Квантовые вычисления
Глава 4

Сысоев Сергей Сергеевич

Санкт-Петербургский государственный университет
Математико-механический факультет
http://se.math.spbu.ru/

1 Введение

Материал этой главы посвящен, наверно, наиболее известному и нашумевшему квантовому алгоритму – алгоритму Шора, предложенному американским математиком Питером Шором в 1994 году. Алгоритм Шора – это квантовый алгоритм, позволяющий разложить составное число на простые множители. Процесс разложения чисел на простые множители называется факторизацией.

Важным параметром алгоритмов факторизации является динамика роста ресурсов, требуемых для выполнения задачи в зависимости от размеров факторизуемого числа. Представим, например, что некоторое большое число N состоит из простых множителей p и q, нам неизвестных ($N = p \cdot q$). Если мы захотим найти эти множители простым перебором, то нам потребуется попробовать все потенциальные множители от 2 до $\sqrt{N}$, что является практически невыполнимой операцией для достаточно больших N. Классические алгоритмы решения этой задачи, известные на настоящий момент, не намного лучше такого перебора. Это дает возможность как бы "спрятать" два разных простых числа в их произведении. Все могут видеть произведение, но никто не может узнать сами числа.

Оказывается, пользуясь этой несимметричностью процессов умножения и факторизации, можно прятать у всех на виду не только сами известные нам большие простые числа, но и вообще что угодно! Более того, вы можете предоставить всему миру возможность зашифровывать информацию таким образом, что прочитать ее сможете только вы. Подобное шифрование называется ассиметричным, или шифрованием с открытым ключом. Идея такова: у нас есть два ключа – один секретный, второй – открытый. Открытый ключ знают все вокруг. Если кто-то хочет послать нам секретное сообщение, он шифрует его открытым ключом, после чего никто, кроме нас расшифровать это сообщение уже не может. Это можно сделать только секретным ключом.

Ассиметричные алгоритмы шифрования очень важны, поскольку они позволяют, например, наладить закрытый канал передачи данных по открытой сети между заранее незнакомыми корреспондентами. Например, без ассиметричного шифрования стал бы неосуществим процесс "рукопожатия"

(handshake) в протоколе https, и, следовательно, стало бы невозможным защищенное соединение без предварительной договоренности.

Впервые алгоритм ассиметричного шифрования, основанный на сложности процесса факторизации, был предложен англичанином Клиффордом Коксом в 1973 году. Результат Кокса был настолько высоко оценен английским правительством, что его немедленно засекретили. Поэтому официально первооткрывателями алгоритма считаются трое американцев – Ron **R**ivest, Adi **S**hamir и Leonard **A**dleman, опубликовавшие его в 1977 году. В их честь алгоритм назван по первым буквам фамилий – RSA.

2 Факторизация и RSA

Нам будет полезно вспомнить алгоритм RSA.

Пусть p и q – большие не равные друг другу простые числа, а число $N = p \cdot q$. Тогда, по теореме Эйлера

$$\forall a < N : \ (a, N) = 1$$

$$a^{\Phi(N)} = 1(N), \tag{1}$$

где $\Phi(N)$ – функция Эйлера, равная количеству чисел, меньших аргумента (N), взаимопростых с ним (включая единицу).

$$\Phi(N) = (p-1)(q-1)$$

Выберем некоторое число $e < N, \ (e, N) = 1, \ (e, \Phi(N)) = 1$. Тогда

$$\exists d < N : \ e \cdot d = 1(\Phi(N))$$

или

$$\exists d, k : \ e \cdot d + \Phi(N) \cdot k = 1 \tag{2}$$

Единица является наибольшим общим делителем чисел e и $\Phi(N)$, а (2) является линейным представлением НОД, которое можно найти, например, с помощью расширенного алгоритма Евклида. Назовем:
$m < N, (m, N) = 1$ – сообщением,
e, N – открытым ключом,
d, N – закрытым ключом.

Открытый ключ, как правило, делается доступным широкому кругу лиц (потенциальных корреспондентов), а числа $d, \Phi(N), p$ и q держаться в секрете.

Сообщения для нас теперь может зашифровать любой, кому известен открытый ключ:

$$encode(m) = m^e(N),$$

а расшифровать только мы:

$$decode(encode(m)) = (encode(m))^d(N) = (m^e)^d(N) =$$

$$= m^{e \cdot d}(N) = m^{1+\Phi(N) \cdot k}(N) = m \cdot m^{\Phi(N) \cdot k}(N) \overset{(1)}{=} m$$

Рассмотрим пример. Пусть

$$p = 11,\ q = 13$$

$$N = p \cdot q = 143$$

$$\Phi(N) = 10 * 12 = 120$$

$$e = 17$$

Пара $\{N, e\} = \{143, 17\}$ – открытый ключ. Зашифруем с помощью этого ключа сообщение "7":

$$7^{17}(143) = 7 \cdot 49^8(143) = 7 \cdot 2401^4(143) = 7 \cdot 113^4(143) =$$

$$= 7 \cdot (-30)^4(143) = 7 \cdot 900^2(143) = 7 \cdot 42^2(143) = 7 \cdot 48(143) = 50(143)$$

