Курс МФТИ-МИАН «Квантовые вычисления», Весна 2024. Лекция 12: Алгоритм поиска в неупорядоченной базе данных, преобразование Фурье.

Яшин Всеволод Игоревич (yashin.vi@mi-ras.ru)

На этой Лекции мы поговорили об алгоритме Гровера и о реализации преобразования Фурье квантовыми схемами. Алгоритм Гровера позволяет решить проблему нахождения элемента в неупорядоченной базе данных. Решение этой проблемы с использованием возможностей квантовой механики даёт квадратичное преимущество относительно классического решения этой задачи. При помощи элементов вида $C\mathrm{NOT}+U(2)$ можно реализовать преобразование Фурье над абелевой группой $\mathbb{Z}_{2^n}$. При помощи такого преобразования Фурье можно приближённо решать задачу оценки фазы, возникаемой при действии унитарного преобразования на собственный вектор. Благодаря алгоритму оценки фазы получается реализовать преобразование Фурье над произвольной конечно абелевой группой.

Литература к Лекции: [1–3].

Задача 1

На Лекции мы рассмотрели случай, когда алгоритм Гровера применяется для нахождения *единственного* решения $x_0 \in \{0, \dots, N-1\}$. Как будет работать алгоритм Гровера в случае, если решений множество? Допустим, дана неупорядоченная база данных $N = 2^n$ с числом некоторым множеством решений $A \subseteq \{0, \dots, N-1\}$. Функция f определена как

$$f(x) = \begin{cases} 1, & x \in A, \\ 0, & \text{иначе.} \end{cases} \tag{1}$$

Покажите, что для нахождения какого-то решения простейшим классическим алгоритмом потребуется $\mathcal{O}(N/|A|)$ обращений к оракулу.

Покажите, что при решении этой задачи алгоритмом Гровера потребуется $\mathcal{O}(\sqrt{N/|A|})$ обращений к оракулу. При решении задачи модет быть полезно воспользоваться обозначениями

$$|A\rangle = \frac{1}{\sqrt{|A|}} \sum_{x\in A} |x\rangle, \qquad |B\rangle = \frac{1}{\sqrt{N-|A|}} \sum_{x\notin A} |x\rangle. \tag{2}$$

(Работа алгоритма Гровера может быть визаулизирована геометрически в плоскости $\{|A\rangle, |B\rangle\}$.) Как работает алгоритм Гровера, если решений нет?

Задача 2

Одно из вожможный применений алгоритма Гровера – решение задачи раскраски графа. Допустим, что задан некоторый граф G и некоторое натуральное число k. Задачей раскраски графа называется задача нахождения такой раскраски вершин в k цветов, чтобы соседние вершины графа не имели одинакого цвета. Как решить эту задачу при помощи алгоритма Гровера? Сколько при решении понадобится кубитов? Сколько времени будет работать алгоритм?

Задача 3

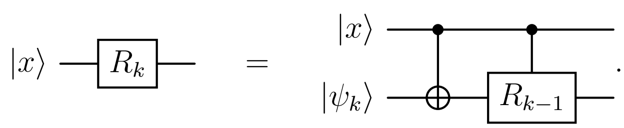
В работе [4] была предложена усовершенствованная схема для квантового преобразования Фурье, она использует технику каталитических вложений. Рассмотрим вращения вида

$$R_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix} \tag{3}$$

и состояния на одном кубите вида

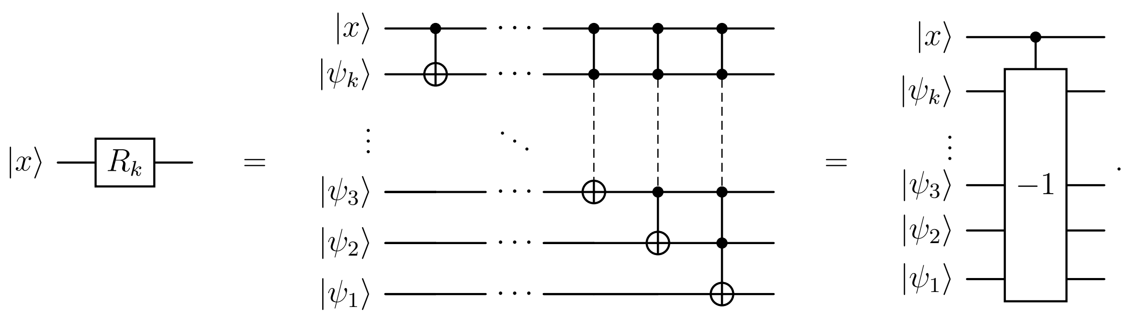
$$|\psi_k\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i/2^k}|1\rangle). \tag{4}$$

Покажите, что для реализации поворота R_k можно использовать CR_{k-1} и состояние $|\psi_k\rangle$ в качестве катализатора, то есть верна схема



(5)

В таком случае, поворот на R_k также можно переписать при помощи приготовления состояния $|\psi_1\rangle \cdots |\psi_k\rangle$ и вентилей C^jX как



(6)

Здесь обозначение "-1" используется потому, что предлагаемая операция отнимает единицу от бинарной записи числа. Как выглядит преобразование Фурье, выписанное в таком виде? Покажите, что если выбрать точность $\varepsilon > 0$ и убрать все $|\psi_k\rangle$ с малыми вращениями, то потребуется $\mathcal{O}(n \log n)$ вентилей вида C^jX. Покажите, что чтобы совершить обратное преобразование Фурье, достаточно подействовать на состояния вида $|\psi_k\rangle$ вентилями X и повторить схему.

---

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition* (Cambridge University Press, 2010).

[2] L. K. Grover, Quantum mechanics helps in searching for a needle in a haystack, Physical review letters **79**, 325 (1997).

[3] A. M. Childs and W. Van Dam, Quantum algorithms for algebraic problems, Reviews of Modern Physics **82**, 1 (2010).

[4] M. Amy, M. Crawford, A. N. Glaudell, M. L. Macasieb, S. S. Mendelson, and N. J. Ross, Catalytic embeddings of quantum circuits (2023), arXiv:2305.07720 [quant-ph].