Алгоритм Шора

Сергей Николенко

Криптография — АФТУ РАН, весна 2010

Outline

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 $|1\rangle, |2\rangle, \ldots, |n\rangle$.
- Квантовое состояние $|\phi\rangle$ – суперпозиция классических:

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

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

Что можно с ними делать

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

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

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

Что можно с ними делать

- Можно применить унитарный оператор

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

  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:

$$\alpha_0 \left|0\right\rangle + \alpha_1 \left|1\right\rangle, \quad \left|\alpha_0\right|^2 + \left|\beta_0\right|^2 = 1.$$

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

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

Преобразование Адамара

- Пример унитарного преобразования – преобразование Адамара.
- Матрица Адамара

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

- На кубитах:

$$H\left|0\right\rangle = \frac{1}{\sqrt{2}}\left|0\right\rangle + \frac{1}{\sqrt{2}}\left|1\right\rangle = \left|+\right\rangle,$$
$$H\left|1\right\rangle = \frac{1}{\sqrt{2}}\left|0\right\rangle - \frac{1}{\sqrt{2}}\left|1\right\rangle = \left|-\right\rangle.$$

Запутывание

- Бывают запутанные состояния, например:

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

- 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
$$\frac{1}{\sqrt{2}}\left|00\right\rangle + \frac{1}{\sqrt{2}}\left|11\right\rangle .$$
- И измерим первый из кубитов.
- Система спроецируется либо на $\left|00\right\rangle$, либо на $\left|11\right\rangle$.
- 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

- Дальше: 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:

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

Примеры

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

$$C\left|0x\right\rangle = \left|0x\right\rangle, \quad C\left|1x\right\rangle = \left|1\right\rangle\left|1-x\right\rangle.$$

- Какая матрица у этого унитарного преобразования?
- Другой пример – можно повернуть один из компонентов; например:

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{pmatrix}.$$

Параллелизм

- Квантовый трюк номер три: параллелизм.
- Рассмотрим функцию $f : \{0,1\}^n \to \{0,1\}^m$. Её квантовая версия:
$$U_f \left|x\right\rangle \left|0^m\right\rangle = \left|x\right\rangle \left|f(x)\right\rangle .$$
- Давайте через H подготовим комбинацию всех входов:
$$U_f \left(\frac{1}{\sqrt{2^n}} \sum_x \left|x\right\rangle \left|0^m\right\rangle \right) = \frac{1}{\sqrt{2^n}} \sum_x \left|x\right\rangle \left|f(x)\right\rangle .$$
- 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

Задача Deutsch-Jozsa

- Задача Deutsch-Jozsa: дана функция $f : \{0,1\}^n \to \{0,1\}$, 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

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

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

Simon's problem

- Задача Саймона: дана функция $f : \{0,1\}^n \to \{0,1\}^n$, известно, что есть такой s, что $f(x) = f(y)$ iff $x = y \oplus s$. Верно ли, что $s = 0$?
- Если $s = 0$, это биекция, если $s \neq 0$, это 2-1-функция.
- Классически: нужно $\sqrt{2^n}$ запросов к функции, даже в среднем, даже для рандомизированных алгоритмов, потому что нужно попасть в коллизию, а это нелегко.

Simon's problem

- Квантово: возьмём $2n$ кубитов, приготовим смесь в первых n, применим U_f; получится

$$\frac{1}{\sqrt{2^n}} \sum_x |x\rangle\, |f(x)\rangle\, .$$

- Измерим некоторый $f(x)$; в первых регистрах останется $\frac{1}{\sqrt{2}}(|x\rangle + |x \oplus s\rangle)$.
- Теперь ещё n Адамаров применим. Получится

$$\frac{1}{\sqrt{2^{n+1}}} \left(\sum_y (-1)^{x \cdot y}\, |y\rangle + (-1)^{(x \oplus s) \cdot y}\, |y\rangle \right).$$

Simon's problem

- Получили
$$\frac{1}{\sqrt{2^{n+1}}}\left(\sum_y (-1)^{x\cdot y}\left(1+(-1)^{s\cdot y}\right)|y\rangle\right).$$
- У $|y\rangle$ ненулевая амплитуда iff $s \cdot y = 0 \pmod 2$.
- Значит, измерим и получим случайную строку y, для которой $s \cdot y = 0 \pmod 2$.
- Когда повторим $2n$ раз, наберём с высокой вероятностью n линейно независимых y и решим систему.

Outline

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.
- Дискретное преобразование Фурье дискретной функции $f_1, \ldots, f_N$:
$$\tilde{f}_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi i \frac{jk}{N}} f_j.$$
- А квантовое – это преобразование Фурье на амплитудах:
$$\sum_j \alpha_j \left| j \right\rangle \mapsto \sum_k \tilde{\alpha}_k \left| k \right\rangle .$$
- Базис Фурье размерности q:
$$\left| \xi_j \right\rangle = \frac{1}{\sqrt{q}} \sum_{k=0}^{q-1} e^{2\pi i \frac{jk}{q}} \left| k \right\rangle .$$
- Квантовое преобразование Фурье – это $\left| j \right\rangle \mapsto \left| \xi_j \right\rangle$.

