Курс МФТИ-МИАН «Квантовые вычисления», Весна 2025.

Задачи III: Квантовые алгоритмы

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

Здесь собраны задачи в дополнение к лекциям по курсу. На эти задачи полезно посмотреть, или даже решить. Когда в задаче написано "разребитесь в", подразумевается, что желательно выписать доказательство утверждения на бумаге. Решения можно обсудить с лектором очно или прислать оформленные задачи по почте. Работа над задачами примерно следующим образом влияет на итоговую оценку по курсу: если Вы совсем не решали задач, Вы не сможете претендовать на «отлично»; если Вы сдали все задачи, Вы не получите менее, чем «хорошо».

Третья серия задач посвящена изучению работы простейших квантовых алгоритмов.

Задача III.1

В стандартной задаче Бернштейна-Вазирани, оракул скрывает некоторую линейную функцию, вид которой требуется найти. Эту задачу можно несколько усовершенствовать, чтобы получить осмысленную задачу без чёрного ящика. Рассмотрим квадратичную форму $q : \mathbb{Z}_2^n \to \mathbb{Z}_4$ (обратите внимание на область значений) вида

$$q(x) = 2\sum_{\alpha<\beta} A_{\alpha,\beta} x_\alpha x_\beta + \sum_\gamma b_\gamma x_\gamma, \tag{1}$$

где A квадратичная часть (нижнетреугольная матрица с нулевой диагональю) с бинарными элементами из $\mathbb{Z}_2$, и b линейная часть с элементами из $\mathbb{Z}_4$. В области определения квадратичной формы q есть некоторое подмножество $\mathcal{L}_q$, в котором она действует линейно:

$$\mathcal{L}_q = \{x \in \mathbb{Z}_2^n : q(x \oplus y) = q(x) + q(y)\}. \tag{2}$$

Покажите, что множество $\mathcal{L}_q$ является векторным подпространством в $\mathbb{Z}_2^n$. Покажите, что на этом подпространстве q является булевой линейной формой, то есть что существует вектор $z \in \mathbb{Z}_2^n$, такой что $q(x) = 2\langle z, x\rangle$ для всех $x \in \mathcal{L}_q$.

Значит, в квадратичной форме q можно "спрятать" некоторую линейную форму. Допустим, заданы метрица A и вектор b, определяющие квадратичную форму q. *Задачей скрытой линейной функции* назовём задачу нахождения вектора z, такого что $q(x) = 2\langle z, x\rangle$ для всех $x \in \mathcal{L}_q$ (такой вектор может быть не единственным). Для решения этой задачи на классическом компьютере, достаточно воспользоваться алгоритмами линейной алгебры. В то же время, можно ещё более эффективно решить эту задачу на квантовой схеме.

Пусть даны n кубитов. Рассмотрим унитарную операцию вида

$$U_q|x\rangle = i^{q(x)}|x\rangle = (-1)^{\sum_{\alpha<\beta} A_{\alpha,\beta}x_\alpha x_\beta}\, i^{\sum_\gamma b_\gamma x_\gamma}|x\rangle. \tag{3}$$

Эту операцию можно реализовать, воспользовавшись вентилями CZ и S:

$$U_q = \prod_{\alpha<\beta} CZ_{\alpha,\beta}^{A_{\alpha,\beta}} \cdot \prod_\gamma S_\gamma^{b_\gamma}. \tag{4}$$

Теперь, следуя алгоритму Бернштейна-Вазирани, исследуем Фурье-спектр этой унитарной операции – сделаем выборку из

$$p(z) = |\langle z|H^{\otimes n}U_q H^{\otimes n}|0\rangle|^2. \tag{5}$$

Докажите, что $p(z) > 0$ тогда и только тогда, когда z является решением задачи скрытой линейной функции.

В статье [1] было показано, что для некоторых (A, b) задачу можно эффективно решить на квантовой схеме с конечной глубиной, в то время как любой классический вероятностный алгоритм потребует логарифмической глубины.

Задача III.2

Пусть задана группа G и её подгруппа H. Функция $f : G \to X$ *скрывает* подгруппу H, если $f(g_1) = f(g_2)$ эквивалентно $g_1H = g_2H$. *Задача о скрытой подгруппе* состоит в нахождении подгруппы H при помощи обращений к фунции f.

