1 Order Finding

Let x and N be two integers, and let $x = a_1 \cdot ... \cdot a_s$ and $N = b_1 \cdot ... \cdot b_t$, where a_i, b_j are primes. We say that x and N are coprime if

$$\{a_1, \cdots, a_s\} \cap \{b_1, \cdots, b_t\} = \emptyset.$$

For example integers $x = 15 = 5 \cdot 3,\ N = 28 = 2 \dots 2 \cdot 7$ are comprime.

Definition 1 *The least positive r such that $x^r \pmod N = 1$ is called the* **order** *of $x \pmod N$.*

Example 1 *Let $x = 3$ and $N = 4$. Then*

$$\begin{aligned} &3^1 \pmod 4 = 3 \\ &3^2 \pmod 4 = 9 \pmod 4 = 1 \\ &\Rightarrow r = 2. \end{aligned}$$

Let $L = \lceil \log_2 N \rceil$.
There are no classical algorithms for finding r with complexity $O(L)$(polynomial in L).

1.1 Unitary rotation corresponding to multiplication $\pmod N$ and its eigenvectors

For $0 \leqslant y \leqslant 2^L - 1$ we define $2^L \times 2^L$ matrix U by

$$U|y\rangle = \begin{cases} |xy \pmod N\rangle, & y < N, \\ |y\rangle, & N \leqslant y \leqslant 2^L - 1. \end{cases} \tag{1}$$

Example 2 *Let $x = 3,\ N = 4, \Rightarrow L = 2$*

$$\begin{array}{lr} |y\rangle : & |xy \pmod N\rangle : \\ |0\rangle & |0\rangle \\ |1\rangle & |3 \cdot 1 \pmod 4\rangle = |3\rangle \\ |2\rangle & |3 \cdot 2 \pmod 4\rangle = |2\rangle \\ |3\rangle & |3 \cdot 3 \pmod 4\rangle = |1\rangle \end{array}$$

It is not difficult to see that

$$U = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

It is easy to check that U is unitary: $U^\dagger U = \cdots = I_4$.

Lemma 1 *U is unitary.*

Proof $x = a_1 \cdots a_s,\ N = b_1 \cdots b_t,\ a_i \neq b_j$ for $\forall i, j \Rightarrow b_j \nmid x$.
All $xy \pmod N$ are distinct. To show this let us assume that $y_1,\ y_2$ are such that

$$y_2 < y_1 < N, \text{ and } xy_1 \pmod N = xy_2 \pmod N = c.$$

Then

$$xy_1 = Nt_1 + c,\ xy_2 = Nt_2 + c, \text{ for some } t_1, t2, \text{ and } t_1 > t_2.$$

Hence

$$xy_1 - xy_2 = x(y_1 - y_2) = N(t_1 - t_2) = \underbrace{b_1 \cdots b_t}_{\text{Do not contribute to } x, \text{ only to } (y_1 - y_2)} p_1 \cdots p_q \text{ (here } t_1 - t_2 = p_1 \cdots p_q).$$

$$\Rightarrow y_1 - y_2 = b_1 \cdot \ldots \cdot b_t \cdot \text{(maybe some } p_j)$$
$$\Rightarrow y_1 - y_2 \geqslant N \text{ which is a contradiction, since we assumed } y_2 < y_1 < N.$$

Thus we have

$$\begin{array}{lcl}
|0\rangle & \xrightarrow{\text{U}} & |0\rangle \\
|1\rangle & \xrightarrow{\text{U}} & |\pi(1)\rangle \\
\vdots & & \\
|N-1\rangle & \xrightarrow{\text{U}} & |\pi(N-1)\rangle \\
|N\rangle & \xrightarrow{\text{U}} & |N\rangle \\
\vdots & & \\
|2^L - 1\rangle & \xrightarrow{\text{U}} & |2^L - 1\rangle,
\end{array}$$

where π is a permutation of the set $\{1, \ldots, N-1\}$. Thus U is a permutation matrix $\Rightarrow U$ is unitary. ∎

For $0 \leqslant s \leqslant r-1$ we define the state

$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp[-\frac{2\pi i s}{r} \cdot k] |x^k \pmod N\rangle$$

