Understanding of Shor’s Quantum Algorithm

Aug. 2022

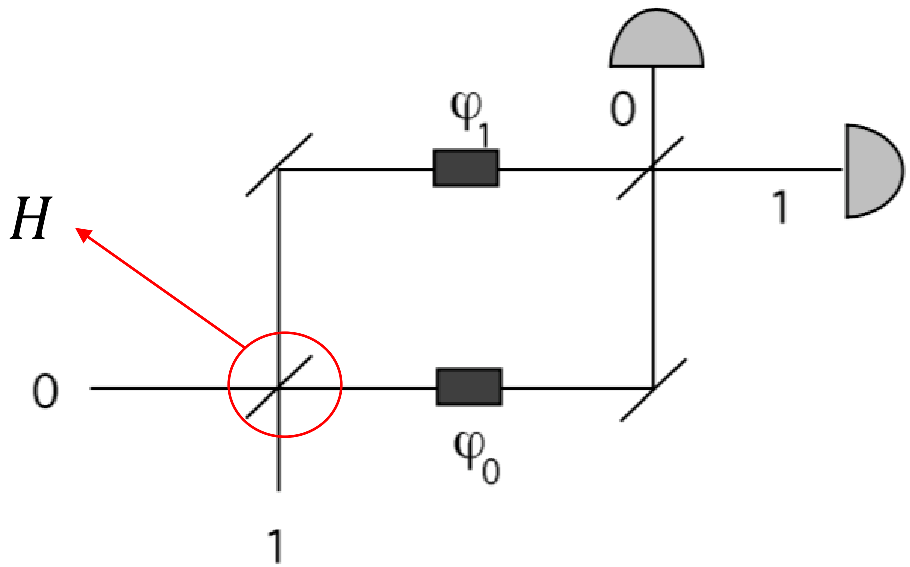
고려대학교
인공지능사이버보안학과
(최두호)

목차

Motivation and Deutsch's Algorithm

[Reference] Quantum Algorithms Revisited, R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca, arXiv 1997

(1) Consider

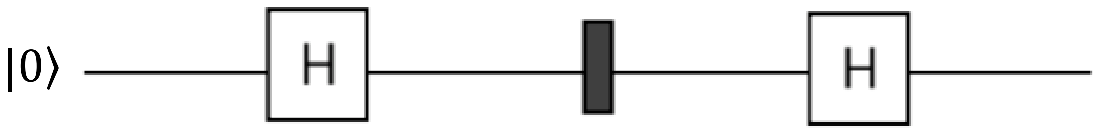


$$|0\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad \mapsto \frac{1}{\sqrt{2}}\left(e^{i\varphi_0}|0\rangle + e^{i\varphi_1}|1\rangle\right) \quad = e^{i\varphi_0}\boxed{\frac{1}{\sqrt{2}}\left(|0\rangle + e^{i(\varphi_1-\varphi_0)}|1\rangle\right)}$$

$$\boxed{(\varphi = \varphi_1 - \varphi_1)} \qquad \mapsto \frac{1}{2}\left(|0\rangle + |1\rangle + e^{i\varphi}(|0\rangle - |1\rangle)\right)$$

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

Motivation and Deutsch's Algorithm



$$\frac{1}{2}\Big((1+e^{i\varphi})|0\rangle + (1-e^{i\varphi})|1\rangle\Big)$$

$$\varphi = \varphi_1 - \varphi_0$$

$$\boxed{\begin{aligned} \cos\varphi &= cos^2\frac{\varphi}{2} - sin^2\frac{\varphi}{2} \\ \sin\varphi &= 2sin\frac{\varphi}{2}\cos\frac{\varphi}{2} \end{aligned}}$$

$$1 + e^{i\varphi} = 1 + (cos\varphi + isin\varphi)$$

$$= cos^2\frac{\varphi}{2} + \cancel{sin^2\frac{\varphi}{2}} + \left(cos^2\frac{\varphi}{2} - \cancel{sin^2\frac{\varphi}{2}}\right) + i2sin\frac{\varphi}{2}\cos\frac{\varphi}{2}$$

$$= 2cos^2\frac{\varphi}{2} + i2sin\frac{\varphi}{2}\cos\frac{\varphi}{2} \;\; = 2cos\frac{\varphi}{2}\left(cos\frac{\varphi}{2} + isin\frac{\varphi}{2}\right) = \boxed{2cos\frac{\varphi}{2}e^{i\frac{\varphi}{2}}}$$

Similarly,

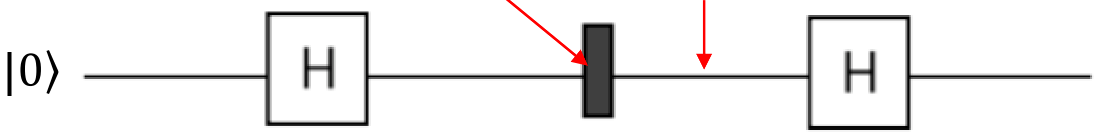
$$1 - e^{i\varphi} = 1 - (cos\varphi + isin\varphi) \;\; = 2sin\frac{\varphi}{2}\left(sin\frac{\varphi}{2} - icos\frac{\varphi}{2}\right)$$

$$= 2sin\frac{\varphi}{2}\left(-i\left(cos\frac{\varphi}{2} + isin\frac{\varphi}{2}\right)\right) = \boxed{-i2sin\frac{\varphi}{2}e^{i\frac{\varphi}{2}}}$$

Motivation and Deutsch's Algorithm

$$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{bmatrix}$$

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



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

$$\varphi = \varphi_1 - \varphi_0$$

$$= \boxed{e^{i\frac{\varphi}{2}}\left(cos\frac{\varphi}{2}|0\rangle - isin\frac{\varphi}{2}|1\rangle\right)}$$

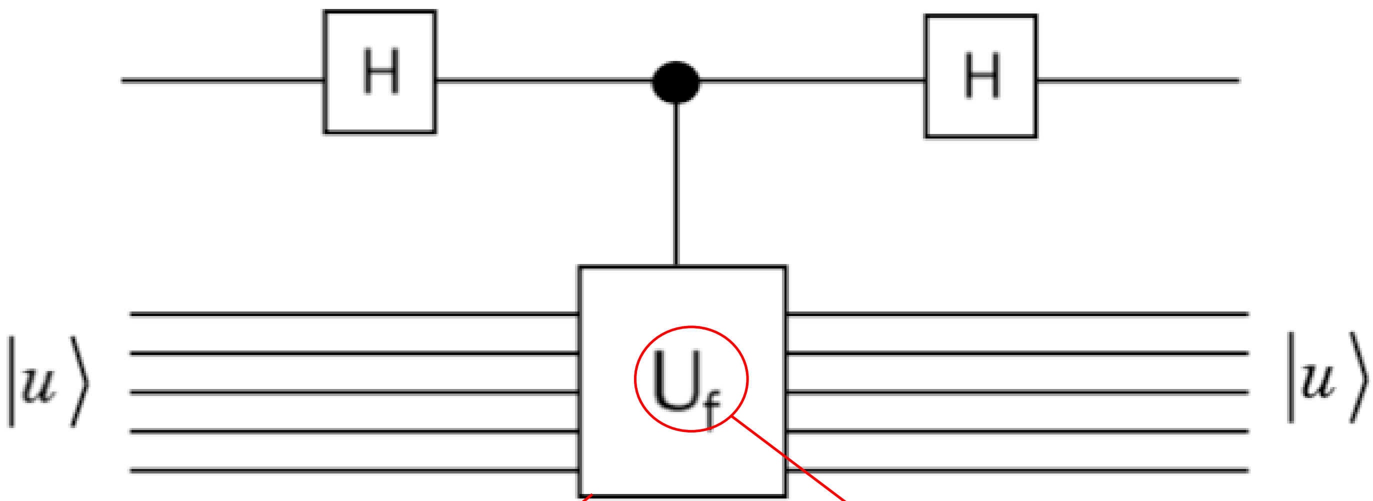
After measuring,

$|0\rangle$ **with the probability** $cos^2\frac{\varphi}{2} = \frac{1}{2}(1+\cos\varphi)$

$|1\rangle$ **with the probability** $sin^2\frac{\varphi}{2} = \frac{1}{2}(1-\cos\varphi)$

Motivation and Deutsch's Algorithm

(2) Consider



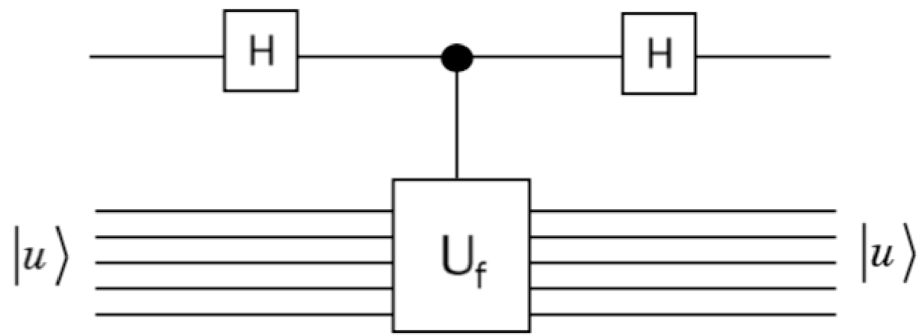
A unitary operator

Control qubit $|0\rangle$ $\Longrightarrow$ Identity

Control qubit $|1\rangle$ $\Longrightarrow$ U

Set $|u\rangle$: Eigenstate of U with its eigenvalue $e^{i\phi}$

Motivation and Deutsch's Algorithm



Then

$$|0\rangle|u\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|u\rangle \xrightarrow{c-U} \frac{1}{\sqrt{2}}(|0\rangle Id|u\rangle + |1\rangle U|u\rangle) = \frac{1}{\sqrt{2}}\left(|0\rangle|u\rangle + |1\rangle e^{i\phi}|u\rangle\right)$$

$$= \frac{1}{\sqrt{2}}(|0\rangle + e^{i\phi}|1\rangle)|u\rangle$$

$$\xrightarrow{H} \left(\cos\frac{\phi}{2}|0\rangle - i\sin\frac{\phi}{2}|1\rangle\right) e^{i\frac{\phi}{2}}|u\rangle$$

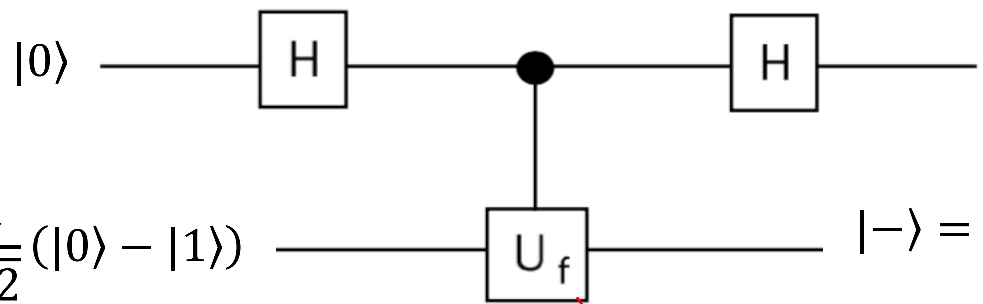
The eigenvalue is "kicked back" in front of |1> on the first qubit

The state of the auxiliary register |u>(an eigenstate of U) is not altered

Motivation and Deutsch’s Algorithm

Example: recall Deutsch’s Problem

$f:\{0,1\} \to \{0,1\}$ **Determine f is constant or balanced only one evaluation of f**



$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \qquad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$|x\rangle|y\rangle \mapsto |x\rangle|y \oplus f(x)\rangle$$

$|-\rangle$ **Is an eigenstate of** c-U_f **with its eigenvalue** $(-1)^{f(x)} = e^{i\pi f(x)}$

(Why) $|x\rangle|-\rangle = |x\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \mapsto \frac{1}{\sqrt{2}}|x\rangle(|f(x)\rangle - |1 \oplus f(x)\rangle)$

$f(x)=0 \implies \frac{1}{\sqrt{2}}|x\rangle(|0\rangle - |1\rangle) = |x\rangle|-\rangle$

