как доказывается, что транспозиции порождают все перестановки.

Наблюдение

Для любых c_1, c_2 существует такая унитарная матрица V размера 2×2, что

$$V \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} \sqrt{|c_1|^2 + |c_2|^2} \\ 0 \end{pmatrix}.$$

Упражнение

Докажите справедливость этого наблюдения.

Доказательство теоремы об универсальности: шаг 1

Лемма 1

Любой унитарный оператор $U\colon \mathbb{C}^M \to \mathbb{C}^M$, где $M \geqslant 2$, является композицией подкрученных транспозиций.

Доказываем индукцией по порядку матрицы аналогично тому, как доказывается, что транспозиции порождают все перестановки.

Наблюдение

Для любых c_1, c_2 существует такая унитарная матрица V размера 2×2, что

$$V \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} \sqrt{|c_1|^2 + |c_2|^2} \\ 0 \end{pmatrix}.$$

Упражнение

Докажите справедливость этого наблюдения.

Доказательство теоремы об универсальности: шаг 1

Лемма 1

Любой унитарный оператор $U\colon \mathbb{C}^M \to \mathbb{C}^M$, где $M \geqslant 2$, является композицией подкрученных транспозиций.

Доказываем индукцией по порядку матрицы аналогично тому, как доказывается, что транспозиции порождают все перестановки.

Наблюдение

Для любых c_1, c_2 существует такая унитарная матрица V размера 2×2, что

$$V \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} \sqrt{|c_1|^2 + |c_2|^2} \\ 0 \end{pmatrix}.$$

Упражнение

Докажите справедливость этого наблюдения.

Доказательство теоремы об универсальности: шаг 1

- Для любого $|\xi\rangle \in \mathbb{C}^M$ существует последовательность $V^{(1)}, \ldots, V^{(M-1)}$ такая, что
$$V^{(1)} \cdot \ldots \cdot V^{(M-1)} |\xi\rangle = |1\rangle,$$
где $V^{(s)}$ — подкрученная транспозиция, действующая на $\mathbb{C}(|s\rangle, |s+1\rangle)$.
- Поэтому умножениями на подкрученные транспозиции можно перевести первый столбец любой унитарной матрицы в единичный.
- Из условия унитарности следует, что и первая строка станет единичной:
$$V^{(1)} \cdot \ldots \cdot V^{(M-1)} U = \begin{pmatrix} 1 & 0^{M-1} \\ 0^{M-1} & U_1 \end{pmatrix}$$
- Теперь применим индуктивное предположение к U_1.

Доказательство теоремы об универсальности: шаг 1

- Для любого $|\xi\rangle \in \mathbb{C}^M$ существует последовательность $V^{(1)}, \ldots, V^{(M-1)}$ такая, что
$$V^{(1)} \cdot \ldots \cdot V^{(M-1)} |\xi\rangle = |1\rangle,$$
где $V^{(s)}$ — подкрученная транспозиция, действующая на $\mathbb{C}(|s\rangle, |s+1\rangle)$.
- Поэтому умножениями на подкрученные транспозиции можно перевести первый столбец любой унитарной матрицы в единичный.
- Из условия унитарности следует, что и первая строка станет единичной:
$$V^{(1)} \cdot \ldots \cdot V^{(M-1)} U = \begin{pmatrix} 1 & 0^{M-1} \\ 0^{M-1} & U_1 \end{pmatrix}$$
- Теперь применим индуктивное предположение к U_1.

Доказательство теоремы об универсальности: шаг 1

- Для любого $|\xi\rangle \in \mathbb{C}^M$ существует последовательность $V^{(1)}, \ldots, V^{(M-1)}$ такая, что

$$V^{(1)} \cdot \ldots \cdot V^{(M-1)} |\xi\rangle = |1\rangle,$$

где $V^{(s)}$ — подкрученная транспозиция, действующая на $\mathbb{C}(|s\rangle, |s+1\rangle)$.

- Поэтому умножениями на подкрученные транспозиции можно перевести первый столбец любой унитарной матрицы в единичный.
- Из условия унитарности следует, что и первая строка станет единичной:

$$V^{(1)} \cdot \ldots \cdot V^{(M-1)} U = \begin{pmatrix} 1 & 0^{M-1} \\ 0^{M-1} & U_1 \end{pmatrix}$$

- Теперь применим индуктивное предположение к U_1.

Доказательство теоремы об универсальности: шаг 1

- Для любого $|\xi\rangle \in \mathbb{C}^M$ существует последовательность $V^{(1)}, \ldots, V^{(M-1)}$ такая, что
$$V^{(1)} \cdot \ldots \cdot V^{(M-1)} |\xi\rangle = |1\rangle,$$
где $V^{(s)}$ — подкрученная транспозиция, действующая на $\mathbb{C}(|s\rangle, |s+1\rangle)$.
- Поэтому умножениями на подкрученные транспозиции можно перевести первый столбец любой унитарной матрицы в единичный.
- Из условия унитарности следует, что и первая строка станет единичной:
$$V^{(1)} \cdot \ldots \cdot V^{(M-1)} U = \begin{pmatrix} 1 & 0^{M-1} \\ 0^{M-1} & U_1 \end{pmatrix}$$
- Теперь применим индуктивное предположение к U_1.

