2.4 Shor's factoring algorithm

How to factor a large composite number N into the product of primes?

⇨ best classical solution (number field sieve)

$$\sim \exp\left[c(\log N)^{\frac{1}{3}}(\log\log N)^{\frac{2}{3}}\right]$$ ⇨ exponential scaling

input bits in length

⇨ shor's quantum algorithm

$$\sim (\log N)^2(\log\log N)(\log\log\log N)$$ ⇨ polynomial scaling

$$N = c_n \cdot 2^n + c_{n-1}2^{n-1} + \cdots + c_0 \quad (n\text{+1-bit})$$

2.4.1. Quantum algorithm for finding the order *r*

$$x^r \equiv 1 \pmod N \quad \text{or} \quad x^r = pN + 1$$

⇨ r : least positive integer

○ ○ ⋮ ○ } l qubit 1st register

● ● ⋮ ● } l qubit 2nd register

$$N^2 < 2^l < 2N^2$$

q : # of distinct states

$$2n < l < 2n+1$$

Step 1: initialization

$$|0\rangle_1 |0\rangle_2$$

second register

first register

Step 2: Walsh-Hadamard transform on the 1st register

$$\xrightarrow{\hat{H}_1} \left(\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a\rangle \right)_1 \otimes |0\rangle_2 \quad \Rightarrow \boxed{\text{linear superposition}}$$

Step 3: Calculate $x^a \pmod N$ and store it in the 2nd register

$$\xrightarrow{\hat{U}} \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a\rangle_1 \left| x^a \pmod N \right\rangle_2 \quad \Rightarrow \boxed{\text{entanglement}}$$

Step 4: Fourier transform of the 1st register

$$\xrightarrow{\hat{F}} \frac{1}{q} \sum_{a=0}^{q-1} \sum_{c=0}^{q-1} \exp\left(i \frac{2\pi ac}{q} \right) |c\rangle_1 \left| x^a \pmod N \right\rangle_2$$

$$\left[|a\rangle_1 \xrightarrow{\hat{F}} \frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} \exp\left(i \frac{2\pi ac}{q} \right) |c\rangle_1 \quad \text{(quantum Fourier transform)} \right]$$

Step 5: Measure the 1st register in the computational basis

The probability of finding the 1st register in the state $|c\rangle$:

$$\text{Prob}(c) = \sum_{k=0}^{r-1} \left| \frac{1}{q} \sum_{a} \exp\left(i \frac{2\pi a c}{q} \right) \right|^2 \Rightarrow$$

projective measurement without quantum erasure

$$x^a \equiv x^k \pmod N$$

different 2nd register state ⇩ no interference ⇩ power sum

same 2nd register state $|x^k\rangle_2$ ⇩ interference ⇩ amplitude sum

$$x^a \pmod N = x^k$$

or $x^a \equiv x^k \pmod N$ is equivalent to $a \equiv k \pmod r$.

$k = 0, 1, 2, \cdots r-1$

proof: $a \equiv k \pmod r \Rightarrow a = br + k$

[0, q -1] zero or positive integer order

$k = 0$	1	2	k	r - 1	
$a = 0$	1	2	k	r - 1	⇨ $b = 0$
r	$r + 1$	$r + 2$	$r + k$	$2r$ - 1	⇨ $b = 1$
$2r$	$2r + 1$	$2r + 2$	$2r + k$	$3r$ - 1	⇨ $b = 2$
⋮					⋮
			q - 1		

$$x^a \pmod N = x^{br+k} \pmod N$$

$$= \left(x^r\right)^b x^k \pmod N$$

$$x^r \equiv 1 \pmod N \Longrightarrow x^r \equiv pN + 1$$

r is an order

$$x^a \pmod N = (pN+1)^b x^k \pmod N$$

$$= \left[(pN)^b + \cdots + b(pN) + 1\right] x^k \pmod N$$

$$= x^k$$

x^k is relatively prime to N.

$$\Downarrow \quad (k = 0, 1, 2, \cdots r-1)$$

$$\boxed{\text{There are only } r \text{ different values of } x^a \pmod N.}$$

2.4.2. Probability of success

How many different a's contribute to the amplitude sum?