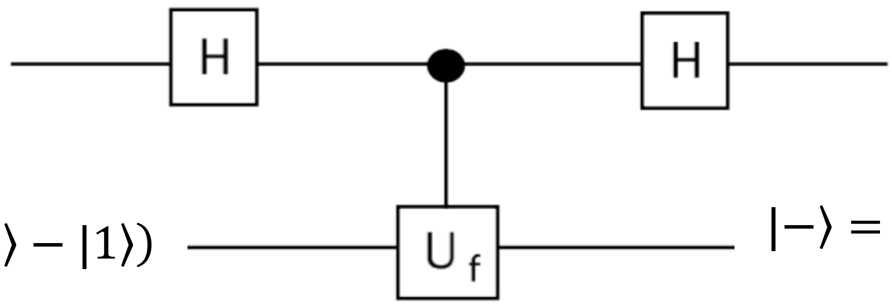
$f(x)=1 \implies \frac{1}{\sqrt{2}}|x\rangle(|1\rangle - |0\rangle) = (-1)|x\rangle|-\rangle$

$\Big\} \; |x\rangle(-1)^{f(x)}|-\rangle$

Motivation and Deutsch's Algorithm

Example: recall Deutsch's Problem

$|0\rangle$



$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ $\qquad$ $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

$$|0\rangle|-\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|-\rangle \mapsto \frac{1}{\sqrt{2}}\Big((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\Big)|-\rangle$$

$$= (-1)^{f(0)}\frac{1}{\sqrt{2}}\big(|0\rangle + (-1)^{f(1)\oplus f(0)}|1\rangle\big)|-\rangle$$

$$\mapsto \frac{1}{2}\Big((|0\rangle + |1\rangle) + (-1)^{f(1)\oplus f(0)}(|0\rangle - |1\rangle)\Big)|-\rangle$$

$$\mapsto \Big(cos\frac{\pi}{2}f(1)\oplus f(0)|0\rangle - isin\frac{\pi}{2}f(1)\oplus f(0)|1\rangle\Big)|-\rangle$$

$$= \frac{1}{2}\Big(\big(1 + (-1)^{f(1)\oplus f(0)}\big)|0\rangle + \big(1 - (-1)^{f(1)\oplus f(0)}\big)|1\rangle\Big)|-\rangle$$

$$= |f(1)\oplus f(0)\rangle|-\rangle$$

Quantum Fourier Transform

Recall Quantum Fourier Transform

For $a \in \{0, \dots, 2^m - 1\}$ $\quad |a\rangle \xrightarrow{QFT} \frac{1}{\sqrt{2^m}} \sum_{y=0}^{2^m-1} e^{\frac{2\pi i a y}{2^m}} |y\rangle$

$$a = 2^{m-1}a_1 + 2^{m-2}a_2 + \cdots + 2^1 a_{m-1} + 2^0 a_m$$

$$y = 2^{m-1}y_1 + 2^{m-2}y_2 + \cdots + 2^1 y_{m-1} + 2^0 y_m = \sum_{j=1}^{m} 2^{m-j} y_j$$

Binary representations

Focus on the amplitude $e^{\frac{2\pi i a y}{2^m}} = Exp\left(\frac{2\pi i a y}{2^m}\right)$

$$Exp\left(\frac{2\pi i a y}{2^m}\right) = Exp\left(\frac{2\pi i a \sum_{j=1}^{m} \cancel{2^m}^{-j} y_j}{\cancel{2^m}}\right) = Exp\left(2\pi i a \sum_{j=1}^{m} 2^{-j} y_j\right)$$

$$= Exp\left(2\pi i \sum_{j=1}^{m} (2^{-j} a) y_j\right)$$

(*)

Quantum Fourier Transform

Recall Quantum Fourier Transform

(*) $2^{-1}a = 2^{m-2}a_1 + 2^{m-3}a_2 + \cdots + 2^0 a_{m-1} + 2^{-1}a_m = a_1 a_2 \cdots a_{m-1} + 0.a_m$

$$2^{-2}a = 2^{m-3}a_1 + \cdots + 2^0 a_{m-2} + 2^{-1}a_{m-1} + 2^{-2}a_m = a_1 \cdots a_{m-2} + 0.a_{m-1}a_m$$

$$\vdots$$

$$2^{-(m-1)}a = a_1 + 0.a_2 \cdots a_{m-1}a_m$$

$$2^{-m}a = 0.a_1 a_2 \cdots a_{m-1}a_m$$

$$\boxed{2^{-j}a = a_1 \cdots a_{m-j} + 0.a_{m-(j-1)} \cdots a_{m-1}a_m}$$

$$Exp\left(2\pi i \sum_{j=1}^{m} (a2^{-j})y_j\right) = Exp\left(\sum_{i=1}^{m} 2\pi i(a_1 \cdots a_{m-j} + 0.a_{m-(j-1)} \cdots a_{m-1}a_m)y_j\right)$$

$$= \prod_{j=1}^{m} Exp(2\pi i(a_1 \cdots a_{m-j})Exp\big(2\pi i(0.a_{m-(j-1)} \cdots a_{m-1}a_m)y_j\big)$$

$$= \prod_{j=1}^{m} Exp\big(2\pi i(0.a_{m-(j-1)} \cdots a_{m-1}a_m)y_j\big)$$

Quantum Fourier Transform

Recall Quantum Fourier Transform

$$\prod_{j=1}^{m} Exp\left(2\pi i(0.a_{m-(j-1)}\cdots a_{m-1}a_m)y_j\right) = e^{2\pi i(0.a_m)y_1}e^{2\pi i(0.a_{m-1}a_m)y_2}\ldots$$

$$e^{\frac{2\pi i a y}{2^m}}|y\rangle = e^{\frac{2\pi i a y}{2^m}}|y_1\cdots y_m\rangle$$

$$= e^{2\pi i(0.a_m)y_1}|y_1\rangle e^{2\pi i(0.a_{m-1}a_m)y_2}|y_2\rangle\cdots e^{2\pi i(0.a_1a_2\cdots a_m)y_m}|y_m\rangle$$

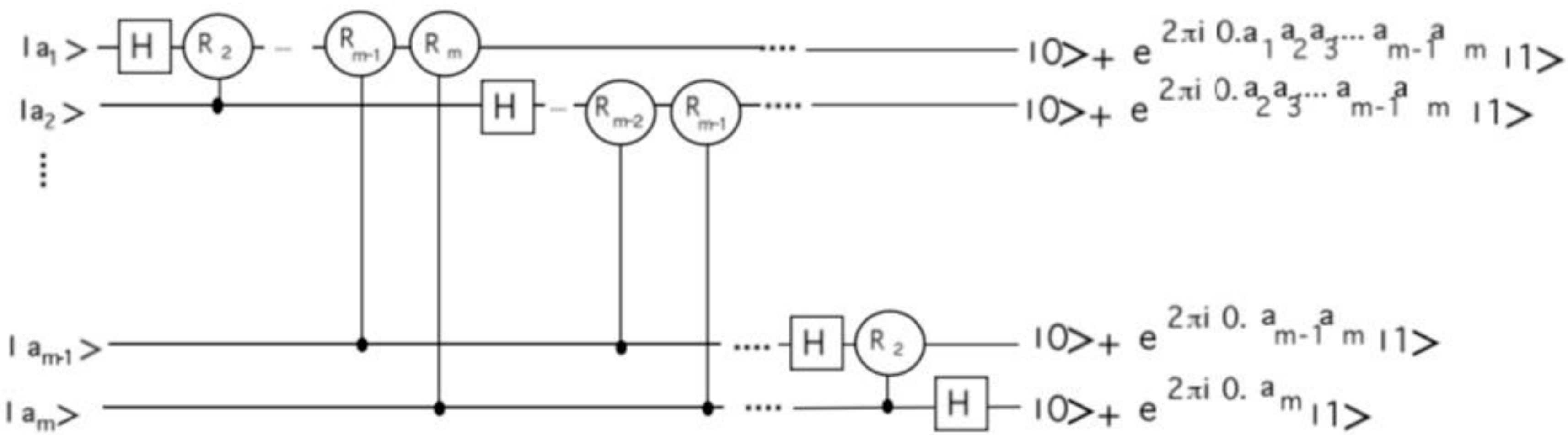
$(\therefore)$ $$\frac{1}{\sqrt{2^m}}\sum_{y=0}^{2^m-1} e^{\frac{2\pi i a y}{2^m}}|y\rangle$$

$$= \boxed{\left(\frac{|0\rangle + e^{2\pi i(0.a_m)}|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle + e^{2\pi i(0.a_{m-1}a_m)}|1\rangle}{\sqrt{2}}\right)\cdots\left(\frac{|0\rangle + e^{2\pi i(0.a_1a_2\cdots a_m)}|1\rangle}{\sqrt{2}}\right)}$$

Quantum Fourier Transform

Recall Quantum Fourier Transform

$$\left(\frac{|0\rangle + e^{2\pi i(0.a_m)}\,|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle + e^{2\pi i(0.a_{m-1}a_m)}\,|1\rangle}{\sqrt{2}}\right)\cdots\left(\frac{|0\rangle + e^{2\pi i(0.a_1a_2\cdots a_m)}\,|1\rangle}{\sqrt{2}}\right)$$



$$R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{pmatrix} \qquad |a_m\rangle \;—\boxed{H}—\; \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i(0.a_m)}|1\rangle\right)$$

Phase Estimation Algorithm

How to estimate arbitrary phases

Suppose U : an unitary transformation,

$|\psi\rangle$: an eigenstate of U with eigenvalue $e^{2\pi i\phi}$, $0 \leq \phi < 1$

Unknown : $\boldsymbol{U}$ or $|\psi\rangle$ or $e^{2\pi i\phi}$

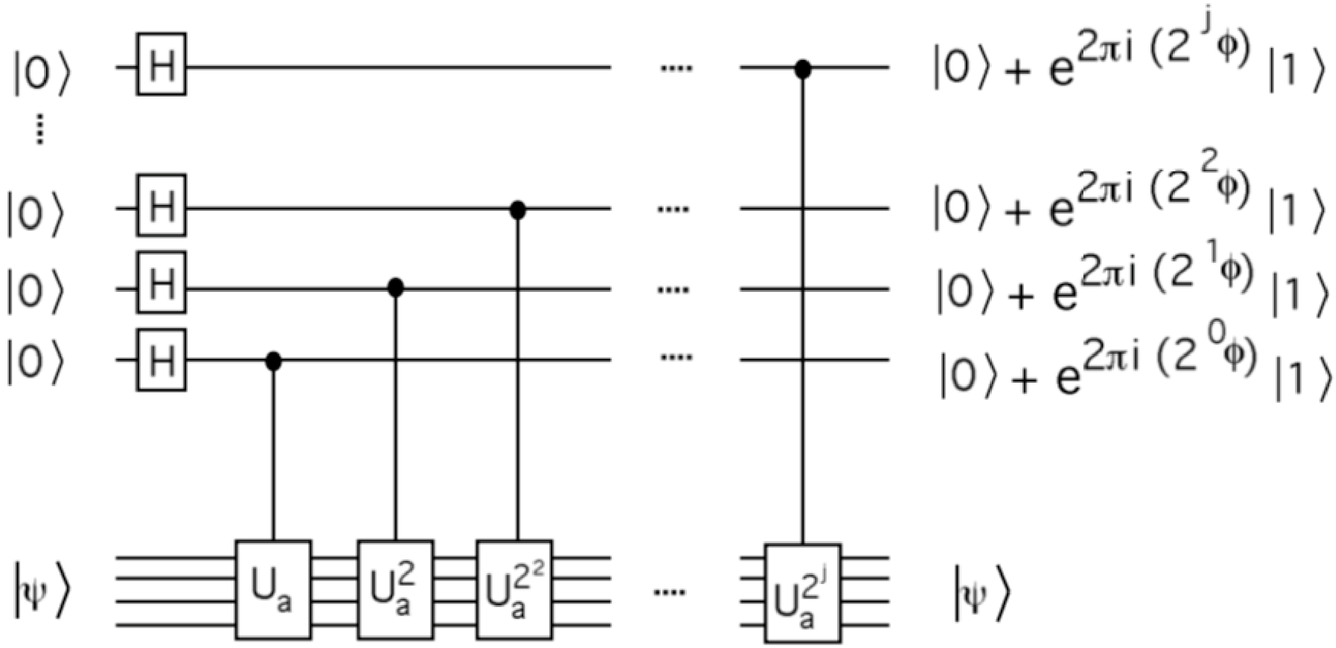
Given : $\mathbf{c}-\boldsymbol{U}$, $\mathbf{c}-\boldsymbol{U}^{2}$, $\mathbf{c}-\boldsymbol{U}^{2^2}$, and so on operations