Несколько управляющих кубитов

Определение

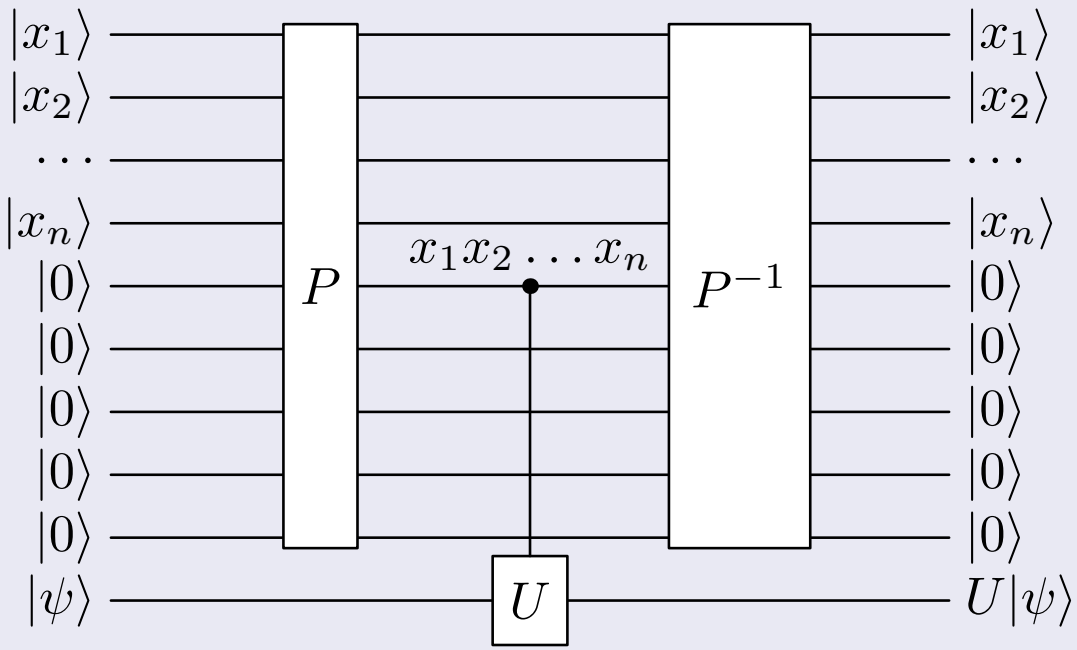
$$\mathrm{c}^{(n)}\text{-}U\colon |x_1,\ldots,x_n\rangle\otimes|\psi\rangle = \begin{cases} |x_1,\ldots,x_n\rangle\otimes U|\psi\rangle, & \text{если } x_1x_2\ldots x_n = 1;\\ |x_1,\ldots,x_n\rangle\otimes|\psi\rangle, & \text{иначе.}\end{cases}$$

Несколько управляющих кубитов

Определение

$$\text{c}^{(n)}\text{-}U\colon |x_1,\ldots,x_n\rangle\otimes|\psi\rangle = \begin{cases} |x_1,\ldots,x_n\rangle\otimes U|\psi\rangle, & \text{если } x_1x_2\ldots x_n = 1;\\ |x_1,\ldots,x_n\rangle\otimes|\psi\rangle, & \text{иначе.}\end{cases}$$

Реализация $\text{c}^{(n)}\text{-}U$ в базисе $\mathcal{B}_2\cup\{\text{NOT},\text{c-NOT},\text{cc-NOT}\}$



Доказательство теоремы об универсальности: шаг 2

- Операторы $\mathrm{c}^{(n)}$-U являются подкрученными транспозициями, действующими на пространстве $\mathbb{C}(|1\ldots10\rangle, |1\ldots11\rangle)$.
- Любая другая подкрученная транспозиция T получается из $\mathrm{c}^{(n)}$-U сопряжением перестановочным оператором:

$$T = P\mathrm{c}^{(n)}\text{-}UP^{-1}, \quad P\colon |1\ldots10\rangle \mapsto |x\rangle, \quad P\colon |1\ldots11\rangle \mapsto |y\rangle.$$

- Оператор P реализуется в NOT-базисе в расширенном смысле.

Доказательство теоремы об универсальности: шаг 2

- Операторы $\mathrm{c}^{(n)}$-U являются подкрученными транспозициями, действующими на пространстве $\mathbb{C}(|1\ldots10\rangle, |1\ldots11\rangle)$.
- Любая другая подкрученная транспозиция T получается из $\mathrm{c}^{(n)}$-U сопряжением перестановочным оператором:

$$T = P\mathrm{c}^{(n)}\text{-}UP^{-1}, \quad P\colon |1\ldots10\rangle \mapsto |x\rangle, \quad P\colon |1\ldots11\rangle \mapsto |y\rangle.$$

- Оператор P реализуется в NOT-базисе в расширенном смысле.