Итак, "50" – зашифрованное сообщение. Для того, чтобы расшифровать его, необходимо найти число d, удовлетворяющее (2):

$$17 \cdot d = 1 + 120 \cdot k$$

Для этого мы можем воспользоваться расширенным алгоритмом Евклида или, например, заметить, что:

$$17 \cdot 7 = 119 = 120 - 1$$

$$17 \cdot (-7) = 1 + 120 \cdot (-1)$$

$$d = -7 = 113(120)$$

Пара $\{N, d\} = \{143, 113\}$ является закрытым ключом, с помощью которого мы можем расшифровать сообщение:

$$50^{113} = 7(143)$$

Как видите, вся надежность алгоритма RSA основана на том, что злоумышленник не может узнать разложения числа N на множители за разумное время, чтобы получить значение $\Phi(N)$ и, далее d.

Все изменилось с появлением алгоритма Шора!

3 Поиск периода и факторизация

Алгоритм Шора предназначен для поиска неизвестного периода некоторой периодической функции. Почему же тогда я обещал, что он позволит раскладывать числа на множители? Давайте разберемся.

Пусть p и q различные простые числа и $N = p \cdot q$. Для некоторого числа $a < N :\ (a, N) = 1$ определим функцию $f_a(x)$:

$$f_a(x) = a^x(N)$$

Функция f_a периодическая, и ее период r является порядком числа a в кольце $\mathbb{Z}_N$:

$$a^r = 1(N)$$

$$\forall r_1 < r \quad a^{r_1} \neq 1(N)$$

Если в нашем распоряжении есть устройство, умеющее находить период любой периодической функции, то с помощью этого устройства, выбрав случайным образом число a, мы можем найти период r функции f_a.
Допустим, что число r – четное.

$$r = 0(2) \tag{3}$$

Тогда выражение

$$a^r - 1 = 0(N)$$

мы можем представить в виде

$$(a^{r/2} - 1)(a^{r/2} + 1) = N \cdot k$$

Число $(a^{r/2} - 1)$ не делится на N, так как иначе $a^{r/2}$ было бы сравнимо с 0 по модулю N, и число $r/2$ было бы периодом.
Допустим также, что

$$(a^{r/2} + 1) \neq 0(N) \tag{4}$$

Тогда произведение $(a^{r/2} - 1)(a^{r/2} + 1)$ делится на N, но ни один из множителей $(a^{r/2} - 1)$, $(a^{r/2} + 1)$ не делится на N целиком. Следовательно, числа $(a^{r/2} - 1)$, $(a^{r/2} + 1)$ не взаимнопросты с N, и мы можем найти p и q с помощью алгоритма Евклида:

$$p, q = GCD(a^{r/2} \pm 1,\ N)$$

(Здесь GCD – Greatest Common Divisor, НОД).

В ходе рассуждения мы сделали два допущения – (3) и (4). Нам необходимо оценить, с какой вероятностью для наугад выбранного числа a его порядок r удовлетворяет этим условиям.

Рассмотрим числа a_1 и a_2:

$$a_1 = a(p)$$

$$a_2 = a(q)$$

и их порядки r_1 и r_2 в кольцах $\mathbb{Z}_p$ и $\mathbb{Z}_q$ соответственно. В кольце $\mathbb{Z}_p$ выполняется равенство

$$a_1^r(p) = a^r(p) = 1,$$

так как $a^r = 1(pq)$. Поскольку r_1 – порядок числа a_1 в $\mathbb{Z}_p$, число r должно делиться на r_1. Аналогичные рассуждения для $\mathbb{Z}_q$ приводят нас к выводу, что число r должно делиться также и на r_2.

Кроме того, для произвольного числа s его делимости на r_1 и r_2 достаточно, чтобы s делилось также и на r:

$$a^s = p \cdot k_1 + 1 \tag{5}$$

т.к. s делится на r_1.

$$a^s = q \cdot k_2 + 1 \tag{6}$$

т.к. s делится на r_2.

Вычитая (6) из (5), получаем

$$p \cdot k_1 = q \cdot k_2 \tag{7}$$

Поскольку p не делится на q, из (7) следует, что k_1 должно делиться на q и, следовательно, из (5) мы имеем

$$a^s = p \cdot q \cdot \frac{k_1}{q} + 1 \implies a^s = 1(p \cdot q) \implies s|r$$

Поскольку число r делится на числа r_1 и r_2, и любое число, делящееся на r_1 и r_2, делится также и на r, мы получаем, что r есть наименьшее общее кратное чисел r_1 и r_2 ($r = \text{НОК}(r_1, r_2)$).