Given : a single preparation of the state $|\psi\rangle$

Goal : find an m-bit estimator of ϕ

Phase Estimation Algorithm

How to estimate arbitrary phases

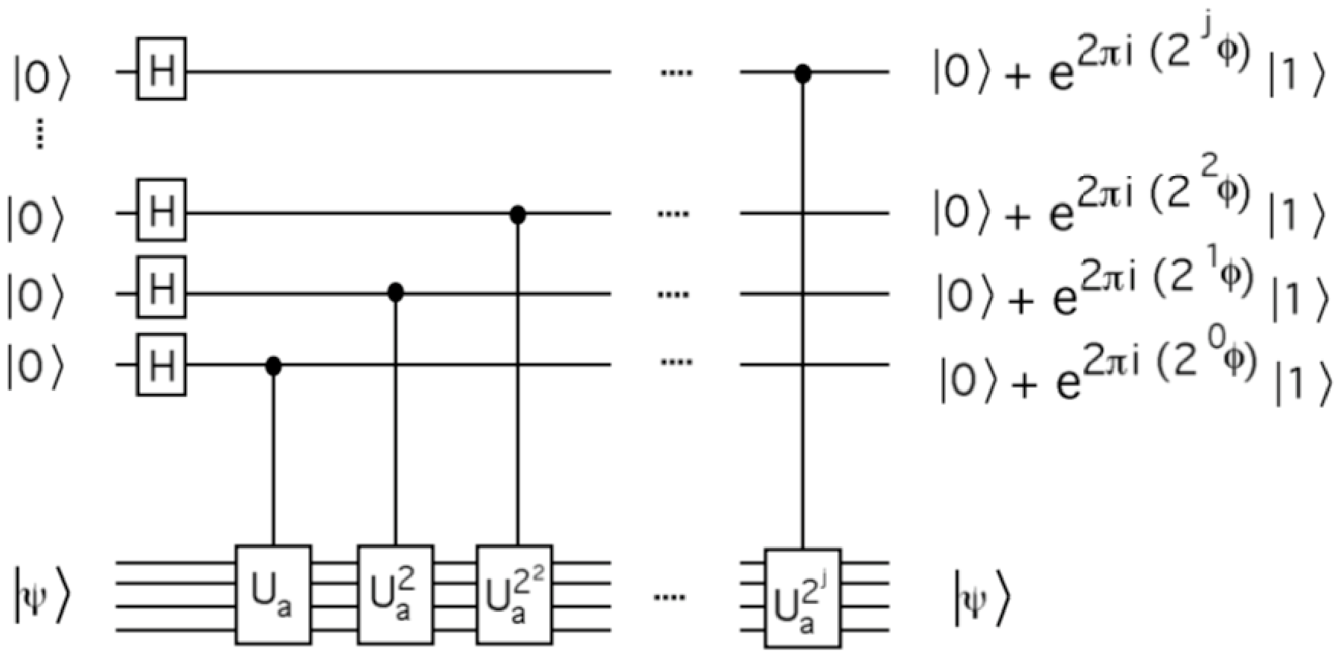


$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|\psi\rangle \xrightarrow{c-U} \frac{1}{\sqrt{2}}\left(\left|0\right\rangle + e^{2\pi i\left(2^0\phi\right)}\middle|\, 1\right\rangle\right)\ |\psi\rangle$$

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|\psi\rangle \xrightarrow{c-U^2} \frac{1}{\sqrt{2}}\left(\left|0\right\rangle + e^{2\pi i\left(2^1\phi\right)}\middle|\, 1\right\rangle\right)\ |\psi\rangle$$

Phase Estimation Algorithm

How to estimate arbitrary phases



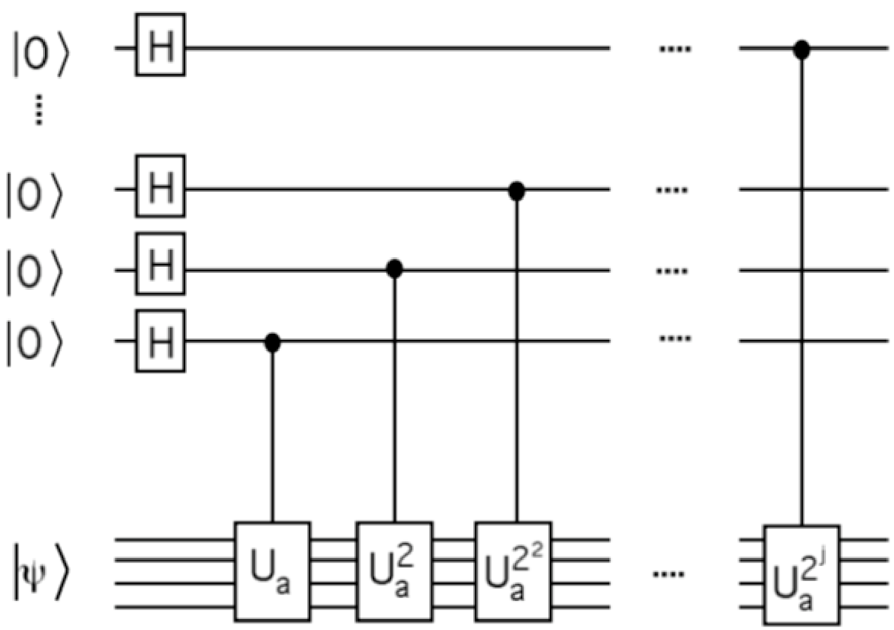
(∴)

$$\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\left(2^{m-1}\phi\right)}\Big|\,1\rangle\right)\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\left(2^{m-2}\phi\right)}\Big|\,1\rangle\right)\cdots\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\phi}|1\rangle\right)|\psi\rangle$$

$$= \frac{1}{\sqrt{2^m}}\sum_{y=0}^{2^m-1} e^{2\pi i\phi y}|y\rangle\,|\psi\rangle$$

Phase Estimation Algorithm

How to estimate arbitrary phases: (1) When $\emptyset = 0.a_1 a_2 \cdots a_m$



$m-1$

$$|0\rangle + e^{2\pi i(2^{j}\phi)}|1\rangle = |0\rangle + e^{2\pi i(0.a_m)}|1\rangle$$

$$|0\rangle + e^{2\pi i(2^{2}\phi)}|1\rangle = |0\rangle + e^{2\pi i(0.a_3\cdots a_m)}|1\rangle$$

$$|0\rangle + e^{2\pi i(2^{1}\phi)}|1\rangle = |0\rangle + e^{2\pi i(0.a_2\cdots a_m)}|1\rangle$$

$$|0\rangle + e^{2\pi i(2^{0}\phi)}|1\rangle = |0\rangle + e^{2\pi i(0.a_1\cdots a_m)}|1\rangle$$

$|\psi\rangle$

If we apply the inverse QFT, then we can obtain $|\emptyset/2^m\rangle = |a_1 a_2 \cdots a_m\rangle$

Phase Estimation Approach

(2) When $\emptyset \neq 0.a_1 a_2 \cdots a_m$ → the best m-bit approximation of $\emptyset$ with prob. $\geq \frac{4}{\pi^2} = 0.405 \ldots$

($\because$) Let $\emptyset = \frac{a}{2^m} + \delta$, where $0 < |\delta| \leq \frac{1}{2^{m+1}}$

If we apply the **inverse QFT**, then

$$\frac{1}{\sqrt{2^m}} \sum_{y=0}^{2^m-1} e^{2\pi i \phi y} |y\rangle \xrightarrow{QFT^{-1}} \frac{1}{2^m} \sum_{x=0}^{2^m-1} \sum_{y=0}^{2^m-1} e^{\frac{-2\pi i x y}{2^m}} e^{2\pi i \phi y} |x\rangle$$

$$= \frac{1}{2^m} \sum_{x=0}^{2^m-1} \sum_{y=0}^{2^m-1} e^{\frac{2\pi i (a-x) y}{2^m}} e^{2\pi i \delta y} |x\rangle$$

The amplitude of the $|x\rangle = |a_1 \ldots a_m\rangle$

$$\frac{1}{2^m} \sum_{y=0}^{2^m-1} e^{\frac{2\pi i (a-x) y}{2^m}} e^{2\pi i \delta y} = \frac{1}{2^m} \sum_{y=0}^{2^m-1} e^{2\pi i \delta y} = \frac{1}{2^m} \frac{1-(e^{2\pi i \delta})^{2^m}}{1-e^{2\pi i \delta}}$$

0

Phase Estimation Algorithm

(2) When $\emptyset \neq 0.a_1 a_2 \cdots a_m$ → the best m-bit approximation of $\emptyset$ with prob. $\geq \frac{4}{\pi^2} = 0.405 \ldots$

$(\therefore)$ **The prob. that the $|x\rangle = |a_1 \ldots a_m\rangle$ is measured**

$$\left|\frac{1}{2^m}\frac{1-\left(e^{2\pi i\delta}\right)^{2^m}}{1-e^{2\pi i\delta}}\right|^2 \geq \left(\frac{1}{2^m}\frac{2\delta 2^m}{\pi\delta}\right)^2 = \frac{4}{\pi^2}$$

$$\begin{cases} \cos\phi = \cos^2\frac{\phi}{2} - \sin^2\frac{\phi}{2} \\ \sin\phi = 2\cos\frac{\phi}{2}\sin\frac{\phi}{2} \end{cases}$$

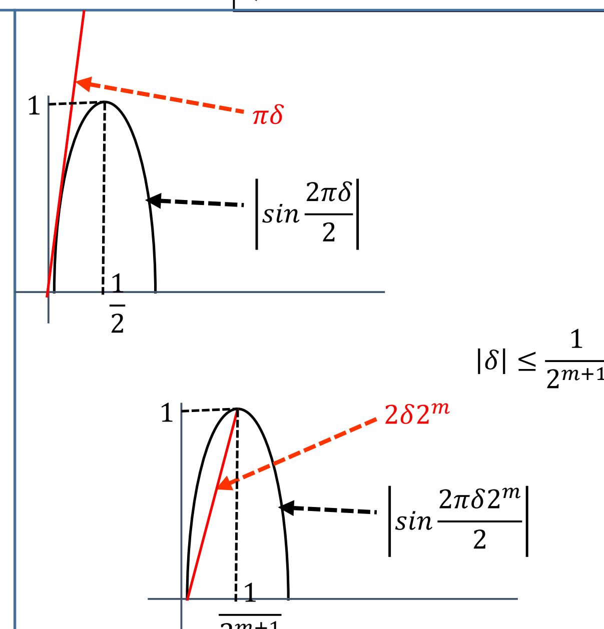
$(\because)$ $$\left|1-e^{ix}\right| = 2\left|sin\frac{x}{2}\right|$$

$$1-e^{ix} = 1-(cosx + isinx)$$

$$= 1-\left(\left(cos^2\frac{x}{2} - sin^2\frac{x}{2}\right) + 2icos\frac{x}{2}sin\frac{x}{2}\right)$$

$$= \cancel{cos^2\frac{x}{2}} + sin^2\frac{x}{2} - \cancel{cos^2\frac{x}{2}} + sin^2\frac{x}{2} - 2icos\frac{x}{2}sin\frac{x}{2}$$

$$= 2sin^2\frac{x}{2} - 2icos\frac{x}{2}sin\frac{x}{2} = 2sin\frac{x}{2}\left(sin\frac{x}{2} - icos\frac{x}{2}\right)$$



Shor's Order Finding Algorithm

Peter Shor

소인수 분해 문제: Classical Complexity ~ $O\left(e^{1.9(\log N)^{1/3}(\log\log N)^{2/3}}\right)$

Shor's Algorithm ~ $O\left((\log N)^2(\log\log N)(\log\log\log N)\right)$

- N = p·q, find p or q

Classical Algorithms

1. Pick a random number g < N
2. Compute gcd(g, N) (만약 1이면, g가 p 또는 q)
3. Find the period r of $f:[0,2^n-1]\rightarrow Z_N,\ f(x)=g^x \bmod N$

   $g^r = 1 \bmod N$

(Quantum Algorithm)
Shor's Order Finding Algorithm

Classical Algorithms

4. r : odd ➔ go back to step 1 and r : even, $g^{r/2} = -1 \bmod N$ ➔ go back to step 1
5. Otherwise, $(g^{r/2}-1), (g^{r/2}+1)$: nontrivial factors of N

$$(\because)(g^{r/2}-1)(g^{r/2}+1) = g^r - 1 = 0 \bmod N$$

Shor's Order Finding Algorithm

$N = p \cdot q$, where p,q prime. For $f: [0, 2^n - 1] \to Z_N$, $f(x) = a^x \mathrm{mod} N$, find the period r, i.e. the minimum r such that $g^r = 1 \mathrm{mod} N$