Доказательство теоремы об универсальности: шаг 2

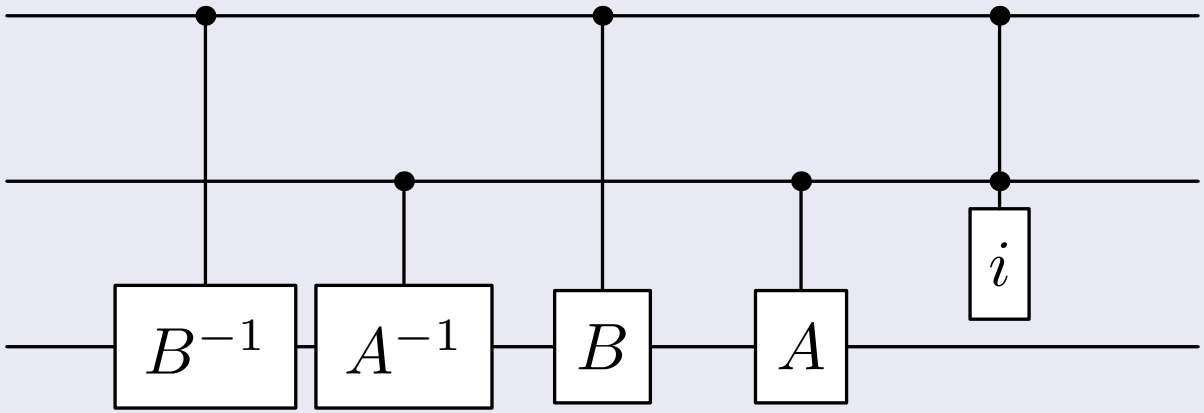
- Операторы $\mathrm{c}^{(n)}$-U являются подкрученными транспозициями, действующими на пространстве $\mathbb{C}(|1\ldots10\rangle, |1\ldots11\rangle)$.
- Любая другая подкрученная транспозиция T получается из $\mathrm{c}^{(n)}$-U сопряжением перестановочным оператором:

$$T = P\mathrm{c}^{(n)}\text{-}UP^{-1}, \quad P\colon |1\ldots10\rangle \mapsto |x\rangle, \quad P\colon |1\ldots11\rangle \mapsto |y\rangle.$$

- Оператор P реализуется в NOT-базисе в расширенном смысле.

Доказательство теоремы об универсальности: шаг 3

Элемент Тоффоли c$^{(2)}$-σ_x в базисе $\mathcal{B}_2$



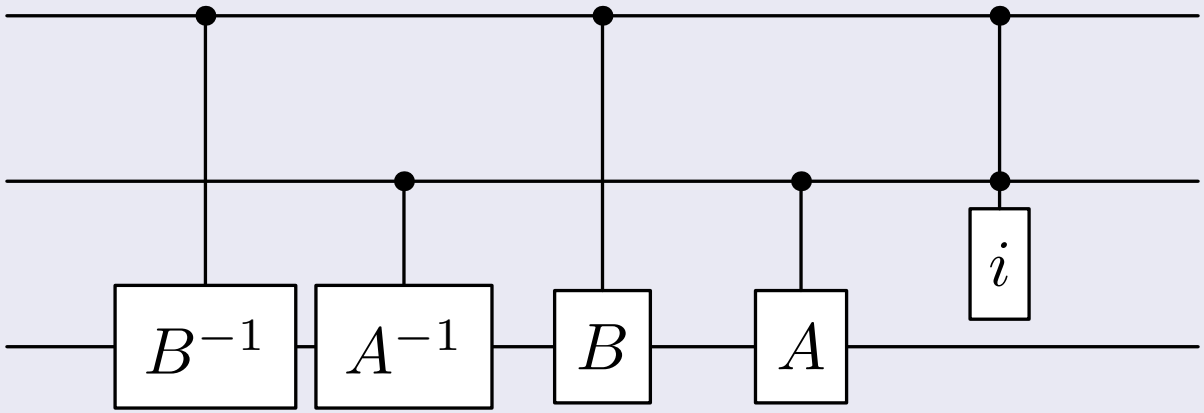
где $A = \frac{1}{\sqrt{2}} \begin{pmatrix} -i & -1 \\ 1 & i \end{pmatrix}$; $B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$

Упражнение

Проверьте, что $A^2 = -I$, $B^2 = -I$, $ABA^{-1}B^{-1} = -i\sigma_x$.

Доказательство теоремы об универсальности: шаг 3

Элемент Тоффоли c$^{(2)}$-σ_x в базисе $\mathcal{B}_2$



где $A = \frac{1}{\sqrt{2}} \begin{pmatrix} -i & -1 \\ 1 & i \end{pmatrix}$; $B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$

Упражнение

Проверьте, что $A^2 = -I$, $B^2 = -I$, $ABA^{-1}B^{-1} = -i\sigma_x$.

