Алгоритм Шора

Квантовые вычисления–2023

19 декабря 2023 г.

Outline

Постановка задачи

- числа сложно разложить на простые множители
- например, в криптографии — RSA
- алгоритм Шора — за полиномиальное время
- (экспоненциально быстрее классических алгоритмов)

Постановка задачи

- числа сложно разложить на простые множители
- например, в криптографии — RSA
- алгоритм Шора — за полиномиальное время
- (экспоненциально быстрее классических алгоритмов)

Время работы

Разложение числа n длиной m битов требует:

- около $n^{1/3} = 2^{m/3}$ шагов (классический)
- $O(m^3)$ шагов (квантовый — алгоритм Шора)

Нахождение порядка

Формулировка задачи

- Пусть $n = pq$, произведение двух простых чисел. Найти p, q
- Задача сводится к вычислению порядка $\mathbb{Z}_n^\times$.

$$\mathbb{Z}_n^\times = \{x \in \mathbb{Z}_+ : x < n, \gcd(x, n) = 1\}.$$

- Для $x \in \mathbb{Z}_n^\times$ найти наименьший порядок r: $x^r = 1 \pmod{n}$.

Решение

- Зададим возведение в степень по модулю как квантовую схему
- Найдём r алгоритмом оценки фазы
- Имея r, вычислим множители n.

Период и порядок

Порядок группы

- Для любой G и $g \in G$ выполняется $g^{|G|} = 1_G$
- Но порядок r может быть меньше