Consider $|\psi_1\rangle = \sum_{j=0}^{r-1} e^{\frac{-2\pi i j}{r}} |a^j mod\ N\rangle$ and let U: $|x\rangle \mapsto |ax\ mod\ N\rangle$

Then

$$U|\psi_1\rangle = \sum_{j=0}^{r-1} e^{\frac{-2\pi i j}{r}} U|a^j mod\ N\rangle = \sum_{j=0}^{r-1} e^{\frac{-2\pi i j}{r}} |a^{j+1} mod\ N\rangle$$

$$= \sum_{k=1}^{r-1} e^{\frac{-2\pi i (k-1)}{r}} |a^k mod\ N\rangle + e^{\frac{-2\pi i (r-1)}{r}} |a^r\ mod\ N\rangle$$

$$= e^{\frac{2\pi i}{r}} \sum_{k=1}^{r-1} e^{\frac{-2\pi i k}{r}} |a^k mod\ N\rangle + e^{\frac{2\pi i}{r}} e^{-2\pi i} |1\ mod\ N\rangle$$

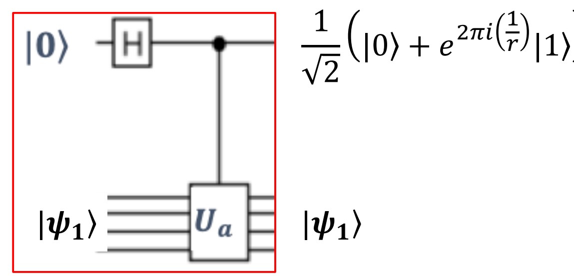
$$= e^{\frac{2\pi i}{r}} \left(e^{-2\pi i} |1\ mod\ N\rangle + \sum_{k=1}^{r-1} e^{\frac{-2\pi i k}{r}} |a^k mod\ N\rangle \right) = e^{\frac{2\pi i}{r}} |\psi_1\rangle$$

Shor's Order Finding Algorithm

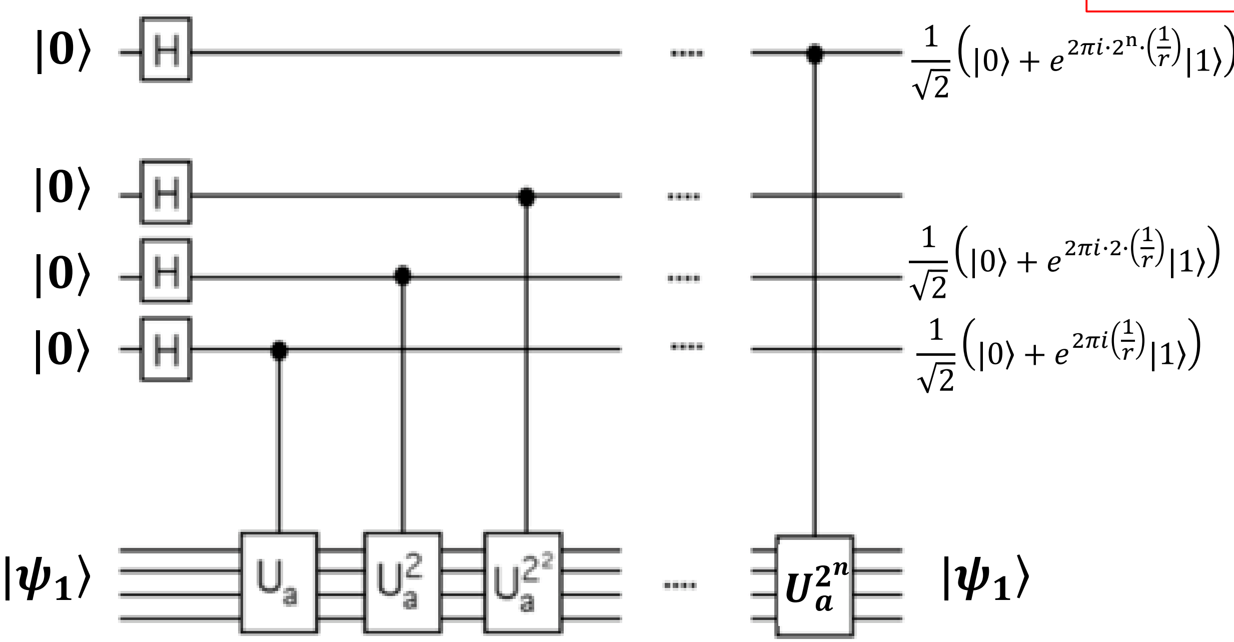
$N = p \cdot q$, where p,q prime. For $f: [0, 2^n - 1] \rightarrow Z_N$, $f(x) = a^x \mathrm{mod} N$, find the period r, i.e. the minimum r such that $g^r = 1 \mathrm{mod} N$

Therefore, $|\psi_1\rangle$ is an eigenstate of U and its eigenvalue $e^{\frac{2\pi i}{r}}$

If we can prepare the state $|\psi_1\rangle$, then



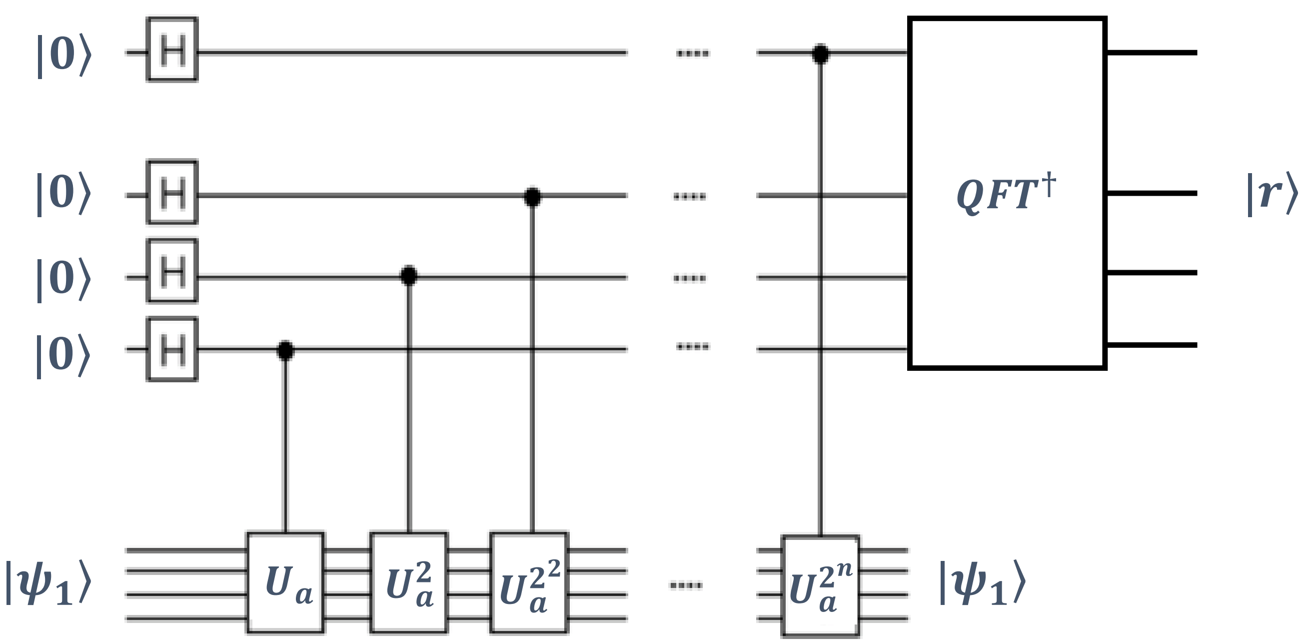
and



Shor's Order Finding Algorithm

$N = p \cdot q$, where p,q prime. For $f\colon [0, 2^n - 1] \to Z_N$, $f(x) = a^x \mathrm{mod} N$, find the period r, i.e. the minimum r such that $g^r = 1 \mathrm{mod} N$

Therefore, we can find the period, if we prepare $|\psi_1\rangle$



(*)

Shor's Order Finding Algorithm

$N = p \cdot q$, where p,q prime. For $f: [0, 2^n - 1] \to Z_N$, $f(x) = a^x \mathrm{mod} N$, find the period r, i.e. the minimum r such that $g^r = 1 \mathrm{mod} N$

However, it it impossible to prepare $|\psi_1\rangle$

Consider $|\psi_k\rangle = \sum_{j=0}^{r-1} e^{\frac{-2\pi i k j}{r}} |a^j mod\ N\rangle$ where $k \in \{1, \dots, r\}$ at random

Then similarly, $|\psi_k\rangle$: eigenstate of the U and its eigenvalue $e^{2\pi i \frac{k}{r}}$

Therefore, if we apply (*) with $|\psi_k\rangle$ then the best estimator x of $\frac{k}{r}$ can be obtained

That is, $\left|\frac{k}{r} - x\right| \le \frac{1}{2^{n+1}}$

By continued fraction method, r can be extracted, if r and k is coprime.

(Continued Fraction)

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots \atop a_{k-1} + \cfrac{1}{\ddots}}} \qquad \frac{n_k}{d_k} := a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots \atop a_{k-1} + \cfrac{1}{a_k}}} \qquad \Rightarrow \lim_{k \to \infty} \frac{n_k}{d_k} = x$$

If x is rational, the limit is finite, i.e.

$\exists K \ni \frac{\mathrm{n}_K}{\mathrm{d}_K} = x$ If $\left|\frac{c}{a} - x\right| < \frac{1}{2a^2}$ then $\frac{c}{a} = \frac{n_{k_0}}{d_{k_0}} \in \left\{\frac{n_k}{d_k}\right\}_{k=0}^{K}$

Shor's Order Finding Algorithm

$N = p \cdot q$, where p,q prime. For $f: [0, 2^n - 1] \rightarrow Z_N$, $f(x) = a^x \text{mod} N$, find the period r, i.e. the minimum r such that $g^r = 1 \text{mod} N$

Otherwise, a divisor of r, r', is obtained where $k = k' \cdot c$, $r = r' \cdot c$

and it is checked by $a^{r'} modN \neq 1$

(Probability of r, k coprime)

$P(r\ coprime\ to\ k) = P$(no prime that divides both r, k)

$= P(\neg(2|r \wedge 2|k) \wedge \neg(3|r \wedge 3|k) \wedge \cdots \wedge \neg(p_l|r \wedge p_l|k) \wedge \cdots)$, p_l: l−th prime

$$= P\left(\bigwedge_{p:prime}^{finite} \neg(p|r \wedge p|k)\right) = \prod_{p:prime}^{finite} \neg(p_l|r \wedge p_l|k) \geq \prod_{p:prime}^{\infty}\left(1 - \frac{1}{p^2}\right)$$

$\zeta(s) = \prod_{p:prime}^{\infty}\left(1 - \frac{1}{p^s}\right)$: Riemann zeta function and $\zeta(2) \approx 0.607$

Hence, $P(r\ coprime\ to\ k) \geq \zeta(2) \approx 0.607$

$P(\neg(p|r \wedge p|k)) \geq 1 - \frac{1}{p^2}$

since for given x,

$x \leq lp$,

for some l

$\therefore\ P(p|x) \leq \frac{l}{lp} = \frac{1}{p}$

Therefore, the problem is solved, if we can set $|\psi_k\rangle = \sum_{j=0}^{r-1} e^{\frac{-2\pi i k j}{r}} U|a^j mod\ N\rangle$

Shor's Order Finding Algorithm

$N = p \cdot q$, where p,q prime. For $f: [0, 2^n - 1] \rightarrow Z_N$, $f(x) = a^x \text{mod} N$, find the period r, i.e. the minimum r such that $g^r = 1 \text{mod} N$

How to set $|\psi_k\rangle = \sum_{j=0}^{r-1} e^{\frac{-2\pi i k j}{r}} |a^j mod\ N\rangle$ for arbitrary k

Fortunately, $|1\rangle = \sum_{k=1}^{r} |\psi_k\rangle$

$$\sum_{k=1}^{r} e^{-\frac{2\pi i k j}{r}} = e^{-\frac{2\pi i}{r} j} + e^{-\frac{2\pi i}{r} 2j} + \cdots + e^{-\frac{2\pi i}{r} rj}$$

