Специальные разделы криптологии

Савчук М.Н.

5 апреля 2015 г.

Глава 1

Алгоритм Шора для факторизации

1.1 Введение

Есть число N

$$N = a \cdot b, \qquad a \neq b$$

Задача факторизации: для числа $N = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$

- либо получить каноническую форму
- либо получить нетривиальный делитель

Число $a \in \mathbb{Z}_N$ **принадлежит показателю** δ, если δ — минимальное число, для которого $a^\delta \equiv 1 \mod n$. Обозначаем $\delta_N(a)$.

Показатель существует только если a и N взаимно просты ($a \in \mathbb{Z}_N$) и по сути является порядком a в группе $\mathbb{Z}_N : \delta_n(a) = ord_N(a)$. Если $gcd(a, N) \neq 1$, то мы нашли нетривиальный делитель.

Допустим, что для заданного $a \in \mathbb{Z}_N$ у нас есть оракул O_f, который возвращает показатель числа. Если этот оракул полиномиален, то можно факторизовать число (вероятностно)

Пусть r — чётное и $gcd\left(a^{r/2} + 1, N\right) = 1$, где $O_f(a) = r$

$$a^r \geq 1 \mod N$$

$$\left(a^{r/2} - 1\right) \cdot \left(a^{r/2} + 1\right) \equiv 0 \mod N$$

Но $a^{r/2} \neq 1 \mod N$, потому что иначе r — не минимальное число (нарушение определения показателя). Значит, $\left(a^{r/2} - 1\right)$ и N имеет нетривиальный общий делитель.

Важно: условие $gcd\left(a^{r/2} + 1, N\right) = 1$ можно заменить на условие $a^{r/2} + 1 \nmid N$.

Утверждение 1.1.1. *Пусть* $N = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$ *и*

$$S = \left\{a \in \mathbb{Z}_N : ord(a)\, mod 2 = 0 \vee a^{ord(a)/2} + 1 \nmid N\right\}$$

Тогда

$$|S| \leq \frac{\varphi(N)}{2^k}$$

То есть, подходящих нам a очень мало.

1.2 Алгоритм факторизации с оракулом

1. Генерируем такое a, чтобы при $r = O_f(a)$ выполняясь

$$r = 2 \cdot r_1, a^{r_\alpha} + 1 \nmid N$$

2. $gcd(a^{r_1} - 1, N)$ — нетривиальный делитель.

Утверждение 1.2.1. *В классической модели найти оракул O_f не получилось. Шору удалось построить его в квантовой модели.*

Рассмотрим функцию $f : \mathbb{Z}_N \to \mathbb{Z}_N$

$$f(x) = a^x \mod N$$

Это почти непериодическая функция — её период не кратен N.

1.3 Квантовая система

У нас есть $|0\rangle$, $|1\rangle$; кубит находится в суперпозиции состояний $\alpha_1 \cdot |0\rangle + \alpha_2 |1\rangle$, над которыми можно выполнять унитарные операции в пространстве Гильберта $C \cdot \mathbb{Z}_2$.

Коэффициенты α_1, α_2:

- $\alpha_1, \alpha_2 \in \mathbb{C}$,
- $|\alpha_1|^2 + |\alpha_2|^2 = 1$,
- $|\alpha_1|^2$ — вероятность попасть в $|0\rangle$,
- $|\alpha_2|^2$ — вероятность попасть в $|1\rangle$.

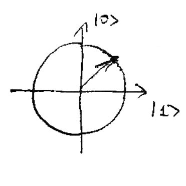

Рис. 1.1: Состояние кубита

К кубитам можно применять преобразование Уолша-Адамара

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

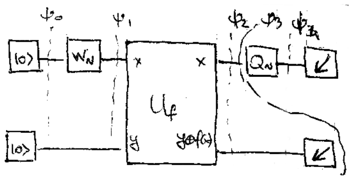

Рис. 1.2: Алгоритм Шора

Набор кубитов — одна из возможных интерпретаций квантово-механической системы. Другой вариант — N-уровневая система, в которое есть N состояний $|0\rangle$, $|1\rangle$, ..., $|N-1\rangle$, и эти состояния ортонормированы (то есть, при измерении выпадают только эти состояния и ничего среднего между ними).

Обозначения на рис. 1.2:

- ψ_i — состояние системы,
- W_N — преобразование Уолша (или преобразование Фурье),
- U_f — стандартный оракул (базисный в квантовой модели),
- Q_N — преобразование Фурье,
- стрелочка — измерение.

Что происходит?

1. $$|\psi_0\rangle = |0\rangle\,|0\rangle$$

2. $$|\psi_1\rangle = W_N\left(|0\rangle\right) \otimes |0\rangle$$

   Свойство: $W_N\left(|0\rangle\right)$ даёт равномерную суперпозицию (что Уолш, что Фурье), то есть

   $$W_N\left(|0\rangle\right) = \frac{1}{\sqrt{N}} \cdot \left(|0\rangle + |1\rangle + \dots + |N-1\rangle\right)$$

3. Суперпозиция всех значений функции $f(x) = a^x \mod N$

   $$|\psi_2\rangle = \frac{1}{\sqrt{N}} \cdot \Big(|0\rangle \cdot \left|a^0 \mod N\right\rangle + |1\rangle \cdot \left|a^1 \mod N\right\rangle + \dots + |N-1\rangle \cdot \left|a^{N-1}\right\rangle \mod N\Big)$$

4. Мы измерили второй регистр – там второй кубит принял некоторое значение $|y_0\rangle$

   $$|\psi_0\rangle = \frac{1}{\sqrt{k}} \cdot \left(|x_0\rangle + |x_0 + r\rangle + \dots + |x_0 + (k-1) \cdot r\rangle\right) \cdot |y_0\rangle\,,$$

   где $|x_0\rangle$ — все состояния $|x\rangle$, для которых $f(x) = y_0$, $k = \lfloor \frac{N}{r} \rfloor$.

5. Преобразование Фурье

$$Q_N\left(|k\rangle\right) = \frac{1}{\sqrt{N}} \cdot \sum_t \exp\frac{2 \cdot \pi \cdot i}{N} \cdot k \cdot t \cdot |t\rangle$$

Применяя его к первому регистру, получаем

$$|\psi_4\rangle = \sum_S c\left(S\right) \cdot |S\rangle \cdot |y_0\rangle\,,$$

где

$$c\left(S\right) = \begin{cases} \dfrac{\sqrt{N}}{r} & , S \equiv 0 \mod \dfrac{N}{r}, \\ 0 & , S \not\equiv 0 \mod \dfrac{N}{r}. \end{cases}$$

Таким образом это будет или 0, или равномерная суперпозиция.

6. Измеряем первый регистр — можем получить тоьлко те S, у которых $c\left(S\right) \neq 0$, т.е. состояния вида $\left|\beta \cdot \dfrac{N}{r}\right\rangle$, где β — неизвестная константа.

Таким образом мы знаем какое-то число S такое, что

$$S = \beta \cdot \frac{N}{r}.$$

Если $gcd\left(S, N\right) = 1$ и $N \mid r$, то всё, но у нас $N \nmid r$! Поэтому на самом деле

$$\frac{S}{N} = \frac{\beta}{r},$$

и мы строим рациональные приближения при помощи цепных дробей.

Итоговая сложность алгоритма Шора — $O\left(\log^3 N\right)$.

Оглавление