Квантовые алгоритмы: возможности и ограничения. Лекция 2: Квантовые запросы к «черному ящику»

М. Вялый

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

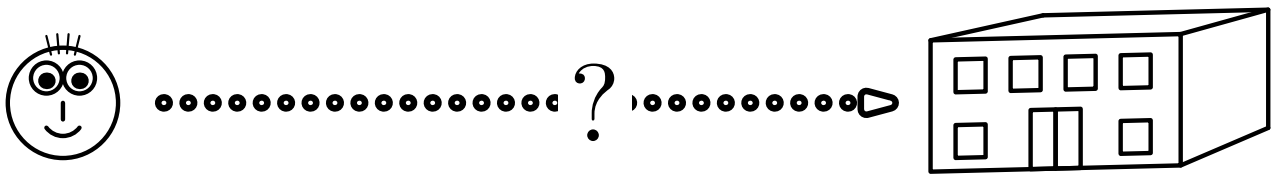
Санкт-Петербург, 2011

План

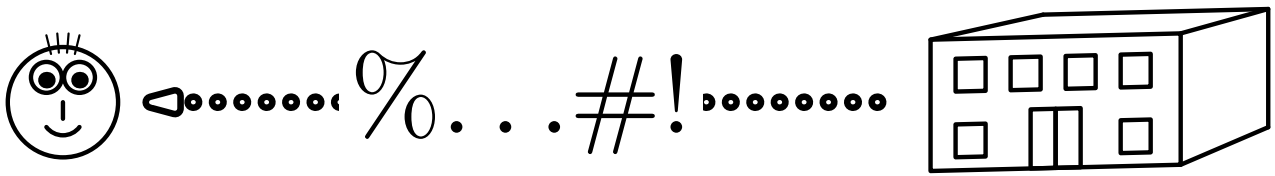
Алгоритмы «черного ящика»

Они же: оракульные алгоритмы (неудачное название), решающие деревья.
Стандартный английский термин — query algorithms.

Общение с «черным ящиком»



запрос



ответ

Сложность алгоритмов «черного ящика»

Чем меньше запросов, тем лучше.
На сложность обработки запросов внимания не обращаем — лишнее обращение к «черному ящику» стоит дороже.

Запрос на значение булевозначной функции

Классический запрос

Функция $x \mapsto f(x), \quad x \in X,\ f(x) \in \{0, 1\}$.

Запрос x.

Ответ $f(x)$.

Общий вид задачи

Дано: «черный ящик», который вычисляет функцию f.

Проверить: функция f обладает некоторым свойством.

Сложность алгоритма: количество запросов.

Запрос на значение булевозначной функции

Классический запрос

Функция $x \mapsto f(x), \quad x \in X,\ f(x) \in \{0, 1\}$.

Запрос x.

Ответ $f(x)$.

Общий вид задачи

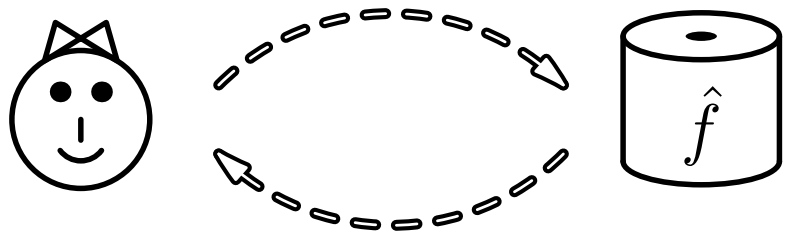
Дано: «черный ящик», который вычисляет функцию f.

Проверить: функция f обладает некоторым свойством.

Сложность алгоритма: количество запросов.

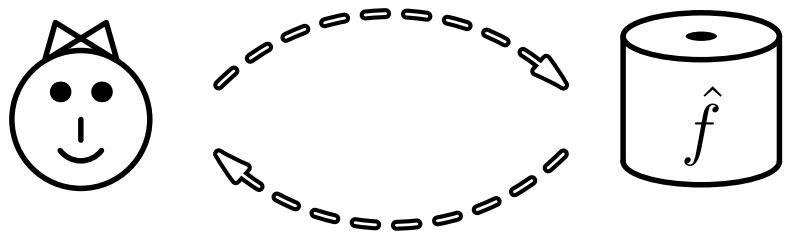
План

Квантовый запрос: проблема с необратимостью



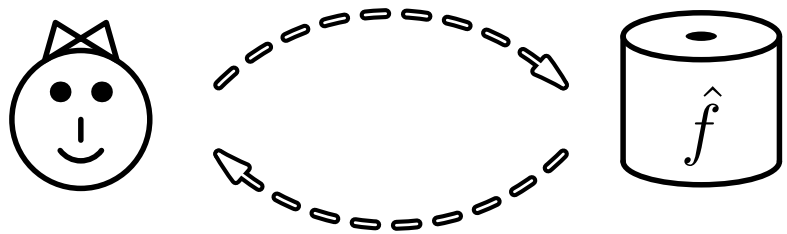
- Унитарные операторы обратимы.
- Некоторые булевы функции необратимы.
- Как квантовое устройство выдает результат вычисления булевой функции? (Какое преобразование происходит с кубитом?)

Квантовый запрос: проблема с необратимостью



- Унитарные операторы обратимы.
- Некоторые булевы функции необратимы.
- Как квантовое устройство выдает результат вычисления булевой функции? (Какое преобразование происходит с кубитом?)

Квантовый запрос: проблема с необратимостью



- Унитарные операторы обратимы.
- Некоторые булевы функции необратимы.
- Как квантовое устройство выдает результат вычисления булевой функции? (Какое преобразование происходит с кубитом?)

Необратимое вычисление: взгляд на микроуровне

- На микроуровне вычисление обратимо и в классической, и в квантовой физике.
- Обратимое вычисление булевозначной функции (идеализированный пример):

$$\hat{f} : (x, y) \mapsto (x, y \oplus f(x)).$$

- Внутри «черного ящика» происходит нечто вроде

Необратимое вычисление: взгляд на микроуровне

- На микроуровне вычисление обратимо и в классической, и в квантовой физике.
- Обратимое вычисление булевозначной функции (идеализированный пример):

$$\hat{f} : (x, y) \mapsto (x, y \oplus f(x)).$$

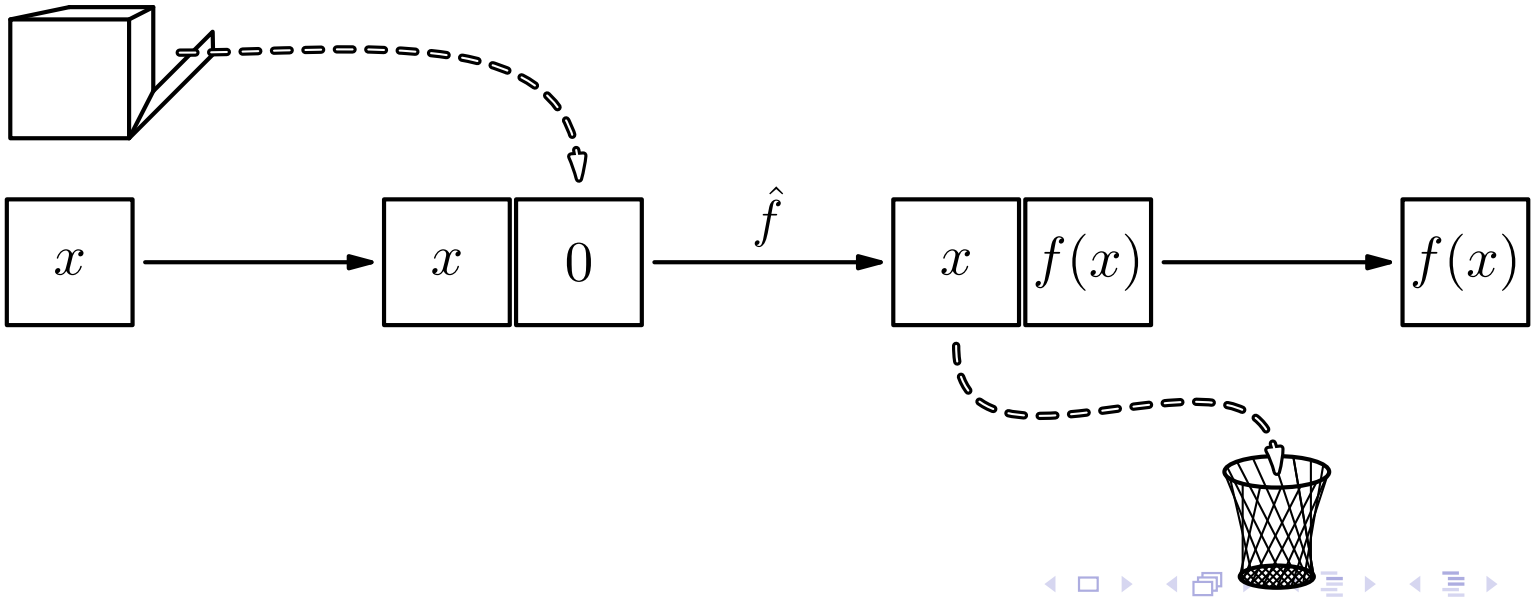
- Внутри «черного ящика» происходит нечто вроде

Необратимое вычисление: взгляд на микроуровне

- На микроуровне вычисление обратимо и в классической, и в квантовой физике.
- Обратимое вычисление булевозначной функции (идеализированный пример):

$$\hat{f} : (x, y) \mapsto (x, y \oplus f(x)).$$

- Внутри «черного ящика» происходит нечто вроде



Обратимый (квантовый) запрос

- $\hat{f}$ продолжается до унитарного оператора (перестановочного). Пример с функцией $f : \{0,1\} \to \{0,1\}$, $f(x) = x$:

$$\hat{f} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

(При записи матриц в вычислительном базисе мы упорядочиваем битовые строки в лексикографическом порядке.)

- Будем считать оператор

$$\hat{f} : |x, b\rangle \mapsto |x, b \oplus f(x)\rangle$$

квантовым запросом общего вида.