$= (\omega_r + \omega_r^2 + \cdots + \omega_r^{r-1} + 1)^{-j}$, where $\omega_r = e^{\frac{2\pi i}{r}}$

$= 1$(or 0), if $j = 0$(or $j \neq 0$)

(why)

$$\sum_{k=1}^{r} |\psi_k\rangle = \sum_{k=1}^{r} \sum_{j=0}^{r-1} e^{-\frac{2\pi i k j}{r}} |a^j modN\rangle = \sum_{j=0}^{r-1} \sum_{k=1}^{r} e^{-\frac{2\pi i k j}{r}} |a^j modN\rangle$$

$$= |1 modN\rangle + \cancel{\sum_{j \neq 0} (1 + \omega_r + \cdots + \omega_r^{r-1})^{-j} |a^j modN\rangle} = |1\rangle$$

$$\therefore\ U_a\ |1\rangle = \sum_{k=1}^{r} e^{2\pi i (\frac{k}{r})} |\psi_k\rangle$$

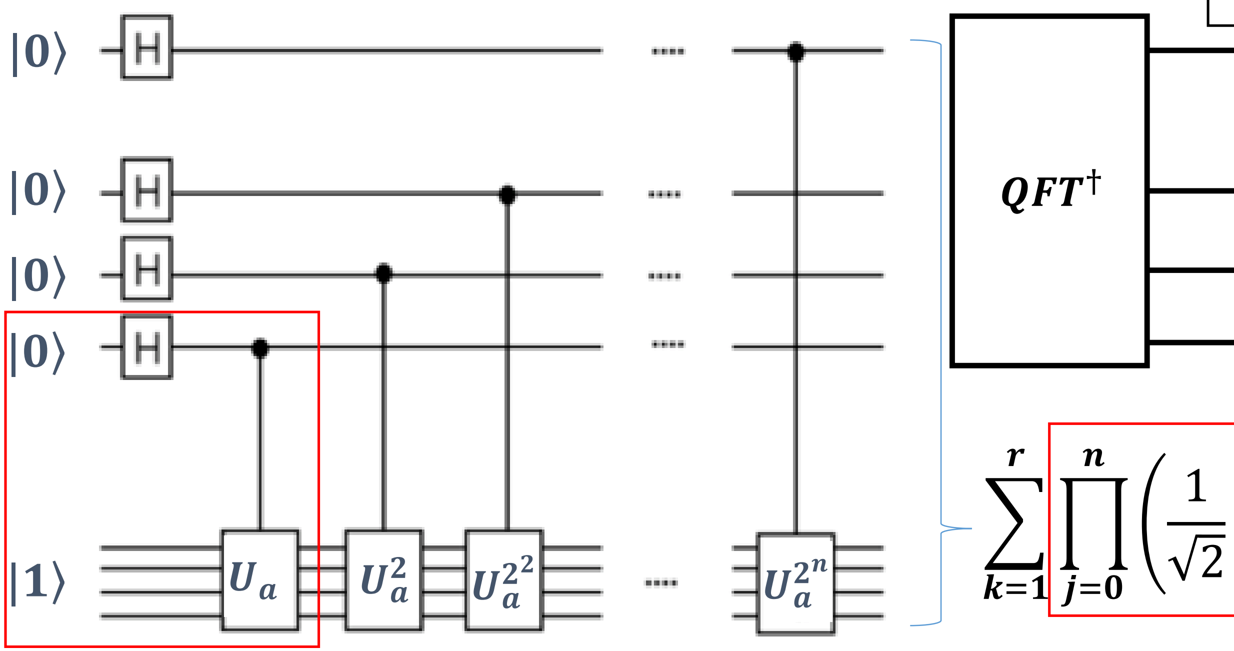
Shor's Order Finding Algorithm

$N = p \cdot q$, where p,q prime. For $f: [0, 2^n - 1] \rightarrow Z_N$, $f(x) = a^x \mathrm{mod} N$, find the period r, i.e. the minimum r such that $g^r = 1 \mathrm{mod} N$

We prepare the state $|1\rangle$ instead of $|\psi_k\rangle$, then $U_a|1\rangle = \sum_{k=1}^{r} e^{2\pi i(\frac{k}{r})}|\boldsymbol{\psi_k}\rangle$

$|\boldsymbol{x_k}\rangle$: the best estimator of $\frac{k}{r}$

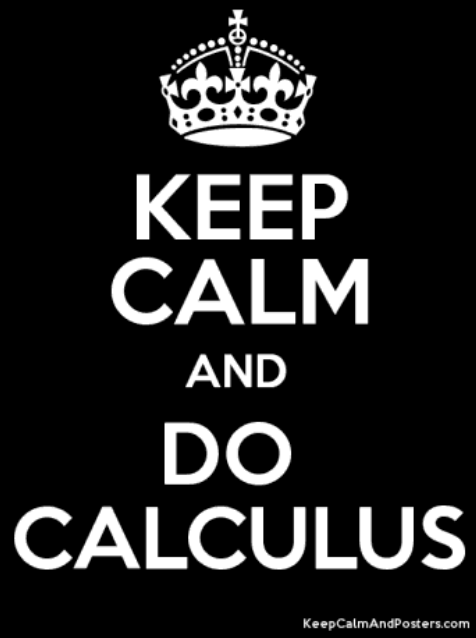
i.e. $\left|\frac{\boldsymbol{k}}{\boldsymbol{r}} - \boldsymbol{x_k}\right| \leq \frac{\boldsymbol{1}}{\boldsymbol{2^{n+1}}}$



$$\sum_{k=1}^{r} \boxed{|\boldsymbol{x_k}\rangle}|\boldsymbol{\psi_k}\rangle$$

$\boldsymbol{QFT^\dagger}$

$$\sum_{k=1}^{r} \boxed{\prod_{j=0}^{n}\left(\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i \cdot 2^j \cdot \left(\frac{k}{r}\right)}|1\rangle\right)\right)} |\boldsymbol{\psi_k}\rangle$$



$\langle Q|Crypton\rangle$

[Appendix 1] Quantum Fourier Transform

Preliminary : Discrete Fourier Transform(DFT) and Fast Fourier Transform(FFT)

Recap: Continuous Fourier Transform

$$F = \Gamma(f) \qquad F(s) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} f(x) e^{-isx} dx \qquad f(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} F(s) e^{isx} ds$$

- **Integrals → sums from 0 to N-1**
- **The factor of** $1/\sqrt{2\pi}$ **→** $1/\sqrt{N}$
- e^{isx} **→ Nth roots of unity,** ω^{jk}

$$f = (f_k) \xrightarrow[\text{DFT}]{} F_j = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} f_k \omega^{-jk}, \; j = 0, \ldots, N-1 \qquad \omega = \omega_N = e^{2\pi i/N}$$

N-component vector

N-component vector

The primitive Nth root of 1

$$f_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} F_j \omega^{kj} \xleftarrow[\text{Inverse DFT}]{} F = \{F_j\}$$

[Appendix 1] Quantum Fourier Transform

Preliminary : Discrete Fourier Transform(DFT) and Fast Fourier Transform(FFT)

Fast Fourier Transform(FFT)

1. Assume $N = 2^n$

$$\begin{pmatrix} f_0 \\ f_1 \\ f_2 \\ f_3 \end{pmatrix} \rightarrow \begin{pmatrix} f_0 \\ f_1 \\ f_2 \\ f_3 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

2. Splitting f **into** f^{even} **and** f^{odd}

$$f^{even} \equiv \begin{pmatrix} f_0 \\ f_2 \\ f_4 \\ \vdots \\ f_{N/2} \end{pmatrix} \qquad f^{odd} \equiv \begin{pmatrix} f_1 \\ f_3 \\ f_5 \\ \vdots \\ f_{(N/2)+1} \end{pmatrix}$$

$$f_k^{even} = f_{2k} \qquad f_k^{odd} = f_{2k+1}$$

[Appendix 1] Quantum Fourier Transform

Preliminary : Discrete Fourier Transform(DFT) and Fast Fourier Transform(FFT)

Fast Fourier Transform(FFT)

3. Now,

$$DFT[f]_j = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} f_k \omega^{-jk} = \frac{1}{\sqrt{N}} \left(\sum_{k=0}^{\frac{N}{2}-1} f_k^{even} \omega^{-j2k} + \sum_{k=0}^{\frac{N}{2}-1} f_k^{odd} \omega^{-j(2k+1)} \right)$$

$$= \frac{1}{\sqrt{N}} \left(\sum_{k=0}^{\frac{N}{2}-1} f_k^{even} \omega^{-j(2k)} + \omega^{-j} \sum_{k=0}^{\frac{N}{2}-1} f_k^{odd} \omega^{-j(2k)} \right) = \frac{1}{\sqrt{N}} \left(\sum_{k=0}^{\frac{N}{2}-1} f_k^{even} \left(\omega^2\right)^{-jk} + \omega^{-j} \sum_{k=0}^{\frac{N}{2}-1} f_k^{odd} \left(\omega^2\right)^{-jk} \right)$$

$$DFT[f]_j = \frac{1}{\sqrt{2}} \left(\frac{1}{\sqrt{N'}} \sum_{k=0}^{N'-1} f_k^{even} (\omega')^{-jk} + \omega_N^{-j} \frac{1}{\sqrt{N'}} \sum_{k=0}^{N'-1} f_k^{odd} (\omega')^{-jk} \right) \quad N' = \frac{N}{2}, \omega' = e^{2\pi i/N'}$$

$$= \frac{1}{\sqrt{2}} \left(DFT^{(N/2)}[f^{even}]_j + \omega_N^{-j} \cdot DFT^{(N/2)}[f^{odd}]_j \right)$$

4. Therefore, complexity of DFT $O(N^2)$ **, complexity of FFT** $O(N(\log N))$

[Appendix 1] Quantum Fourier Transform

Quantum Fourier Transform

Now , define Quantum Fourier Transform(QFT)

$$|\psi\rangle^n = \sum_{x=0}^{2^n-1} c_x |x\rangle^n \quad \Longrightarrow \quad QFT|\psi\rangle^n = \sum_{y=0}^{2^n-1} \tilde{c}_x |y\rangle^n$$

If we think $|\psi\rangle^n$ **as a complex vector** $c = (c_x)$ **with size** 2^n **then,**

$$QFT|\psi\rangle^n = \sum_{y=0}^{2^n-1} [DFT(c)]_y |y\rangle^n$$

That is, $$\left[QFT|\psi\rangle^n\right]_y = \frac{1}{\sqrt{N}} \sum_{x=0}^{2^n-1} c_x \omega^{yx}$$

$$QFT|\psi\rangle^n = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} c_x \omega^{yx} |y\rangle^n$$

[Appendix 1] Quantum Fourier Transform

Quantum Fourier Transform

$$QFT|y\rangle^n = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} c_x \mathrm{w}^{yx} |y\rangle^n$$

For each basis $|x\rangle^n$ **in the Hilbert space,**

$$QFT|x\rangle^n = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} \mathrm{w}^{yx} |y\rangle^n$$

QFT 1) Linear and 2) Unitary operator

1) Linearity

$$|\psi\rangle^n = \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ \vdots \end{pmatrix} \quad \Rightarrow \quad QFT|\psi\rangle^n = \begin{pmatrix} \tilde{c}_0 \\ \tilde{c}_1 \\ \tilde{c}_2 \\ \vdots \end{pmatrix} = \frac{1}{\sqrt{2^n}} \begin{pmatrix} \sum_x c_x \omega^{0x} \\ \sum_x c_x \omega^{1x} \\ \sum_x c_x \omega^{2x} \\ \vdots \end{pmatrix} = \frac{1}{\sqrt{2^n}} \begin{pmatrix} 1 & 1 & 1 & \cdots \\ 1 & \omega & \omega^2 & \cdots \\ 1 & \omega^2 & \omega^4 & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ \vdots \end{pmatrix}$$

[Appendix 1] Quantum Fourier Transform

Quantum Fourier Transform

$$QFT|y\rangle^n = \frac{1}{\sqrt{2^n}}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1} c_x w^{yx}|y\rangle^n$$

