

Оракулы и их построение

Квантовые вычисления–2023

3 октября 2023 г.

Outline

- 1 Оракулы
- 2 Теорема о запрете клонирования
- 3 Реализация классических функций
- 4 Uncomputation

Что такое оракул?



- кодирование входных данных

Что такое оракул?



- кодирование входных данных
- с возможностью получения суперпозиции

Что такое оракул?



- кодирование входных данных
- с возможностью получения суперпозиции
- оракул для функции $f : \{0, 1\}^n \rightarrow \{0, 1\}$ — гейт, который помечает входные наборы

Что такое оракул?



- кодирование входных данных
- с возможностью получения суперпозиции
- оракул для функции $f : \{0, 1\}^n \rightarrow \{0, 1\}$ — гейт, который помечает входные наборы
- несколько бит на выходе — несколько оракулов

Два способа кодирования

Кодирование в фазе

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

Два способа кодирования

Кодирование в фазе

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

Кодирование вспомогательным кубитом

Ancilla — вспомогательный кубит в состоянии $|0\rangle$ (его нужно вернуть в исходном состоянии)

$$|x\rangle|y\rangle \mapsto |x\rangle|y \oplus f(x)\rangle.$$

Преобразование способов друг в друга

- Оракул O_2 кодирует функцию в ancilla.

Преобразование способов друг в друга

- Оракул O_2 кодирует функцию в ancilla.
- Построим оракул O_1 : применим O_2 к

$$|x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Можно ли копировать кубиты?

- Зачем нужен вспомогательный кубит?

Можно ли копировать кубиты?

- Зачем нужен вспомогательный кубит?
- Предположим, существует U_{copy} :

$$U_{copy}|x\rangle|y\rangle = |x\rangle|x\rangle.$$

Можно ли копировать кубиты?

- Зачем нужен вспомогательный кубит?
- Предположим, существует U_{copy} :

$$U_{copy}|x\rangle|y\rangle = |x\rangle|x\rangle.$$

- Оно копирует произвольные состояния — можно получить *всю* информацию из них.

Можно ли копировать кубиты? — Нет!

Theorem (Запрет клонирования)

Не существует унитарного оператора U , такого, что для любых состояний ϕ и e

$$U(|\phi\rangle \otimes |e\rangle) = e^{i\alpha(\phi,e)}|\phi\rangle \otimes |\phi\rangle,$$

где $\alpha(\phi, e)$ — вещественное число, зависящее только от ϕ и e .

Можно ли копировать кубиты? — Нет!

Доказательство.

- Допустим, $U = U_{copy}$ существует.



Можно ли копировать кубиты? — Нет!

Доказательство.

- Допустим, $U = U_{copy}$ существует.
- Рассмотрим произвольные ϕ и ψ :

$$\begin{aligned}\langle \phi | \psi \rangle \langle e | e \rangle &= \langle \phi | \langle e | e \rangle | \psi \rangle = \langle \phi | \langle e | U^\dagger U | e \rangle | \psi \rangle = \\ &= e^{i\alpha(\psi, e) - i\alpha(\phi, e)} \langle \phi | \langle \phi | \psi \rangle | \psi \rangle = e^{i\alpha(\psi, e) - i\alpha(\phi, e)} (\langle \phi | \psi \rangle)^2.\end{aligned}$$



Можно ли копировать кубиты? — Нет!

Доказательство.

- Допустим, $U = U_{copy}$ существует.
- Рассмотрим произвольные ϕ и ψ :

$$\begin{aligned}\langle \phi | \psi \rangle \langle e | e \rangle &= \langle \phi | \langle e | e \rangle | \psi \rangle = \langle \phi | \langle e | U^\dagger U | e \rangle | \psi \rangle = \\ &= e^{i\alpha(\psi, e) - i\alpha(\phi, e)} \langle \phi | \langle \phi | \psi \rangle | \psi \rangle = e^{i\alpha(\psi, e) - i\alpha(\phi, e)} (\langle \phi | \psi \rangle)^2.\end{aligned}$$

- Получаем, что

$$|\langle \phi | \psi \rangle| = |\langle \phi | \psi \rangle|^2.$$



Можно ли копировать кубиты? — Нет!

Доказательство.

- Допустим, $U = U_{copy}$ существует.
- Рассмотрим произвольные ϕ и ψ :

$$\begin{aligned}\langle \phi | \psi \rangle \langle e | e \rangle &= \langle \phi | \langle e | e \rangle | \psi \rangle = \langle \phi | \langle e | U^\dagger U | e \rangle | \psi \rangle = \\ &= e^{i\alpha(\psi, e) - i\alpha(\phi, e)} \langle \phi | \langle \phi | \psi \rangle | \psi \rangle = e^{i\alpha(\psi, e) - i\alpha(\phi, e)} (\langle \phi | \psi \rangle)^2.\end{aligned}$$

- Получаем, что

$$|\langle \phi | \psi \rangle| = |\langle \phi | \psi \rangle|^2.$$

- Тогда это либо 0, либо 1. Противоречие!



Пример кодирования оракула

Оракул

- На вход подаются числа от 0 до 15.
- Помечает элемент 11 (в двоичной системе $11_{10} = 1011_2$).
- Мы считаем, что старшие биты находятся сверху, а младшие снизу.

Пример кодирования оракула

Оракул

- На вход подаются числа от 0 до 15.
- Помечает элемент 11 (в двоичной системе $11_{10} = 1011_2$).
- Мы считаем, что старшие биты находятся сверху, а младшие снизу.

Реализация U_{11}

$$U_{11}|10110\rangle = |10111\rangle,$$

$$U_{11}|10111\rangle = |10110\rangle.$$

Обратимые функции

- Любую булеву функцию можно задать, используя схемы из «И», «ИЛИ», «НЕ»
- Чтобы квантовая схема могла вычислить классическую L , достаточно, чтобы эта функция была обратимой.

Обратимые функции

- Любую булеву функцию можно задать, используя схемы из «И», «ИЛИ», «НЕ»
- Чтобы квантовая схема могла вычислить классическую L , достаточно, чтобы эта функция была обратимой.

Definition (Обратимая функция)

Функция $L : \{0, 1\}^n \rightarrow \{0, 1\}^m$ — обратимая, если $\exists L' : \{0, 1\}^m \rightarrow \{0, 1\}^n$ такая, что $\forall x$ выполняется: если $L(x) = y$, то $L'(y) = x$.
Функция L' — обратная для L .

Универсальные классические гейты

Использование вспомогательных кубитов

Произвольную f можно преобразовать в обратимую F , если использовать вспомогательный вход: $F(x, y) = (x, y \oplus f(x))$.

Универсальные классические гейты

Использование вспомогательных кубитов

Произвольную f можно преобразовать в обратимую F , если использовать вспомогательный вход: $F(x, y) = (x, y \oplus f(x))$.

Универсальные гейты

Произвольную обратимую функцию можно построить из гейтов Тоффоли (гейтов CCNOT) и вспомогательных входных битов. Гейт Тоффоли является универсальным гейтом.

Гейт Фредкина — гейт Controlled-SWAP — тоже универсальный.

Реализация C^5NOT

Восстановление вспомогательных кубитов

- После использования ancilla нужно вернуть в исходное состояние
- Как это сделать?

Восстановление вспомогательных кубитов

- После использования ancilla нужно вернуть в исходное состояние
- Как это сделать?