Обратимый (квантовый) запрос

- $\hat{f}$ продолжается до унитарного оператора (перестановочного). Пример с функцией $f : \{0,1\} \to \{0,1\}$, $f(x) = x$:

$$\hat{f} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

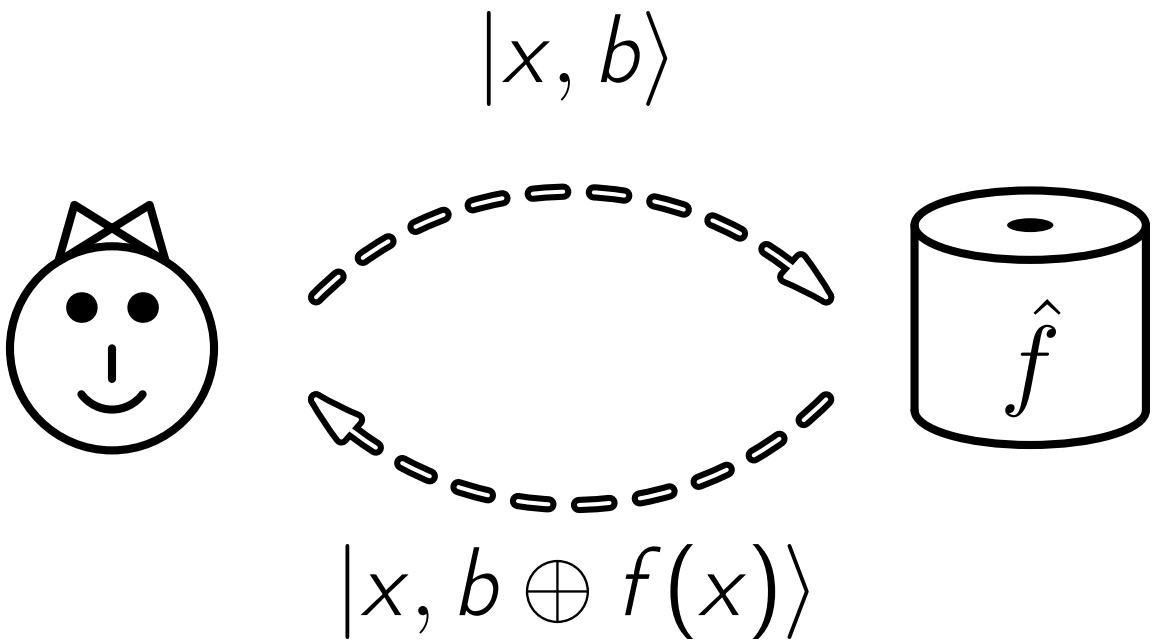
  (При записи матриц в вычислительном базисе мы упорядочиваем битовые строки в лексикографическом порядке.)

- Будем считать оператор

$$\hat{f} : |x, b\rangle \mapsto |x, b \oplus f(x)\rangle$$

  квантовым запросом общего вида.

Посылаем и получаем и регистр аргумента, и регистр значения



План

Имитация детерминированного запроса

- Квантовый алгоритм может реализовать любую перестановку векторов вычислительного базиса.
- Этому соответствует обратимое классическое преобразование.
- Избавление от необратимости: использование «свежей» памяти, как в уже рассмотренном случае

$$\hat{f} : |x, b\rangle \mapsto |x, b \oplus f(x)\rangle.$$

- В общем случае необратимое отображение $f : A \to A$ можно имитировать подходящим обратимым $\tilde{f}$ со свежей копией памяти A в фиксированном состоянии a_0:

$$\tilde{f} : (a, a_0) \mapsto (a, f(a))$$

продолжается до перестановки на $A \times A$.

Имитация детерминированного запроса

- Квантовый алгоритм может реализовать любую перестановку векторов вычислительного базиса.
- Этому соответствует обратимое классическое преобразование.
- Избавление от необратимости: использование «свежей» памяти, как в уже рассмотренном случае

$$\hat{f} : |x, b\rangle \mapsto |x, b \oplus f(x)\rangle.$$

- В общем случае необратимое отображение $f : A \to A$ можно имитировать подходящим обратимым $\tilde{f}$ со свежей копией памяти A в фиксированном состоянии a_0:

$$\tilde{f} : (a, a_0) \mapsto (a, f(a))$$

продолжается до перестановки на $A \times A$.

Имитация детерминированного запроса

- Квантовый алгоритм может реализовать любую перестановку векторов вычислительного базиса.
- Этому соответствует обратимое классическое преобразование.
- Избавление от необратимости: использование «свежей» памяти, как в уже рассмотренном случае

$$\hat{f} : |x, b\rangle \mapsto |x, b \oplus f(x)\rangle.$$

- В общем случае необратимое отображение $f : A \to A$ можно имитировать подходящим обратимым $\tilde{f}$ со свежей копией памяти A в фиксированном состоянии a_0:

$$\tilde{f} : (a, a_0) \mapsto (a, f(a))$$

продолжается до перестановки на $A \times A$.

Имитация детерминированного запроса

- Квантовый алгоритм может реализовать любую перестановку векторов вычислительного базиса.
- Этому соответствует обратимое классическое преобразование.
- Избавление от необратимости: использование «свежей» памяти, как в уже рассмотренном случае

$$\hat{f} : |x, b\rangle \mapsto |x, b \oplus f(x)\rangle.$$

- В общем случае необратимое отображение $f : A \to A$ можно имитировать подходящим обратимым $\tilde{f}$ со свежей копией памяти A в фиксированном состоянии a_0:

$$\tilde{f} : (a, a_0) \mapsto (a, f(a))$$

продолжается до перестановки на $A \times A$.

Имитация вероятностного запроса

- Запрос по распределению p_k имитируем приготовлением вектора

$$|p\rangle = \sum_k \sqrt{p_k}|k\rangle$$

в регистре аргумента и применением квантового запроса к $|p, 0\rangle$.

- Получится

$$\sum_k \sqrt{p_k}|k, f(k)\rangle$$

- Если в этот момент провести измерение, получится запрос по распределению p_k.

Имитация вероятностного запроса

- Запрос по распределению p_k имитируем приготовлением вектора

$$|p\rangle = \sum_k \sqrt{p_k}|k\rangle$$

в регистре аргумента и применением квантового запроса к $|p, 0\rangle$.

- Получится

$$\sum_k \sqrt{p_k}|k, f(k)\rangle$$

- Если в этот момент провести измерение, получится запрос по распределению p_k.

Имитация вероятностного запроса

- Запрос по распределению p_k имитируем приготовлением вектора

$$|p\rangle = \sum_k \sqrt{p_k}|k\rangle$$

в регистре аргумента и применением квантового запроса к $|p, 0\rangle$.

- Получится

$$\sum_k \sqrt{p_k}|k, f(k)\rangle$$

- Если в этот момент провести измерение, получится запрос по распределению p_k.

Как избавиться от промежуточных измерений?

- Использовать каждый раз свежую копию регистра аргумента, выполняя обратимое копирование.
- Тогда распределение исходов после финального измерения в точности совпадает с распределением, порождаемым вероятностным алгоритмом.
- Вычисление в случае двух запросов по распределениям $p^{(1)}$, $p^{(2,k)}$ (второе распределение зависит от результатов первого). Вектор состояния перед измерением

$$\sum_{k_1} \sqrt{p_k^{(1)}} |k_1\rangle \otimes \sum_{k_2} \sqrt{p_{k_2}^{(2,k_1)}} |k_2, F(k_1,k_2)\rangle =$$

$$= \sum_{k_1,k_2} \sqrt{p_k^{(1)}} \sqrt{p_{k_2}^{(2,k_1)}} |k_1, k_2, F(k_1,k_2)\rangle$$

Как избавиться от промежуточных измерений?

- Использовать каждый раз свежую копию регистра аргумента, выполняя обратимое копирование.
- Тогда распределение исходов после финального измерения в точности совпадает с распределением, порождаемым вероятностным алгоритмом.
- Вычисление в случае двух запросов по распределениям $p^{(1)}$, $p^{(2,k)}$ (второе распределение зависит от результатов первого). Вектор состояния перед измерением

$$\sum_{k_1} \sqrt{p_k^{(1)}} |k_1\rangle \otimes \sum_{k_2} \sqrt{p_{k_2}^{(2,k_1)}} |k_2, F(k_1,k_2)\rangle =$$

$$= \sum_{k_1,k_2} \sqrt{p_k^{(1)}} \sqrt{p_{k_2}^{(2,k_1)}} |k_1, k_2, F(k_1,k_2)\rangle$$

Как избавиться от промежуточных измерений?

- Использовать каждый раз свежую копию регистра аргумента, выполняя обратимое копирование.
- Тогда распределение исходов после финального измерения в точности совпадает с распределением, порождаемым вероятностным алгоритмом.
- Вычисление в случае двух запросов по распределениям $p^{(1)}$, $p^{(2,k)}$ (второе распределение зависит от результатов первого). Вектор состояния перед измерением

$$\sum_{k_1} \sqrt{p_k^{(1)}} |k_1\rangle \otimes \sum_{k_2} \sqrt{p_{k_2}^{(2,k_1)}} |k_2, F(k_1, k_2)\rangle =$$

$$= \sum_{k_1, k_2} \sqrt{p_k^{(1)}} \sqrt{p_{k_2}^{(2,k_1)}} |k_1, k_2, F(k_1, k_2)\rangle$$

Как избавиться от промежуточных измерений?

- Вычисление в случае двух запросов по распределениям $p^{(1)}$, $p^{(2,k)}$ (второе распределение зависит от результатов первого). Вектор состояния перед измерением

$$\sum_{k_1} \sqrt{p_{k_1}^{(1)}} |k_1\rangle \otimes \sum_{k_2} \sqrt{p_{k_2}^{(2,k_1)}} |k_2, F(k_1,k_2)\rangle =$$

$$= \sum_{k_1,k_2} \sqrt{p_{k_1}^{(1)}} \sqrt{p_{k_2}^{(2,k_1)}} |k_1, k_2, F(k_1,k_2)\rangle$$

- Вероятность исхода $(k_1, k_2, F(k_1,k_2))$ равна

$$p_{k_1}^{(1)} p_{k_2}^{(2,k_1)},$$

как и случае вероятностного алгоритма.

- Для нескольких запросов вычисление аналогично.

Как избавиться от промежуточных измерений?

- Вычисление в случае двух запросов по распределениям $p^{(1)}$, $p^{(2,k)}$ (второе распределение зависит от результатов первого). Вектор состояния перед измерением

$$\sum_{k_1} \sqrt{p_{k_1}^{(1)}} |k_1\rangle \otimes \sum_{k_2} \sqrt{p_{k_2}^{(2,k_1)}} |k_2, F(k_1,k_2)\rangle =$$

$$= \sum_{k_1,k_2} \sqrt{p_{k_1}^{(1)}} \sqrt{p_{k_2}^{(2,k_1)}} |k_1, k_2, F(k_1,k_2)\rangle$$

- Вероятность исхода $(k_1, k_2, F(k_1,k_2))$ равна

$$p_{k_1}^{(1)} p_{k_2}^{(2,k_1)},$$

как и случае вероятностного алгоритма.