2) Unitary Operator: $(M_{QFT})^* M_{QFT} = 1$

$$(w^x)^* = (e^{2\pi i/N\cdot x})^* = e^{-2\pi i/N\cdot x} = w^{-x}$$

$$M_{QFT} = \frac{1}{\sqrt{2^n}}\begin{pmatrix} 1 & 1 & 1 & \cdots \\ 1 & \omega & \omega^2 & \cdots \\ 1 & \omega^2 & \omega^4 & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

$$\frac{1}{\sqrt{2^n}}\begin{pmatrix} 1 & (\omega^x)^* & (\omega^{2x})^* & \cdots \end{pmatrix}\frac{1}{\sqrt{2^n}}\begin{pmatrix} 1 \\ \omega^y \\ \omega^{2y} \\ \vdots \end{pmatrix}$$

$$= \frac{1}{2^n}\sum_{k=0}^{2^n-1}\omega^{k(y-x)} = \frac{1}{2^n}\delta_{xy}2^n = \delta_{xy}$$

$$(\because)\ (1+\omega+\omega^2+\cdots+\omega^{N-1})^{y-x} = \begin{cases} 1 & , y = x \\ 0 & , y \neq x \end{cases} = \delta_{xy}$$

Note that $\omega^N = 1 \Leftrightarrow \omega^N - 1 = (\omega-1)(1+\omega+\omega^2+\cdots+\omega^{N-1}) = 0$

[Appendix 1] Quantum Fourier Transform

Quantum Fourier Transform

$$QFT\left|x\right\rangle^{n} = \frac{1}{\sqrt{2^{n}}}\sum_{y=0}^{2^{n}-1} w^{yx}\left|y\right\rangle^{n}$$

Comparison between QFT and Hadamard Gate, H

$$H^{\otimes n}\left|x\right\rangle^{n} = \left(\frac{1}{\sqrt{2}}\right)^{n}\sum_{y=0}^{2^{n}-1}(-1)^{x\cdot y}\left|y\right\rangle = \left(\frac{1}{\sqrt{2}}\right)^{n}\sum_{y=0}^{2^{n}-1} w_{2}^{\;x\cdot y}\left|y\right\rangle^{n} \qquad w_{2}(= e^{2pi/2} = e^{pi} = -1)$$

- QFT uses a primitive 2^nth root of unity : H uses a square root of unity
- The exponent of QFT – ordinary integer product : mod-2 dot product

QFT == H for N = 2

$$QFT^{(2)}\left|x\right\rangle = \left(\frac{1}{\sqrt{2}}\right)^{1}\sum_{y=0}^{1}(-1)^{yx}\left|y\right\rangle = \frac{1}{\sqrt{2}}\left((-1)^{0\cdot x}\left|0\right\rangle + (-1)^{1\cdot x}\left|1\right\rangle\right) = \begin{cases} \dfrac{\left|0\right\rangle + \left|1\right\rangle}{\sqrt{2}}, x = 0 \\ \dfrac{\left|0\right\rangle - \left|1\right\rangle}{\sqrt{2}}, x = 1 \end{cases}$$

And $QFT\left|0\right\rangle^{n} = \left(\frac{1}{\sqrt{2}}\right)^{n}\sum_{y=0}^{2^{n}-1} w^{y\cdot 0}\left|y\right\rangle^{n} = \left(\frac{1}{\sqrt{2}}\right)^{n}\sum_{y=0}^{2^{n}-1}\left|y\right\rangle^{n} = H^{\otimes n}\left|0\right\rangle^{n}$

[Appendix 1] Quantum Fourier Transform

Quantum Fourier Transform

$$QFT|y\rangle^n = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} c_x w^{yx} |y\rangle^n$$

QFT Circuit – QFT operation을 elementary gates의 조합으로 만들기

$$\left(\sqrt{N}\right)QFT^{(N)}|x\rangle^n = \sum_{y=0}^{N-1} \omega^{xy}|y\rangle^n = \sum_{y=0}^{N-1} \omega^{x\sum_{k=0}^{n-1} y_k 2^k} |y_{n-1}\cdots y_1 y_0\rangle$$

$$= \sum_{y=0}^{N-1}\left(\prod_{k=0}^{n-1} \omega^{xy_k 2^k}\right)|y_{n-1}\cdots y_1 y_0\rangle$$

Let $P_{xy} := \prod_{k=0}^{n-1} w^{xy_k 2^k}$ **, then** $\left(\sqrt{N}\right)QFT^{(N)}|x\rangle^n = \sum_{y=0}^{N-1} \Pi_{xy}|y_{n-1}\cdots y_1 y_0\rangle$

n=3, then $\left(\sqrt{8}\right)QFT|x\rangle^3 = P_{x\cdot 0}|000\rangle + P_{x\cdot 1}|001\rangle + P_{x\cdot 2}|010\rangle + P_{x\cdot 3}|011\rangle$

$$+ P_{x\cdot 4}|100\rangle + P_{x\cdot 5}|101\rangle + P_{x\cdot 6}|110\rangle + P_{x\cdot 7}|111\rangle$$

[Appendix 1] Quantum Fourier Transform

Quantum Fourier Transform

$$QFT|y\rangle^n = \frac{1}{\sqrt{2^n}}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1} c_x w^{yx}|y\rangle^n$$

QFT Circuit

$$\left(\sqrt{8}\right)QFT|x\rangle^3 = P_{x\cdot 0}|000\rangle + P_{x\cdot 2}|010\rangle + P_{x\cdot 4}|100\rangle + P_{x\cdot 6}|110\rangle$$
$$+ P_{x\cdot 1}|001\rangle + P_{x\cdot 3}|011\rangle + P_{x\cdot 5}|101\rangle + P_{x\cdot 7}|111\rangle$$

= sum of y-even group + sum of y-odd group

(i) Sum of y-even group $= P_{x\cdot 0}|000\rangle + P_{x\cdot 2}|010\rangle + P_{x\cdot 4}|100\rangle + P_{x\cdot 6}|110\rangle$

$$= \left(P_{x\cdot 0}|00\rangle + P_{x\cdot 2}|01\rangle + P_{x\cdot 4}|10\rangle + P_{x\cdot 6}|11\rangle\right)|0\rangle$$

$$= \left(\sum_{\substack{y=0 \\ y:\text{even}}}^{7}\left(\prod_{k=1}^{2} w^{xy_k 2^k}\right)|y_2 y_1\rangle\right)|0\rangle$$

$$(\because)\, y_0 = 0$$

$$\Rightarrow \omega^{xy_0 2^0} = \omega^{x\cdot 0\cdot 1} = 1$$

$$\therefore \Pi_{xy} = \prod_{k=0}^{2}\omega^{xy_k 2^k} = \prod_{k=1}^{2}\omega^{xy_k 2^k}$$

[Appendix 1] Quantum Fourier Transform

Quantum Fourier Transform

$$QFT\left|y\right\rangle^n = \frac{1}{\sqrt{2^n}}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1} c_x w^{yx}\left|y\right\rangle^n$$

QFT Circuit

Sum of y−even group $= \left(\sum_{\substack{y=0 \\ y:\text{even}}}^{7}\left(\prod_{k=1}^{2} w^{xy_k 2^k}\right)\left|y_2 y_1\right\rangle\right)\left|0\right\rangle$

$$= \left(\sum_{y=0}^{3}\left(\prod_{k=0}^{1} w^{xy_k 2^{k+1}}\right)\left|y_1 y_0\right\rangle\right)\left|0\right\rangle = \left(\sum_{y=0}^{3}\left(\prod_{k=0}^{1} \left(w^2\right)^{xy_k 2^k}\right)\left|y_1 y_0\right\rangle\right)\left|0\right\rangle$$

Since ω^2 **4th root of unity,** $\left(w^2\right)^{xy_k 2^k} = \left(w^2\right)^{(x \bmod 4)y_k 2^k}$

Therefore, sum of y−even group $= \left(\sum_{y=0}^{3}\left(\prod_{k=0}^{1} \left(w^2\right)^{(x \bmod 4)y_k 2^k}\right)\left|y_1 y_0\right\rangle\right)\left|0\right\rangle$

In general,

$$\left(\sum_{y=0}^{\frac{N}{2}-1}\left(\prod_{k=0}^{n-2} \left(\omega^2\right)^{(x \bmod N/2)y_k 2^k}\right)\left|y_{n-2}\cdots y_1 y_0\right\rangle\right)\left|0\right\rangle$$

[Appendix 1] Quantum Fourier Transform

Quantum Fourier Transform

$$QFT\left|y\right\rangle^{n} = \frac{1}{\sqrt{2^{n}}}\sum_{y=0}^{2^{n}-1}\sum_{x=0}^{2^{n}-1} c_x w^{yx}\left|y\right\rangle^{n}$$

QFT Circuit

Therefore, sum of y-even group =

$$\left(\sum_{y=0}^{\frac{N}{2}-1}\left(\prod_{k=0}^{n-2}\left(\omega^{2}\right)^{(x \bmod N/2) y_k 2^k}\right)\left|y_{n-2}\cdots y_1 y_0\right\rangle\right)\left|0\right\rangle$$

$$= \left(\sqrt{\frac{N}{2}}QFT^{(N/2)}\left|x \bmod (N/2)\right\rangle^{(n-1)}\right)\left|0\right\rangle$$

(ii) Sum of y-odd group

Since $y_0 = 1 \Rightarrow w^{xy_0 2^0} = w^{x\cdot 1\cdot 1} = w^{x}$ $\qquad P_{xy} = \prod_{k=0}^{2} w^{xy_k 2^k} = w^{x}\prod_{k=1}^{2} w^{xy_k 2^k}$

Therefore, similarly,

$$= w^{x}\left(\sqrt{\frac{N}{2}}QFT^{(N/2)}\left|x \bmod (N/2)\right\rangle^{(n-1)}\right)\left|1\right\rangle$$

[Appendix 1] Quantum Fourier Transform

Quantum Fourier Transform

$$\text{QFT}|y\rangle^n = \frac{1}{\sqrt{2^n}}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1} c_x w^{yx}|y\rangle^n$$

QFT Circuit

From the result of (i) and (ii),

$$\left(\sqrt{N}\right)\text{QFT}|x\rangle^n = \left(\sqrt{\frac{N}{2}}\text{QFT}^{(N/2)}|\tilde{x}\rangle^{(n-1)}\right)|0\rangle + w^x\left(\sqrt{\frac{N}{2}}\text{QFT}^{(N/2)}|\tilde{x}\rangle^{(n-1)}\right)|1\rangle$$

$$= \left(\sqrt{\frac{N}{2}}\text{QFT}^{(N/2)}|\tilde{x}\rangle^{(n-1)}\right)\left(|0\rangle + w^x|1\rangle\right) \qquad \tilde{x} = x \bmod N/2$$

Therefore,

$$\boxed{\text{QFT}^{(2^n)}|x\rangle^n = \text{QFT}^{(2^{n-1})}|\tilde{x}\rangle^{n-1}\left(\frac{|0\rangle + w_{2^n}^x|1\rangle}{\sqrt{2}}\right)} \qquad \tilde{x} = x \bmod 2^{n-1}$$

[Appendix 1] Quantum Fourier Transform

Quantum Fourier Transform

$$QFT^{(2^n)}|x\rangle^n = \prod_{k=1}^{n}\left(\frac{|0\rangle + w^{2^{n-k}\cdot x}|1\rangle}{\sqrt{2}}\right)$$

QFT Circuit

Recursively, we get

$$QFT^{(2^n)}|x\rangle^n = QFT^{(2^{n-2})}|\widetilde{\widetilde{x}}\rangle^{n-2}\left(\frac{|0\rangle + w_{2^{n-1}}^{x}|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle + w_{2^n}^{x}|1\rangle}{\sqrt{2}}\right)$$

$$= \prod_{k=1}^{n}\left(\frac{|0\rangle + w_{2^k}^{x}|1\rangle}{\sqrt{2}}\right)$$

$\prod$: Tensor product

Set $\omega \coloneqq \omega_N$, since $\omega_{2^k} = \omega^{2^{n-k}}$

$$\boxed{QFT^{(2^n)}|x\rangle^n = \prod_{k=1}^{n}\left(\frac{|0\rangle + w^{2^{n-k}\cdot x}|1\rangle}{\sqrt{2}}\right)}$$

$\prod$: Tensor product

[Appendix 1] Quantum Fourier Transform

Quantum Fourier Transform

$$QFT^{(2^n)}|x\rangle^n = \prod_{k=1}^{n}\left(\frac{|0\rangle + w^{2^{n-k}\cdot x}|1\rangle}{\sqrt{2}}\right)$$