We further find

$$\begin{aligned} U|u_s\rangle &= \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp[-\frac{2\pi i s}{r} \cdot k]\ U|x^k \pmod N\rangle \\ &= \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp[-\frac{2\pi i s}{r} \cdot k] |x^{k+1} \pmod N\rangle \\ &= \frac{1}{\sqrt{r}} \sum_{k'=1}^{r} \exp[-\frac{2\pi i s}{r} \cdot (k'-1)] |x^{k'} \pmod N\rangle \\ &= \frac{1}{\sqrt{r}} \sum_{k'=1}^{r} \exp[-\frac{2\pi i s}{r} \cdot k'] \exp[\frac{2\pi i s}{r}] |x^{k'} \pmod N\rangle \\ &= \exp[\frac{2\pi i s}{r}] \frac{1}{\sqrt{r}} \sum_{k'=0}^{r-1} \exp[-\frac{2\pi i s}{r} \cdot k'] |x^{k'} \pmod N\rangle \\ &= \exp[\frac{2\pi i s}{r}] |u_s\rangle. \end{aligned} \tag{2}$$

Note that we used here

$$\begin{aligned} & U|x^k \pmod N\rangle \\ & |x \cdot (x^k \pmod N) \pmod N\rangle \\ =& |x \cdot x^k \pmod N\rangle \\ =& |x^{k+1} \pmod N\rangle. \end{aligned}$$

We also used the observation that in the summation we can replace $k' = r$ with $k' = 0$. Indeed

$$\begin{aligned} &\exp[-\frac{2\pi i s}{r} \cdot r] = \exp[-2\pi i s] = 1 = \exp[-\frac{2\pi i s}{r} \cdot 0], \text{ and} \\ &|x^r \pmod N\rangle = |1\rangle = |x^0 \pmod N\rangle. \end{aligned}$$

According to (2), we have

$$U|u_s\rangle = \exp[\frac{2\pi i s}{r}]|u_s\rangle,$$

which means that $|u_s\rangle,\ s = 0, \ldots, r-1$, are eigenvectors of U with phases $\psi^{(s)} = \frac{s}{r}$.
Note that (details are omitted)

$$\sum_{s=0}^{r-1} \exp[-2\pi i \cdot \frac{k}{r} \cdot s] = \begin{cases} r, & k = 0, \\ 0, & k \neq 0. \end{cases}$$

For example, for $r = 3$ and $k = 1$ the roots of unity are shown on Fig. 1, and one can see that their sum is 0.

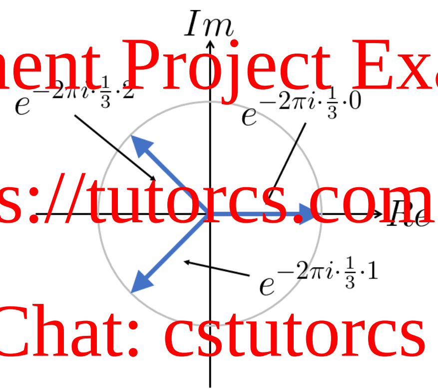

Figure 1: Sum of the powers of a root of unity is 0

Using this observation we can compute the sum of the vectors $|u_s\rangle$:

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle = \frac{1}{r} \sum_{k=0}^{r-1} |x^k \pmod N\rangle \sum_{s=0}^{r-1} \exp[-2\pi i \cdot \frac{k}{r} \cdot s] = |1\rangle.$$

Thus

$$|1\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} \underbrace{|u_s\rangle}_{\text{eigenvectors of } U}$$

Remark 1 *Note that quantum circuits that do not involve measurement blocks are linear. So, a linear combination of inputs leads to the linear combination of the corresponding outputs, as it is shown in Fig. 2.*