Об избыточности базиса $\mathcal{B}_2$

Из доказательства теоремы видно, что любой унитарный оператор выражается в базисе, который содержит все однокубитовые операторы и все операторы вида c-U, где U — однокубитовый.

Оказывается, из второй группы операторов достаточно оставить только c-NOT $=$ c-σ_x.

Об избыточности базиса $\mathcal{B}_2$

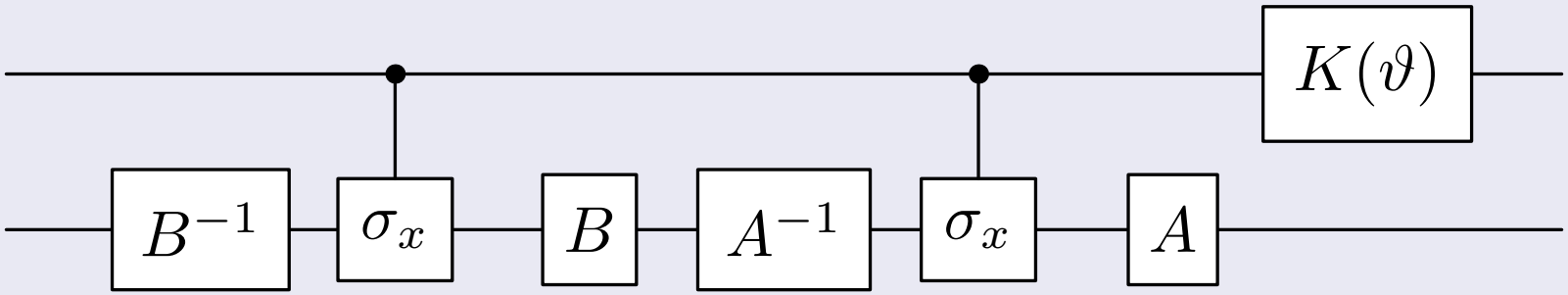
Из доказательства теоремы видно, что любой унитарный оператор выражается в базисе, который содержит все однокубитовые операторы и все операторы вида c-U, где U — однокубитовый.
Оказывается, из второй группы операторов достаточно оставить только c-NOT $=$ c-σ_x.

Об избыточности базиса $\mathcal{B}_2$

Из доказательства теоремы видно, что любой унитарный оператор выражается в базисе, который содержит все однокубитовые операторы и все операторы вида c-U, где U — однокубитовый.
Оказывается, из второй группы операторов достаточно оставить только c-NOT $=$ c-σ_x.

Теорема 2

Любой оператор вида c-U представляется в виде



$$\text{где } K(\vartheta) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\vartheta} \end{pmatrix}$$

План

1. Трудоемкость квантового вычисления

2. Точная реализация унитарных операторов квантовыми схемами
   - Обратимые вычисления: мостик между классическими и квантовыми
   - Базис из операторов, действующих на одном кубите
   - Базис из операторов, действующих на двух кубитах

3. Об унитарных преобразованиях одного кубита

Еще раз о сфере Блоха

Матрицы Паули:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \ \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Утверждение

Если $|\psi\rangle = a|0\rangle + b|1\rangle$ — состояние кубита, то

$$|\psi\rangle\langle\psi| = \frac{1}{2}(I + x\sigma_x + y\sigma_y + z\sigma_z), \quad x^2 + y^2 + z^2 = 1, \ x, y, z \in \mathbb{R}.$$

Без ограничения общности $a \in [0; 1]$ (общий фазовый множитель ненаблюдаем).

Тогда $a = \cos(\theta/2), \ b = e^{i\varphi}\sin(\theta/2), \quad \theta \in [0; \pi], \quad \varphi \in [0; 2\pi)$;

$$x = \cos\varphi \sin\theta; \quad y = \sin\varphi \sin\theta; \quad z = \cos\theta$$

(сферические координаты).

Еще раз о сфере Блоха

Матрицы Паули:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \ \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Утверждение

Если $|\psi\rangle = a|0\rangle + b|1\rangle$ — состояние кубита, то

$$|\psi\rangle\langle\psi| = \frac{1}{2}(I + x\sigma_x + y\sigma_y + z\sigma_z), \quad x^2 + y^2 + z^2 = 1, \ x, y, z \in \mathbb{R}.$$

Без ограничения общности $a \in [0; 1]$ (общий фазовый множитель ненаблюдаем).
Тогда $a = \cos(\theta/2), \ b = e^{i\varphi}\sin(\theta/2), \quad \theta \in [0; \pi]; \quad \varphi \in [0; 2\pi);$

$$x = \cos\varphi \sin\theta; \quad y = \sin\varphi \sin\theta; \quad z = \cos\theta$$

(сферические координаты).