Выделим в числах r_1 и r_2 степени 2:

$$r_1 = 2^{c_1} \cdot odd_1,\ c_1 \geq 0$$

$$r_2 = 2^{c_2} \cdot odd_2,\ c_2 \geq 0$$

Если предположить, что, например, $c_1 > c_2$, то r в своем составе будет содержать полностью r_2 и, как минимум, одну двойку:

$$r = 2 \cdot r_2 \cdot int$$

$$a^{r/2} = a^{r_2 \cdot int} = 1(q) \implies a^{r/2} \neq -1(q) \implies a^{r/2} \neq -1(p \cdot q)$$

Таким образом, если степени 2 в составе чисел r_1 и r_2 не совпадают, то оба условия (3) и (4) выполняются, и задача разложения на множители успешно сводится к задаче поиска периода функции.

Число a мы выбирали случайно, но случайны ли степени двойки в числах r_1 и r_2? Для ответа на этот вопрос выделим степень 2 в числе $p - 1$:

$$p = 2^k \cdot s + 1, \quad s = 1(2)$$

В кольце $\mathbb{Z}_p$ есть примитивный элемент b, степени которого образуют все кольцо. Порядок b равен $2^k \cdot s$. Выбрав число a мы тем самым случайно выбрали число $a_1 = a(p)$, и случайно выбрали число $m \in \{1, \cdots, 2^k \cdot s\}$:

$$a_1 = b^m(p)$$

Мы помним, что r_1 – порядок числа a_1:

$$a_1^{r_1}(p) = 1 \implies b^{m \cdot r_1} = 1 = b^{2^k \cdot s} \implies m \cdot r_1 = 0(2^k \cdot s)$$

Получается, что произведение чисел m и r_1 делится на 2^k, при этом число m выбрано случайно из интервала $\{1, \cdots, 2^k \cdot s\}$. Таким образом, вероятность P_i того, что r_1 делится на 2^i при $i \in \{0, \cdots, k\}$ равна вероятности того, что случайно выбранное число m делится на 2^{k-i}. Из этого мы можем заключить, что степени 2 в числах r_1 и r_2 встречаются так же случайно, как и в случайно выбранных числах.

Нам осталось определить вероятность того, что в двух случайно выбранных числах встретится одинаковая степень 2. Обозначим P_i – вероятность того, что в случайно выбранном числе содержится 2 ровно в степени i. Тогда:

$$P_0 = \frac{1}{2},\ P_1 = \frac{1}{4},\ P_2 = \frac{1}{8},$$

$$P_i = P_{i-1} - \frac{1}{2}P_{i-1} = \frac{1}{2^i} - \frac{1}{2^{i+1}} = \frac{1}{2^{i+1}}$$

Для степеней 2 от 0 до k, вероятность встретить одинаковые степени 2 в двух случайно выбранных числах равна:

$$P = \sum_{i=0}^{k} P_i^2 = \left(\frac{1}{2}\right)^2 + \left(\frac{1}{4}\right)^2 + \left(\frac{1}{8}\right)^2 + \cdots + \left(\frac{1}{2^{k+1}}\right)^2 =$$

$$\left(\frac{1}{2^{k+1}}\right)^2 (1 + 2^2 + 4^2 + \cdots 2^{2k}) \leq \tag{8}$$

Число в скобках в (8) помещается в регистр длиной $2k$ битов, следовательно оно меньше числа 2^{2k+1}:

$$\leq \left(\frac{1}{2^{k+1}}\right)^2 2^{2k+1} = \frac{1}{2}$$

Получается, что вероятность неудачи сведения задачи факторизации к задаче поиска периода при выборе числа a не больше $1/2$.

4 Квантовое преобразование Фурье

Для алгоритма Шора нам потребуется новый квантовый оператор – квантовое преобразование Фурье (Quantum Fourier Transform, QFT):

$$N := 2^n$$

$$QFT\,|x\rangle = \frac{\|x\|}{2^{n/2}} \sum_{y=0}^{2^n-1} e^{2\pi i \frac{xy}{N}}\,|y\rangle \tag{9}$$

Унитарность QFT

По традиции проверим унитарность нового оператора:

$$\|QFT\,|x\rangle\,\|^2 = \frac{\|x\|^2}{2^n} \sum_{y=0}^{2^n-1} |e^{2\pi i \frac{xy}{N}}|^2 =$$

$$= \frac{\|x\|^2}{2^n} \sum_{y=0}^{2^n-1} 1 = \frac{\|x\|^2}{2^n} 2^n = \|x\|^2$$