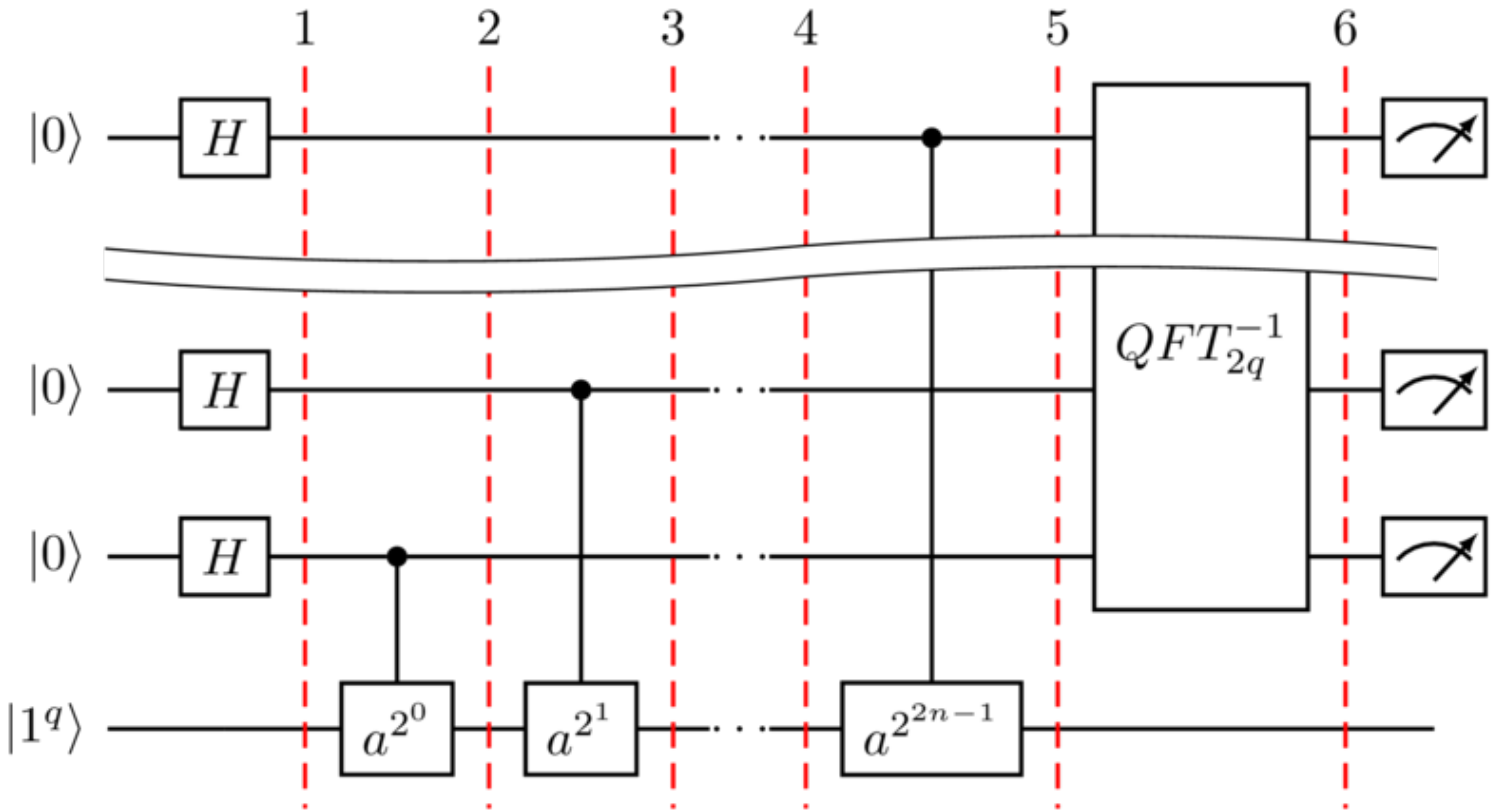
Примеры

- Мультипликативная группа $\mathbb{Z}_{15}^{\times} = \{1, 2, 4, 7, 8, 11, 13, 14\}$,
- т.е. $|\mathbb{Z}_{15}^{\times}| = 8$.
- Для $a = 7$ выполняется $7^8 = 1 \pmod{15}$;