- Для нескольких запросов вычисление аналогично.

План

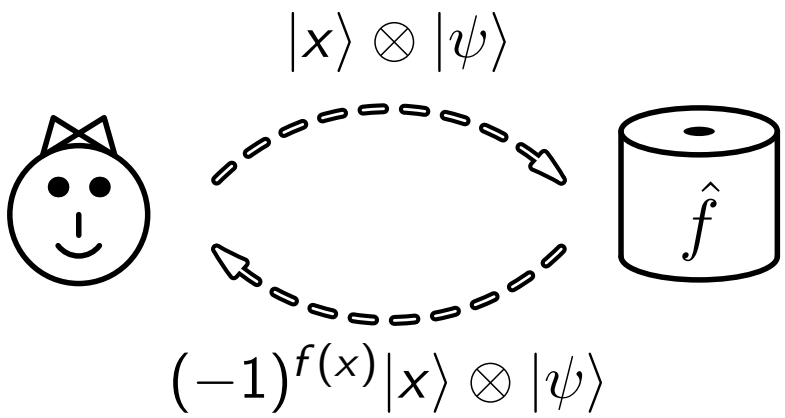
Пример использования квантового «черного ящика»

«Магическое состояние» $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

Пример использования квантового «черного ящика»

«Магическое состояние» $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

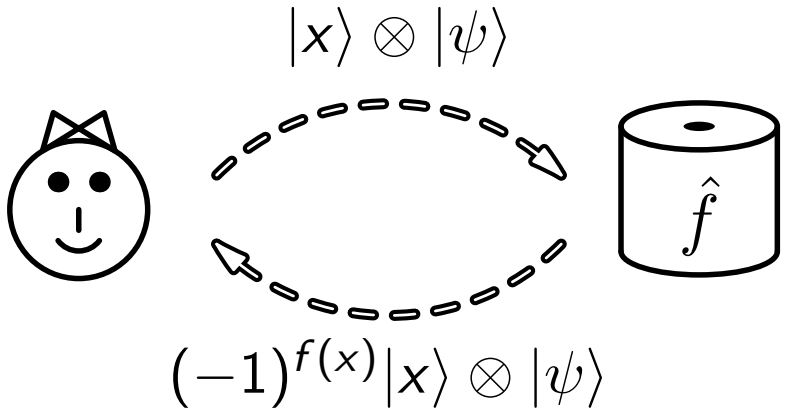
Запрос и ответ:



Пример использования квантового «черного ящика»

«Магическое состояние» $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

Запрос и ответ:



Фазовый запрос

$$O_f : |x\rangle \mapsto (-1)^{f(x)}|x\rangle$$

(вспомогательный кубит не пишем — его состояние не меняется).

Проверка работы фазового запроса

Рассмотрим применение $\hat{f}$ к $|x\rangle \otimes |\psi\rangle$:

$$|x\rangle \otimes \frac{1}{\sqrt{2}}\Big(|0\rangle - |1\rangle\Big) \overset{\hat{f}}{\mapsto} \frac{1}{\sqrt{2}}\Big(|x\rangle \otimes |f(x)\rangle - |x\rangle \otimes |1 \oplus f(x)\rangle\Big) =$$

$$= \begin{cases} |x\rangle \otimes \frac{1}{\sqrt{2}}\Big(|0\rangle - |1\rangle\Big), & \text{если } f(x) = 0, \\ -|x\rangle \otimes \frac{1}{\sqrt{2}}\Big(|0\rangle - |1\rangle\Big), & \text{если } f(x) = 1, \end{cases} =$$

$$= (-1)^{f(x)}|x\rangle \otimes \frac{1}{\sqrt{2}}\Big(|0\rangle - |1\rangle\Big).$$

Упражнение

Проверьте, что собственные числа оператора $\hat{f}$ равны ± 1. Найдите соответствующие им собственные пространства.

Проверка работы фазового запроса

Рассмотрим применение $\hat{f}$ к $|x\rangle \otimes |\psi\rangle$:

$$|x\rangle \otimes \frac{1}{\sqrt{2}}\Big(|0\rangle - |1\rangle\Big) \overset{\hat{f}}{\mapsto} \frac{1}{\sqrt{2}}\Big(|x\rangle \otimes |f(x)\rangle - |x\rangle \otimes |1 \oplus f(x)\rangle\Big) =$$

$$= \left\{ \begin{array}{ll} |x\rangle \otimes \frac{1}{\sqrt{2}}\Big(|0\rangle - |1\rangle\Big), & \text{если } f(x) = 0, \\ -|x\rangle \otimes \frac{1}{\sqrt{2}}\Big(|0\rangle - |1\rangle\Big), & \text{если } f(x) = 1, \end{array} \right\} =$$

$$= (-1)^{f(x)}|x\rangle \otimes \frac{1}{\sqrt{2}}\Big(|0\rangle - |1\rangle\Big).$$

Упражнение

Проверьте, что собственные числа оператора $\hat{f}$ равны ± 1. Найдите соответствующие им собственные пространства.

Проверка работы фазового запроса

Рассмотрим применение $\hat{f}$ к $|x\rangle \otimes |\psi\rangle$:

$$|x\rangle \otimes \frac{1}{\sqrt{2}}\Big(|0\rangle - |1\rangle\Big) \overset{\hat{f}}{\mapsto} \frac{1}{\sqrt{2}}\Big(|x\rangle \otimes |f(x)\rangle - |x\rangle \otimes |1 \oplus f(x)\rangle\Big) =$$

$$= \left\{ \begin{array}{ll} |x\rangle \otimes \frac{1}{\sqrt{2}}\Big(|0\rangle - |1\rangle\Big), & \text{если } f(x) = 0, \\ -|x\rangle \otimes \frac{1}{\sqrt{2}}\Big(|0\rangle - |1\rangle\Big), & \text{если } f(x) = 1, \end{array} \right\} =$$

$$= (-1)^{f(x)}|x\rangle \otimes \frac{1}{\sqrt{2}}\Big(|0\rangle - |1\rangle\Big).$$

Упражнение

Проверьте, что собственные числа оператора $\hat{f}$ равны ± 1. Найдите соответствующие им собственные пространства.

Проверка работы фазового запроса

Рассмотрим применение $\hat{f}$ к $|x\rangle \otimes |\psi\rangle$:

$$|x\rangle \otimes \frac{1}{\sqrt{2}}\Big(|0\rangle - |1\rangle\Big) \overset{\hat{f}}{\mapsto} \frac{1}{\sqrt{2}}\Big(|x\rangle \otimes |f(x)\rangle - |x\rangle \otimes |1 \oplus f(x)\rangle\Big) =$$

$$= \left\{ \begin{array}{ll} |x\rangle \otimes \frac{1}{\sqrt{2}}\Big(|0\rangle - |1\rangle\Big), & \text{если } f(x) = 0, \\ -|x\rangle \otimes \frac{1}{\sqrt{2}}\Big(|0\rangle - |1\rangle\Big), & \text{если } f(x) = 1, \end{array} \right\} =$$

$$= (-1)^{f(x)}|x\rangle \otimes \frac{1}{\sqrt{2}}\Big(|0\rangle - |1\rangle\Big).$$

Упражнение

Проверьте, что собственные числа оператора $\hat{f}$ равны ± 1. Найдите соответствующие им собственные пространства.

Проверка работы фазового запроса

Рассмотрим применение $\hat{f}$ к $|x\rangle \otimes |\psi\rangle$:

$$|x\rangle \otimes \frac{1}{\sqrt{2}}\Big(|0\rangle - |1\rangle\Big) \overset{\hat{f}}{\mapsto} \frac{1}{\sqrt{2}}\Big(|x\rangle \otimes |f(x)\rangle - |x\rangle \otimes |1 \oplus f(x)\rangle\Big) =$$

$$= \left\{ \begin{array}{ll} |x\rangle \otimes \frac{1}{\sqrt{2}}\Big(|0\rangle - |1\rangle\Big), & \text{если } f(x) = 0, \\ -|x\rangle \otimes \frac{1}{\sqrt{2}}\Big(|0\rangle - |1\rangle\Big), & \text{если } f(x) = 1, \end{array} \right\} =$$

$$= (-1)^{f(x)}|x\rangle \otimes \frac{1}{\sqrt{2}}\Big(|0\rangle - |1\rangle\Big).$$

Упражнение

Проверьте, что собственные числа оператора $\hat{f}$ равны ± 1. Найдите соответствующие им собственные пространства.

План

Задача Дойча

Булевых функций от одной переменной ровно 4:

$$0,\ 1,\ x,\ \neg x.$$

Первые две из них — константы, вторые две — нет.

Задача Дойча

Определить, является ли функция, вычисляемая «черным ящиком», константой.

Одного запроса для решения задачи Дойча в классическом случае недостаточно: по значению в одной точке нельзя понять, является ли функция константой.

Задача Дойча

Булевых функций от одной переменной ровно 4:

$$0,\ 1,\ x,\ \neg x.$$

Первые две из них — константы, вторые две — нет.

Задача Дойча

Определить, является ли функция, вычисляемая «черным ящиком», константой.

Одного запроса для решения задачи Дойча в классическом случае недостаточно: по значению в одной точке нельзя понять, является ли функция константой.

Задача Дойча

Булевых функций от одной переменной ровно 4:

$$0,\ 1,\ x,\ \neg x.$$

Первые две из них — константы, вторые две — нет.

Задача Дойча

Определить, является ли функция, вычисляемая «черным ящиком», константой.

Одного запроса для решения задачи Дойча в классическом случае недостаточно: по значению в одной точке нельзя понять, является ли функция константой.

Квантовое решение задачи Дойча за один запрос

1. Применим к состоянию $|0\rangle$ унитарный оператор $HO_f H$, где

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad \text{(преобразование Адамара)}.$$

2. Произведем измерение в вычислительном базисе.
3. Ответ 0 будет означать, что функция — константа.

Квантовое решение задачи Дойча за один запрос

1. Применим к состоянию $|0\rangle$ унитарный оператор $HO_f H$, где

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad \text{(преобразование Адамара)}.$$

2. Произведем измерение в вычислительном базисе.
3. Ответ 0 будет означать, что функция — константа.

Квантовое решение задачи Дойча за один запрос

1. Применим к состоянию $|0\rangle$ унитарный оператор $HO_f H$, где

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad \text{(преобразование Адамара)}.$$

2. Произведем измерение в вычислительном базисе.
3. Ответ 0 будет означать, что функция — константа.