Известны алгоритмы, решающие проблему скрытой подгруппы для конечных абелевых групп (алгоритм Саймона), а также для некоторых более общих групп. Умение решать задачи скрытых подгрупп для более общих групп позволяет решать более сложные задачи. Задача изоморфизма графов спрашивает, являются ли два заданных графа изоморфными. Ожидается, что эта задача NP-промежуточная, то есть лежит в NP, и при этом сложнее P. Оказывается, что задачу изоморфизма графов можно свести к проблеме скрытой подгруппы в симметричных группах $\mathcal{S}_N$.

Пусть даны два графа G_1 и G_2 на n вершинах. Рассмотрим группу $\mathcal{S}_{2n}$ и определим на ней функцию $F(\sigma) = \sigma(G_1 \cup G_2)$, то есть F переставляет вершины $G_1 \cup G_2$. Какую подгруппу в $\mathcal{S}_{2n}$ скрывает эта функция? Как, зная структуру этой подгруппы, проверить, что G_1 и G_2 изоморны?

Задача III.3

Чаще всего рассматривается случай, когда алгоритм Гровера применяется для нахождения *единственного* решения $x_0 \in \{0, \ldots, N-1\}$. Как будет работать алгоритм Гровера, если решений множество? Допустим, дана неупорядоченная база данных $N = 2^n$ с некоторым множеством решений $A \subseteq \{0, \ldots, N-1\}$. Функция f определена как

$$f(x) = \begin{cases} 1, & x \in A, \\ 0, & \text{иначе.} \end{cases} \tag{6}$$

Покажите, что для нахождения какого-нибудь 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 может быть полезно воспользоваться обозначениями

$$|A\rangle = \frac{1}{\sqrt{|A|}}\sum_{x\in A}|x\rangle, \qquad |B\rangle = \frac{1}{\sqrt{N-|A|}}\sum_{x\notin A}|x\rangle. \tag{7}$$

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

Задача III.4

Одно из возможных 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 III.5

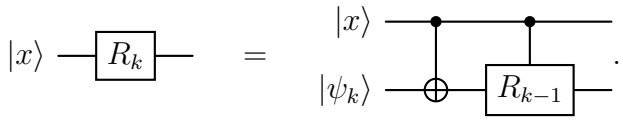
В работе [2] была предложена усовершенствованная схема для квантового преобразования Фурье, она использует технику каталитических вложений. Рассмотрим вращения вида

$$R_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix} \tag{8}$$

и состояния на одном кубите вида

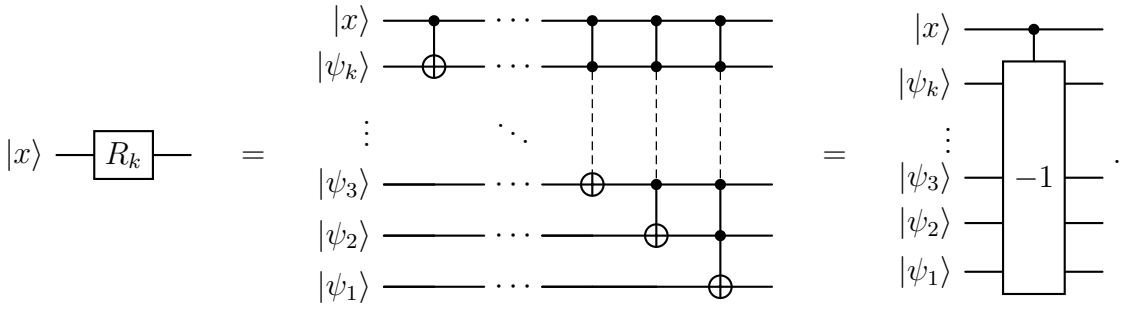
$$|\psi_k\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i/2^k}|1\rangle). \tag{9}$$

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



(10)

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



(11)

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.

Задача III.6

Предложите классическое решение задачи дискретного логарифма, занимающее не более $\tilde{\mathcal{O}}(\sqrt{N})$ времени. (Можно воспользоваться парадоксом о днях рождения, либо почитать о более сложных алгоритмах.)

