

# Алгоритм Шора

Сергей Николенко

Computer Science Club, 2015

# Outline

- 1 **Квантовые вычисления**
  - Введение
  - Свойства квантовых систем
- 2 Где квантовые вычисления превосходят классические
  - Простой пример
  - Алгоритм Шора

# Классические и квантовые вычисления

- Машины Тьюринга, схемы — классические объекты.
- Они локальны и подчиняются классическим законам.
- Но ведь мы живём в квантовом мире! Как это использовать?
- Квантовые вычисления — вычисления, существенно использующие квантовые эффекты.
- Сейчас увидим, как именно.

# Квантовые состояния

- Рассмотрим физическую систему, у которой может быть  $n$  состояний.
- Назовём их  $|1\rangle, |2\rangle, \dots, |n\rangle$ .
- Квантовое состояние  $|\phi\rangle$  – суперпозиция классических:

$$|\phi\rangle = \alpha_1 |1\rangle + \alpha_2 |2\rangle + \dots + \alpha_n |n\rangle.$$

- $\alpha_i \in \mathbb{C}$  – амплитуда  $|i\rangle$  в  $|\phi\rangle$ ,  $\sum_i |\alpha_i|^2 = 1$ .

## Что можно с ними делать

- Математически говоря – состояния  $|1\rangle, |2\rangle, \dots, |n\rangle$  образуют ортонормированный базис гильбертова пространства размерности  $n$ .
- Квантовое состояние мы можем либо унитарно изменять, либо измерять.
- Измерение схлопывает его в классическое: измеряя

$$|\phi\rangle = \alpha_1 |1\rangle + \alpha_2 |2\rangle + \dots + \alpha_n |n\rangle,$$

мы видим  $|i\rangle$  с вероятностью  $|\alpha_i|^2$ .

# Что можно с ними делать

- Можно применить унитарный оператор

$$U\left(\sum_i \alpha_i |i\rangle\right) = \sum_i \beta_i |i\rangle,$$

т.е. умножить на унитарную матрицу

$$U\alpha = \beta, \quad U^{-1} = U^*.$$

- Все унитарные преобразования обратимы, т.е. если мы преобразовываем квантовую систему, мы можем вернуться обратно.
- Измерение необратимо.

# Кубиты

- Кубит (qubit) – это суперпозиция 0 и 1, два базовых состояния:

$$\alpha_0 |0\rangle + \alpha_1 |1\rangle, \quad |\alpha_0|^2 + |\alpha_1|^2 = 1.$$

- Можно рассмотреть два кубита, базис будет  $|00\rangle = |0\rangle |0\rangle$ ,  $|01\rangle$ ,  $|10\rangle$ ,  $|11\rangle$ :

$$|0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

# Преобразование Адамара

- Пример унитарного преобразования – преобразование Адамара.
- Матрица Адамара

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

- На кубитах:

$$H|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle = |+\rangle,$$

$$H|1\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle = |-\rangle.$$



# Запутывание

- Бывают запутанные состояния, например:

$$\frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle .$$

- Математически – тензорное произведение гильбертовых пространств.
- Система из  $n$  кубитов описывается набором из  $2^n$  комплексных координат.

# Запутывание

- Квантовый трюк номер один: запутывание (entanglement). Это как раз свойство нелокальности.
- Рассмотрим состояние

$$\frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle.$$

- И измерим первый из кубитов.
- Система спроецируется либо на  $|00\rangle$ , либо на  $|11\rangle$ .
- И мы будем знать второй кубит, не измеряя его!
- А он может быть за миллион световых лет.

# Интерференция

- Запутанные состояния могут под действием унитарных преобразований распутываться.
- Это квантовый трюк номер два: интерференция (interference).
- На примере Адамара:

$$H|+\rangle = \frac{1}{\sqrt{2}}(H|0\rangle + H|1\rangle) = \frac{1}{2}(|0\rangle + |1\rangle + |0\rangle - |1\rangle) = |0\rangle,$$

$$H|-\rangle = \frac{1}{\sqrt{2}}(H|0\rangle - H|1\rangle) = \frac{1}{2}(|0\rangle + |1\rangle - |0\rangle + |1\rangle) = |1\rangle.$$

# Вычисление функций

- Далее: можно вычислять функции унитарными преобразованиями.
- Но функции бывают необратимые; как сделать обратимую функцию?