Проверка корректности

$$|0\rangle \overset{H}{\longmapsto} \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \overset{O_f}{\longmapsto} \frac{1}{\sqrt{2}}(-1)^{f(0)}|0\rangle + \frac{1}{\sqrt{2}}(-1)^{f(1)}|1\rangle \overset{H}{\longmapsto}$$

$$\frac{1}{2}(-1)^{f(0)}(|0\rangle + |1\rangle) + \frac{1}{2}(-1)^{f(1)}(|0\rangle - |1\rangle) =$$

$$= \frac{1}{2}((-1)^{f(0)} + (-1)^{f(1)})|0\rangle + \frac{1}{2}((-1)^{f(0)} - (-1)^{f(1)})|1\rangle =$$

$$= \begin{cases} \pm|0\rangle, & \text{если } f \text{ константа,} \\ \pm|1\rangle, & \text{в противном случае.} \end{cases}$$

Проверка корректности

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

$$|0\rangle \overset{H}{\longmapsto} \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \overset{O_f}{\longmapsto} \frac{1}{\sqrt{2}}(-1)^{f(0)}|0\rangle + \frac{1}{\sqrt{2}}(-1)^{f(1)}|1\rangle \overset{H}{\longmapsto}$$

$$\frac{1}{2}(-1)^{f(0)}(|0\rangle + |1\rangle) + \frac{1}{2}(-1)^{f(1)}(|0\rangle - |1\rangle) =$$

$$= \frac{1}{2}((-1)^{f(0)} + (-1)^{f(1)})|0\rangle + \frac{1}{2}((-1)^{f(0)} - (-1)^{f(1)})|1\rangle =$$

$$= \begin{cases} \pm|0\rangle, & \text{если } f \text{ константа,} \\ \pm|1\rangle, & \text{в противном случае.} \end{cases}$$

Проверка корректности

$$|0\rangle \overset{H}{\longmapsto} \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \overset{O_f}{\longmapsto} \frac{1}{\sqrt{2}}(-1)^{f(0)}|0\rangle + \frac{1}{\sqrt{2}}(-1)^{f(1)}|1\rangle \overset{H}{\longmapsto}$$

$$\frac{1}{2}(-1)^{f(0)}(|0\rangle + |1\rangle) + \frac{1}{2}(-1)^{f(1)}(|0\rangle - |1\rangle) =$$

$$= \frac{1}{2}((-1)^{f(0)} + (-1)^{f(1)})|0\rangle + \frac{1}{2}((-1)^{f(0)} - (-1)^{f(1)})|1\rangle =$$

$$= \begin{cases} \pm|0\rangle, & \text{если } f \text{ константа,} \\ \pm|1\rangle, & \text{в противном случае.} \end{cases}$$

Проверка корректности

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

$$|0\rangle \xmapsto{O_f H} \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \xmapsto{O_f} \frac{1}{\sqrt{2}}(-1)^{f(0)}|0\rangle + \frac{1}{\sqrt{2}}(-1)^{f(1)}|1\rangle \xmapsto{H}$$

$$\frac{1}{2}(-1)^{f(0)}(|0\rangle + |1\rangle) + \frac{1}{2}(-1)^{f(1)}(|0\rangle - |1\rangle) =$$

$$= \frac{1}{2}((-1)^{f(0)} + (-1)^{f(1)})|0\rangle + \frac{1}{2}((-1)^{f(0)} - (-1)^{f(1)})|1\rangle =$$

$$= \begin{cases} \pm|0\rangle, & \text{если } f \text{ константа,} \\ \pm|1\rangle, & \text{в противном случае.} \end{cases}$$

Проверка корректности

$$|0\rangle \xrightarrow{HO_f H} \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \xmapsto{O_f} \frac{1}{\sqrt{2}}(-1)^{f(0)}|0\rangle + \frac{1}{\sqrt{2}}(-1)^{f(1)}|1\rangle \xmapsto{H}$$

$$\frac{1}{2}(-1)^{f(0)}(|0\rangle + |1\rangle) + \frac{1}{2}(-1)^{f(1)}(|0\rangle - |1\rangle) =$$

$$= \frac{1}{2}((-1)^{f(0)} + (-1)^{f(1)})|0\rangle + \frac{1}{2}((-1)^{f(0)} - (-1)^{f(1)})|1\rangle =$$

$$= \begin{cases} \pm|0\rangle, & \text{если } f \text{ константа,} \\ \pm|1\rangle, & \text{в противном случае.} \end{cases}$$

Проверка корректности

$$|0\rangle \xmapsto{HO_f H} \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \xmapsto{O_f} \frac{1}{\sqrt{2}}(-1)^{f(0)}|0\rangle + \frac{1}{\sqrt{2}}(-1)^{f(1)}|1\rangle \xmapsto{H}$$

$$\frac{1}{2}(-1)^{f(0)}(|0\rangle + |1\rangle) + \frac{1}{2}(-1)^{f(1)}(|0\rangle - |1\rangle) =$$

$$= \frac{1}{2}\left((-1)^{f(0)} + (-1)^{f(1)}\right)|0\rangle + \frac{1}{2}\left((-1)^{f(0)} - (-1)^{f(1)}\right)|1\rangle =$$

$$= \begin{cases} \pm|0\rangle, & \text{если } f \text{ константа,} \\ \pm|1\rangle, & \text{в противном случае.} \end{cases}.$$

План

Формулировка

Задача Дойча – Джоза

Дано: «черный ящик», который вычисляет функцию $f : \{0,1\}^n \to \{0,1\}$.

Заранее известно: выполняется одно из двух:

(к) функция f — константа;

(б) функция f сбалансирована, т. е. число нулей и единиц у нее одинаково.

Выяснить: какой из случаев имеет место.

Это пример задачи с априорными ограничениями на входные данные (promise problem).

Формулировка

Задача Дойча – Джоза

Дано: «черный ящик», который вычисляет функцию $f : \{0,1\}^n \to \{0,1\}$.

Заранее известно: выполняется одно из двух:

(к) функция f — константа;

(б) функция f сбалансирована, т. е. число нулей и единиц у нее одинаково.

Выяснить: какой из случаев имеет место.

Это пример задачи с априорными ограничениями на входные данные (promise problem).

Решение задачи Дойча – Джоза за один квантовый запрос

1. Применим к состоянию $|0^n\rangle$ унитарный оператор $J = H^{\otimes n} O_f H^{\otimes n}$.
2. Произведем измерение в вычислительном базисе.
3. Если результат измерения — $|0^n\rangle$, то f — константа, т. е. имеет место случай (к). В противном случае имеет место случай (б).

Решение задачи Дойча – Джоза за один квантовый запрос

1. Применим к состоянию $|0^n\rangle$ унитарный оператор $J = H^{\otimes n} O_f H^{\otimes n}$.
2. Произведем измерение в вычислительном базисе.
3. Если результат измерения — $|0^n\rangle$, то f — константа, т. е. имеет место случай (к). В противном случае имеет место случай (б).

Решение задачи Дойча – Джоза за один квантовый запрос

1. Применим к состоянию $|0^n\rangle$ унитарный оператор $J = H^{\otimes n} O_f H^{\otimes n}$.
2. Произведем измерение в вычислительном базисе.
3. Если результат измерения — $|0^n\rangle$, то f — константа, т. е. имеет место случай (к). В противном случае имеет место случай (б).

Действие $H^{\otimes n}$ на базисных векторах

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

$$H|\alpha\rangle = \frac{1}{\sqrt{2}} \sum_{\beta \in \{0,1\}} (-1)^{\alpha \cdot \beta} |\beta\rangle.$$

$$H^{\otimes n}|\alpha\rangle = H^{\otimes n}|\alpha_1, \ldots, \alpha_n\rangle = \bigotimes_{k=1}^{n} H|\alpha_k\rangle =$$

$$= \frac{1}{2^{n/2}} \bigotimes_{k=1}^{n} \sum_{\beta_k \in \{0,1\}} (-1)^{\alpha_k \cdot \beta_k} |\beta_k\rangle =$$

$$= \frac{1}{2^{n/2}} \sum_{(\beta_1, \ldots, \beta_k) \in \{0,1\}^n} (-1)^{\alpha_1\beta_1 \oplus \alpha_2\beta_2 \oplus \ldots \oplus \alpha_n\beta_n} |\beta_1\beta_2 \ldots \beta_n\rangle =$$

$$= \frac{1}{2^{n/2}} \sum_{\beta \in \{0,1\}^n} (-1)^{(\alpha,\beta)} |\beta\rangle.$$

Действие $H^{\otimes n}$ на базисных векторах

$$H|\alpha\rangle = \frac{1}{\sqrt{2}} \sum_{\beta\in\{0,1\}} (-1)^{\alpha\cdot\beta}|\beta\rangle.$$

$$H^{\otimes n}|\alpha\rangle = H^{\otimes n}|\alpha_1,\ldots,\alpha_n\rangle = \bigotimes_{k=1}^{n} H|\alpha_k\rangle =$$

$$= \frac{1}{2^{n/2}} \bigotimes_{k=1}^{n} \sum_{\beta_k\in\{0,1\}} (-1)^{\alpha_k\cdot\beta_k}|\beta_k\rangle =$$

$$= \frac{1}{2^{n/2}} \sum_{(\beta_1,\ldots,\beta_k)\in\{0,1\}^n} (-1)^{\alpha_1\beta_1\oplus\alpha_2\beta_2\oplus\ldots\oplus\alpha_n\beta_n}|\beta_1\beta_2\ldots\beta_n\rangle =$$

$$= \frac{1}{2^{n/2}} \sum_{\beta\in\{0,1\}^n} (-1)^{(\alpha,\beta)}|\beta\rangle.$$

Действие $H^{\otimes n}$ на базисных векторах

$$H|\alpha\rangle = \frac{1}{\sqrt{2}} \sum_{\beta\in\{0,1\}} (-1)^{\alpha\cdot\beta}|\beta\rangle.$$

$$H^{\otimes n}|\alpha\rangle = H^{\otimes n}|\alpha_1,\ldots,\alpha_n\rangle = \bigotimes_{k=1}^{n} H|\alpha_k\rangle =$$

$$= \frac{1}{2^{n/2}} \bigotimes_{k=1}^{n} \sum_{\beta_k\in\{0,1\}} (-1)^{\alpha_k\cdot\beta_k}|\beta_k\rangle =$$

$$= \frac{1}{2^{n/2}} \sum_{(\beta_1,\ldots,\beta_k)\in\{0,1\}^n} (-1)^{\alpha_1\beta_1\oplus\alpha_2\beta_2\oplus\ldots\oplus\alpha_n\beta_n}|\beta_1\beta_2\ldots\beta_n\rangle =$$

$$= \frac{1}{2^{n/2}} \sum_{\beta\in\{0,1\}^n} (-1)^{(\alpha,\beta)}|\beta\rangle.$$

