Алгоритм Гровера

Квантовые вычисления–2023

24 октября 2023 г.

Outline

Пределы роста

Примеры успеха

Задача	Квантовый	Классический
Дойча-Йожи	$O(1)$	$\Omega(2^n)$
Саймона	$O(n)$	$\Omega(2^{n/2})$

Пределы роста

Примеры успеха

Задача	Квантовый	Классический
Дойча-Йожи	$O(1)$	$\Omega(2^n)$
Саймона	$O(n)$	$\Omega(2^{n/2})$

Вопрос

Любую ли задачу можно решить экспоненциально быстрее?

Задача поиска в неупорядоченной БД

Условие задачи

- В БД есть N записей

Задача поиска в неупорядоченной БД

Условие задачи

- В БД есть N записей
- Требуется найти конкретную запись

Задача поиска в неупорядоченной БД

Условие задачи

- В БД есть N записей
- Требуется найти конкретную запись
- Больше никакой информации нет.

Задача поиска в неупорядоченной БД

Условие задачи

- В БД есть N записей
- Требуется найти конкретную запись
- Больше никакой информации нет.

Задача поиска в неупорядоченной БД

Условие задачи

- В БД есть N записей
- Требуется найти конкретную запись
- Больше никакой информации нет.

Интерфейс БД

- классическая f возвращает «подходит / не подходит»

Задача поиска в неупорядоченной БД

Условие задачи

- В БД есть N записей
- Требуется найти конкретную запись
- Больше никакой информации нет.

Интерфейс БД

- классическая f возвращает «подходит / не подходит»
- квантовый оракул U_f

Классическое решение

???

Классическое решение

???

- N запросов к базе

Квантовое решение - интерфейс

- оракул меняет фазу нужной записи

Квантовое решение - интерфейс

- оракул меняет фазу нужной записи
- если нужный индекс $\omega \in \{0, 1, \ldots, N-1\}$:

$$U_\omega |x\rangle = -|x\rangle, \quad x = \omega$$

$$U_\omega |x\rangle = |x\rangle, \quad x \neq \omega$$

Квантовое решение - идея

- итеративное решение;

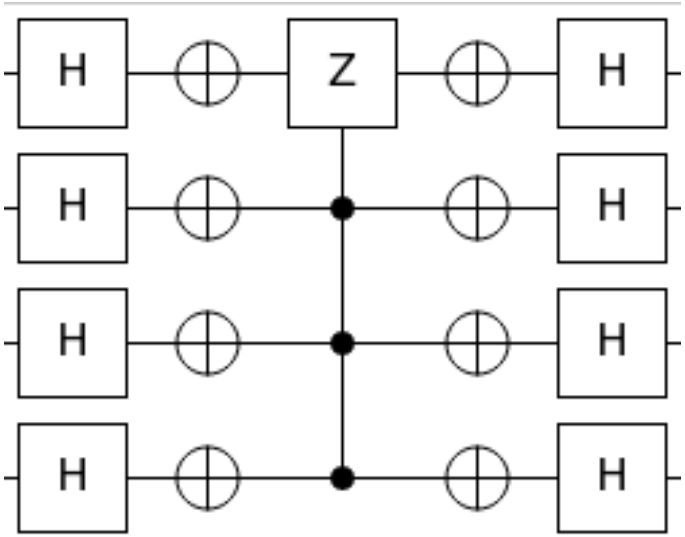
Квантовое решение - идея

- итеративное решение;
- начинаем с наиболее запутанного состояния;