- но порядок 7 меньше, потому что $7^4 = 1 \pmod{15}$.
- Если период a равен r, то $f_a(x) = a^x \pmod{n}$ — периодическая (с периодом r):

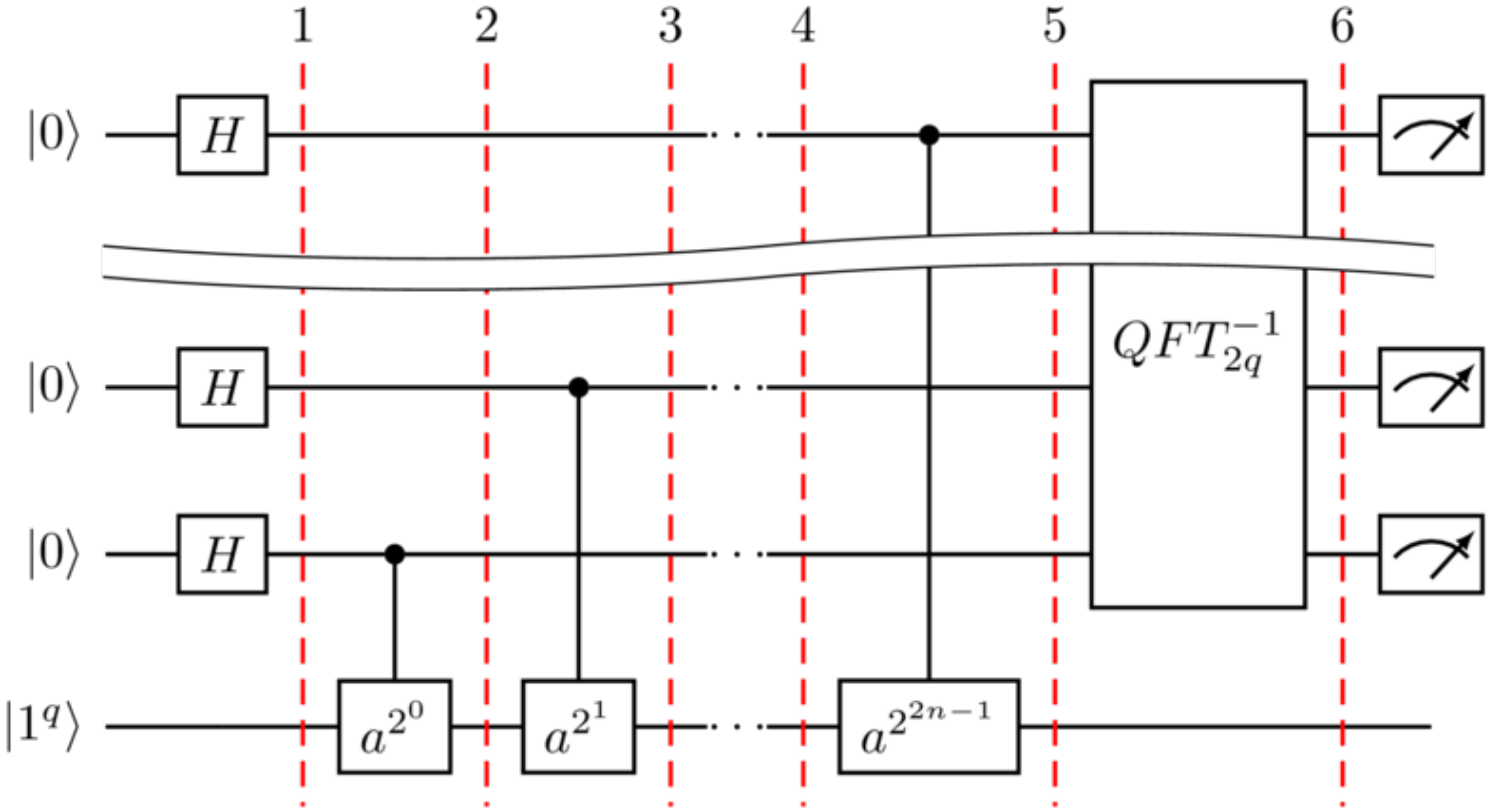
$$7^1 = 7; 7^2 = 4; 7^3 = 13; 7^4 = 1; 7^5 = 7; \ldots \pmod{n}.$$