# Вычисление функций

- Эту идею мы уже видели: график  $(x, 0) \mapsto (x, f(x))$  будет биективен.
- Т.е. если в кубитах, то применять булевскую функцию так:

$$U_f(|x\rangle|0\rangle) = |x\rangle|f(x)\rangle,$$

или, в более общем виде,

$$U_f|x\rangle|b\rangle = |x\rangle|b \oplus f(x)\rangle.$$

- В частности, потом понадобится:

$$U_f|x\rangle|-\rangle = (-1)^{f(x)}|x\rangle|-\rangle.$$

# Пример: controlled NOT

- Например, функция controlled not (C-NOT):

$$C |0x\rangle = |0x\rangle, \quad C |1x\rangle = |1(1-x)\rangle.$$

- Какая матрица у этого унитарного преобразования?

# Параллелизм

- Квантовый трюк номер три: параллелизм.
- Рассмотрим функцию  $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$ . Её квантовая версия:

$$U_f |x\rangle |0^m\rangle = |x\rangle |f(x)\rangle.$$

- Давайте через  $H$  подготовим комбинацию всех входов:

$$U_f \left( \frac{1}{\sqrt{2^n}} \sum_x |x\rangle |0^m\rangle \right) = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle |f(x)\rangle.$$

- То есть мы одновременно вычислили все  $2^n$  значений функции!

# Параллелизм

- Всё не так просто, конечно: если теперь измерить, то получим только один случайный  $|x\rangle |f(x)\rangle$ .
- Но если, например, использовать запутывание и измерить только последние  $m$  кубитов, то получится состояние

$$c \sum_{x:f(x)=a} |x\rangle |a\rangle,$$

где  $a$  взято по распределению  $f$  (равномерного).



# Outline

- 1 Квантовые вычисления
  - Введение
  - Свойства квантовых систем
- 2 Где квантовые вычисления превосходят классические
  - Простой пример
  - Алгоритм Шора

# Задача Deutsch-Jozsa

- Задача Deutsch-Jozsa: дана функция  $f : \{0, 1\}^n \rightarrow \{0, 1\}$ , известно, что она либо равна 0, либо сбалансирована (равна 0 на половине входов). Какая именно это функция?
- Классически в худшем случае надо  $2^{n/2} + 1$  вычислений функции.
- Квантово: вспомним

$$U_f |x\rangle |-\rangle = (-1)^{f(x)} |x\rangle |-\rangle.$$

# Задача Deutsch-Jozsa

- Начнём с состояния  $|0^n\rangle |1\rangle$ .
- Применим  $(n + 1)$ -го Адамара, получим

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |-\rangle.$$

- Затем вычислим функцию, получим

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle |-\rangle.$$

- Теперь ещё  $n$  Адамаров применим, получим в первых  $n$  кубитах

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} |y\rangle.$$

# Задача Deutsch-Jozsa

- Теперь первая координата

$$\alpha_{00\dots 0} = \frac{1}{2^n} \sum_x (-1)^{f(x)}$$

равна 1, если  $f = 0$ , и 0, если  $f$  сбалансирована.

- Достаточно измерить и посмотреть, попадём ли в состояние  $|0^n\rangle$ .
- Но тут классически, конечно, достаточно просто рандомизировать слегка, и тоже быстро получится.

# Поиск периода

- Теперь давайте рассмотрим алгоритм Шора.
- Дано  $n = pq$ , надо вычислить  $p$  и  $q$ .
- На самом деле алгоритм Шора по числу  $x \in \mathbb{Z}_n^*$  находит период  $f(a) = x^a \pmod{n}$ , т.е. минимальное  $r$ , для которого  $x^r \equiv 1 \pmod{n}$  начнёт повторяться.
- Почему этого достаточно, чтобы разложить  $n$ ?

# Поиск периода

- Для по крайней мере  $\frac{1}{4}$  всех  $x$ 'ов  $r$  чётный, и  $x^{r/2} \not\equiv \pm 1 \pmod{n}$ .
- А тогда  $(x^{r/2} - 1)(x^{r/2} + 1) = 0 \pmod{n}$ , и мы всё раскладываем.

# Квантовое преобразование Фурье

- Находить будем через квантовое преобразование Фурье.
- Базис Фурье размерности  $q$ :

$$|\xi_j\rangle = \frac{1}{\sqrt{q}} \sum_{k=0}^{q-1} e^{2\pi i \frac{jk}{q}} |k\rangle.$$

- Квантовое преобразование Фурье – это  $|j\rangle \mapsto |\xi_j\rangle$ .