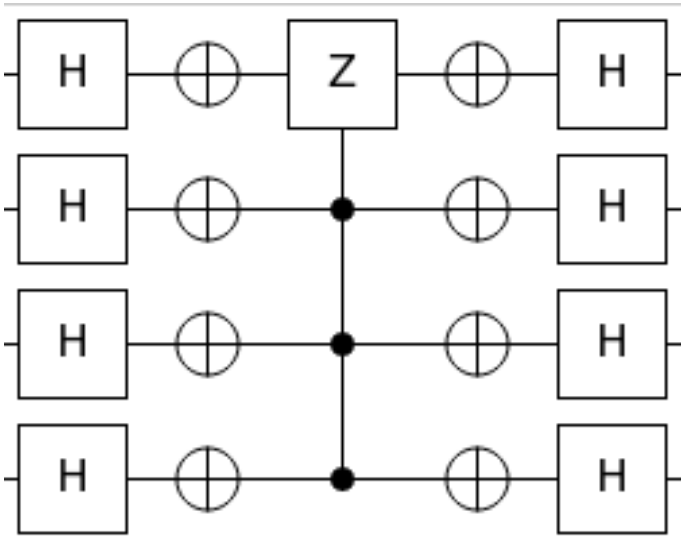
Квантовое решение - идея

- итеративное решение;
- начинаем с наиболее запутанного состояния;
- на каждом шаге: U_ω и оператор Гровера.

Оператор Гровера

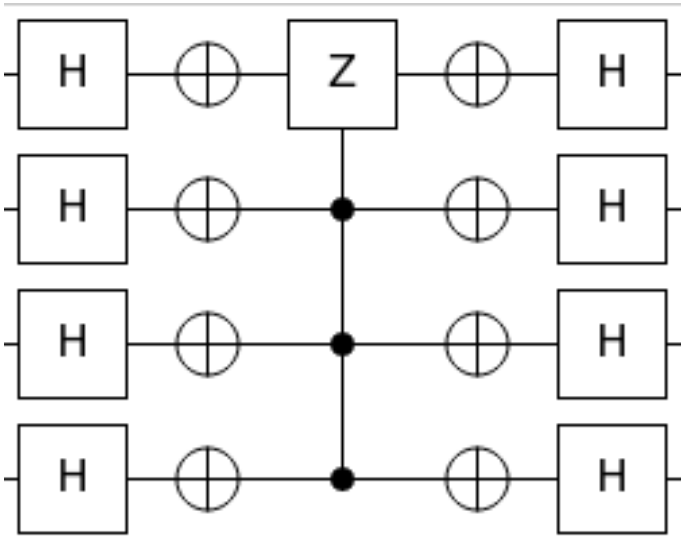


Оператор Гровера



- гейты Адамара $H^{\otimes n}$,

Оператор Гровера

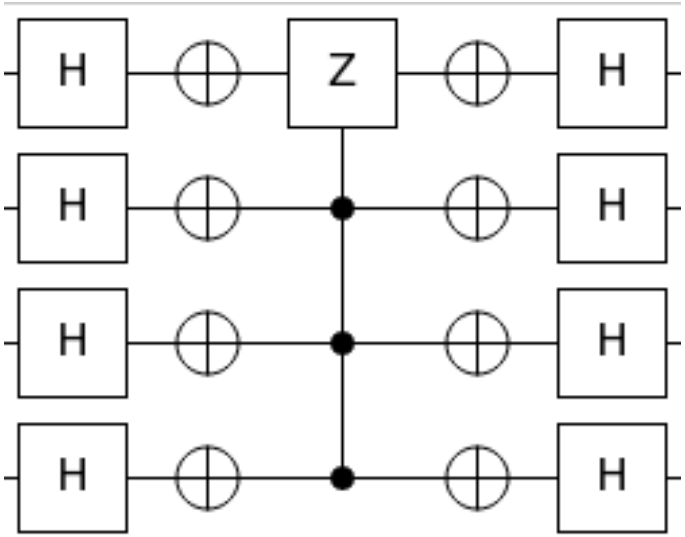


- гейты Адамара $H^{\otimes n}$,
- условный сдвиг фазы:

$$|0\rangle \mapsto -|0\rangle$$

$$|x\rangle \mapsto |x\rangle, \quad x \neq 0$$

Оператор Гровера



- гейты Адамара $H^{\otimes n}$,
- условный сдвиг фазы:

$$|0\rangle \mapsto -|0\rangle$$

$$|x\rangle \mapsto |x\rangle, \quad x \neq 0$$

- гейты Адамара $H^{\otimes n}$.