Еще раз о сфере Блоха

Матрицы Паули:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \ \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Утверждение

Если $|\psi\rangle = a|0\rangle + b|1\rangle$ — состояние кубита, то

$$|\psi\rangle\langle\psi| = \frac{1}{2}(I + x\sigma_x + y\sigma_y + z\sigma_z), \quad x^2 + y^2 + z^2 = 1, \ x, y, z \in \mathbb{R}.$$

Без ограничения общности $a \in [0; 1]$ (общий фазовый множитель ненаблюдаем).
Тогда $a = \cos(\theta/2)$, $b = e^{i\varphi}\sin(\theta/2)$, $\theta \in [0; \pi]$; $\varphi \in [0; 2\pi)$;

$$x = \cos\varphi \sin\theta; \quad y = \sin\varphi \sin\theta; \quad z = \cos\theta$$

(сферические координаты).

Проверка утверждения

$$|\psi\rangle\langle\psi| = \begin{pmatrix} \cos(\theta/2) \\ e^{i\varphi}\sin(\theta/2) \end{pmatrix} \begin{pmatrix} \cos(\theta/2) & e^{-i\varphi}\sin(\theta/2) \end{pmatrix} =$$

$$= \begin{pmatrix} \cos^2(\theta/2) & e^{-i\varphi}\cos(\theta/2)\sin(\theta/2) \\ e^{i\varphi}\cos(\theta/2)\sin(\theta/2) & \sin^2(\theta/2) \end{pmatrix} =$$

$$= \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \frac{1}{2}\cos\theta \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} +$$

$$+ \frac{1}{2}\cos\varphi\sin\theta \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + \frac{1}{2}\sin\varphi\sin\theta \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} =$$

$$= \frac{1}{2}(I + x\sigma_x + y\sigma_y + z\sigma_z)$$

Проверка утверждения

$$|\psi\rangle\langle\psi| = \begin{pmatrix} \cos(\theta/2) \\ e^{i\varphi}\sin(\theta/2) \end{pmatrix} \begin{pmatrix} \cos(\theta/2) & e^{-i\varphi}\sin(\theta/2) \end{pmatrix} =$$

$$= \begin{pmatrix} \cos^2(\theta/2) & e^{-i\varphi}\cos(\theta/2)\sin(\theta/2) \\ e^{i\varphi}\cos(\theta/2)\sin(\theta/2) & \sin^2(\theta/2) \end{pmatrix} =$$

$$= \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \frac{1}{2}\cos\theta \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} +$$

$$+ \frac{1}{2}\cos\varphi\sin\theta \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + \frac{1}{2}\sin\varphi\sin\theta \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} =$$

$$= \frac{1}{2}(I + x\sigma_x + y\sigma_y + z\sigma_z)$$

Проверка утверждения

$$|\psi\rangle\langle\psi| = \begin{pmatrix} \cos(\theta/2) \\ e^{i\varphi}\sin(\theta/2) \end{pmatrix} \begin{pmatrix} \cos(\theta/2) & e^{-i\varphi}\sin(\theta/2) \end{pmatrix} =$$

$$= \begin{pmatrix} \cos^2(\theta/2) & e^{-i\varphi}\cos(\theta/2)\sin(\theta/2) \\ e^{i\varphi}\cos(\theta/2)\sin(\theta/2) & \sin^2(\theta/2) \end{pmatrix} =$$

$$= \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \frac{1}{2}\cos\theta \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} +$$

$$+ \frac{1}{2}\cos\varphi\sin\theta \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + \frac{1}{2}\sin\varphi\sin\theta \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} =$$

$$= \frac{1}{2}(I + x\sigma_x + y\sigma_y + z\sigma_z)$$

Проверка утверждения

$$|\psi\rangle\langle\psi| = \begin{pmatrix} \cos(\theta/2) \\ e^{i\varphi}\sin(\theta/2) \end{pmatrix} \begin{pmatrix} \cos(\theta/2) & e^{-i\varphi}\sin(\theta/2) \end{pmatrix} =$$

$$= \begin{pmatrix} \cos^2(\theta/2) & e^{-i\varphi}\cos(\theta/2)\sin(\theta/2) \\ e^{i\varphi}\cos(\theta/2)\sin(\theta/2) & \sin^2(\theta/2) \end{pmatrix} =$$

$$= \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \frac{1}{2}\cos\theta \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} +$$

$$+ \frac{1}{2}\cos\varphi\sin\theta \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + \frac{1}{2}\sin\varphi\sin\theta \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} =$$

$$= \frac{1}{2}(I + x\sigma_x + y\sigma_y + z\sigma_z)$$

Проверка утверждения

$$|\psi\rangle\langle\psi| = \begin{pmatrix} \cos(\theta/2) \\ e^{i\varphi}\sin(\theta/2) \end{pmatrix} \begin{pmatrix} \cos(\theta/2) & e^{-i\varphi}\sin(\theta/2) \end{pmatrix} =$$

$$= \begin{pmatrix} \cos^2(\theta/2) & e^{-i\varphi}\cos(\theta/2)\sin(\theta/2) \\ e^{i\varphi}\cos(\theta/2)\sin(\theta/2) & \sin^2(\theta/2) \end{pmatrix} =$$

$$= \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \frac{1}{2}\cos\theta \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} +$$