Оператор QFT не меняет норму вектора. Здесь и далее мы имеем дело только с векторами единичной длины, поэтому вместо $\|x\|$ в выражении (9) мы будем писать 1.
Проверим, что QFT не меняет также углы между векторами:

$$\|x_1\| = \|x_2\| = 1,\ \langle x_1|x_2\rangle = 0$$

$$\langle QFT\,|x_1\rangle \ |\ QFT\,|x_2\rangle\rangle = \frac{1}{2^n}\left\langle \sum_{y_1=0}^{2^n-1} e^{2\pi i \frac{x_1 y_1}{N}}\,|y_1\rangle \,\middle|\, \sum_{y_2=0}^{2^n-1} e^{-2\pi i \frac{x_2 y_2}{N}}\,|y_2\rangle \right\rangle =$$

$$= \frac{1}{2^n} \sum_{y_1=y_2} \left\langle e^{2\pi i \frac{x_1 y_1}{N}}\,|y_1\rangle \,\middle|\, e^{-2\pi i \frac{x_2 y_2}{N}}\,|y_2\rangle \right\rangle + \frac{1}{2^n} \sum_{y_1\neq y_2} \left\langle e^{2\pi i \frac{x_1 y_1}{N}}\,|y_1\rangle \,\middle|\, e^{-2\pi i \frac{x_2 y_2}{N}}\,|y_2\rangle \right\rangle =$$

$$= \frac{1}{2^n} \sum_{y_1=y_2} \left\langle e^{2\pi i \frac{x_1 y_1}{N}}\,|y_1\rangle \,\middle|\, e^{-2\pi i \frac{x_2 y_2}{N}}\,|y_2\rangle \right\rangle = \frac{1}{2^n} \sum_{y=0}^{2^n-1} e^{2\pi i \frac{(x_1-x_2)y}{N}} \qquad (10)$$

Выражение, полученное нами в конце, является суммой арифмитической прогрессии:

$$\sum_{y=0}^{2^n-1} a^y = \frac{a^{2^n}-1}{a-1} \qquad (11)$$

Применяя (11) к (10), получаем:

$$(10) = \frac{e^{2\pi i(x_1-x_2)}-1}{e^{2\pi i \frac{(x_1-x_2)}{N}}-1} = \frac{1-1}{e^{2\pi i \frac{(x_1-x_2)}{N}}-1} = 0$$

Преобразование QFT отображает ортонормированный базис в ортонормированный базис, следовательно оно унитарно.

QFT. Реализация.
Оценим сложность реализации оператора QFT на квантовом компьютере.
Во-первых, заметим, что:

$$QFT\,|x\rangle = \frac{1}{2^{n/2}} \sum_{y=0}^{2^n-1} e^{2\pi i \frac{xy}{N}}\,|y\rangle = \frac{1}{2^{n/2}} \sum_{y=0}^{2^n-1} e^{2\pi i \frac{xy(N)}{N} + k\cdot 2\pi i}\,|y\rangle =$$

$$= \frac{1}{2^{n/2}} \sum_{y=0}^{2^n-1} e^{2\pi i \frac{xy(N)}{N}}\,|y\rangle \qquad (12)$$

Здесь:
$xy(N)$ – $x \cdot y$ по модулю N,
k – результат деления xy на N нацело.

Запишем числа x и y в двоичной системе счисления:

$$x = x_0 + x_1 \cdot 2 + x_2 \cdot 2^2 + \cdots + x_{n-1} \cdot 2^{n-1}$$

$$y = y_{n-1} \cdot 2^{n-1} + y_{n-2} \cdot 2^{n-2} + \cdots + y_1 \cdot 2 + y_0$$

Выражение $\frac{xy(N)}{N}$ тогда можно записать так:

$$\frac{xy(N)}{N} = y_{n-1}\frac{x_0}{2} + y_{n-2}\left(\frac{x_0}{4} + \frac{x_1}{2}\right) + \cdots + y_0\left(\frac{x_0}{2^n} + \frac{x_1}{2^{n-1}} + \cdots + \frac{x_{n-1}}{2}\right) \quad (13)$$

Подставив (13) в (12), получаем:

$$(12) = \frac{1}{2^{n/2}} \sum_{y=0}^{2^n-1} e^{2\pi i\left(y_{n-1}\frac{x_0}{2} + y_{n-2}\left(\frac{x_0}{4}+\frac{x_1}{2}\right) + \cdots + y_0\left(\frac{x_0}{2^n} + \frac{x_1}{2^{n-1}} + \cdots + \frac{x_{n-1}}{2}\right)\right)} |y\rangle =$$

$$= \frac{1}{2^{n/2}} \sum_{y=0}^{2^n-1} e^{2\pi i y_{n-1}\frac{x_0}{2}} e^{2\pi i y_{n-2}\left(\frac{x_0}{4}+\frac{x_1}{2}\right)} \cdots e^{2\pi i y_0\left(\frac{x_0}{2^n} + \frac{x_1}{2^{n-1}} + \cdots + \frac{x_{n-1}}{2}\right)} |y\rangle =$$