($\Longrightarrow$ How many different b's?)

$$0 \le b \le \underbrace{\left\lfloor \frac{q-k-1}{r} \right\rfloor}_{\text{positive integer less than } \frac{q-k-1}{r}} \equiv b_{\max}$$

$$\text{Prob}(c) = \sum_{k=0}^{r-1} \left| \frac{1}{q} \sum_a \exp\left(i \frac{2\pi a c}{q} \right) \right|^2$$

$x^a \equiv x^k \pmod N$

$$= \sum_{k=0}^{r-1} \left| \frac{1}{q} \sum_{b=0}^{b_{\max}} \exp\left[i \frac{2\pi (br+k) c}{q} \right] \right|^2$$

$\exp\left(i \frac{2\pi k c}{q} \right)$ can be neglected because it is independent of b.

$$\left(\left| \exp\left(i \frac{2\pi k c}{q} \right) \right|^2 = 1 \right)$$

$\{rc\}_q$ $\quad rc \pmod q \Longrightarrow -\frac{q}{2} < \{rc\}_q \le \frac{q}{2}$

residue $\quad$ congruent to

$$= \sum_{k=0}^{r-1} \left| \frac{1}{q} \sum_{b=0}^{b_{\max}} \exp\left(i \frac{2\pi b \{rc\}_q}{q} \right) \right|^2$$

If $\{rc\}_q$ is small enough, all the amplitudes in this sum will be in the nearly same phase and make the sum large. This is a desired result.

$$\{rc\}_q = 0 \Rightarrow c = \frac{d \cdot q}{r} \quad (d : \text{zero or positive integer})$$

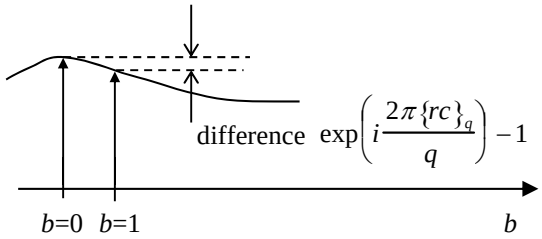
Measurement of c provides the value of r. However, the measured c does not necessarily satisfy the above equality exactly.

$$\boxed{\text{Measurement error}}$$

integral form: $\frac{1}{q} \sum_{b=0}^{b_{\max}} \exp\left(i \frac{2\pi b \{rc\}_q}{q} \right)$

$$= \frac{1}{q} \int_0^{b_{\max}} \exp\left(i \frac{2\pi b \{rc\}_q}{q} \right) db + O\left\{ \frac{b_{\max}}{q} \left[\exp\left(i \frac{2\pi \{rc\}_q}{q} \right) - 1 \right] \right\}$$

If $\left| \{rc\}_q \right| \le \frac{r}{2}$, $\exp\left(i \frac{2\pi \{rc\}_q}{q} \right) \le 1 + i \frac{2\pi \frac{r}{2}}{q}$



$$\Downarrow$$

$$\frac{b_{\max}}{q} \left[\exp\left(i \frac{2\pi \{rc\}_q}{q} \right) - 1 \right] \approx \frac{q-k-1}{rq} \times i \frac{\pi r}{q} \sim O\left(\frac{1}{q} \right)$$

$$\Downarrow$$

negligible

$$\frac{1}{q} \int_0^{b_{\max}} \exp\left(i \frac{2\pi b \{rc\}_q}{q} \right) db = \frac{1}{r} \int_0^{\left\lfloor \frac{q-k-1}{r} \right\rfloor \frac{r}{q}} \exp\left(i \frac{2\pi \{rc\}_q}{r} u \right) du$$