Действие $H^{\otimes n}$ на базисных векторах

$$H|\alpha\rangle = \frac{1}{\sqrt{2}} \sum_{\beta\in\{0,1\}} (-1)^{\alpha\cdot\beta}|\beta\rangle.$$

$$H^{\otimes n}|\alpha\rangle = H^{\otimes n}|\alpha_1,\ldots,\alpha_n\rangle = \bigotimes_{k=1}^{n} H|\alpha_k\rangle =$$

$$= \frac{1}{2^{n/2}} \bigotimes_{k=1}^{n} \sum_{\beta_k\in\{0,1\}} (-1)^{\alpha_k\cdot\beta_k}|\beta_k\rangle =$$

$$= \frac{1}{2^{n/2}} \sum_{(\beta_1,\ldots,\beta_k)\in\{0,1\}^n} (-1)^{\alpha_1\beta_1\oplus\alpha_2\beta_2\oplus\ldots\oplus\alpha_n\beta_n}|\beta_1\beta_2\ldots\beta_n\rangle =$$

$$= \frac{1}{2^{n/2}} \sum_{\beta\in\{0,1\}^n} (-1)^{(\alpha,\beta)}|\beta\rangle.$$

Действие $H^{\otimes n}$ на базисных векторах

$$H|\alpha\rangle = \frac{1}{\sqrt{2}} \sum_{\beta\in\{0,1\}} (-1)^{\alpha\cdot\beta}|\beta\rangle.$$

$$H^{\otimes n}|\alpha\rangle = H^{\otimes n}|\alpha_1,\ldots,\alpha_n\rangle = \bigotimes_{k=1}^{n} H|\alpha_k\rangle =$$

$$= \frac{1}{2^{n/2}} \bigotimes_{k=1}^{n} \sum_{\beta_k\in\{0,1\}} (-1)^{\alpha_k\cdot\beta_k}|\beta_k\rangle =$$

$$= \frac{1}{2^{n/2}} \sum_{(\beta_1,\ldots,\beta_k)\in\{0,1\}^n} (-1)^{\alpha_1\beta_1\oplus\alpha_2\beta_2\oplus\ldots\oplus\alpha_n\beta_n}|\beta_1\beta_2\ldots\beta_n\rangle =$$

$$= \frac{1}{2^{n/2}} \sum_{\beta\in\{0,1\}^n} (-1)^{(\alpha,\beta)}|\beta\rangle.$$

Действие $H^{\otimes n}$ на базисных векторах

$$H|\alpha\rangle = \frac{1}{\sqrt{2}} \sum_{\beta\in\{0,1\}} (-1)^{\alpha\cdot\beta}|\beta\rangle.$$

$$H^{\otimes n}|\alpha\rangle = H^{\otimes n}|\alpha_1,\ldots,\alpha_n\rangle = \bigotimes_{k=1}^{n} H|\alpha_k\rangle =$$

$$= \frac{1}{2^{n/2}} \bigotimes_{k=1}^{n} \sum_{\beta_k\in\{0,1\}} (-1)^{\alpha_k\cdot\beta_k}|\beta_k\rangle =$$

$$= \frac{1}{2^{n/2}} \sum_{(\beta_1,\ldots,\beta_k)\in\{0,1\}^n} (-1)^{\alpha_1\beta_1\oplus\alpha_2\beta_2\oplus\ldots\oplus\alpha_n\beta_n}|\beta_1\beta_2\ldots\beta_n\rangle =$$

$$= \frac{1}{2^{n/2}} \sum_{\beta\in\{0,1\}^n} (-1)^{(\alpha,\beta)}|\beta\rangle.$$

Действие $H^{\otimes n}$ на базисных векторах

$$H|\alpha\rangle = \frac{1}{\sqrt{2}} \sum_{\beta\in\{0,1\}} (-1)^{\alpha\cdot\beta}|\beta\rangle.$$

$$H^{\otimes n}|\alpha\rangle = H^{\otimes n}|\alpha_1,\ldots,\alpha_n\rangle = \bigotimes_{k=1}^{n} H|\alpha_k\rangle =$$

$$= \frac{1}{2^{n/2}} \bigotimes_{k=1}^{n} \sum_{\beta_k\in\{0,1\}} (-1)^{\alpha_k\cdot\beta_k}|\beta_k\rangle =$$

$$= \frac{1}{2^{n/2}} \sum_{(\beta_1,\ldots,\beta_k)\in\{0,1\}^n} (-1)^{\alpha_1\beta_1\oplus\alpha_2\beta_2\oplus\ldots\oplus\alpha_n\beta_n}|\beta_1\beta_2\ldots\beta_n\rangle =$$

$$= \frac{1}{2^{n/2}} \sum_{\beta\in\{0,1\}^n} (-1)^{(\alpha,\beta)}|\beta\rangle.$$

Действие J на векторе $|0^n\rangle$

$$|0^n\rangle \xmapsto{H^{\otimes n}} \frac{1}{2^{n/2}} \sum_{\alpha\in\{0,1\}^n} |\alpha\rangle \xmapsto{O_f} \frac{1}{2^{n/2}} \sum_{\alpha\in\{0,1\}^n} (-1)^{f(\alpha)}|\alpha\rangle \xmapsto{H^{\otimes n}}$$

$$\frac{1}{2^n} \sum_{\alpha\in\{0,1\}^n} \sum_{\beta\in\{0,1\}^n} (-1)^{f(\alpha)+(\alpha\cdot\beta)}|\beta\rangle =$$

$$= \frac{1}{2^n} \sum_{\beta\in\{0,1\}^n} \left(\sum_{\alpha\in\{0,1\}^n} (-1)^{f(\alpha)+(\alpha,\beta)} \right) |\beta\rangle.$$

Действие J на векторе $|0^n\rangle$

$$|0^n\rangle \overset{H^{\otimes n}}{\longmapsto} \frac{1}{2^{n/2}} \sum_{\alpha\in\{0,1\}^n} |\alpha\rangle \overset{O_f}{\longmapsto} \frac{1}{2^{n/2}} \sum_{\alpha\in\{0,1\}^n} (-1)^{f(\alpha)}|\alpha\rangle \overset{H^{\otimes n}}{\longmapsto}$$

$$\frac{1}{2^n} \sum_{\alpha\in\{0,1\}^n} \sum_{\beta\in\{0,1\}^n} (-1)^{f(\alpha)+(\alpha\cdot\beta)}|\beta\rangle =$$

$$= \frac{1}{2^n} \sum_{\beta\in\{0,1\}^n} \left(\sum_{\alpha\in\{0,1\}^n} (-1)^{f(\alpha)+(\alpha,\beta)} \right) |\beta\rangle.$$

Действие J на векторе $|0^n\rangle$

$$|0^n\rangle \overset{H^{\otimes n}}{\longmapsto} \frac{1}{2^{n/2}} \sum_{\alpha\in\{0,1\}^n} |\alpha\rangle \overset{O_f}{\longmapsto} \frac{1}{2^{n/2}} \sum_{\alpha\in\{0,1\}^n} (-1)^{f(\alpha)}|\alpha\rangle \overset{H^{\otimes n}}{\longmapsto}$$

$$\frac{1}{2^n} \sum_{\alpha\in\{0,1\}^n} \sum_{\beta\in\{0,1\}^n} (-1)^{f(\alpha)+(\alpha\cdot\beta)}|\beta\rangle =$$

$$= \frac{1}{2^n} \sum_{\beta\in\{0,1\}^n} \left(\sum_{\alpha\in\{0,1\}^n} (-1)^{f(\alpha)+(\alpha,\beta)} \right) |\beta\rangle.$$

Действие J на векторе $|0^n\rangle$

$$|0^n\rangle \xmapsto{O_f H^{\otimes n}} \frac{1}{2^{n/2}} \sum_{\alpha\in\{0,1\}^n} |\alpha\rangle \xmapsto{O_f} \frac{1}{2^{n/2}} \sum_{\alpha\in\{0,1\}^n} (-1)^{f(\alpha)}|\alpha\rangle \xmapsto{H^{\otimes n}}$$

$$\frac{1}{2^n} \sum_{\alpha\in\{0,1\}^n} \sum_{\beta\in\{0,1\}^n} (-1)^{f(\alpha)+(\alpha\cdot\beta)}|\beta\rangle =$$

$$= \frac{1}{2^n} \sum_{\beta\in\{0,1\}^n} \left(\sum_{\alpha\in\{0,1\}^n} (-1)^{f(\alpha)+(\alpha,\beta)} \right) |\beta\rangle.$$

Действие J на векторе $|0^n\rangle$

$$|0^n\rangle \xmapsto{H^{\otimes n} O_f H^{\otimes n}} \frac{1}{2^{n/2}} \sum_{\alpha\in\{0,1\}^n} |\alpha\rangle \xmapsto{O_f} \frac{1}{2^{n/2}} \sum_{\alpha\in\{0,1\}^n} (-1)^{f(\alpha)}|\alpha\rangle \xmapsto{H^{\otimes n}}$$

$$\frac{1}{2^n} \sum_{\alpha\in\{0,1\}^n} \sum_{\beta\in\{0,1\}^n} (-1)^{f(\alpha)+(\alpha\cdot\beta)}|\beta\rangle =$$

$$= \frac{1}{2^n} \sum_{\beta\in\{0,1\}^n} \left(\sum_{\alpha\in\{0,1\}^n} (-1)^{f(\alpha)+(\alpha,\beta)} \right) |\beta\rangle.$$

Действие J на векторе $|0^n\rangle$

$$|0^n\rangle \xmapsto{H^{\otimes n} O_f H^{\otimes n}} \frac{1}{2^{n/2}} \sum_{\alpha\in\{0,1\}^n} |\alpha\rangle \xmapsto{O_f} \frac{1}{2^{n/2}} \sum_{\alpha\in\{0,1\}^n} (-1)^{f(\alpha)}|\alpha\rangle \xmapsto{H^{\otimes n}}$$

$$\frac{1}{2^n} \sum_{\alpha\in\{0,1\}^n} \sum_{\beta\in\{0,1\}^n} (-1)^{f(\alpha)+(\alpha\cdot\beta)}|\beta\rangle =$$

$$= \frac{1}{2^n} \sum_{\beta\in\{0,1\}^n} \left(\sum_{\alpha\in\{0,1\}^n} (-1)^{f(\alpha)+(\alpha,\beta)} \right) |\beta\rangle.$$

Проверка корректности решения задачи Дойча – Джоза

$$|0^n\rangle \xmapsto{H^{\otimes n} O_f H^{\otimes n}} \frac{1}{2^n} \sum_{\beta\in\{0,1\}^n} \left(\sum_{\alpha\in\{0,1\}^n} (-1)^{f(\alpha)+(\alpha,\beta)} \right) |\beta\rangle$$

Так как $(\alpha, 0^n) = 0$, то вероятность наблюдения исхода 0^n равна

$$\left(\frac{1}{2^n} \sum_{\alpha\in\{0,1\}^n} (-1)^{f(\alpha)} \right)^2 = \begin{cases} 1, & \text{в случае (к)}, \\ 0, & \text{в случае (б)}. \end{cases}$$

Классические алгоритмы для задачи Дойча – Джоза

Детерминированный: должен сделать не менее 2^{n-1} запросов, чтобы различить случаи (б) и (к).

