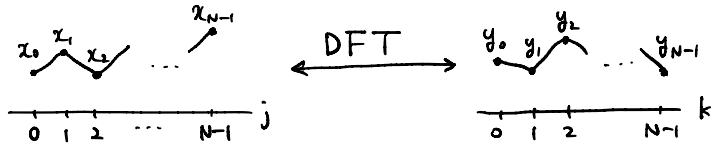
9-1 Shor's Factoring Algorithm

§5.1 Quantum Fourier transform

discrete Fourier transform



$\omega = e^{i\frac{2\pi}{N}}$

Fourier transform: $\{x_j\} \to \{y_k\}$, $y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \omega^{kj} x_j$

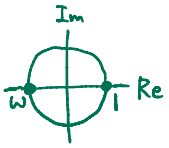
inverse Fourier transform: $\{y_k\} \to \{x_j\}$, $x_j = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} (\omega^*)^{jk} y_k$

$$\frac{1}{\sqrt{N}} \sum_j \omega^{kj} x_j = \frac{1}{\sqrt{N}} \sum_j \omega^{kj} \frac{1}{\sqrt{N}} \sum_l (\omega^*)^{jl} y_l = \frac{1}{N} \sum_{j,l} \omega^{j(k-l)} y_l$$
$$= \sum_l \delta_{k,l} y_l = y_k$$

$$\delta_{k,l} = \begin{cases} 1, & k = l \\ 0, & k \neq l \end{cases}$$

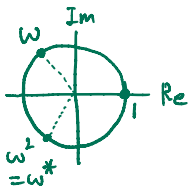
$N = 2$ $\omega = -1$

$$\begin{pmatrix} y_0 \\ y_1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & \omega \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \end{pmatrix}$$



$N = 3$ $\omega = e^{i\frac{2\pi}{3}}$

$$\begin{pmatrix} y_0 \\ y_1 \\ y_2 \end{pmatrix} = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega^4 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix}$$



quantum Fourier transform

$$\sum_j x_j |j\rangle \xrightarrow{\text{QFT}} \sum_k y_k |k\rangle = \sum_k \left(\frac{1}{\sqrt{N}} \sum_j \omega^{kj} x_j \right) |k\rangle = \sum_j x_j \left(\frac{1}{\sqrt{N}} \sum_k \omega^{jk} |k\rangle \right)$$

$$|j\rangle \xrightarrow{\text{QFT}} \frac{1}{\sqrt{N}} \sum_k \omega^{jk} |k\rangle$$

ex) $N = 2^2 = 4$ (two qubits)

$\omega = i$

$|0\rangle \to \frac{1}{2}(|0\rangle + |1\rangle + |2\rangle + |3\rangle)$

$|1\rangle \to \frac{1}{2}(|0\rangle + i|1\rangle + i^2|2\rangle + i^3|3\rangle) \to \frac{1}{2}(|0\rangle + i|1\rangle - |2\rangle - i|3\rangle)$

$|2\rangle \to \frac{1}{2}(|0\rangle + i^2|1\rangle + i^4|2\rangle + i^6|3\rangle) \to \frac{1}{2}(|0\rangle - |1\rangle + |2\rangle - |3\rangle)$

$|1\rangle \to \frac{1}{2}(|0\rangle + i^3|1\rangle + i^6|2\rangle + i^9|3\rangle) \to \frac{1}{2}(|0\rangle - i|1\rangle - |2\rangle + i|3\rangle)$

$N = 2^n$: Classically, you need $\sim N \log N = n2^n$ steps

In QC, $\sim (\log N)^2 = n^2$

💬 However, measurement destroys the state! Then, is this helpful?

§5.3 Quantum factoring algorithm

(slightly modified)

objective Given N, where $N = pq$ (p, q: positive integers), find p and q.

If $1 < m < N$ satisfies $m^2 = 1 \bmod N$ and $m \neq \pm 1 \bmod N$

$m^2 = (\text{integer}) \times N + 1$ and $m \neq (\text{integer}) \times N \pm 1$

$\Rightarrow m^2 - 1 = 0 \bmod N$

$\Rightarrow (m-1)(m+1) = 0 \bmod N$ note that $m \neq \pm 1 \bmod N \Rightarrow m \pm 1 \neq 0 \bmod N$

$\Rightarrow \gcd(m-1, N) > 1$ or $\gcd(m+1, N) > 1$

💬 you can efficiently find GCDs(최대공약수) using the Euclidean algorithm.

ex) $N = 15$, $m = 4$

$\gcd(m-1, N) = \gcd(3, 15) = 3$, $\gcd(m+1, N) = \gcd(5, 15) = 5$

Now, how to find such m?