Выделим в y старший бит:

$$= \frac{1}{\sqrt{2}} e^{2\pi i \cdot 0 \cdot \frac{x_0}{2}} |0\rangle \otimes \frac{1}{2^{\frac{n-1}{2}}} \sum_{y=0}^{2^n-2} e^{2\pi i y_{n-2}(\cdots)} \cdots e^{2\pi i y_0(\cdots)} |y_{n-2}y_{n-1}\cdots y_0\rangle +$$

$$+ \frac{1}{\sqrt{2}} e^{2\pi i \cdot 1 \cdot \frac{x_0}{2}} |1\rangle \otimes \frac{1}{2^{\frac{n-1}{2}}} \sum_{y=0}^{2^n-2} e^{2\pi i y_{n-2}(\cdots)} \cdots e^{2\pi i y_0(\cdots)} |y_{n-2}y_{n-1}\cdots y_0\rangle =$$

$$= \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i \frac{x_0}{2}} |1\rangle\right) \otimes \frac{1}{2^{\frac{n-1}{2}}} \sum_{y=0}^{2^n-2} e^{2\pi i y_{n-2}(\cdots)} \cdots e^{2\pi i y_0(\cdots)} |y_{n-2}y_{n-1}\cdots y_0\rangle =$$

Аналогичным образом выделим остальные биты в y:

$$= \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i \frac{x_0}{2}} |1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\left(\frac{x_0}{4}+\frac{x_1}{2}\right)} |1\rangle\right) \otimes \cdots$$

$$\cdots \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\left(\frac{x_0}{2^n} + \cdots + \frac{x_{n-1}}{2}\right)} |1\rangle\right) \quad (14)$$

Получается, что $QFT\,|x\rangle$ раскладывается в тензорное произведение из n операторов, каждый из которых действует на один кубит.

Определим унитарный оператор R_k, действующий на 1 кубит:

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

На (fig. 1) приведена схема $QFT\,|x\rangle$ на 3-х кубитах, реализованная с помощью операторов R_k и H. Обратите внимание, что схема меняет порядок

кубитов, делая старшие кубиты младшими.
Верхняя линия схемы соответствует первой скобке в (14):

$$\frac{1}{\sqrt{2}}\big(\,|0\rangle + e^{2\pi i\frac{x_0}{2}}\,|1\rangle\,\big) = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_0}\,|1\rangle) = H\,|x_0\rangle\,,$$

которая в свою очередь соответствует старшему биту $QFT\,|x\rangle$.
Вторая линия схемы соответствует второй скобке:

$$H\,|x_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_1}\,|1\rangle) = \frac{1}{\sqrt{2}}\big(\,|0\rangle + e^{2\pi i\frac{x_1}{2}}\,|1\rangle\,\big) \xrightarrow{R_2(x_0)}$$

$$\xrightarrow{R_2(x_0)} \frac{1}{\sqrt{2}}\big(\,|0\rangle + e^{2\pi i(\frac{x_0}{4}+\frac{x_1}{2})}\,|1\rangle\,\big),$$

и, наконец, третья линия соответствует третьей скобке:

$$|x_2\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}\big(\,|0\rangle + e^{2\pi i\frac{x_2}{2}}\,|1\rangle\,\big) \xrightarrow{R_3(x_0)}$$

$$\xrightarrow{R_3(x_0)} \frac{1}{\sqrt{2}}\big(\,|0\rangle + e^{2\pi i(\frac{x_2}{2}+\frac{x_0}{8})}\,|1\rangle\,\big) \xrightarrow{R_2(x_1)}$$

$$\xrightarrow{R_2(x_1)} \frac{1}{\sqrt{2}}\big(\,|0\rangle + e^{2\pi i(\frac{x_2}{2}+\frac{x_1}{4}+\frac{x_0}{8})}\,|1\rangle\,\big)$$

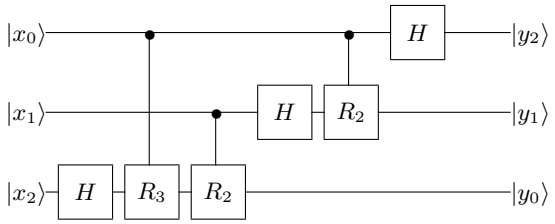

Fig. 1. QFT на трех кубитах.

Обобщая схему (1) на n кубитов, мы можем увидеть, что для реализации QFT требуется

$$\sum_{j=1}^{n} j \approx O(n^2)$$

операторов R_k и H.

5 Алгоритм Шора

Подготовка закончена, настала пора перейти к самому алгоритму. Схема алгоритма Шора представлена на (fig. 2). Практически полностью эта схема повторяет алгоритм Саймона, за исключением последнего шага – прямо перед измерением входного регистра вместо оператора Адамара H_n вызывается описанный в предыдущем параграфе оператор QFT.

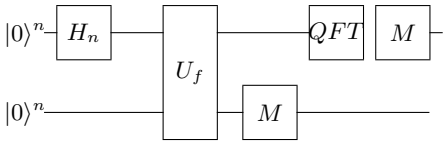

Fig. 2. Алгоритм Шора.