Задача III.7

Одна из главных идей алгоритма Шора состоит в том, что возможно находить период функции над $\mathbb{Z}$, а значит и над любыми конечно порождёнными абелевыми группами [3]. Оказывается, что также существует способ нахождения периода над группой вещественных чисел $\mathbb{R}$. Допустим, нам дана функция $f : \mathbb{R} \to S$, которая является периодической с периодом r (период может быть любым вещественным числом):

$$f(x + r) = f(x). \tag{12}$$

Во избежание сложностей, допустим, что функция инъективна на каждом периоде r. Далее, чтобы решить задачу на цифровом компьютере, требуется дискретизовать функцию f, при этом мы надеемся, что дискретизация будет содержать некоторую информацию о периодичности. Будем называть дискретизованную функцию $f : \mathbb{Z} \to S$ *псевдопериодичной в точке* $k \in \mathbb{Z}$, если для всех $l \in \mathbb{Z}$ верно либо $f(k) = f(k+\lceil lr \rceil)$, либо $f(k) = f(k+\lfloor lr \rfloor)$. Будем называть функцию ε-*псевдопериодичной*, если она квазипериодична для почти всех значений $k \in \{0, \ldots, \lfloor r \rfloor\}$, исключая долю ε от этого множества. Будем допускать, что непрерывая функция $f : \mathbb{R} \to S$ допускает ε-псевдопериодичную дискретизацию $f : \mathbb{Z} \to S$ для некоторого $\varepsilon > 0$, и является инъективной на тех значениях, где она псевдопериодична.

Зафиксируем некоторое большое число $N > \Omega(r^2)$. Изучим, как ведёт себя Фурье-выборка от псевдопериодических функций. Для начала, создадим суперпозицию и применим эту функцию

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{x=0}^{n-1} |x\rangle|f(x)\rangle \tag{13}$$

Измерим второй регистр, получим некоторое значение $y = f(x_0)$. С некоторой вероятностью (какой?) функция псевдопериодична в точке x_0. На первом регистре остаётся состояние

$$\frac{1}{\sqrt{n}} \sum_{j=0}^{n-1} |x_0 + [jr]\rangle, \tag{14}$$

где $[jr]$ обозначает либо округление сверху, либо снизу, в зависимости от j. Число состояний в суперпозиции равно $n \approx \lfloor N/r \rfloor$. Какие конкретно может принимать значения n в различных ситуациях?

Сделав преобразование Фурье над $\mathbb{Z}_N$, получим

$$\frac{1}{\sqrt{nN}} \sum_{k=0}^{N-1} \omega_N^{kx_0} \sum_{j=0}^{n-1} \omega_N^{k[jr]} |k\rangle. \tag{15}$$

Разложим $[jr] = jr + \delta_j$, где $-1 < \delta_j < +1$. Покажите, что сумма экпонент близка к случаю $\delta_j = 0$:

$$|\sum_{j=0}^{n-1} \omega_N^{kjr} \omega_N^{k\delta_j} - \sum_{j=0}^{n-1} \omega_N^{kjr}| \leqslant \frac{2\pi kn}{N}. \tag{16}$$

Измерим последующий регистр и будем считать, что выпал результат $k < N/\log r$ (это произойдёт с вероятностью $1/\log r$). В этом случае, результат измерения будет оптимальной рациональной оценкой $k = \lfloor jN/r \rceil$ вещественной величины jN/r, с вероятностью порядка $\Omega(1/\mathrm{poly}(\log r))$.

Поскольку r не является целым числом, воспользоваться стандартным алгоритмом цепных дробей недостаточно. Проведя процедуру достаточное (полиномиальное) число раз, с некоторой вероятностью получим взамино простые числа j, j'. Если $N > 3r^2$, то оказывается, что j/j' возникает в разложении в цепные дроби числа $\lfloor jN/r \rceil / \lfloor j'N/r \rceil$. Поэтому, мы можем эффективно найти j, и получить приближение $r \approx jN/\lfloor jN/r \rceil$. Подробности можно найти в [4].

При помощи такого обобщения задачи о скрытой подгруппе можно решать широкий круг задач алгебраической теории чисел, такие как решение уравнения Пелля, нахождение генератора главного идеала, и много больше. В принципе, такого рода алгоритмы обобщаются на любые числовые поля.

Задача III.8

Поищите в интернете информацию о том, какие существуют организации, работающие в сфере квантовых вычислений. Составьте список из не менее чем 10 таких оранизаций и для каждой из них в одном предложении опишите, чем конкретно они занимаются.

---

[1] S. Bravyi, D. Gosset, and R. König, Quantum advantage with shallow circuits, Science **362**, 308–311 (2018).

[2] 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].

[3] M. Mosca and A. Ekert, The hidden subgroup problem and eigenvalue estimation on a quantum computer (1999), arXiv:quant-ph/9903071 [quant-ph].

[4] S. Hallgren, Polynomial-time quantum algorithms for pell's equation and the principal ideal problem, Journal of the ACM (JACM) **54**, 1 (2007).