$$+ \frac{1}{2}\cos\varphi\sin\theta \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + \frac{1}{2}\sin\varphi\sin\theta \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} =$$

$$= \frac{1}{2}(I + x\sigma_x + y\sigma_y + z\sigma_z)$$

Скалярное произведение и эрмитово произведение

- Пусть $|\psi\rangle$ на сфере Блоха попадает в (x', y', z'), $|\xi\rangle$ — в (x'', y'', z'').
- Матрицы Паули (включая единичную) ортогональны относительно произведения Фробениуса: $\frac{1}{2}\operatorname{Tr}(\sigma_\alpha \sigma_\beta) = \delta_{\alpha\beta}$ (упражнение).
- Поэтому

$$|\langle\psi|\xi\rangle|^2 = \operatorname{Tr}(|\psi\rangle\langle\psi|\,|\xi\rangle\langle\xi|) = \frac{1}{2}(1 + x'x'' + y'y'' + z'z'').$$

- Следствие 1: пара ортогональных состояний попадает на сфере Блоха в диаметрально противоположные точки.
- Следствие 2: унитарное преобразование действует на сфере Блоха по правилу $U\colon |\psi\rangle\langle\psi| \mapsto U|\psi\rangle\langle\psi|U^\dagger$ и это действие — движение трехмерного пространства, сохраняющее центр сферы.

Скалярное произведение и эрмитово произведение

- Пусть $|\psi\rangle$ на сфере Блоха попадает в (x', y', z'), $|\xi\rangle$ — в (x'', y'', z'').
- Матрицы Паули (включая единичную) ортогональны относительно произведения Фробениуса: $\frac{1}{2}\operatorname{Tr}(\sigma_\alpha\sigma_\beta) = \delta_{\alpha\beta}$ (упражнение).
- Поэтому

$$|\langle\psi|\xi\rangle|^2 = \operatorname{Tr}(|\psi\rangle\langle\psi|\,|\xi\rangle\langle\xi|) = \frac{1}{2}(1 + x'x'' + y'y'' + z'z'').$$

- Следствие 1: пара ортогональных состояний попадает на сфере Блоха в диаметрально противоположные точки.
- Следствие 2: унитарное преобразование действует на сфере Блоха по правилу $U\colon |\psi\rangle\langle\psi| \mapsto U|\psi\rangle\langle\psi|U^\dagger$ и это действие — движение трехмерного пространства, сохраняющее центр сферы.

Скалярное произведение и эрмитово произведение

- Пусть $|\psi\rangle$ на сфере Блоха попадает в (x', y', z'), $|\xi\rangle$ — в (x'', y'', z'').
- Матрицы Паули (включая единичную) ортогональны относительно произведения Фробениуса: $\frac{1}{2}\operatorname{Tr}(\sigma_\alpha\sigma_\beta) = \delta_{\alpha\beta}$ (упражнение).
- Поэтому

$$|\langle\psi|\xi\rangle|^2 = \operatorname{Tr}(|\psi\rangle\langle\psi|\ |\xi\rangle\langle\xi|) = \frac{1}{2}(1 + x'x'' + y'y'' + z'z'').$$

- Следствие 1: пара ортогональных состояний попадает на сфере Блоха в диаметрально противоположные точки.
- Следствие 2: унитарное преобразование действует на сфере Блоха по правилу U: $|\psi\rangle\langle\psi| \mapsto U|\psi\rangle\langle\psi|U^\dagger$ и это действие — движение трехмерного пространства, сохраняющее центр сферы.

Скалярное произведение и эрмитово произведение

- Пусть $|\psi\rangle$ на сфере Блоха попадает в (x', y', z'), $|\xi\rangle$ — в (x'', y'', z'').
- Матрицы Паули (включая единичную) ортогональны относительно произведения Фробениуса: $\frac{1}{2}\operatorname{Tr}(\sigma_\alpha\sigma_\beta) = \delta_{\alpha\beta}$ (упражнение).
- Поэтому

$$|\langle\psi|\xi\rangle|^2 = \operatorname{Tr}(|\psi\rangle\langle\psi|\ |\xi\rangle\langle\xi|) = \frac{1}{2}(1 + x'x'' + y'y'' + z'z'').$$

- Следствие 1: пара ортогональных состояний попадает на сфере Блоха в диаметрально противоположные точки.
- Следствие 2: унитарное преобразование действует на сфере Блоха по правилу $U\colon |\psi\rangle\langle\psi| \mapsto U|\psi\rangle\langle\psi|U^\dagger$ и это действие — движение трехмерного пространства, сохраняющее центр сферы.