$$u = \frac{rb}{q} \qquad \left| \{rc\}_q \right| \le \frac{r}{2}$$

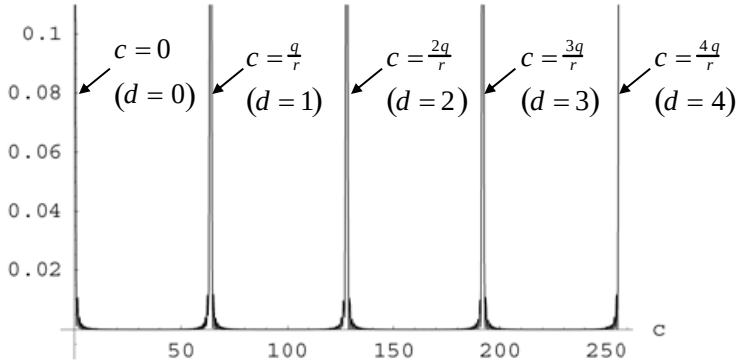
$$\approx \frac{1}{r} \int_0^1 \exp\left(i \frac{2\pi \{rc\}_q}{r} u \right) du$$

$$\Downarrow$$

The lower bound for the probability of finding the state $|c\rangle_1$ is

$$\sum_{k=0}^{r-1}\left|\frac{1}{r}\int_0^1 \exp(\pm i\pi u)du\right|^2 = \frac{4}{\pi^2 r} \sim \frac{1}{3r}$$

Numerical example: $N = 15$, $q = 2^l = 256$, $x = 2$ ⇨ $r = 4$



$$-\frac{1}{2q} \le \frac{c}{q} - \frac{d}{r} \le \frac{1}{2q}$$

$$-\frac{r}{2} \le \{rc\}_q \le \frac{r}{2} \longrightarrow -\frac{r}{2} \le rc - dq \le \frac{r}{2} \quad \times\frac{1}{rq}$$

zero or positive integer

Since $q > N^2$ and $r < N$, there is at most one fraction $\frac{d}{r}$ that satisfies the above inequality.

⇩

If we obtain the value c by projective measurement, we can estimate $\frac{d}{r}$ in lowest terms by rounding c/q to the nearest fraction having a denominator smaller than N.

Example: $N = 15$. $q = 16^2 = 256 > N^2 = 225$

$x = 4$ is assumed.

⇩

$c = 18$ was obtained.

$$\frac{c}{q} = \frac{18}{256} = \cfrac{1}{14 + \cfrac{1}{4 + \cfrac{1}{2}}} \Rightarrow \begin{array}{l} d = 1 \\ r = 14 \quad (< N = 15) \end{array}$$