QFT Circuit

n=3, then $QFT^{(8)}|x\rangle^3 = \left(\frac{|0\rangle + w^{4x}|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle + w^{2x}|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle + w^{x}|1\rangle}{\sqrt{2}}\right)$

$$w^{2^0} = w = e^{2pi/2^3} \qquad w^{2^2} = w^4 = \left(e^{2pi/2^3}\right)^4 = e^{2pi/2} = e^{pi} = -1$$

$$w^{2^3} = w^8 = \left(e^{2pi/2^3}\right)^8 = 1 \qquad w^{2^1} = w^2 = \left(e^{2pi/2^3}\right)^2 = e^{2pi/4} = e^{\frac{p}{2}i} = i$$

(1) $w^{4x} = w^{4(4x_2+2x_1+x_0)} = \left(w^8\right)^{2x_2}\left(w^8\right)^{x_1}w^{4x_0} = (-1)^{x_0}$

(2) $w^{2x} = w^{2(4x_2+2x_1+x_0)} = \left(w^8\right)^{x_2}\left(w^4\right)^{x_1}\left(w^2\right)^{x_0} = (-1)^{x_1}(i)^{x_0}$

(3) $w^{x} = w^{(4x_2+2x_1+x_0)} = \left(w^4\right)^{x_2}\left(w^2\right)^{x_1}(w)^{x_0} = (-1)^{x_2}(i)^{x_1}(w)^{x_0}$

[Appendix 1] Quantum Fourier Transform

Quantum Fourier Transform

$$QFT^{(2^n)}|x\rangle^n = \prod_{k=1}^{n}\left(\frac{|0\rangle + w^{2^{n-k}\cdot x}|1\rangle}{\sqrt{2}}\right)$$

QFT Circuit

(1) $\omega^{4x} = (-1)^{x_0}$

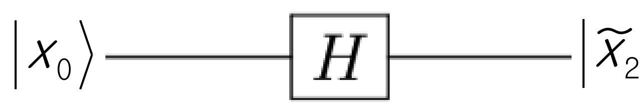
(2) $\omega^{2x} = (-1)^{x_1}(i)^{x_0}$

(3) $\omega^{x} = (-1)^{x_2}(i)^{x_1}(\omega)^{x_0}$

$$QFT^{(8)}|x\rangle^3 = \underbrace{\left(\frac{|0\rangle + w^{4x}|1\rangle}{\sqrt{2}}\right)}_{(1)}\left(\frac{|0\rangle + w^{2x}|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle + w^{x}|1\rangle}{\sqrt{2}}\right)$$

$$(1) = \left(\frac{|0\rangle + (-1)^{x_0}|1\rangle}{\sqrt{2}}\right) = \begin{cases} \dfrac{|0\rangle + |1\rangle}{\sqrt{2}}, x_0 = 0 \\ \dfrac{|0\rangle - |1\rangle}{\sqrt{2}}, x_0 = 1 \end{cases} = H|x_0\rangle$$

$$\boxed{|\tilde{x}_2\rangle = H|x_0\rangle}$$



[Appendix 1] Quantum Fourier Transform

Quantum Fourier Transform

$$QFT^{(2^n)}|x\rangle^n = \prod_{k=1}^{n}\left(\frac{|0\rangle + w^{2^{n-k}\cdot x}|1\rangle}{\sqrt{2}}\right)$$

QFT Circuit

(1) $\omega^{4x} = (-1)^{x_0}$ (2) $\omega^{2x} = (-1)^{x_1}(i)^{x_0}$ (3) $\omega^{x} = (-1)^{x_2}(i)^{x_1}(\omega)^{x_0}$

$$QFT^{(8)}|x\rangle^3 = \left(\frac{|0\rangle + \omega^{4x}|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle + \omega^{2x}|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle + \omega^{x}|1\rangle}{\sqrt{2}}\right)$$

(2)

$$\textbf{(2)} = \left(\frac{|0\rangle + (-1)^{x_1}(i)^{x_0}|1\rangle}{\sqrt{2}}\right) = \begin{cases} H|x_1\rangle, x_0 = 0 \\ \left(\frac{|0\rangle + (-1)^{x_1}\cdot i|1\rangle}{\sqrt{2}}\right), x_0 = 1 \end{cases}$$

$$|x_1\rangle \mapsto \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ (-1)^{x_1} \end{pmatrix}, x_0 = 0$$

$$|x_1\rangle \mapsto \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ (-1)^{x_1}\cdot i \end{pmatrix}, x_0 = 1$$

$$R_1 := \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \Rightarrow$$

$$R_1\begin{pmatrix} 1 \\ (-1)^{x_1} \end{pmatrix} = \begin{pmatrix} 1 \\ (-1)^{x_1}\cdot i \end{pmatrix}$$

$$\textbf{(2)} = \begin{cases} H|x_1\rangle, x_0 = 0 \\ R_1 H|x_1\rangle, x_0 = 1 \end{cases}$$

$$|\widetilde{x}_1\rangle = \begin{cases} H|x_1\rangle, x_0 = 0 \\ R_1 H|x_1\rangle, x_0 = 1 \end{cases}$$

[Appendix 1] Quantum Fourier Transform

Quantum Fourier Transform

$$QFT^{(2^n)}\left|x\right\rangle^n = \prod_{k=1}^{n}\left(\frac{\left|0\right\rangle + w^{2^{n-k}\cdot x}\left|1\right\rangle}{\sqrt{2}}\right)$$

QFT Circuit

(1) $\omega^{4x} = (-1)^{x_0}$ (2) $\omega^{2x} = (-1)^{x_1}(i)^{x_0}$ (3) $\omega^{x} = (-1)^{x_2}(i)^{x_1}(\omega)^{x_0}$

$$QFT^{(8)}\left|x\right\rangle^3 = \left(\frac{\left|0\right\rangle + \omega^{4x}\left|1\right\rangle}{\sqrt{2}}\right)\left(\frac{\left|0\right\rangle + \omega^{2x}\left|1\right\rangle}{\sqrt{2}}\right)\underbrace{\left(\frac{\left|0\right\rangle + \omega^{x}\left|1\right\rangle}{\sqrt{2}}\right)}_{(3)}$$

$$\textbf{(3)} = \left(\frac{\left|0\right\rangle + (-1)^{x_2}(i)^{x_1}(\omega)^{x_0}\left|1\right\rangle}{\sqrt{2}}\right) = \begin{cases}\left(\frac{\left|0\right\rangle + (-1)^{x_2}(i)^{x_1}\left|1\right\rangle}{\sqrt{2}}\right), x_0 = 0 \\ \left(\frac{\left|0\right\rangle + (-1)^{x_2}(i)^{x_1}(\omega)^{x_0}\left|1\right\rangle}{\sqrt{2}}\right), x_0 = 1\end{cases}$$

$$R_1 := \begin{pmatrix}1 & 0 \\ 0 & i\end{pmatrix}, \quad R_2 := \begin{pmatrix}1 & 0 \\ 0 & \omega\end{pmatrix}$$

$(\ )$

$$\textbf{(3)} \quad = \begin{cases}H\left|x_2\right\rangle, x_0 = 0, x_1 = 0 \\ R_1H\left|x_2\right\rangle, x_0 = 0, x_1 = 1\end{cases}, \begin{cases}R_2H\left|x_2\right\rangle, x_0 = 1, x_1 = 0 \\ R_2R_1H\left|x_2\right\rangle, x_0 = 1, x_1 = 1\end{cases}$$

[Appendix 1] Quantum Fourier Transform

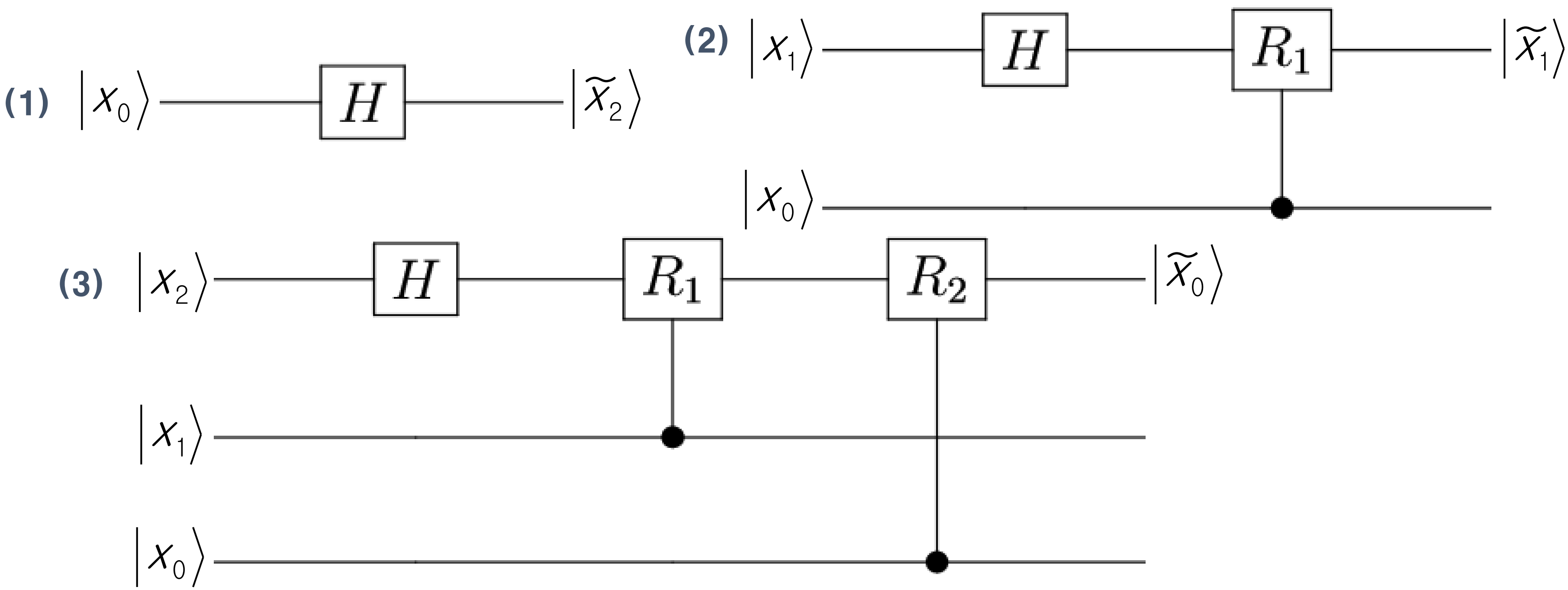
Quantum Fourier Transform

$$QFT^{(2^n)}\left|x\right\rangle^n = \prod_{k=1}^{n}\left(\frac{\left|0\right\rangle + w^{2^{n-k}\cdot x}\left|1\right\rangle}{\sqrt{2}}\right)$$

QFT Circuit

(1) $\omega^{4x} = (-1)^{x_0}$ (2) $\omega^{2x} = (-1)^{x_1}(i)^{x_0}$ (3) $\omega^{x} = (-1)^{x_2}(i)^{x_1}(\omega)^{x_0}$

$$QFT^{(8)}\left|x\right\rangle^3 = \underbrace{\left(\frac{\left|0\right\rangle + \omega^{4x}\left|1\right\rangle}{\sqrt{2}}\right)}_{(1)}\underbrace{\left(\frac{\left|0\right\rangle + \omega^{2x}\left|1\right\rangle}{\sqrt{2}}\right)}_{(2)}\underbrace{\left(\frac{\left|0\right\rangle + \omega^{x}\left|1\right\rangle}{\sqrt{2}}\right)}_{(3)}$$