Скалярное произведение и эрмитово произведение

- Пусть $|\psi\rangle$ на сфере Блоха попадает в (x', y', z'), $|\xi\rangle$ — в (x'', y'', z'').
- Матрицы Паули (включая единичную) ортогональны относительно произведения Фробениуса: $\frac{1}{2}\operatorname{Tr}(\sigma_\alpha\sigma_\beta) = \delta_{\alpha\beta}$ (упражнение).
- Поэтому

$$|\langle\psi|\xi\rangle|^2 = \operatorname{Tr}(|\psi\rangle\langle\psi|\ |\xi\rangle\langle\xi|) = \frac{1}{2}(1 + x'x'' + y'y'' + z'z'').$$

- Следствие 1: пара ортогональных состояний попадает на сфере Блоха в диаметрально противоположные точки.
- Следствие 2: унитарное преобразование действует на сфере Блоха по правилу U: $|\psi\rangle\langle\psi| \mapsto U|\psi\rangle\langle\psi|U^\dagger$ и это действие — движение трехмерного пространства, сохраняющее центр сферы.

Действие унитарного оператора на сфере Блоха: поворот

- Скалярные операторы $|\psi\rangle \mapsto e^{i\alpha}|\psi\rangle$ действуют на сфере Блоха тождественно.
- Верно и обратное: если унитарный оператор U действует на сфере Блоха тождественно, то каждый вектор — собственный, а оператор — скалярный.
- Любой унитарный оператор имеет ортонормированный базис из собственных векторов. Соответствующая пара точек на сфере Блоха не меняется при действии оператора.
- Нетривиальное действие унитарного оператора на сфере Блоха — движение, у которого есть ровно одна пара неподвижных точек на сфере Блоха.
- Это поворот.

Действие унитарного оператора на сфере Блоха: поворот

- Скалярные операторы $|\psi\rangle \mapsto e^{i\alpha}|\psi\rangle$ действуют на сфере Блоха тождественно.
- Верно и обратное: если унитарный оператор U действует на сфере Блоха тождественно, то каждый вектор — собственный, а оператор — скалярный.
- Любой унитарный оператор имеет ортонормированный базис из собственных векторов. Соответствующая пара точек на сфере Блоха не меняется при действии оператора.
- Нетривиальное действие унитарного оператора на сфере Блоха — движение, у которого есть ровно одна пара неподвижных точек на сфере Блоха.
- Это поворот.

Действие унитарного оператора на сфере Блоха: поворот

- Скалярные операторы $|\psi\rangle \mapsto e^{i\alpha}|\psi\rangle$ действуют на сфере Блоха тождественно.
- Верно и обратное: если унитарный оператор U действует на сфере Блоха тождественно, то каждый вектор — собственный, а оператор — скалярный.
- Любой унитарный оператор имеет ортонормированный базис из собственных векторов. Соответствующая пара точек на сфере Блоха не меняется при действии оператора.
- Нетривиальное действие унитарного оператора на сфере Блоха — движение, у которого есть ровно одна пара неподвижных точек на сфере Блоха.
- Это поворот.

Действие унитарного оператора на сфере Блоха: поворот

- Скалярные операторы $|\psi\rangle \mapsto e^{i\alpha}|\psi\rangle$ действуют на сфере Блоха тождественно.
- Верно и обратное: если унитарный оператор U действует на сфере Блоха тождественно, то каждый вектор — собственный, а оператор — скалярный.
- Любой унитарный оператор имеет ортонормированный базис из собственных векторов. Соответствующая пара точек на сфере Блоха не меняется при действии оператора.
- Нетривиальное действие унитарного оператора на сфере Блоха — движение, у которого есть ровно одна пара неподвижных точек на сфере Блоха.
- Это поворот.

Действие унитарного оператора на сфере Блоха: поворот

- Скалярные операторы $|\psi\rangle \mapsto e^{i\alpha}|\psi\rangle$ действуют на сфере Блоха тождественно.
- Верно и обратное: если унитарный оператор U действует на сфере Блоха тождественно, то каждый вектор — собственный, а оператор — скалярный.
- Любой унитарный оператор имеет ортонормированный базис из собственных векторов. Соответствующая пара точек на сфере Блоха не меняется при действии оператора.
- Нетривиальное действие унитарного оператора на сфере Блоха — движение, у которого есть ровно одна пара неподвижных точек на сфере Блоха.
- Это поворот.

О матрицах Паули

Поскольку $\sigma_x^2 = \sigma_y^2 = \sigma_z^2 = I$, матрицы Паули — повороты на π.

Так как

$$\sigma_x \frac{1}{2}(I + \sigma_x)\sigma_x^\dagger = \frac{1}{2}(I + \sigma_x),$$

$$\sigma_y \frac{1}{2}(I + \sigma_y)\sigma_y^\dagger = \frac{1}{2}(I + \sigma_y),$$

$$\sigma_z \frac{1}{2}(I + \sigma_z)\sigma_z^\dagger = \frac{1}{2}(I + \sigma_z),$$

σ_x, σ_y, σ_z — повороты вокруг осей Ox, Oy, Oz соответственно.