Отражение относительно среднего

- амплитуда отмеченного состояния увеличивается!

Отражение относительно среднего

- амплитуда отмеченного состояния увеличивается!
- пусть вначале все одинаковы:

Отражение относительно среднего

- амплитуда отмеченного состояния увеличивается!
- пусть вначале все одинаковы:
- $(1/2, 1/2, 1/2, 1/2)$

Отражение относительно среднего

- амплитуда отмеченного состояния увеличивается!
- пусть вначале все одинаковы:
- $(1/2, 1/2, 1/2, 1/2)$
- отметим базисное состояние 1:

Отражение относительно среднего

- амплитуда отмеченного состояния увеличивается!
- пусть вначале все одинаковы:
- $(1/2, 1/2, 1/2, 1/2)$
- отметим базисное состояние 1:
- $(1/2, -1/2, 1/2, 1/2)$ (среднее — $1/4$)

Отражение относительно среднего

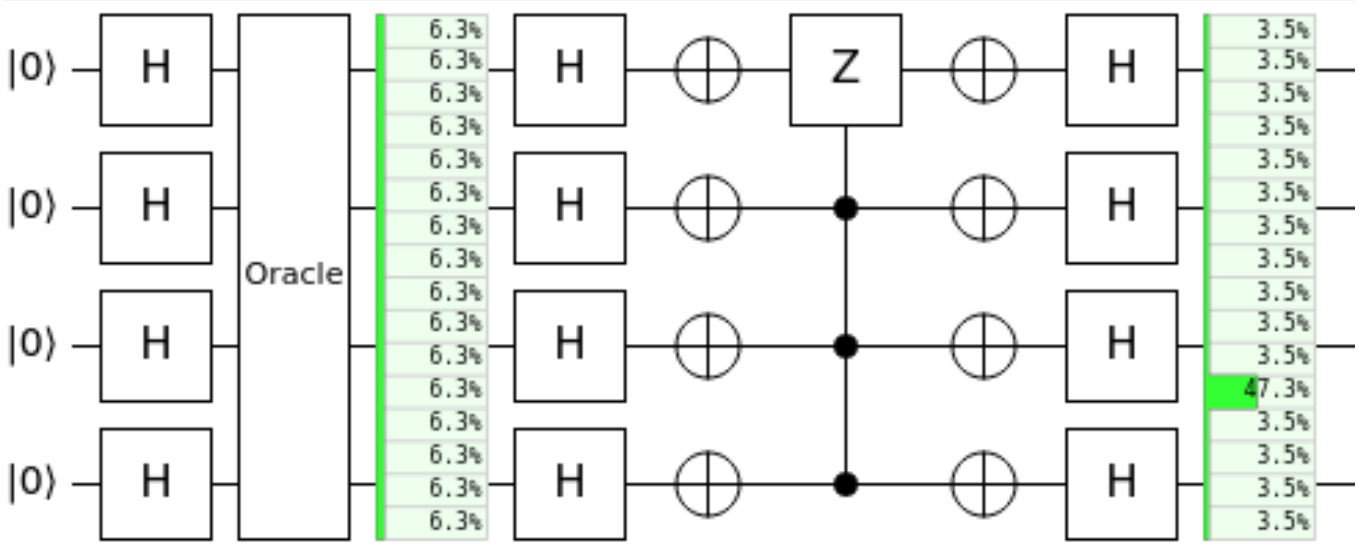
- амплитуда отмеченного состояния увеличивается!
- пусть вначале все одинаковы:
- $(1/2, 1/2, 1/2, 1/2)$
- отметим базисное состояние 1:
- $(1/2, -1/2, 1/2, 1/2)$ (среднее — $1/4$)
- отражаем относительно среднего:

Отражение относительно среднего

- амплитуда отмеченного состояния увеличивается!
- пусть вначале все одинаковы:
- $(1/2, 1/2, 1/2, 1/2)$
- отметим базисное состояние 1:
- $(1/2, -1/2, 1/2, 1/2)$ (среднее — $1/4$)
- отражаем относительно среднего:
- $(0, 1, 0, 0)$

Отражение относительно среднего

- амплитуда отмеченного состояния увеличивается!
- пусть вначале все одинаковы:
- $(1/2, 1/2, 1/2, 1/2)$
- отметим базисное состояние 1:
- $(1/2, -1/2, 1/2, 1/2)$ (среднее — $1/4$)
- отражаем относительно среднего:
- $(0, 1, 0, 0)$
- вероятность «попасть» в искомое состояние растёт:



Количество итераций

Сколько нужно итераций?

- представим всё пространство состояний как плоскость

Количество итераций

Сколько нужно итераций?

- представим всё пространство состояний как плоскость
- одна ось — искомое состояние ω

Количество итераций

Сколько нужно итераций?

- представим всё пространство состояний как плоскость
- одна ось — искомое состояние ω
- другая — все остальные состояния β.

Количество итераций

Сколько нужно итераций?

- представим всё пространство состояний как плоскость
- одна ось — искомое состояние ω
- другая — все остальные состояния β.

Количество итераций

Сколько нужно итераций?

- представим всё пространство состояний как плоскость
- одна ось — искомое состояние ω
- другая — все остальные состояния β.

Произвольное состояние ψ

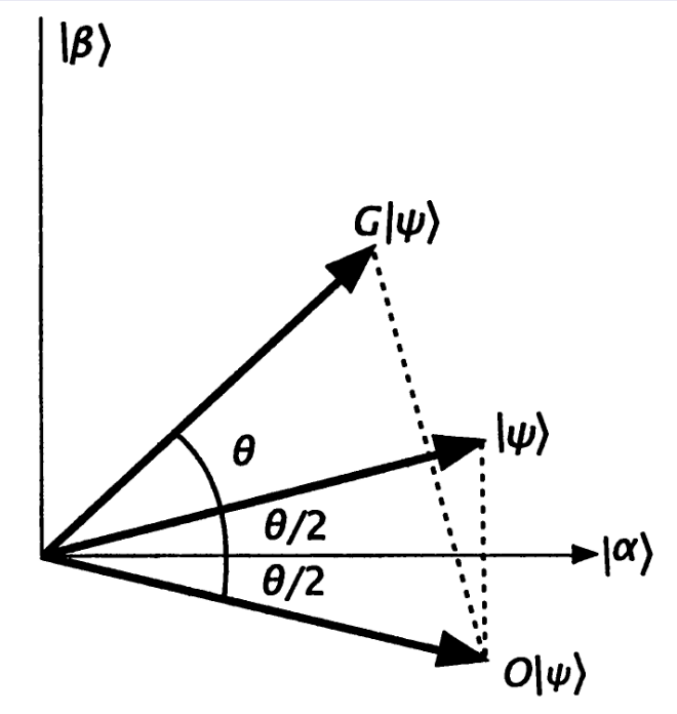
$$|\psi\rangle = \sum_{x=0}^{N-1} \alpha_x |i\rangle = \alpha_\omega |\omega\rangle + \sum_{x \neq \omega} \alpha_x |x\rangle = \alpha_\omega |\omega\rangle + b|\beta\rangle,$$

$$|\beta\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \neq \omega} |x\rangle.$$