Квантовый поиск периода

Потребуется $3q$ кубитов, где q: $n \leq Q = 2^q < 2n$. Выбираем случайно $1 < a < n$ так, что $\gcd(a, n) = 1$

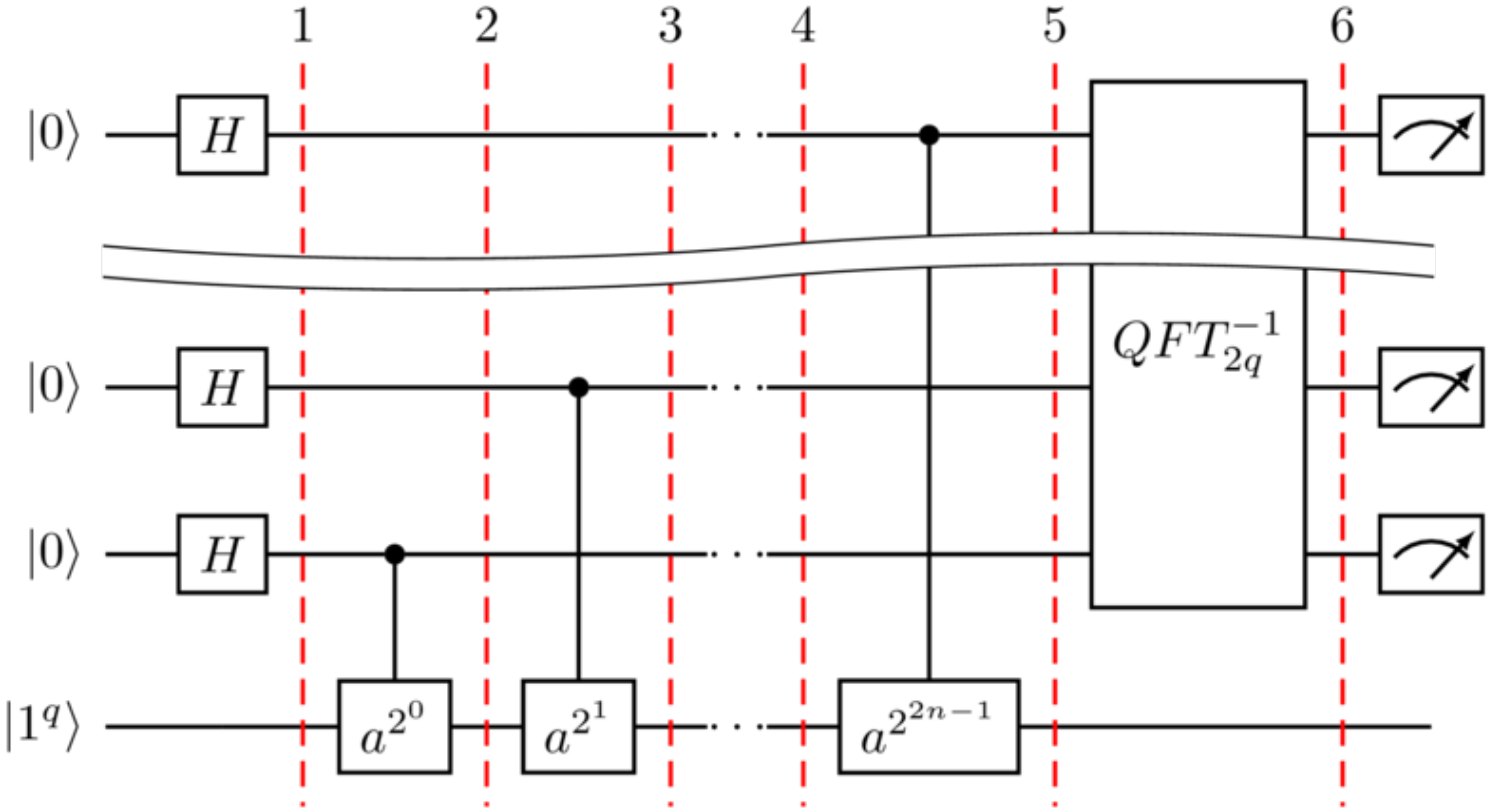


Работа алгоритма