Вероятностный:

1. выберем две случайные точки x, y;
2. запросим значения функции в этих точках $f(x)$, $f(y)$;
3. если $f(x) = f(y)$, отвечаем (к), в противном случае — (б).

Классические алгоритмы для задачи Дойча – Джоза

Детерминированный: должен сделать не менее 2^{n-1} запросов, чтобы различить случаи (б) и (к).

Вероятностный:

1. выберем две случайные точки x, y;
2. запросим значения функции в этих точках $f(x)$, $f(y)$;
3. если $f(x) = f(y)$, отвечаем (к), в противном случае — (б).

Классические алгоритмы для задачи Дойча – Джоза

Детерминированный: должен сделать не менее 2^{n-1} запросов, чтобы различить случаи (б) и (к).

Вероятностный:

1. выберем две случайные точки x, y;
2. запросим значения функции в этих точках $f(x)$, $f(y)$;
3. если $f(x) = f(y)$, отвечаем (к), в противном случае — (б).

Классические алгоритмы для задачи Дойча – Джоза

Детерминированный: должен сделать не менее 2^{n-1} запросов, чтобы различить случаи (б) и (к).

Вероятностный:

1. выберем две случайные точки x, y;
2. запросим значения функции в этих точках $f(x)$, $f(y)$;
3. если $f(x) = f(y)$, отвечаем (к), в противном случае — (б).

Классические алгоритмы для задачи Дойча – Джоза

Детерминированный: должен сделать не менее 2^{n-1} запросов, чтобы различить случаи (б) и (к).

Вероятностный:

1. выберем две случайные точки x, y;
2. запросим значения функции в этих точках $f(x)$, $f(y)$;
3. если $f(x) = f(y)$, отвечаем (к), в противном случае — (б).

Вероятность ошибки

Ошибка односторонняя:

(к) 0 (ответ всегда правильный);

(б) $1/2$ (вероятность того, что $f(x) = f(y)$).

Вероятность ошибки можно уменьшить до 2^{-k}, повторив алгоритм k раз.

Вывод

Для любого $\varepsilon > 0$ существует вероятностный алгоритм, который решает задачу Дойча – Джоза с вероятностью ошибки $< \varepsilon$ за $O(1)$ запросов.

Вероятность ошибки

Ошибка односторонняя:

(к) 0 (ответ всегда правильный);

(б) $1/2$ (вероятность того, что $f(x) = f(y)$).

Вероятность ошибки можно уменьшить до 2^{-k}, повторив алгоритм k раз.

Вывод

Для любого $\varepsilon > 0$ существует вероятностный алгоритм, который решает задачу Дойча – Джоза с вероятностью ошибки $< \varepsilon$ за $O(1)$ запросов.

Вероятность ошибки

Ошибка односторонняя:

(к) 0 (ответ всегда правильный);

(б) $1/2$ (вероятность того, что $f(x) = f(y)$).

Вероятность ошибки можно уменьшить до 2^{-k}, повторив алгоритм k раз.

Вывод

Для любого $\varepsilon > 0$ существует вероятностный алгоритм, который решает задачу Дойча – Джоза с вероятностью ошибки $< \varepsilon$ за $O(1)$ запросов.

План

Задача поиска

Формулировка

Дано: «черный ящик», который вычисляет функцию $f : M \to \{0, 1\}$, где M — некоторое конечное множество размера m.
Заранее известно: функция равна 1 ровно в одной точке y множества M.
Найти: точку y.

Нижняя оценка для вероятностных алгоритмов поиска

Теорема

Любой вероятностный алгоритм, решающий задачу поиска с вероятностью ошибки $< \varepsilon$, делает $\Omega(m)$ запросов.

Доказательство

Нижняя оценка для вероятностных алгоритмов поиска

Теорема

Любой вероятностный алгоритм, решающий задачу поиска с вероятностью ошибки $< \varepsilon$, делает $\Omega(m)$ запросов.

Доказательство

Предполагаем, что алгоритм делает ровно k запросов и смотрит на ответы после выполнения всех запросов. (Неадаптивный алгоритм.)
Это не ограничивает общности, поскольку до момента, когда найдена точка y, все ответы одинаковы и любой алгоритм ведет себя так же, как некоторый неадаптивный.

Нижняя оценка для вероятностных алгоритмов поиска

Теорема

Любой вероятностный алгоритм, решающий задачу поиска с вероятностью ошибки $< \varepsilon$, делает $\Omega(m)$ запросов.

Доказательство

Предполагаем, что алгоритм делает ровно k запросов и смотрит на ответы после выполнения всех запросов. (Неадаптивный алгоритм.)
Это не ограничивает общности, поскольку до момента, когда найдена точка y, все ответы одинаковы и любой алгоритм ведет себя так же, как некоторый неадаптивный.
Оценка в «худшем случае». Ответы готовит «противник», который стремится минимизировать вероятность успеха.

Нижняя оценка для вероятностных алгоритмов поиска

Теорема

Любой вероятностный алгоритм, решающий задачу поиска с вероятностью ошибки $< \varepsilon$, делает $\Omega(m)$ запросов.

Доказательство

Пусть p_S вероятность того, что алгоритм запросил точки из множества $S \subset M$, $|S| = k$.

Нижняя оценка для вероятностных алгоритмов поиска

Теорема

Любой вероятностный алгоритм, решающий задачу поиска с вероятностью ошибки $< \varepsilon$, делает $\Omega(m)$ запросов.

Доказательство

Пусть p_S вероятность того, что алгоритм запросил точки из множества $S \subset M$, $|S| = k$.

Успех алгоритма означает, что $y \in S$.

Нижняя оценка для вероятностных алгоритмов поиска

Теорема

Любой вероятностный алгоритм, решающий задачу поиска с вероятностью ошибки $< \varepsilon$, делает $\Omega(m)$ запросов.

Доказательство

Пусть p_S вероятность того, что алгоритм запросил точки из множества $S \subset M$, $|S| = k$.

Успех алгоритма означает, что $y \in S$. Вероятность успеха:

$$p(y) = \sum_{S \ni y} p_S.$$

Нижняя оценка для вероятностных алгоритмов поиска

Теорема

Любой вероятностный алгоритм, решающий задачу поиска с вероятностью ошибки $< \varepsilon$, делает $\Omega(m)$ запросов.

Доказательство

Пусть p_S вероятность того, что алгоритм запросил точки из множества $S \subset M$, $|S| = k$.

Успех алгоритма означает, что $y \in S$. Вероятность успеха:

$$p(y) = \sum_{S \ni y} p_S.$$

Существует такое y, что $p(y) \leqslant k/m$. Действительно,

$$\frac{1}{m} \sum_y p(y) = \frac{1}{m} \sum_y \sum_{S \ni y} p_S = \frac{k \sum p_S}{m} = \frac{k}{m}.$$

Нижняя оценка для вероятностных алгоритмов поиска

Теорема

Любой вероятностный алгоритм, решающий задачу поиска с вероятностью ошибки $< \varepsilon$, делает $\Omega(m)$ запросов.

Доказательство

Вероятность успеха в худшем случае

$$p^* \leqslant \frac{k}{m}.$$

Если $p^* > 1 - \varepsilon$, то

$$1 - \varepsilon < p^* \leqslant \frac{k}{m},$$

значит,

$$k > (1 - \varepsilon)m, \quad \text{т. е. } k = \Omega(m).$$

Составляющие для алгоритма Гровера

- фазовый запрос $O_y : |x\rangle \mapsto (-1)^{\delta(y,x)}|x\rangle$;
- O_y — отражение относительно гиперплоскости, ортогональной $|y\rangle$;
- еще один оператор $R_\psi = 2|\psi\rangle\langle\psi| - I$, где $|\psi\rangle = \frac{1}{\sqrt{m}}\sum_x |x\rangle$;
- $R_\psi|\psi\rangle = |\psi\rangle$. Если $\langle\psi|\xi\rangle = 0$, то $R_\psi|\xi\rangle = -\xi$;
- R_ψ — симметрия относительно прямой, содержащей $|\psi\rangle$;
- итерация Гровера $G = R_\psi O_y$.

Составляющие для алгоритма Гровера

- фазовый запрос $O_y : |x\rangle \mapsto (-1)^{\delta(y,x)}|x\rangle$;
- O_y — отражение относительно гиперплоскости, ортогональной $|y\rangle$;
- еще один оператор $R_\psi = 2|\psi\rangle\langle\psi| - I$, где $|\psi\rangle = \frac{1}{\sqrt{m}}\sum_x |x\rangle$;
- $R_\psi|\psi\rangle = |\psi\rangle$. Если $\langle\psi|\xi\rangle = 0$, то $R_\psi|\xi\rangle = -\xi$;
- R_ψ — симметрия относительно прямой, содержащей $|\psi\rangle$;
- итерация Гровера $G = R_\psi O_y$.

Составляющие для алгоритма Гровера

- фазовый запрос $O_y : |x\rangle \mapsto (-1)^{\delta(y,x)}|x\rangle$;
- O_y — отражение относительно гиперплоскости, ортогональной $|y\rangle$;
- еще один оператор $R_\psi = 2|\psi\rangle\langle\psi| - I$, где $|\psi\rangle = \frac{1}{\sqrt{m}} \sum_x |x\rangle$;
- $R_\psi|\psi\rangle = |\psi\rangle$. Если $\langle\psi|\xi\rangle = 0$, то $R_\psi|\xi\rangle = -\xi$;
- R_ψ — симметрия относительно прямой, содержащей $|\psi\rangle$;
- итерация Гровера $G = R_\psi O_y$.