О матрицах Паули

Поскольку $\sigma_x^2 = \sigma_y^2 = \sigma_z^2 = I$, матрицы Паули — повороты на π. Так как

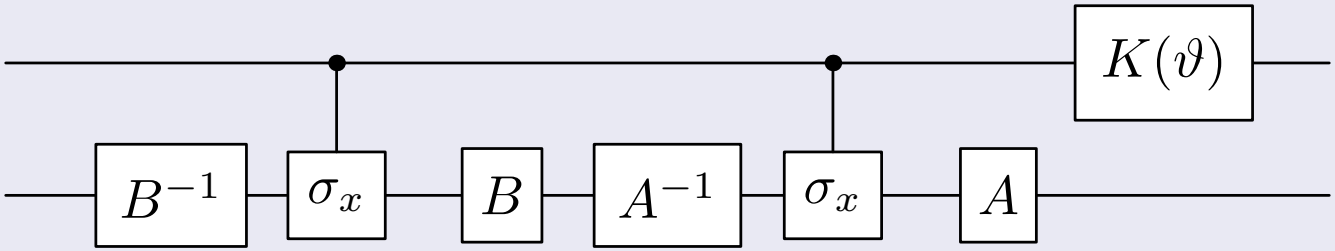
$$\sigma_x \frac{1}{2}(I + \sigma_x)\sigma_x^\dagger = \frac{1}{2}(I + \sigma_x),$$
$$\sigma_y \frac{1}{2}(I + \sigma_y)\sigma_y^\dagger = \frac{1}{2}(I + \sigma_y),$$
$$\sigma_z \frac{1}{2}(I + \sigma_z)\sigma_z^\dagger = \frac{1}{2}(I + \sigma_z),$$

σ_x, σ_y, σ_z — повороты вокруг осей Ox, Oy, Oz соответственно.

Доказательство теоремы 2

Теорема 2

Любой оператор вида c-U представляется в виде



$$\text{где } K(\vartheta) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\vartheta} \end{pmatrix}$$

Достаточно доказать, что для любого U есть представление вида $U = e^{i\vartheta} A\sigma_x A^{-1} B\sigma_x B^{-1}$.

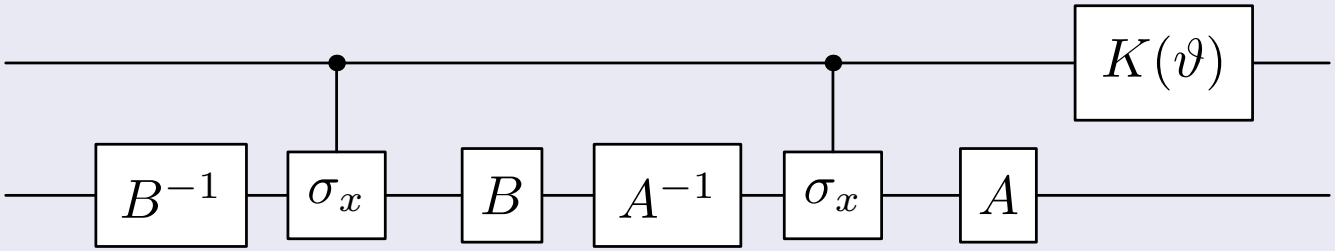
Задача

Докажите, что любой поворот трехмерного пространства является композицией двух поворотов на угол π.

Доказательство теоремы 2

Теорема 2

Любой оператор вида c-U представляется в виде



$$\text{где } K(\vartheta) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\vartheta} \end{pmatrix}$$

Достаточно доказать, что для любого U есть представление вида $U = e^{i\vartheta} A\sigma_x A^{-1} B\sigma_x B^{-1}$.

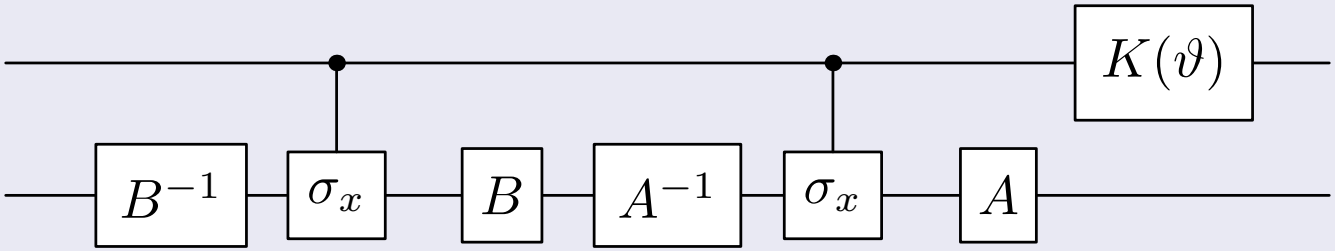
Задача

Докажите, что любой поворот трехмерного пространства является композицией двух поворотов на угол π.

Доказательство теоремы 2

Теорема 2

Любой оператор вида c-U представляется в виде



$$\text{где } K(\vartheta) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\vartheta} \end{pmatrix}$$

Достаточно доказать, что для любого U есть представление вида $U = e^{i\vartheta} A\sigma_x A^{-1} B\sigma_x B^{-1}$.

Задача

Докажите, что любой поворот трехмерного пространства является композицией двух поворотов на угол π.