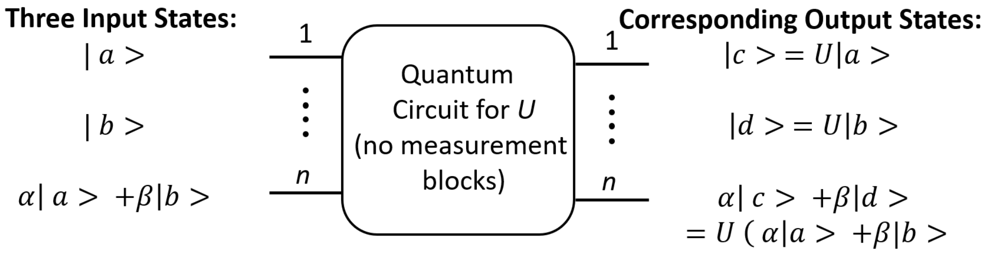

Figure 2: Quantum Circuits are linear

Let us consider the binary expansion of the phase

$$\psi^{(s)} = \frac{s}{r} = \psi_1^{(s)}/2 + \cdots + \psi_t^{(s)}/2^t + \psi_{t+1}^{(s)}/2^{t+1} + \cdots$$

Let us for the moment assume that we use the phase estimation circuit (Fig. 4 of the Lecture Notes on Phase Estimation) with U defined in (1) and with the input $|u\rangle = |u_s\rangle$ (note that we need L qubits for the state $|u_s\rangle$). Then the joint state of the $t + L$ qubtis before the measurement blocks would be

$$|\phi_t^{(s)} \ldots \phi_1^{(s)}\rangle|u_s\rangle,$$

and therefore at the outputs of the measurement blocks we would get the values of the first t bits in the binary expansion of $\psi^{(s)}$.

The problem is, however, that we cannot prepare the state $|u_s\rangle$, since we do not know r. To overcome this problem, we take into account Remark 1 and see that if we use the input

$$|u\rangle = |\underbrace{0\ldots01}_{L\text{bits}}\rangle = \frac{1}{\sqrt{r}}(|u_0\rangle + \ldots + |u_{r-1}\rangle),$$

then the joint state of the $t + L$ qubtis before the measurement blocks is

$$|v\rangle = \sum_{s=0}^{r-1} \frac{1}{\sqrt{r}}|\psi_t^{(s)} \ldots \psi_1^{(s)}\rangle|u_s\rangle.$$

Thus at the classical output of the t measurement blocks we obtain $\psi_t^{(s)}, \ldots, \psi_1^{(s)}$, $s \in [0, r-1]$ with probability $\frac{1}{r}$.

But we do not know s. How do we find r?

1.2 The Continued Fraction Algorithm

$$a_0 \in Z_0^+,\ a_1, \cdots, a_M \in Z^+$$
$$[a_0 \cdots a_M] = a_0 + \cfrac{1}{a_1 + \frac{1}{a_2 \frac{1}{\ddots + \frac{1}{a_M}}}}$$

$a_0, \cdots, a_M$ can be found for any rational number s/r.

Example 3

$$\frac{5}{13} = 0 + \frac{5}{13} = 0 + \frac{1}{\frac{13}{5}} = 0 + \frac{1}{2 + \frac{3}{5}}$$
$$= 0 + \frac{1}{2 + \frac{1}{\frac{5}{3}}} = 0 + \frac{1}{2 + \frac{1}{1 + \frac{2}{3}}} = 0 + \frac{1}{2 + \frac{1}{1 + \frac{1}{\frac{3}{2}}}}$$
$$= 0 + \frac{1}{2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{2}}}} = 0 + \frac{1}{2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1}}}}}$$
$$\begin{bmatrix} a_0 & a_1 & a_2 & a_3 & a_4 \end{bmatrix} = \begin{bmatrix} 0 & 2 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Theorem 1 *If we are given the continued fraction $[a_0, \cdots, a_n]$ of a rational number $\frac{s_n}{r_n}$ then we can find this ration number using the following algorithm*

$$s_0 = a_0,\ r_0 = 1,\ s_1 = 1 + a_0 a_1,\ r_1 = a_1,$$

and for $j = 2, \ldots, n$

$$s_j = a_j s_{j-1} + s_{j-2},\ r_j = a_j r_{j-1} + r_{j-2}.$$

In fact this theorem allows us to find all the rational numbers s_j/r_j corresponding to $[a_0, \cdots, a_j], j = 0, \ldots, n$.