Составляющие для алгоритма Гровера

- фазовый запрос $O_y : |x\rangle \mapsto (-1)^{\delta(y,x)}|x\rangle$;
- O_y — отражение относительно гиперплоскости, ортогональной $|y\rangle$;
- еще один оператор $R_\psi = 2|\psi\rangle\langle\psi| - I$, где $|\psi\rangle = \frac{1}{\sqrt{m}} \sum_x |x\rangle$;
- $R_\psi|\psi\rangle = |\psi\rangle$. Если $\langle\psi|\xi\rangle = 0$, то $R_\psi|\xi\rangle = -\xi$;
- R_ψ — симметрия относительно прямой, содержащей $|\psi\rangle$;
- итерация Гровера $G = R_\psi O_y$.

Составляющие для алгоритма Гровера

- фазовый запрос $O_y : |x\rangle \mapsto (-1)^{\delta(y,x)}|x\rangle$;
- O_y — отражение относительно гиперплоскости, ортогональной $|y\rangle$;
- еще один оператор $R_\psi = 2|\psi\rangle\langle\psi| - I$, где $|\psi\rangle = \frac{1}{\sqrt{m}}\sum_x |x\rangle$;
- $R_\psi|\psi\rangle = |\psi\rangle$. Если $\langle\psi|\xi\rangle = 0$, то $R_\psi|\xi\rangle = -\xi$;
- R_ψ — симметрия относительно прямой, содержащей $|\psi\rangle$;
- итерация Гровера $G = R_\psi O_y$.

Составляющие для алгоритма Гровера

- фазовый запрос $O_y\colon |x\rangle \mapsto (-1)^{\delta(y,x)}|x\rangle$;
- O_y — отражение относительно гиперплоскости, ортогональной $|y\rangle$;
- еще один оператор $R_\psi = 2|\psi\rangle\langle\psi| - I$, где $|\psi\rangle = \frac{1}{\sqrt{m}}\sum_x |x\rangle$;
- $R_\psi|\psi\rangle = |\psi\rangle$. Если $\langle\psi|\xi\rangle = 0$, то $R_\psi|\xi\rangle = -\xi$;
- R_ψ — симметрия относительно прямой, содержащей $|\psi\rangle$;
- итерация Гровера $G = R_\psi O_y$.

Квантовый алгоритм для решения задачи поиска

Алгоритм Гровера

1. Приготавливаем состояние $|0\rangle$.
2. Преобразуем состояние $|0\rangle$ в $|\psi\rangle = \frac{1}{\sqrt{m}} \sum_x |x\rangle$.
3. Применяем $\lfloor (\pi/4)\sqrt{m} \rfloor$ раз оператор G.
4. Измеряем полученное состояние в классическом базисе.
5. Ответ: результат измерения.

Теорема

Число запросов в алгоритме Гровера $O(\sqrt{m})$.
Вероятность ошибки $O(1/m)$.

Квантовый алгоритм для решения задачи поиска

Алгоритм Гровера

1. Приготавливаем состояние $|0\rangle$.
2. Преобразуем состояние $|0\rangle$ в $|\psi\rangle = \frac{1}{\sqrt{m}} \sum_x |x\rangle$.
3. Применяем $\lfloor (\pi/4)\sqrt{m} \rfloor$ раз оператор G.
4. Измеряем полученное состояние в классическом базисе.
5. Ответ: результат измерения.

Теорема

Число запросов в алгоритме Гровера $O(\sqrt{m})$.
Вероятность ошибки $O(1/m)$.

Квантовый алгоритм для решения задачи поиска

Алгоритм Гровера

1. Приготавливаем состояние $|0\rangle$.
2. Преобразуем состояние $|0\rangle$ в $|\psi\rangle = \frac{1}{\sqrt{m}} \sum_x |x\rangle$.
3. Применяем $\lfloor (\pi/4)\sqrt{m} \rfloor$ раз оператор G.
4. Измеряем полученное состояние в классическом базисе.
5. Ответ: результат измерения.

Теорема

Число запросов в алгоритме Гровера $O(\sqrt{m})$.
Вероятность ошибки $O(1/m)$.

Квантовый алгоритм для решения задачи поиска

Алгоритм Гровера

1. Приготавливаем состояние $|0\rangle$.
2. Преобразуем состояние $|0\rangle$ в $|\psi\rangle = \frac{1}{\sqrt{m}} \sum_x |x\rangle$.
3. Применяем $\lfloor (\pi/4)\sqrt{m} \rfloor$ раз оператор G.
4. Измеряем полученное состояние в классическом базисе.
5. Ответ: результат измерения.

Теорема

Число запросов в алгоритме Гровера $O(\sqrt{m})$.
Вероятность ошибки $O(1/m)$.

Квантовый алгоритм для решения задачи поиска

Алгоритм Гровера

1. Приготавливаем состояние $|0\rangle$.
2. Преобразуем состояние $|0\rangle$ в $|\psi\rangle = \frac{1}{\sqrt{m}} \sum_x |x\rangle$.
3. Применяем $\lfloor (\pi/4)\sqrt{m} \rfloor$ раз оператор G.
4. Измеряем полученное состояние в классическом базисе.
5. Ответ: результат измерения.

Теорема

Число запросов в алгоритме Гровера $O(\sqrt{m})$.
Вероятность ошибки $O(1/m)$.

Квантовый алгоритм для решения задачи поиска

Алгоритм Гровера

1. Приготавливаем состояние $|0\rangle$.
2. Преобразуем состояние $|0\rangle$ в $|\psi\rangle = \frac{1}{\sqrt{m}} \sum_x |x\rangle$.
3. Применяем $\lfloor (\pi/4)\sqrt{m} \rfloor$ раз оператор G.
4. Измеряем полученное состояние в классическом базисе.
5. Ответ: результат измерения.

Теорема

Число запросов в алгоритме Гровера $O(\sqrt{m})$.
Вероятность ошибки $O(1/m)$.

Итерация Гровера как поворот в плоскости

$$G\colon \mathbb{C}(|y\rangle, |\psi\rangle) \to \mathbb{C}(|y\rangle, |\psi\rangle)$$

$$\sin\vartheta = \langle\psi|y\rangle = \frac{1}{\sqrt{m}}\,,$$

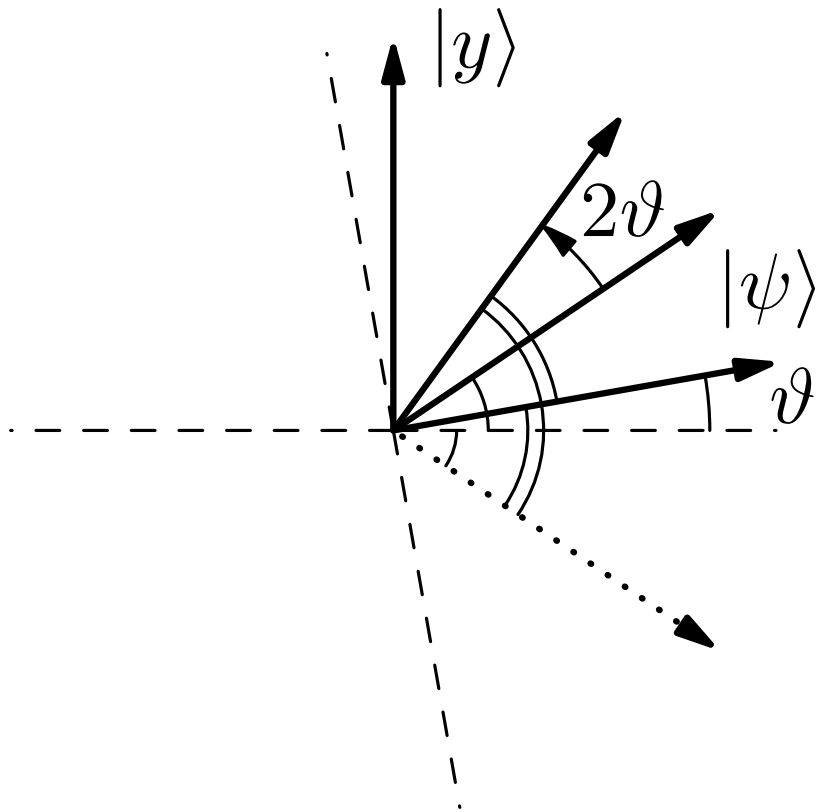
$$\vartheta = \frac{1}{\sqrt{m}} + o(m^{-1}).$$

Вектор состояния поворачивается в направлении $|y\rangle$ на угол $\sim 2/\sqrt{m}$ за итерацию.

Начальный угол почти прямой.

После $k = \lfloor (\pi/4)\sqrt{m} \rfloor$ итераций угол станет $O(1/\sqrt{m})$.

Вероятность ошибки: квадрат синуса угла, т. е. $O(1/m)$.

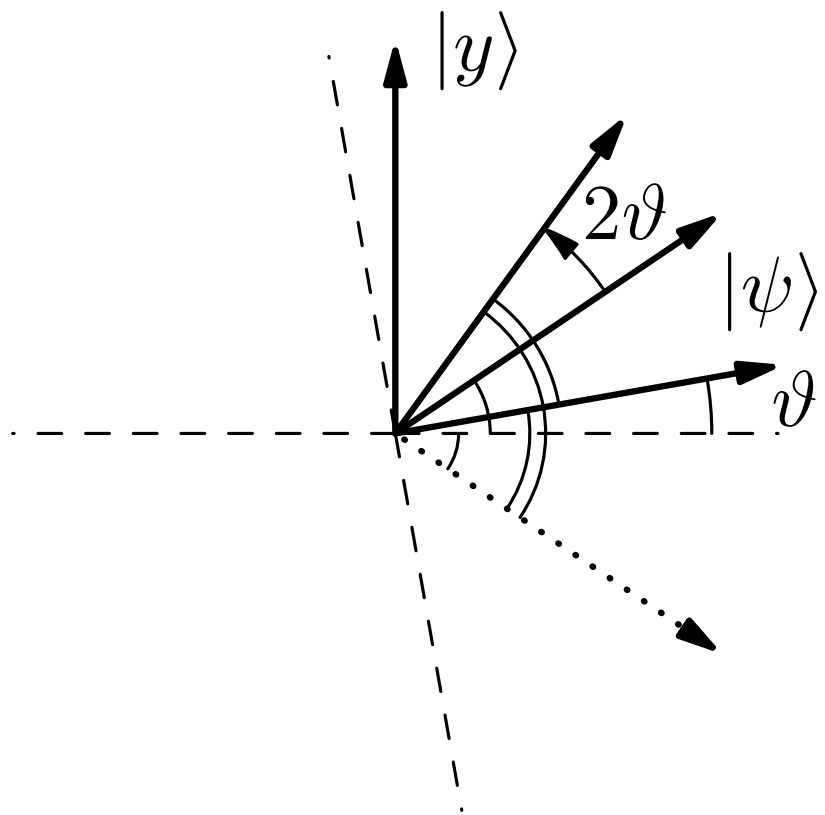


Итерация Гровера как поворот в плоскости

$$G\colon \mathbb{C}(|y\rangle, |\psi\rangle) \to \mathbb{C}(|y\rangle, |\psi\rangle)$$

$$\sin\vartheta = \langle\psi|y\rangle = \frac{1}{\sqrt{m}}\,,$$

$$\vartheta = \frac{1}{\sqrt{m}} + o(m^{-1}).$$



Вектор состояния поворачивается в направлении $|y\rangle$ на угол $\sim 2/\sqrt{m}$ за итерацию.