Рассмотрим действие алгоритма. Как и в алгоритме Саймона, после измерения регистра $|y\rangle$ мы получаем в регистре $|x\rangle$ сумму всех прообразов измеренного нами значения:

$$|0\rangle^n |0\rangle^n \xrightarrow{H_n} \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle |0\rangle^n \xrightarrow{U_f} \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle |f(x)\rangle \xrightarrow{Measure\ Y}$$

$$\xrightarrow{Measure\ Y} \frac{1}{\sqrt{A}} \sum_{j=0}^{A-1} |x_0 + jr\rangle |f(x_0)\rangle$$

Здесь A – количество всех прообразов $f(x_0)$:

$$A \approx \frac{N}{r}$$

$$N - r \leq Ar \leq N + r$$

Далее по схеме следует применение QFT к регистру $|x\rangle$:

$$\frac{1}{\sqrt{A}} \sum_{j=0}^{A-1} |x_0 + jr\rangle \xrightarrow{QFT} \frac{1}{\sqrt{AN}} \sum_{j=0}^{A-1} \sum_{y=0}^{2^n-1} e^{2\pi i \frac{x_0 y}{N}} e^{2\pi i \frac{jry}{N}} |y\rangle =$$

$$= \frac{1}{\sqrt{AN}} \sum_{y=0}^{2^n-1} e^{2\pi i \frac{x_0 y}{N}} \sum_{j=0}^{A-1} e^{2\pi i \frac{jry}{N}} |y\rangle$$

Вероятность измерения конкретного y будет равна:

$$P(y) = \frac{1}{AN} |e^{2\pi i \frac{x_0 y}{N}}|^2 \left| \sum_{j=0}^{A-1} e^{2\pi i \frac{jry}{N}} \right|^2 =$$

$$= \frac{1}{AN}\left|\sum_{j=0}^{A-1} e^{2\pi i \frac{jry}{N}}\right|^2 \tag{15}$$

Обозначим:

$$\theta_y = 2\pi\frac{ry(N)}{N}$$

Заметим, что сумма под модулем в (15) является суммой геометрической прогресии:

$$\sum_{j=0}^{A-1} e^{2\pi i \frac{jry}{N}} = \sum_{j=0}^{A-1} e^{\theta_y j} = \frac{e^{A\theta_y i}-1}{e^{\theta_y i}-1} \tag{16}$$

Назовем "хорошими" такие y, для которых выполняется условие:

$$A|\theta_y| \in [0,\pi] \tag{17}$$

Для "хороших" y верно:

$$|e^{A\theta_y i}-1| \geq \frac{2A|\theta_y|}{\pi} \tag{18}$$

Для доказательства (18) обозначим $A|\theta_y| =: x$. Тогда:

$$|e^{xi}-1| = |\cos x - 1 + i\sin x| = \sqrt{(\cos x - 1)^2 + \sin^2 x} =$$

$$= \sqrt{2-2\cos x} = \sqrt{2(\cos^2\frac{x}{2} + \sin^2\frac{x}{2}) - 2\cos^2\frac{x}{2} + 2\sin^2\frac{x}{2}} = 2\sin\frac{x}{2}$$

т.к. на промежутке $[0,\pi/2]$ $sin(x)$ положителен.

Таким образом, от нас требуется доказать, что

$$\sin\frac{A|\theta_y|}{2} \geq \frac{A|\theta_y|}{\pi}$$

На границах отрезка $[0,\pi]$ левая и правая часть неравенства равны друг другу:

$$\sin 0 = 0$$
$$\sin\frac{\pi}{2} = \frac{\pi}{\pi} = 1$$

Поскольку на отрезке $[0,\pi]$ левая часть неравенства – функция sin выпукла вверх, а правая часть неравенства – линейная функция, то неравенство выполняется на всем отрезке $[0,\pi]$.

Также верно, что

$$|e^{\theta_y i}-1| \leq |\theta_y| \tag{19}$$

поскольку хорда не длиннее стягиваемой ей дуги (fig. 3):

Из (16), (18) и (19) получаем оценку вероятности измерения "хорошего" y:

$$(15) \geq \frac{1}{AN}\left(\frac{2A|\theta_y|}{\pi}\right)^2\left(\frac{1}{|\theta_y|}\right)^2 = \frac{4A}{\pi^2 N} \approx \frac{4}{\pi^2 r} \tag{20}$$

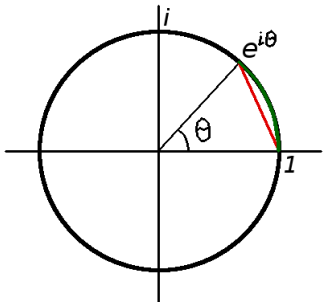

Fig. 3. Значения (19) на комплексной плоскости.