# Квантовое преобразование Фурье

- Если  $q = 2^l$ , то его можно реализовать за  $O(l^2)$  гейтов:

$$\begin{aligned}
 |\xi_{j_0 j_1 j_2}\rangle &= \\
 &= \frac{1}{\sqrt{8}} (|0\rangle + e^{2\pi i 0 \cdot j_2} |1\rangle) (|0\rangle + e^{2\pi i 0 \cdot j_1 j_2} |1\rangle) (|0\rangle + e^{2\pi i 0 \cdot j_0 j_1 j_2} |1\rangle).
 \end{aligned}$$



# Алгоритм Шора

- Для алгоритма Шора: выберем  $q$  – степень двойки между  $n^2$  и  $2n^2$ .
- Простой случай: предположим, что  $r \mid q$ .
- Тогда: применим QFT к первому регистру  $|0^q\rangle |0^q\rangle$ :

$$\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a\rangle |0\rangle .$$

# Алгоритм Шора

- Вычислим  $x^a \bmod n$  (тоже за логарифм):

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

- Пронаблюдаем второй регистр, получим  $|x^s \bmod n\rangle$  для случайного  $s < r$ , а в первом – суперпозиция  $|s\rangle, |r+s\rangle, |2r+s\rangle, \dots, |q-r+s\rangle$ :

$$\frac{1}{\sqrt{q/r}} \sum_{j=0}^{q/r-1} |jr+s\rangle.$$

# Алгоритм Шора

- Теперь опять применим QFT:

$$\begin{aligned} \frac{1}{\sqrt{q/r}} \sum_{j=0}^{q/r-1} \sum_{b=0}^{q-1} e^{2\pi i \frac{(jr+s)b}{q}} |b\rangle &= \\ &= \frac{1}{\sqrt{q/r}} \sum_{b=0}^{q-1} e^{2\pi i \frac{sb}{q}} \left( \sum_{j=0}^{q/r-1} e^{j \cdot 2\pi i \frac{rb}{q}} \right) |b\rangle. \end{aligned}$$

- Сумма в скобках не равна нулю iff  $\frac{rb}{q}$  – целое число, т.е. ненулевая амплитуда будет только у чисел, делящихся  $\frac{q}{r}$ .

# Алгоритм Шора

- Теперь пронаблюдаем первый регистр и получим случайное число вида  $c \frac{q}{r}$ .
- С большой вероятностью (порядка  $\frac{1}{\log \log q}$ )  $c$  и  $r$  взаимно просты.
- Тогда можно просто сократить получившуюся дробь и получить  $r$ . Всё!

## Алгоритм Шора: сложный случай

- Сложный случай: когда  $r \nmid q$ .
- Тогда так просто на последнем шаге не будет, но всё равно с большой вероятностью мы наблюдаем дробь  $\frac{b}{q}$ , для которой  $\left| \frac{b}{q} - \frac{c}{r} \right| \leq \frac{1}{2q}$ .
- На интервале длины  $\frac{1}{q} < \frac{1}{n^2}$  будет не больше одной дроби со знаменателем  $< n$ .
- И эта дробь должна как раз быть  $\frac{c}{r}$ .

**Упражнение.** Эффективно найти  $\frac{c}{r}$  по  $\frac{b}{q}$  (классически :)).

# Алгоритм Шора для дискретного логарифма

- Тот же самый алгоритм подойдёт и для дискретного логарифма.
- Мы ведь на самом деле ищем период элемента  $x$  некоторой коммутативной группы.
- Значит, если даны  $G = \langle g \rangle$ ,  $n = |G|$  и  $y = g^x$ , то можно просто найти период  $y$ , т.е. минимальное  $r$ , для которого  $y^r = 1$ , и сразу получится  $x = \frac{n}{r}$ .
- Эллиптические кривые не спасают – для любой коммутативной группы работает, нужно только умножать уметь.

# Итоги

- Мы взломали всю коммутативную криптографию. Что делать?
- Один ответ – строить квантовую криптографию; этим мы заниматься не будем.
- Другой ответ – строить некоммутативную криптографию; об этом и пойдёт речь в следующий раз.

Thank you!

**Спасибо за внимание!**