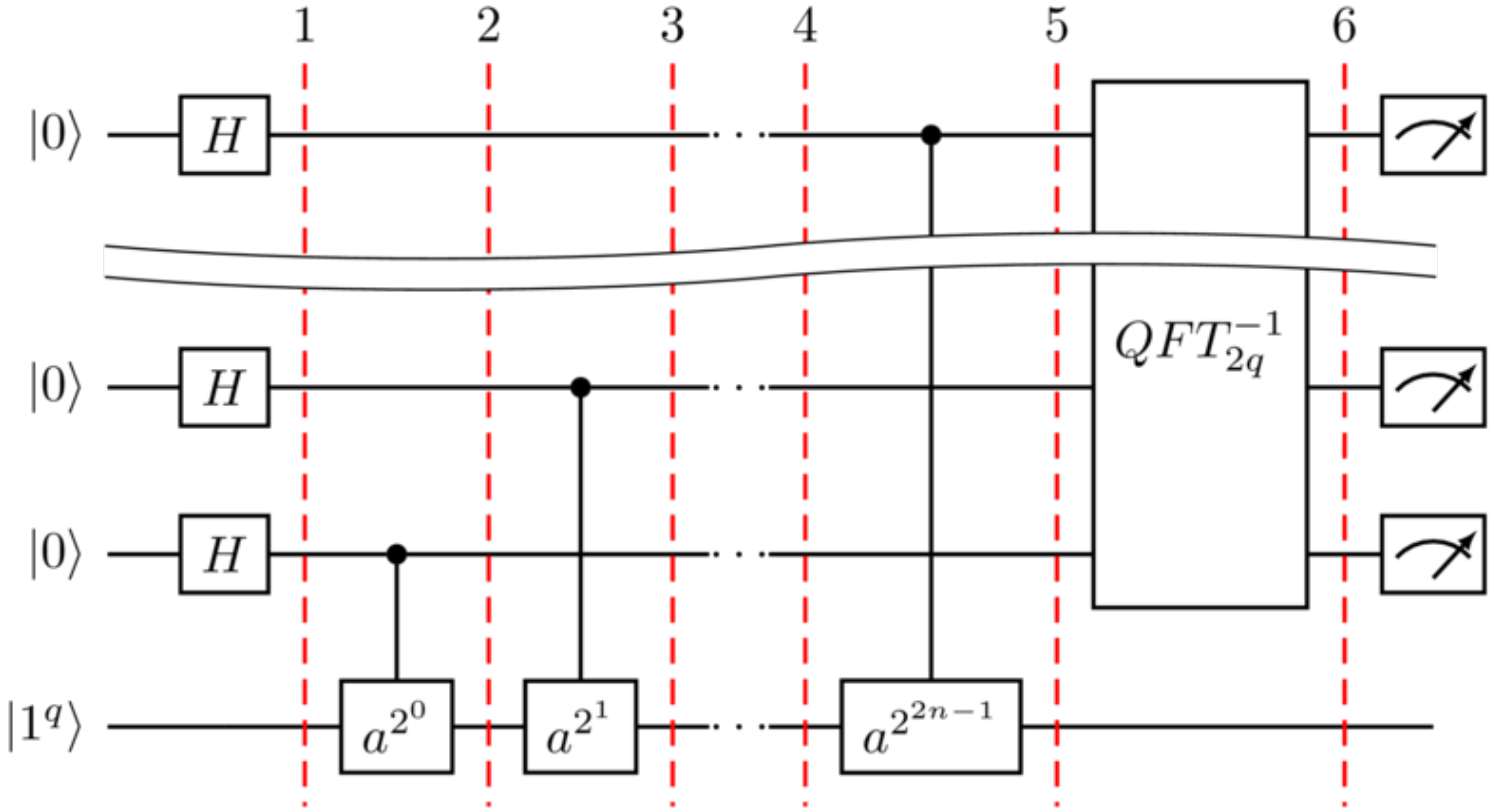
$$|\Psi_1\rangle = \frac{1}{\sqrt{Q}} \sum_{x=0}^{Q-1} |x\rangle$$

Работа алгоритма



$$|\Psi_5\rangle = \frac{1}{\sqrt{Q}} \sum_{x=0}^{Q-1} |x\rangle |a^x \bmod n\rangle$$