Example 4

		s_j/r_j
$[0, 2]$	$\Rightarrow s_1 = 1, r_1 = 2$	$1/2$
$[0, 2, 1]$	$\Rightarrow s_2 = 1, r_2 = 3$	$1/3$
$[0, 2, 1, 1]$	$\Rightarrow s_3 = 2, r_3 = 5$	$2/5$
$[0, 2, 1, 1, 1]$	$\Rightarrow s_4 = 3, r_4 = 8$	$3/8$
$[0, 2, 1, 1, 1, 1]$	$\Rightarrow s_5 = 5, r_5 = 13$	$5/13$

Definition 2 *The j-th convergent of continued fraction is defined as*

$$[\underbrace{a_0 a_1 \cdots a_j}_{j\text{-th convergent}} \cdots a_n]$$

Theorem 2 *Let x and s/r be rational numbers such that*

$$\left|\frac{s}{r} - x\right| \leqslant \frac{1}{2r^2}.$$

Then the continued fraction of s/r is a j-th convergent of the continued fraction of x.

This means that

$$s/r = [a_0 \cdots a_j], \quad x = [a_0, \cdots a_j a_{j+1} \cdots a_l].$$

Note that we do not know j.

Example 5

$$x = \frac{49}{128} = \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{\ddots}{2 + \frac{2}{3}}}}}}}$$

$$\textit{Thus } 49/128 = \begin{bmatrix} 0 & 2 & 1 & 1 & 1 & 1 & 1 & 2 & \ldots \end{bmatrix}$$

For $s/r = 5/13$ we have $|5/13 - x| \approx 0.0018 < \frac{1}{2 \cdot 13^2} \approx 0.00296$. The continued fraction of $5/13$, as we found before, is $[021111]$. So, we see that it is the 5*-convergent of* $[0211112\ldots]$.

If t is not very small, we have

$$\tilde{\psi}^{(s)} = \psi_1^{(s)}/2 + \cdots + \psi_t^{(s)}/2^t \approx \frac{s}{r}.$$

Then with high probability $|\frac{s}{r} - \tilde{\psi}^{(s)}| \leqslant \frac{1}{2r^2}$, and we can find r by the "guess and check" method using the following algorithm.

Algorithm for Order Finding

- We run our quantum circuit and obtain bits $\psi_1^{(s)}, \ldots, \psi_t^{(s)}$. Note that we get only bits, but we do not know s.

- We compute the rational number
$$\tilde{\psi}^{(s)} = \psi_1^{(s)}/2 + \cdots + \psi_t^{(s)}/2^t.$$

- We compute the continued fraction for this ration number
$$\tilde{\psi}^{(s)} = [a_0, a_1, \ldots a_n].$$

- For $j = 1, \ldots, n$ we
  - take the j-th convergent $[a_0, \ldots, a_j]$ and, using Theorem 1, compute the rational s_j/r_j;
  - if $x^{r_j} \bmod N = 1$ then we found the order $r = r_j$. Stop.

Example 6 *Let $x = 4$ and $N = 2713$.*

Let us assume that we use quantum circuit with $t = 7$. Our goal is to find the order r using the above algorithm. (Note that in this example $r = 13$ since $4^{13} \pmod{2713} = 1$ and $4^m \pmod{2713} \neq 1$ for any $m < 13$, but in our algorithm we do not assume, of course, this knowledge.)

Let us assume that our circuit produced for us results corresponding to $s = 5$ (we of course do not know that $s = 5$). The binary expansion of $5/13$:

$$5/13 = 0 \cdot \frac{1}{2} + 1 \cdot \frac{1}{4} + 1 \cdot \frac{1}{8} + 0 \cdot \frac{1}{16} + 0 \cdot \frac{1}{32} + 0 \cdot \frac{1}{64} + 1 \cdot \frac{1}{128} + 0 \cdot \frac{1}{256} + 0 \cdot \frac{1}{512} + 1 \cdot \frac{1}{2^{10}} + 1 \cdot \frac{1}{2^{11}} + \cdots$$

However, since $t = 7$, we get at the output of the measurement blocks only the first 7 bits of this binary expansion:

$$(\psi_1^s, \ldots, \psi_7^{(s)}) = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Using these bits, we obtain the rational number

$$\tilde{\psi}^{(s)} = 0 \cdot \frac{1}{2} + 1 \cdot \frac{1}{4} + 1 \cdot \frac{1}{8} + 0 \cdot \frac{1}{16} + 0 \cdot \frac{1}{32} + 0 \cdot \frac{1}{64} + 1 \cdot \frac{1}{128} = \frac{49}{128}.$$

So, for the moment we did not manage to reconstruct $s/r = 5/13$. However, we hope that this $\tilde{\psi}^{(s)}$ is sufficiently close to the true s/r and that $\tilde{\psi}^{(s)}$ will allow us to find r. (This is indeed the case, since according to Example 5

$$|\frac{5}{13} - \frac{49}{128}| < \frac{1}{2 \cdot 13^2}$$

and therefore the continued fraction of $5/13$ is a j-th convergent of $\frac{49}{128}$.)