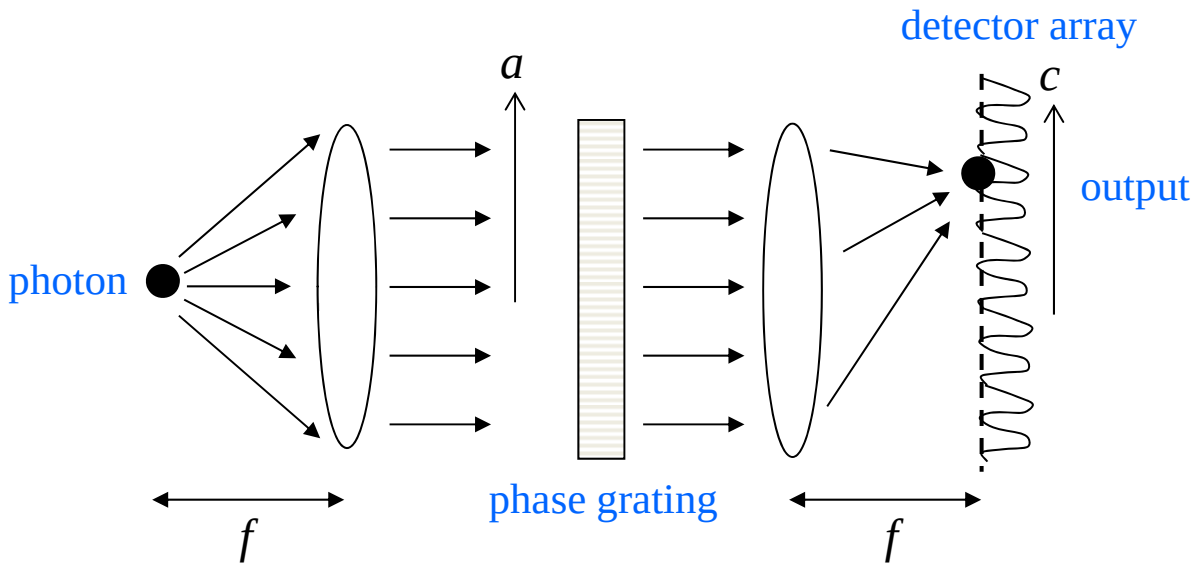
continued fraction

⇩

$$x^{\frac{r}{2}} - 1 = 4^7 - 1 = 16383 \longrightarrow \gcd(16383,15) = 3$$

$$x^{\frac{r}{2}} + 1 = 4^7 + 1 = 16385 \longrightarrow \gcd(16385,15) = 5$$

2.4.3 A single photon interferometer for implementing Shor algorithm



$$\phi(x) = e^{i\frac{\pi}{2N}\left[x^a \bmod(N)\right]}$$

2.5 Phase estimation algorithm

2.5.1 Basics

R. Cleve et al., Proc. Roy. Soc. London, A454, 339 (1998)

Problem

Suppose a unitary operator $\hat{U}$ has an eigenstate $|u\rangle$ which is known, estimate an eigenvalue $e^{2\pi i\varphi}$:

$$\hat{U}|u\rangle = e^{2\pi i\varphi}|u\rangle \quad .$$

Given a quantum black box (oracle) that prepares the state $|u\rangle$ and performs controlled – $\hat{U}^{2^j}$ gate operation (j = non-negative integers), how many black box queries are required to estimate φ ?

Quantum solution

Step 1: initialization

$$|0\rangle_1 |u\rangle_2$$

← necessary qubits to store the eigenstate $|u\rangle$

↗ t qubits (t determines # of digits of accuracy in the estimate of φ and also the success probability)

Step 2: Walsch-Hadamard transformation on the first register

$$\xrightarrow{\hat{H}_1} \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle_1 |u\rangle_2$$

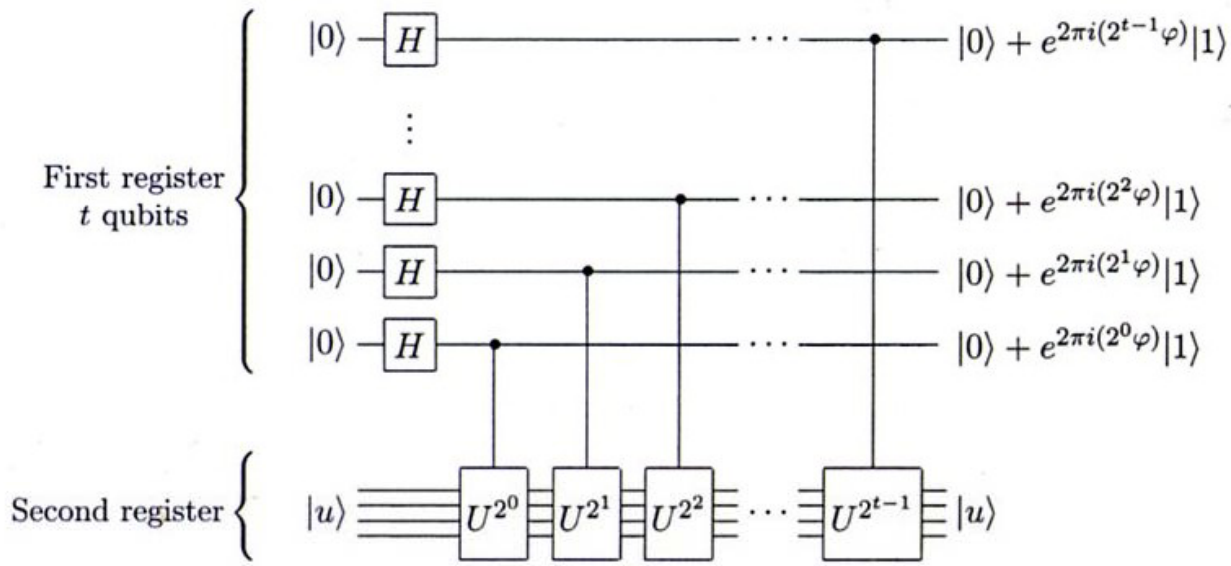
Step 3: sequential application of black box (oracle) queries:

(controlled – $\hat{U}^{2^j}$ operation)

$$\xrightarrow{C-\hat{U}^{2^j}} \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle_1 \hat{U}^{j} |u\rangle_2$$

$$= \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} e^{2\pi i j\varphi} |j\rangle_1 |u\rangle_2$$

(← see the next figure)



First register state:

$$\frac{1}{\sqrt{2^t}}\left(|0\rangle + e^{2\pi i 2^{t-1}\varphi}|1\rangle\right)\left(|0\rangle + e^{2\pi i 2^{t-2}\varphi}|1\rangle\right)\cdots\left(|0\rangle + e^{2\pi i 2^{0}\varphi}|1\rangle\right)$$

$$= \frac{1}{\sqrt{2^t}}\sum_{k=0}^{2^t-1} e^{2\pi i\varphi k} 1k >$$

Step 4: inverse quantum Fourier transform on the first register

$$\xrightarrow{\hat{F}_1^{-1}} |\tilde{\varphi}\rangle_1 |u\rangle_2$$

If $\varphi = 0.\varphi_1\varphi_2\cdots\varphi_t$ (t bits)

$$\Downarrow$$

First register state:

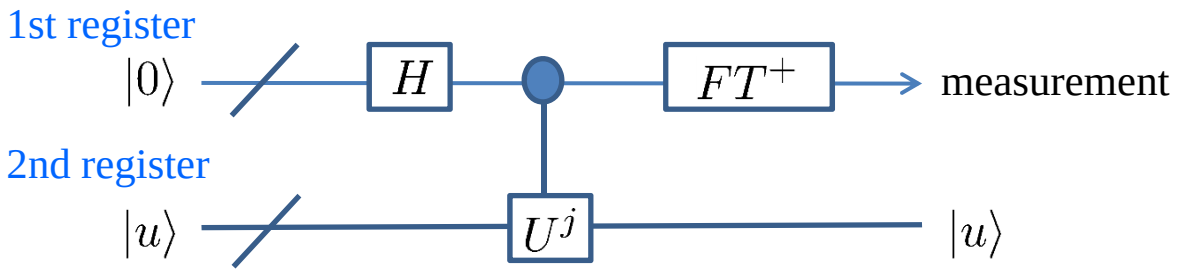
$$\frac{1}{\sqrt{2^t}}\left(|0\rangle + e^{2\pi i 0\cdot\varphi_t}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0\cdot\varphi_{t-1}\varphi_t}|1\rangle\right)\cdots\cdots\left(|0\rangle + e^{2\pi i 0\cdot\varphi_1\varphi_2\cdots\varphi_t}|1\rangle\right)$$

This is the Quantum Fourier transform of $|\tilde{\varphi}\rangle = |\varphi_1\varphi_2\cdots\varphi_t\rangle$

Step 5: projective measurement of the first register

$$\longrightarrow \tilde{\varphi}$$

2.5.2 Accuracy, success probability and unknown eigenstate



n-bit approximation $\tilde{\varphi}_u$ to φ_u $\left(\hat{U}|u\rangle = e^{i2\pi\varphi_u}|u\rangle\right)$

success probability $1-\varepsilon$

$\Downarrow$

1st register size $t = n + \left\lceil \log\left(2 + \frac{1}{2\varepsilon}\right)\right\rceil$

What if we do not know how to prepare an eigenstate $|u\rangle$ of $\hat{U}$?

$\Downarrow$

Prepare some other state $|\psi\rangle = \sum_u C_u|u\rangle$

$\Downarrow$

Final state: $\sum_u C_u|\tilde{\varphi}_u\rangle|u\rangle$

$\Downarrow$

With the probability $|C_u|^2$, the second register contains $|u\rangle$ so that the measurement result $\tilde{\varphi}_u$ is a good approximation to the desired eigenvalue φ_u.

[Further reading, M. Nielsen and I. Chuang, Quantum Computation and Quantum Information, Cambridge Univ. Press, 2000]