Геометрия алгоритма Гровера

Одна итерация

Текущее ψ поворачивается в сторону ω на угол θ:



$$\theta = 2 \arcsin \frac{1}{\sqrt{N}}$$

Несколько итераций

Нужное количество итераций

$\frac{\pi\sqrt{N}}{4} = O(\sqrt{N})$

Несколько итераций

Нужное количество итераций

$\frac{\pi\sqrt{N}}{4} = O(\sqrt{N})$

Нижняя оценка

Любой квантовый алгоритм с оракулом U_ω, требует $\Omega(\sqrt{N})$ запросов

Количество решений больше одного

Несколько решений

- несколько решений и известно их число M

Количество решений больше одного

Несколько решений

- несколько решений и известно их число M
- количество итераций:

$$\frac{\pi}{4}\sqrt{\frac{N}{M}}$$

Количество решений больше одного

Несколько решений

- несколько решений и известно их число M
- количество итераций:

$$\frac{\pi}{4}\sqrt{\frac{N}{M}}$$

Количество решений больше одного

Несколько решений

- несколько решений и известно их число M
- количество итераций:

$$\frac{\pi}{4}\sqrt{\frac{N}{M}}$$

Неизвестное количество решений

- оценить количество решений при помощи квантового алгоритма подсчёта

Количество решений больше одного

Несколько решений

- несколько решений и известно их число M
- количество итераций:

$$\frac{\pi}{4}\sqrt{\frac{N}{M}}$$

Неизвестное количество решений

- оценить количество решений при помощи квантового алгоритма подсчёта
- выполнить поиск Гровера для этого количества

Количество решений больше одного

Несколько решений

- несколько решений и известно их число M
- количество итераций:

$$\frac{\pi}{4}\sqrt{\frac{N}{M}}$$

Неизвестное количество решений

- оценить количество решений при помощи квантового алгоритма подсчёта
- выполнить поиск Гровера для этого количества
- $O(\sqrt{N})$

Другой взгляд на алгоритм

Удовлетворение ограничений

- Алгоритм Гровера — поиск решения $f(x) = 1$

Другой взгляд на алгоритм

Удовлетворение ограничений

- Алгоритм Гровера — поиск решения $f(x) = 1$
- или — задача удовлетворения ограничений

Другой взгляд на алгоритм

Удовлетворение ограничений

- Алгоритм Гровера — поиск решения $f(x) = 1$
- или — задача удовлетворения ограничений
- ограничения кодируются в оракуле, без квантовой памяти

Итог

Сравнение с классическими алгоритмами

- квантовый поиск в неупорядоченной БД — $\Theta(\sqrt{N})$;

Итог

Сравнение с классическими алгоритмами

- квантовый поиск в неупорядоченной БД — $\Theta(\sqrt{N})$;
- (классический - $\Theta(N)$);

Итог

Сравнение с классическими алгоритмами

- квантовый поиск в неупорядоченной БД — $\Theta(\sqrt{N})$;
- (классический - $\Theta(N)$);
- без структуры в задаче нельзя получить экспоненциальное ускорение;

Итог

Сравнение с классическими алгоритмами

- квантовый поиск в неупорядоченной БД — $\Theta(\sqrt{N})$;
- (классический - $\Theta(N)$);
- без структуры в задаче нельзя получить экспоненциальное ускорение;
- только не более, чем полиномиальное.

Итог

Сравнение с классическими алгоритмами

- квантовый поиск в неупорядоченной БД — $\Theta(\sqrt{N})$;
- (классический - $\Theta(N)$);
- без структуры в задаче нельзя получить экспоненциальное ускорение;
- только не более, чем полиномиальное.

Итог

Сравнение с классическими алгоритмами

- квантовый поиск в неупорядоченной БД — $\Theta(\sqrt{N})$;
- (классический - $\Theta(N)$);
- без структуры в задаче нельзя получить экспоненциальное ускорение;
- только не более, чем полиномиальное.

Модификации

- можно модифицировать для поиска нескольких решений;

Итог

Сравнение с классическими алгоритмами

- квантовый поиск в неупорядоченной БД — $\Theta(\sqrt{N})$;
- (классический - $\Theta(N)$);
- без структуры в задаче нельзя получить экспоненциальное ускорение;
- только не более, чем полиномиальное.

Модификации

- можно модифицировать для поиска нескольких решений;
- можно рассматривать как решение уравнения или удовлетворение ограничений.