Начальный угол почти прямой.

После $k = \lfloor(\pi/4)\sqrt{m}\rfloor$ итераций угол станет $O(1/\sqrt{m})$.

Вероятность ошибки: квадрат синуса угла, т. е. $O(1/m)$.

Итерация Гровера как поворот в плоскости

$$G\colon \mathbb{C}(|y\rangle, |\psi\rangle) \to \mathbb{C}(|y\rangle, |\psi\rangle)$$

$$\sin\vartheta = \langle\psi|y\rangle = \frac{1}{\sqrt{m}}\,,$$

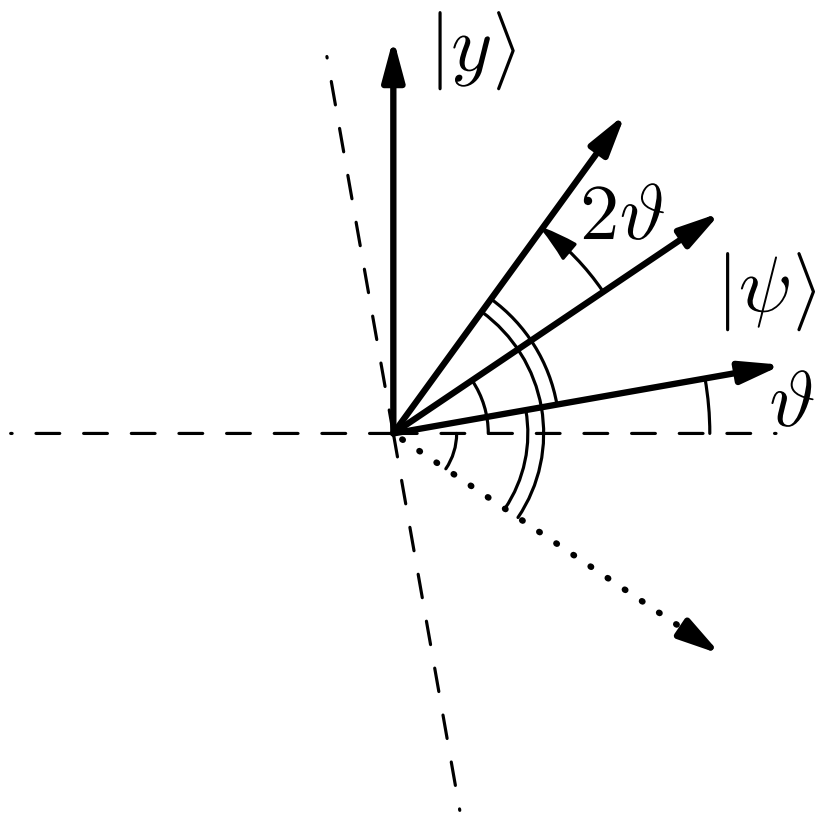
$$\vartheta = \frac{1}{\sqrt{m}} + o(m^{-1}).$$

Вектор состояния поворачивается в направлении $|y\rangle$ на угол $\sim 2/\sqrt{m}$ за итерацию.

Начальный угол почти прямой.

После $k = \lfloor (\pi/4)\sqrt{m} \rfloor$ итераций угол станет $O(1/\sqrt{m})$.

Вероятность ошибки: квадрат синуса угла, т. е. $O(1/m)$.

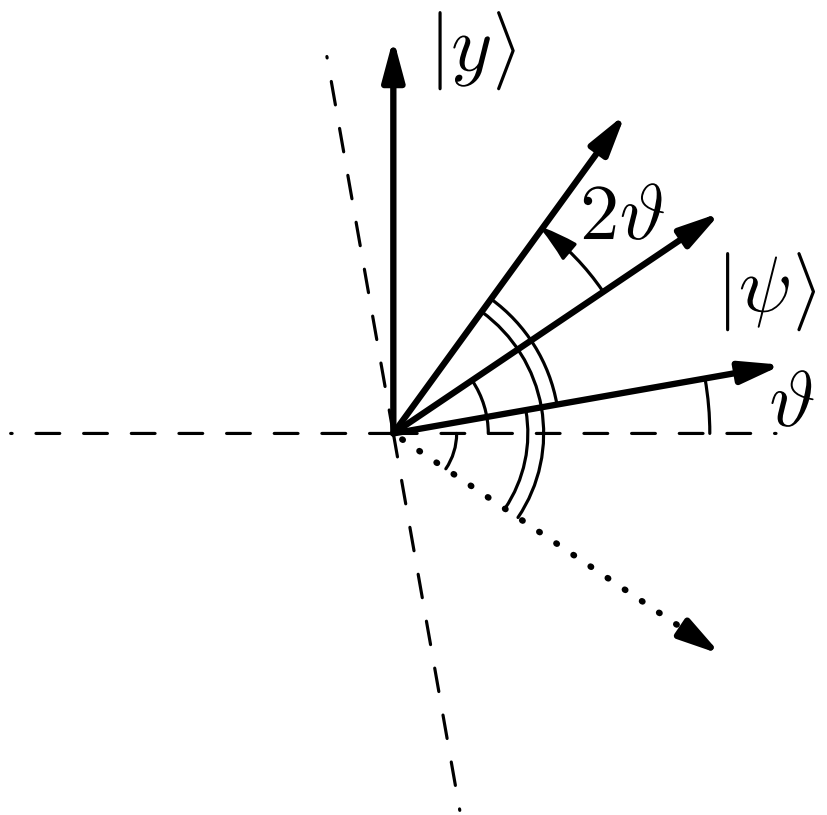


Итерация Гровера как поворот в плоскости

$$G\colon \mathbb{C}(|y\rangle, |\psi\rangle) \to \mathbb{C}(|y\rangle, |\psi\rangle)$$

$$\sin\vartheta = \langle\psi|y\rangle = \frac{1}{\sqrt{m}}\,,$$

$$\vartheta = \frac{1}{\sqrt{m}} + o(m^{-1}).$$



Вектор состояния поворачивается в направлении $|y\rangle$ на угол $\sim 2/\sqrt{m}$ за итерацию.

Начальный угол почти прямой.

После $k = \lfloor(\pi/4)\sqrt{m}\rfloor$ итераций угол станет $O(1/\sqrt{m})$.

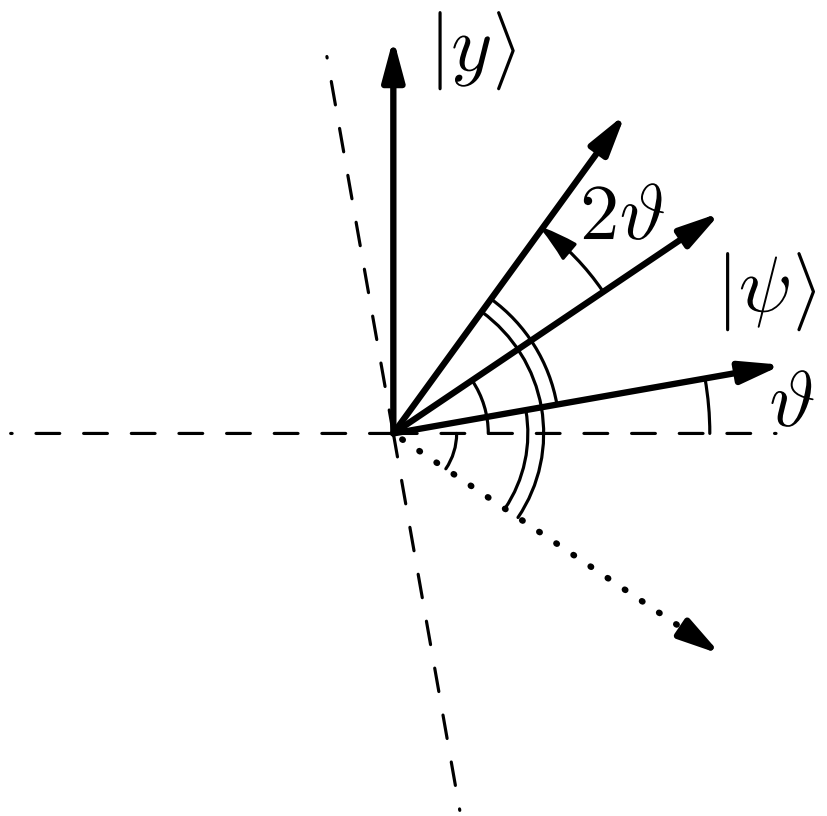
Вероятность ошибки: квадрат синуса угла, т. е. $O(1/m)$.

Итерация Гровера как поворот в плоскости

$$G\colon \mathbb{C}(|y\rangle, |\psi\rangle) \to \mathbb{C}(|y\rangle, |\psi\rangle)$$

$$\sin\vartheta = \langle\psi|y\rangle = \frac{1}{\sqrt{m}}\,,$$

$$\vartheta = \frac{1}{\sqrt{m}} + o(m^{-1}).$$



Вектор состояния поворачивается в направлении $|y\rangle$ на угол $\sim 2/\sqrt{m}$ за итерацию.

Начальный угол почти прямой.

После $k = \lfloor(\pi/4)\sqrt{m}\rfloor$ итераций угол станет $O(1/\sqrt{m})$.

Вероятность ошибки: квадрат синуса угла, т. е. $O(1/m)$.