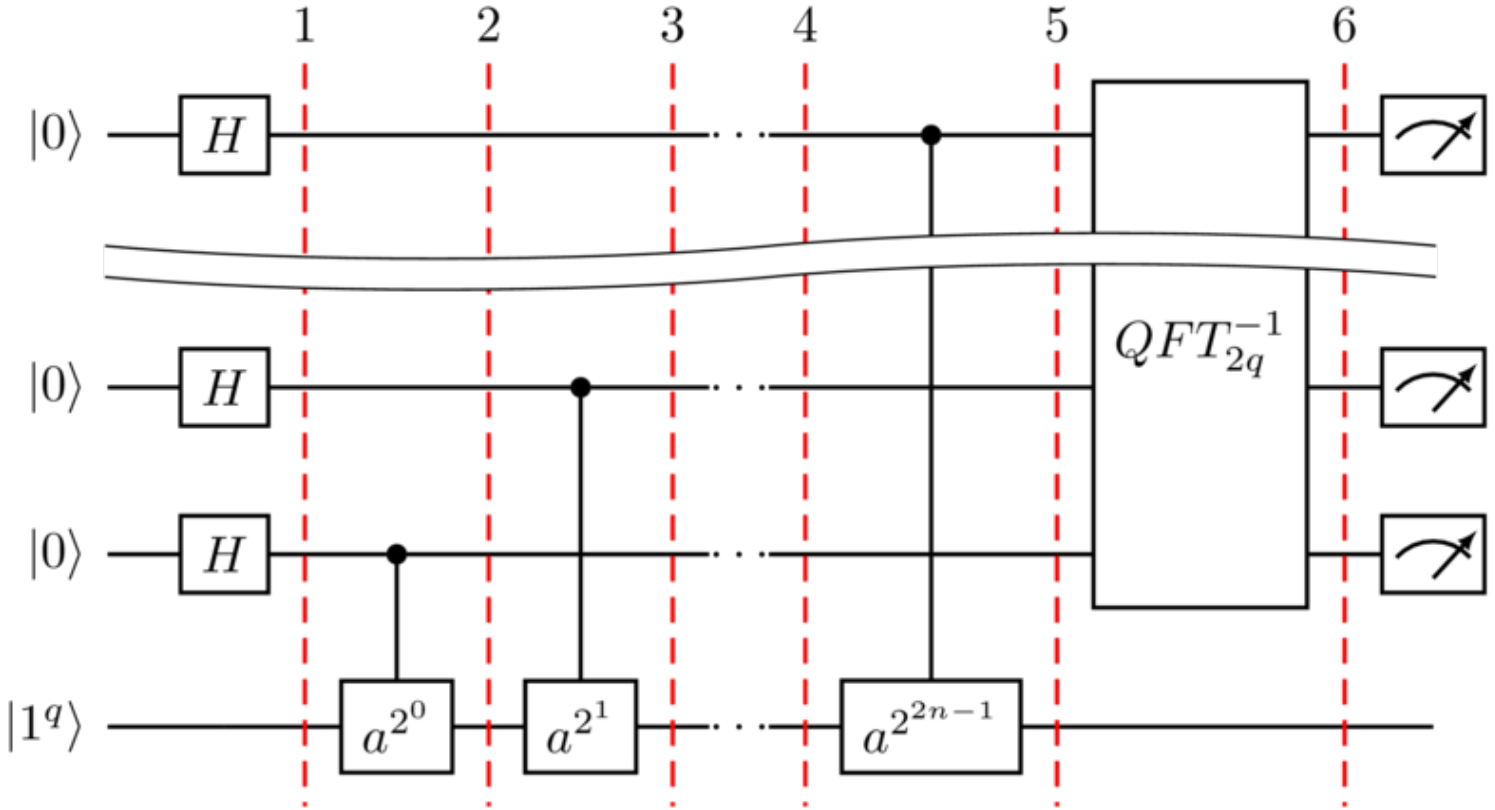
Работа алгоритма



$$|\Psi_6\rangle = \frac{1}{Q}\sum_{z=0}^{N-1}\sum_{y=0}^{Q-1}\left[\sum_{x\in\{0,\ldots,Q-1\};a^x=z \bmod n}\omega^{xy}\right]|y\rangle|z\rangle,$$

где $\omega = \exp(2\pi i/Q)$.

Работа алгоритма



При измерении выше вероятность тех $|y\rangle$, для которых yr/Q близко к целому числу.

Классическая пост-обработка

Остаётся по y найти r, и по нему — разложение n на множители.

Приближение к r

- Так как yr/Q близко к целому c, то y/Q близко к c/r
- Найдём приближение d/s, что $s < n$, и

$$\left|\frac{y}{Q} - \frac{d}{s}\right| < \frac{1}{2Q}.$$

- Тогда s близко к периоду r (или его множитель).
- Перебрав и проверив несколько значений, получим r: $a^r = 1 \pmod{n}$
- (если нет, повторим квантовую часть).

Вычисление множителей по r

- Если r нечётное, то тоже повторим квантовую часть с другим a.
- Пусть r — чётное.
- Обозначим $b = a^{r/2} \bmod n$, где $b \neq 1$.
- Получаем: $b^2 = 1 \pmod{n}$, или

$$b^2 - 1 = (b-1)(b+1) = cn$$

для какого-то c.

- Числа $\gcd(n, b-1)$ и $\gcd(n, b+1)$ делят n.

Домашнее задание

- Заданы n, Q, a и y такое, что yr/Q близко к целому
- Написать классическую процедуру для нахождения делителей n указанным способом
- Процедура должна вернуть либо множители p, q, либо то, что процедуру нужно повторить с другим a