Квантовое преобразование Фурье

- Если $q = 2^l$, то его можно реализовать за $O(l^2)$ гейтов.
- Запишем состояние j в двоичной форме $j_1 j_2 \ldots j_n$:

$$j = j_1 2^{n-1} + \ldots + j_n.$$

- Будем ещё писать двоичные дроби $0.j_1 j_2 \ldots j_n$:

$$0.j_1 j_2 \ldots j_n = j_1/2 + j_2/4 + \ldots + j_n/2^n = j/2^n.$$

Квантовое преобразование Фурье

- Тогда

$$\left|\xi_j\right\rangle = 2^{-n/2}\left(|0\rangle + e^{2\pi i 0.j_n}|1\rangle\right)\otimes \\ \otimes\left(|0\rangle + e^{2\pi i 0.j_{n-1}j_n}|1\rangle\right)\otimes \\ \otimes\ldots\otimes\left(|0\rangle + e^{2\pi i 0.j_1 j_2\ldots j_n}|1\rangle\right).$$

- Например, для трёх:

$$\left|\xi_{j_1 j_2 j_3}\right\rangle = \\ = \frac{1}{\sqrt{8}}\left(|0\rangle + e^{2\pi i 0.j_3}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_2 j_3}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_1 j_2 j_3}|1\rangle\right).$$

Упражнение. Проверить.

Квантовое преобразование Фурье

- А это значит, что легко реализовать схемой; преобразование

$$|0,1\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle \pm e^{i\theta}|1\rangle)$$

представляет собой Адамара, затем повёрнутого вокруг одной из осей на $\theta/2$.

- Значит, нам достаточно определить вращение

$$R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^k}} \end{pmatrix},$$

и получится схема.

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 $x^a \mod n$ (тоже за логарифм):

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

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

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

Алгоритм Шора

- Теперь опять применим QFT:

$$\frac{1}{\sqrt{q/r}}\sum_{j=0}^{q/r-1}\sum_{b=0}^{q-1}e^{2\pi i\frac{(jr+s)b}{q}}\left|b\right\rangle =$$

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

- 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 $r \not| q$.
- Тогда так просто на последнем шаге не будет, но всё равно с большой вероятностью мы пронаблюдаем 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

- Аналогичный алгоритм подойдёт и для дискретного логарифма.
- Пусть $\alpha^q = 1$, q простое, и $\beta = g^d$, где $0 < d < q-1$ неизвестно.
- Рассмотрим функцию $f(x,y) = \alpha^x \beta^y$ для целых x и y.
- У неё два независимых «периода» на $\mathbb{Z}^2$:

$$f(x+q,y) = f(x,y), \qquad f(x+d,y-1) = f(x,y),$$

т.е. $\{x,y \mid f(x,y) = 1\}$ образуют решётку в $\mathbb{Z}^2$.

Алгоритм Шора для дискретного логарифма

- Простой случай: пусть мы умеем вычислять QFT порядка q. Тогда заготовим адамарами

$$\frac{1}{q}\sum_{x=0}^{q-1}\sum_{y=0}^{q-1}|x\rangle\,|y\rangle\,|0\rangle$$

и вычислим функцию:

$$\frac{1}{q}\sum_{x=0}^{q-1}\sum_{y=0}^{q-1}|x\rangle\,|y\rangle\,|\alpha^x\beta^y\rangle\ .$$

Алгоритм Шора для дискретного логарифма

- Имея $\frac{1}{q}\sum_{x=0}^{q-1}\sum_{y=0}^{q-1}|x\rangle|y\rangle|\alpha^x\beta^y\rangle$, измерим последний регистр, получив некоторый α^{x_0}; после этого первые будут в суперпозиции всех x, y, для которых $\alpha^x\beta^y = \alpha^x\alpha^{dy} = \alpha^{x_0}$, т.е.

$$x + dy = x_0 \pmod{q}.$$

- Значит, для каждого y одно решение, и состояние первых регистров получается

$$\frac{1}{\sqrt{q}}\sum_{y=0}^{q-1}|x_0 - dy\rangle|y\rangle .$$

Алгоритм Шора для дискретного логарифма

- Осталось применить QFT к каждому из первых двух регистров:

$$\frac{1}{\sqrt{q}}\frac{1}{q}\sum_{x',y'=0}^{q-1}\sum_{y=0}^{q-1}\omega^{(x_0-dy)x'}\omega^{yy'}\left|x',y'\right\rangle,$$

  где $\omega = e^{2\pi i/q}$.

- Сумма $\sum_{y=0}^{q-1}\omega^{y(y'-dx')}$ равна 0 всегда, кроме случая $y' = dx' \pmod q$, и получится

$$\frac{1}{\sqrt{q}}\sum_{x'=0}^{q-1}\omega^{x_0x'}\left|x'\right\rangle\left|y' = dx' \mod q\right\rangle.$$

- Измерив, получим пару x', y', из которой с большой вероятностью получится $d = y'(x')^{-1} \pmod q$.

Алгоритм Шора для дискретного логарифма

- В сложном случае, когда надо делать QFT по модулю 2^n, всё то же самое, но ещё нужен некоторый postprocessing – округлить результат и т.д.
- В результате получается квантовое решение задачи дискретного логарифма.
- 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.
- Другой ответ – строить некоммутативную криптографию.

Спасибо за внимание!

- Lecture notes и слайды будут появляться на моей homepage:
  `http://logic.pdmi.ras.ru/~sergey/`
- Присылайте любые замечания, решения упражнений, новые численные примеры и прочее по адресам:
  `sergey@logic.pdmi.ras.ru`, `snikolenko@gmail.com`
- Заходите в ЖЖ smartnik.