Вспомним, что "хорошими" мы назвали значения y, для которых выполняется:

$$A|\theta_y| \in [0,\pi] \iff$$
$$\iff -\pi \le 2\pi\frac{A\cdot yr(N)}{N} \le \pi \iff$$
$$\iff -\frac{1}{2} \le \frac{yr(N)}{r} \le \frac{1}{2} \iff$$
$$\iff -\frac{r}{2} \le yr(N) \le \frac{r}{2} \iff$$
$$\iff Nk - \frac{r}{2} \le yr \le Nk + \frac{r}{2} \tag{21}$$

Неравенство (21) для любого значения $k \in \mathbb{N}\cup\{0\}$ имеет единственное решение y_k, при этом:

$$y_0 = 0,$$
$$y_r = N = 0(N) = y_0(N)$$

Получается, что различных "хороших" y может быть всего r штук, а вероятность измерения любого из них в r раз больше, чем вероятность измерения какого-то конкретного:

$$P(y =' good') = \frac{4}{\pi^2 r}\cdot r = \frac{4}{\pi^2} \approx 0,406\cdots \tag{22}$$

Что делать с "хорошим" y?
Мы увидели, что оператор QFT, применяемый в конце схемы алгоритма Шора, значительно повышает вероятность измерения векторов y, которые мы назвали "хорошими". Чтобы понять, почему имеено эти вектора получили у нас такое одобрительное название, разделим определяющее их неравенство (21) на Nr:

$$\frac{(21)}{Nr} \iff \frac{k}{r} - \frac{1}{2N} \le \frac{y}{N} \le \frac{k}{r} + \frac{1}{2N} \iff$$

$$\iff \left|\frac{y}{N} - \frac{k}{r}\right| \leq \frac{1}{2N}$$

Получается, что в окрестности шириной $1/N$ известного нам числа $\frac{y}{N}$ находится число $\frac{k}{r}$, безусловно представляющее для нас интерес из-за своего знаменателя. Знаменатель дроби $\frac{k}{r}$ либо является искомым периодом r, либо одним из его делителей.

Если предположить, что:

$$r < \sqrt{N}, \tag{23}$$

то можно показать, что число со знаменателем, меньшим $\sqrt{N}$ в заданной окрестности единственно:

$$a, b, r_1, r_2 \in \mathbb{N},\ a \neq b$$

$$r_1 < \sqrt{N},\ r_2 < \sqrt{N}$$

$$\left|\frac{a}{r_1} - \frac{b}{r_2}\right| = \frac{|a \cdot r_2 - b \cdot r_1|}{r_1 \cdot r_2} \geq \frac{1}{r_1 \cdot r_2} \geq \frac{1}{\sqrt{N}\sqrt{N}} = \frac{1}{N}$$

Предположение (23) кажется очень вероятным. Число r является делителем $\Phi(N)$. В наихудшем для нас случае числа p и q представляются, как

$$p = 2p_1 + 1,\ q = 2q_1 + 1,$$

где числа p_1 и q_1 простые. Тогда функция Эйлера содержит наименьшее количество простых множителей:

$$\Phi(N) = (p-1)(q-1) = 4p_1q_1,$$

и какой-то из них – p_1 или q_1 может оказаться больше $\sqrt{N}$. Поэтому даже в наихудшем случае вероятность получить $r \geq \sqrt{N}$ не больше $1/2$.

Таким образом, после выполнения алгоритма Шора у нас есть число $\frac{y}{N}$ и окрестность этого числа шириной $\frac{1}{N}$, содержащая интересующее нас число $\frac{k}{r}$ – единственное число со знаменателем меньше $\sqrt{N}$ в этой окрестности.

Поиск числа $\frac{k}{r}$ можно осуществить, например, с помощью метода непрерывной дроби, позволяющего находить числа, близкие к данному рациональному числу и имеющие меньший знаменатель.

Например:

$$n = 10,\ 2^n = N = 1024,\ \sqrt{N} = 32$$

Измеренный нами y оказался равен 139:

$$\frac{y}{N} = \frac{139}{1024}$$

$$\frac{139}{1024} = \frac{1}{\frac{1024}{139}} = \frac{1}{7 + \frac{51}{139}} \approx \frac{1}{7}$$

$$\frac{1}{7+\frac{1}{\frac{139}{51}}} = \frac{1}{7+\frac{1}{\frac{139}{51}}} = \frac{1}{7+\frac{1}{2+\frac{37}{51}}} \approx \frac{2}{15}$$

$$\frac{1}{7+\frac{1}{2+\frac{37}{51}}} = \frac{1}{7+\frac{1}{2+\frac{1}{\frac{51}{37}}}} = \frac{1}{7+\frac{1}{2+\frac{1}{1+\frac{14}{37}}}} \approx \frac{3}{22}$$

Итак, число $22 < 32$ – вероятно, является либо периодом r, либо его делителем, конечно при условии, что y, который нам довелось измерить – "хороший", что случается с вероятностью $\approx 0{,}406...$, а период r меньше $\sqrt{N}$ (тоже с вероятностью не меньшей, чем $1/2$). Теперь, также с вероятностью не меньшей, чем $1/2$, мы можем использовать полученный период для решения изначальной задачи факторизации.