💬 $A = a \bmod N$, $B = b \bmod N$

$\Rightarrow A = nN + a$, $B = mN + b$ (n, m: integers)

$\Rightarrow AB = nmN^2 + amN + bnN + ab$

$\Rightarrow AB = ab \bmod N$

Choose a random number $2 \leq x \leq N - 1$.

Suppose you can find minimum r s.t. $x^r = 1 \bmod N$.

💬 This is called the order r of x modulo N

If r is even, $(x^{r/2})^2 = 1 \bmod N$.

If $x^{r/2} \neq 1 \bmod N$, you can find the answer!

Now, how to find the order r?

(without normalization)

$(|0\rangle + |1\rangle + \cdots + |2^t - 1\rangle)|0\rangle$

$\rightarrow \sum_j |j\rangle |x^j \bmod N\rangle$

ex) $N = 15$, $x = 7$

$(|0\rangle + |1\rangle + |2\rangle + \ldots)|0\rangle$

$\rightarrow |0\rangle|1\rangle + |1\rangle|7\rangle + |2\rangle|4\rangle + |3\rangle|13\rangle + |4\rangle|1\rangle + |5\rangle|7\rangle + |6\rangle|4\rangle + \ldots$

$= (|0\rangle + |4\rangle + |8\rangle + |12\rangle + \ldots)|1\rangle + (|1\rangle + |5\rangle + |9\rangle + |13\rangle + \ldots)|7\rangle$

$+(|2\rangle + |6\rangle + |10\rangle + |14\rangle + \ldots)|4\rangle + (|3\rangle + |7\rangle + |11\rangle + |15\rangle + \ldots)|13\rangle$

For simplicity, suppose you measure the second register (in fact, this is not necessary).

$|a\rangle + |a+r\rangle + |a+2r\rangle + |a+3r\rangle + \ldots \qquad a \in \{0, 1, \ldots, r-1\}$

$$\xrightarrow{\text{QFT}} \sum_k y_k |k\rangle = \sum_k \left(\omega^{ka} + \omega^{k(a+r)} + \omega^{k(a+2r)} + \omega^{k(a+3r)} + \ldots\right)|k\rangle \qquad \omega = \exp\left[i\frac{2\pi}{2^t}\right]$$

$$y_k = \omega^{ka} \sum_j \exp\left[i2\pi \frac{kr}{2^t} j\right] \begin{cases} = \omega^{ka} \sum_j 1, & \frac{k}{2^t} = 0, \frac{1}{r}, \frac{2}{r}, \ldots, \frac{r-1}{r} \\ \to 0, & \text{otherwise} \end{cases}$$

You can get k by measurement.

$\frac{k}{2^t} = \frac{\text{integer}}{r}$ with high probability!

continued fraction of $\frac{k}{2^t} \to$ denominator(분모) $= r$

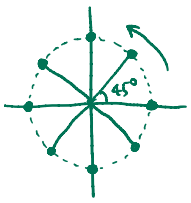
ex) $\frac{28}{64} = \frac{1}{2 + \frac{1}{3+\frac{1}{2}}} = \frac{7}{16}$

§5.4 Abelian Hidden Subgroup Problems (by an example)

💬 A large portion of quantum algorithms (including Deutsch-Jozsa, Shor's) fall into this class.

A group is a set with an operation (and some rules).

Consider a group $G = \{0, 1, 2, \ldots, 7\}$ with $+ \bmod 8$. (show closure)



$\mathbb{Z}_8$.

$\mathbb{Z}/8\mathbb{Z}$.

Subgroup $K = \{0, 4\} = 0 + K$

$1 + K = \{1, 5\}$, $1 + K = \{2, 6\}$, $1 + K = \{3, 7\}$

Cosets of K: K, $1 + K$, $2 + K$, $3 + K$

Quotient group $G/K = \{K, 1 + K, 2 + K, 3 + K\}$ $\quad G \bmod K$

Suppose a function $f : G \to X$ satisfies $f(g_1) = f(g_2)$ iff $g_1 + K = g_2 + K$.

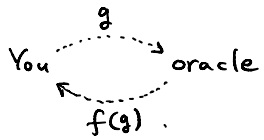
💬 즉, g_1과 g_2가 같은 coset에 속할 때만 $f(g_1) = f(g_2)$.

$f(g_1) = f(g_2)$ only when g_1 and g_2 are members of the same coset.

ex) $f(0) = f(4) = 0$, $f(1) = f(5) = 1$, $f(2) = f(6) = 2$, $f(3) = f(7) = 3$

Problem You know G, but you don't know K!

There is an oracle.



You need to find K by oracle queries.

ex) period finding

$f(x + r) = f(x)$ $\quad r$: period

You need to find the minimum r.