We compute the continued fraction for $\frac{49}{128}$ (it is already found in Example 5), take its j-th convergent, find s_j and r_j and check whether r_j is the order of x:

$$\begin{aligned}
[0,2] &\Rightarrow s_1 = 1,\ r_1 = 2 && (4^2 = 16) \pmod{2713} \neq 1 \\
[0,2,1] &\Rightarrow s_2 = 1,\ r_2 = 3 && (4^3 = 64) \pmod{2713} \neq 1 \\
[0,2,1,1] &\Rightarrow s_3 = 2,\ r_3 = 5 && (4^5 = 1024) \pmod{2713} \neq 1 \\
[0,2,1,1,1] &\Rightarrow s_4 = 3,\ r_4 = 8 && (4^8 = 65536) \pmod{2713} \neq 1 \\
[0,2,1,1,1,1] &\Rightarrow s_5 = 5,\ r_5 = 13 && (4^{13}) \pmod{2713} = 1
\end{aligned}$$

We found $r = 13$!

Please note that in all our computations we did not use values $r = 13$, $s = 5$. We simply followed the above Algorithm and used only the 7 bits produced by the quantum circuit and numbers x and N.

So if t is large enough, so that $|\frac{s}{r} - \psi^{(s)}| \leqslant \frac{1}{2r^2}$, the continued fraction algorithm allows us to find r.

1.3 Possible Problems

1. $\tilde{\psi}^{(s)}$ is not close enough to s/r.

   Theorem 3 *If*

   $$t \geqslant 2L + 1 + \lceil \log_2(2 + \frac{1}{2\epsilon}) \rceil$$

   then with probability $(1-\epsilon)$ the value $\tilde{\psi}^{(s)}$ will allow us to find r.

2. s and r have a common factor. For instance $r = 12$ and at the output of the phase estimation algorithm we get the value

   $$\psi^{(3)} = s/r = 3/12 = 1/4.$$

Then the continued fraction of $1/4$ will never allow us to find $r = 12$. However, according to the well known result of the number theory:

$$(\text{Number of primes} < r) \geqslant \frac{r}{2 \log r}$$

.

Further, it is easy to see that in the prime factorization of

$$r = p_1 \dots p_m \tag{3}$$

the number of distinct primes $m \leqslant \log_2 r$. Hence

$$\Pr(s \text{ and } r \text{ are coprime }) \geqslant \Pr(s \text{ is a prime that does not occur in (3)})$$
$$\geqslant \frac{1}{r}\left(\frac{r}{2\log r} - \log_2 r\right).$$

For a small N the order finding problem can be solved by a classical computer - simply by computing all $x^r \bmod N$ for all $r = 2, \dots, N-1$. So, let us say that we are interested in $N \geqslant 10,000$. We proceed as follows.

- We first use classical computer to compute $x^r \bmod N$ for say $r = 2, \dots, 1000$.

- If the order is not found among these r-s, we use the quantum circuit. It is easy to check that for $N \geqslant 10,000$ we have

$$\max_{r \in [1000, N]} \frac{1}{r}\left(\frac{r}{2\log r} - \log_2 r\right) = \frac{1}{N}\left(\frac{N}{2\log N} - \log_2 N\right)$$

  This expression behaves like $O(\frac{1}{2\log_2 N})$. Hence running our quantum algorithm $O(2\log_2 N)$ times, with high probability, we get s that is coprime to r. Thus the overall complexity is polynomial in $\log_2 N$, while the complexity of any classical algorithm is $O(N)$, and therefore we have an exponential speed up.

3. Complexity of implementing Controlled U defined in (1).
   This complexity is only $O(L^3)$ gates (details are omitted).