6 Пример реализации

Рассмотрим реализацию алгоритма Шора со следующими значениями параметров:

$$p = 3,\ q = 5,\ N = p \cdot q = 15$$

$$\Phi(N) = (5-1)(3-1) = 8$$

$$a = 7,\ f(x) = 7^x(15)$$

Функцию $f(x) : \{0,1\}^4 \to \{0,1\}^4$ представим в следующем виде:

$$f(x) = 7^x(15) = (7^8)^{x_3} \cdot (7^4)^{x_2} \cdot (7^2)^{x_1} \cdot (7^1)^{x_0}(15) = (7^2)^{x_1} \cdot (7^1)^{x_0}(15)$$

так как 4 – порядок числа 7 в $\mathbb{Z}_{15}$, $7^4 = 1(15)$.

$$(7^2)^{x_1} \cdot (7^1)^{x_0}(15) = (4)^{x_1} \cdot (7)^{x_0}(15) \tag{24}$$

Реализация алгорима для выбранных значений на квантовом симуляторе представлена на (fig. 4).

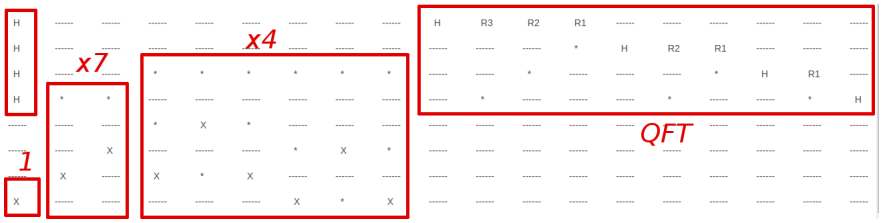

Fig. 4. Алгоритм Шора. $f(x) = 7^x(15)$

Блоки H_n и QFT на (fig. 4) нам уже знакомы. Требуется пояснить действие блоков, помеченных как "1", "x7" и "x4".

Блок "1" – это просто оператор X на младшем кубите регистра $|y\rangle$. В результате действия этого блока в регистре $|y\rangle$ появляется значение "1", которое, в соответствие с (24) необходимо будет домножить на 7, если бит $x_0 = 1$, и домножить на 4, если бит $x_1 = 1$.

Домножение регистра $|y\rangle$, содержащего 1, на 7 в зависимости от бита x_0 – это просто выставление оставшихся битов числа 7 в регистре операторами CNOT(x_0) (fig. 5).

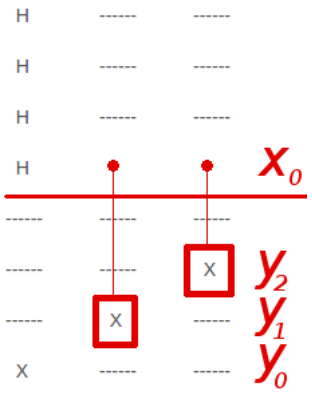

Fig. 5. Алгоритм Шора. Операция "×7"

Домножение регистра $|y\rangle$ на 4 в зависимости от бита x_1 – операция несколько более сложная. Домножение числа на 4 – это циклический сдвиг на 2, который реализуется переменой местами битов – $(y_0 \rightleftarrows y2)$ и $(y_1 \rightleftarrows y3)$ (fig. 6). Каждая замена осуществляется тремя операторами CNOT, которые в свою очередь контролируются еще и битом x_1.

По выполнении указанных операций и квантового преобразования Фурье в регистре $|x\rangle$ оказывается значение "0x0100 = 4".

$$\frac{y}{2^n} = \frac{4}{2^4} = \frac{1}{4}$$

Дробь $1/4$ сама подходит в кандидаты на роль $\frac{k}{r}$ из-за маленького знаменателя. Подставив значение "4" в функцию $f(x)$ получаем:

$$f(4) = 7^4(15) = 1$$

Мы нашли период r! Теперь попробуем найти числа p и q:

$$GCD(7^{\frac{4}{2}} + 1, 15) = GCD(50, 15) = 5$$

$$GCD(7^{\frac{4}{2}} - 1, 15) = GCD(48, 15) = 3$$

Числа p и q найдены. Алгоритм Шора работает!

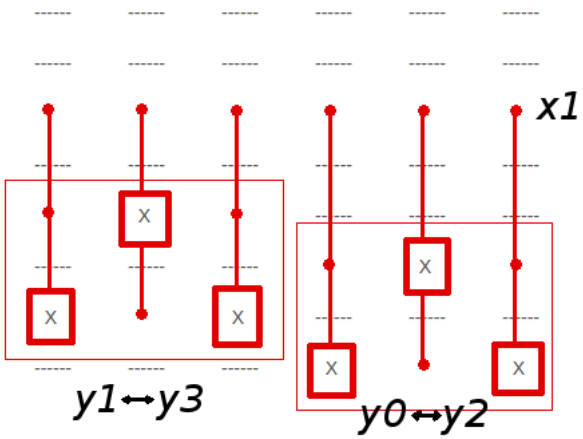

Fig. 6. Алгоритм Шора. Операция "×4"

7 Дополнительные материалы

1. **John Preskill. Lecture notes for "Physics 219/Computer Science 219. Quantum Computation" (Formerly Physics 229)**
   http://www.theory.caltech.edu/people/preskill/ph229/index.html
2. **Симулятор квантового компьютера.** http://qc-sim.appspot.com