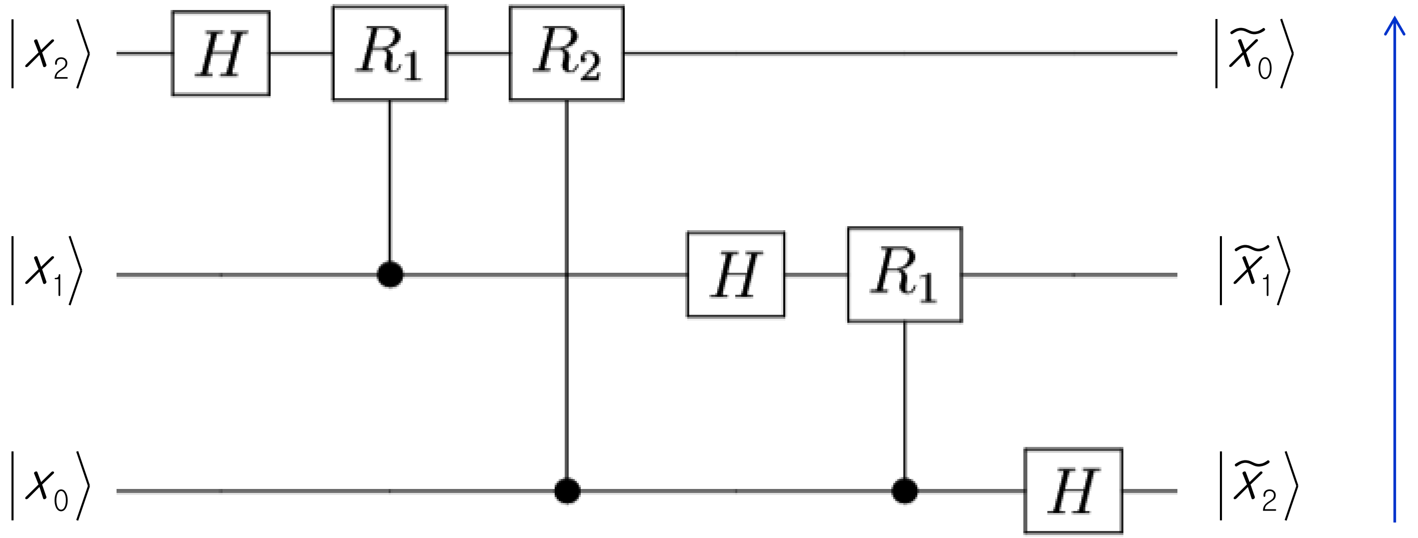


[Appendix 1] Quantum Fourier Transform

Quantum Fourier Transform

$$QFT^{(2^n)}|x\rangle^n = \prod_{k=1}^{n}\left(\frac{|0\rangle + w^{2^{n-k}\cdot x}|1\rangle}{\sqrt{2}}\right)$$

QFT Circuit

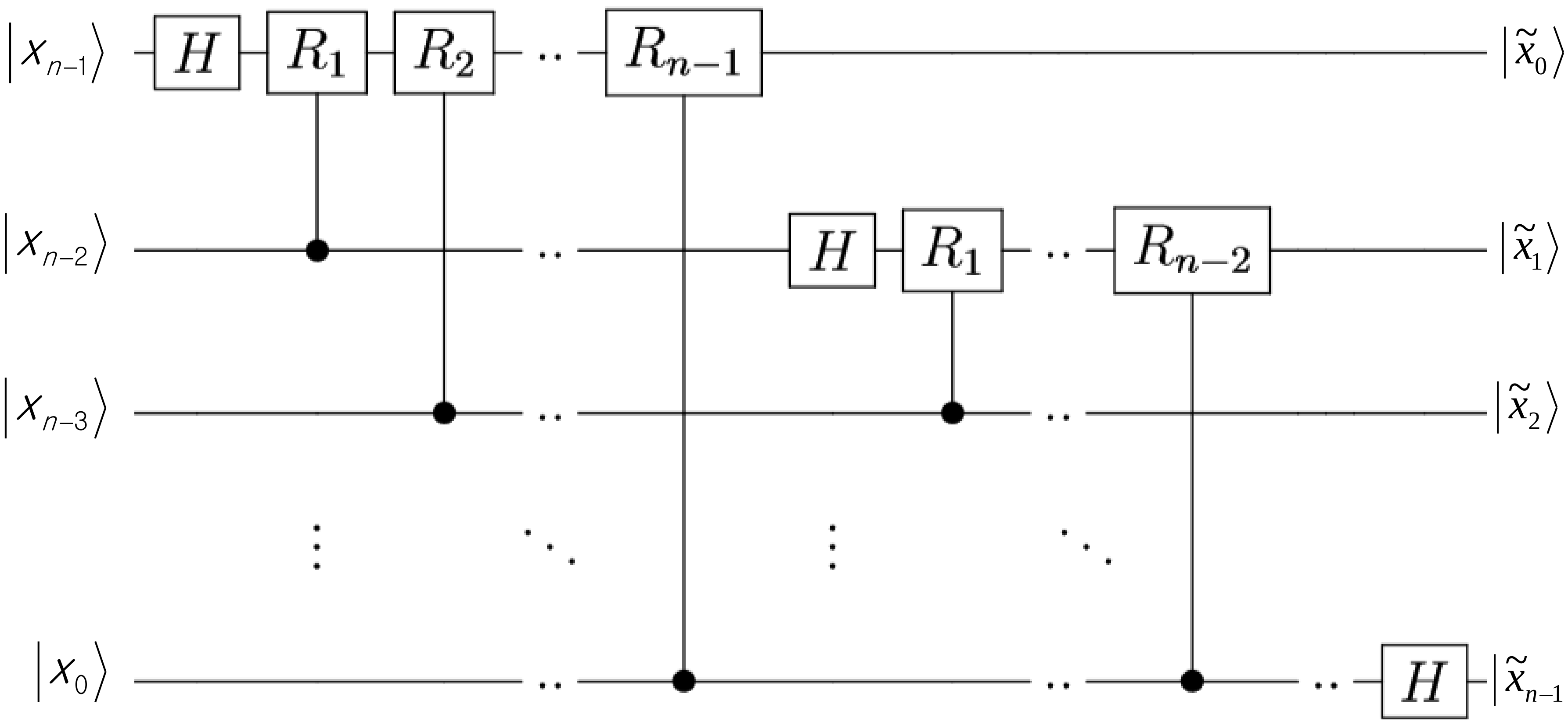


[Appendix 1] Quantum Fourier Transform

Quantum Fourier Transform

$$QFT^{(2^n)}|x\rangle^n = \prod_{k=1}^{n}\left(\frac{|0\rangle + w^{2^{n-k}\cdot x}|1\rangle}{\sqrt{2}}\right)$$

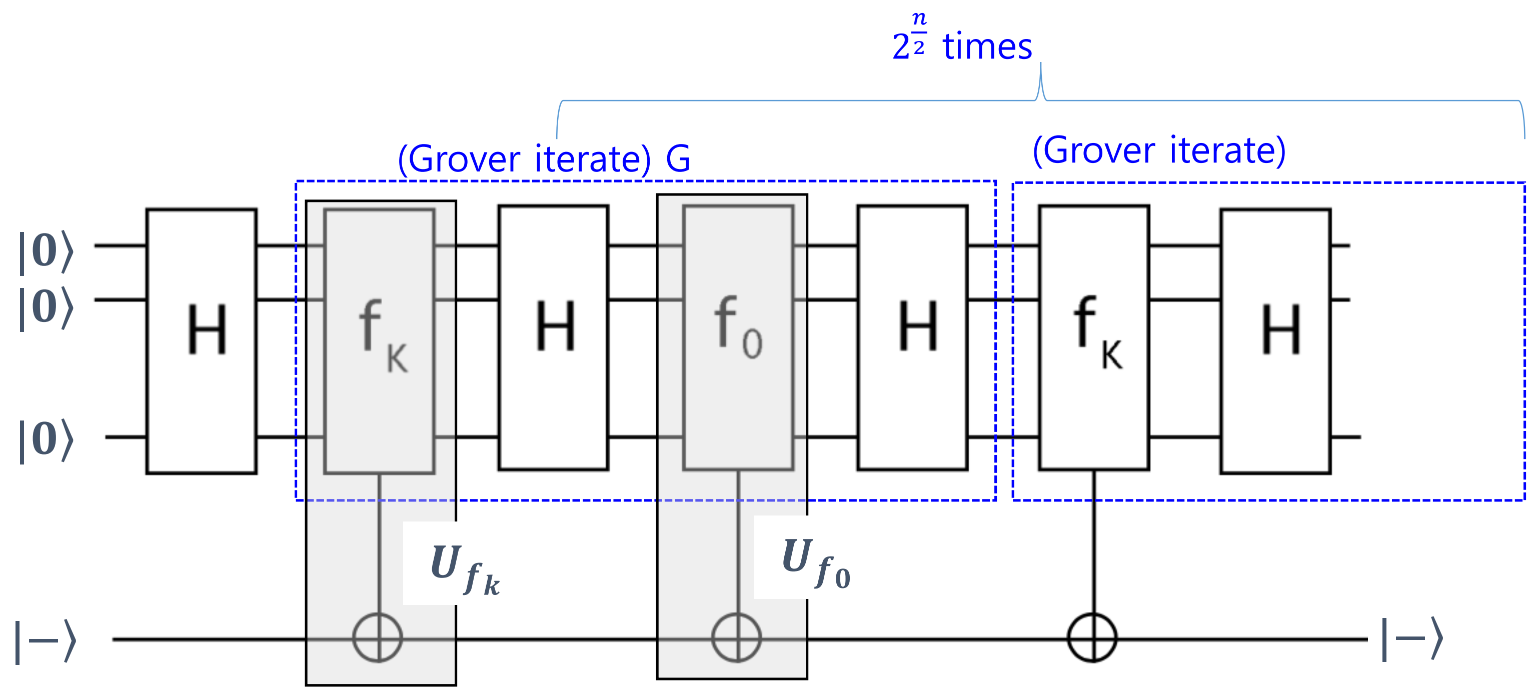
QFT Circuit, in general, $R_k = \begin{pmatrix} 1 & 0 \\ 0 & \omega^{2^{n-k-1}} \end{pmatrix}$



[Appendix 2] Amplitude Amplification : Grover's Algorithm

- **Grover's Algorithm**

$f_k: \{0,1\}^n \to \{0,1\}$, such that $f_k(x) = \delta_{xk}$. Find k $\qquad f_0(x) = \delta_{x0}$



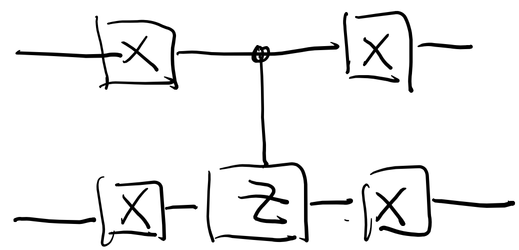
$= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

$U_{f_k}|x\rangle|y\rangle = |x\rangle|y \oplus f_k(x)\rangle \qquad U_{f_k}|x\rangle|-\rangle = (-1)^{f_k(x)}|x\rangle|-\rangle$

[Appendix 2] Amplitude Amplification : Grover's Algorithm

- **Diffusion operator** $D = H^2(2|00\rangle\langle 00| - I)H^2$

$$(2|00\rangle\langle 00| - I) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} = -\begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$



$$\boldsymbol{U_{f_0}}|x\rangle|-\rangle = (-1)^{f_0(x)}|x\rangle|-\rangle$$

$$\boldsymbol{U_{f_0}}|x\rangle|-\rangle = \begin{cases} (-1)^{f_0(0)}|0\rangle|-\rangle = -|0\rangle|-\rangle \text{ if x=0} \\ (-1)^{f_0(x)}|x\rangle|-\rangle = |x\rangle|-\rangle \text{ otherwise} \end{cases}$$

[Appendix 3] Hidden Subgroup Problem

(Example)

$$G = Z = \{\cdots,-1,0,1,2,\cdots\} \qquad K = 3Z = \{\cdots,-3,0,3,6,9,\cdots\}$$

$$K = 0 + K$$

$$1 + K = \{\cdots,-2,1,4,7,10,\cdots\} \Rightarrow G = K \cup (1+K) \cup (2+K)$$

$$2 + K = \{\cdots,-1,2,5,8,11,\cdots\}$$

G : A finitely generated group X : A finite set K : A subgroup of G $\quad G = \bigcup_{x \in G} \underline{xK}$

f : a function from G to X such that $f(g) = f(g'), g, g' \in xK$

$$f(g) \neq f(g'), g \in xK, g' \in x'K, xK \neq x'K$$

coset

Find a generating set for K under a quantum network $U_f : |x\rangle|y\rangle \mapsto |x\rangle|y \oplus f(x)\rangle$

(1) Order Finding Problem

For an element g of a finite group G, find r, the order of g

This is a special case of HSP

$(\because)$ Consider $f : Z \to G$ such that $f(x) = g^x$. Then

$$f(x) = f(y) \Leftrightarrow g^x = g^y \Leftrightarrow x - y \in \{k \cdot r : k \in Z\}$$

Therefore, $f(x) = f(y)$ iff x and y are in the same coset of the hidden subgroup rZ

[Appendix 3] Hidden Subgroup Problem

(2) Discrete Logarithm Problem(DLP)

Given an element a of a finite group G and $b = a^k$, find k

Suppose the order of a is r. Let $f : Z_r \times Z_r \to G$ **by** $f(x_1, x_2) = a^{x_1} b^{x_2}$ **. Then**

$$f(x_1, x_2) = f(y_1, y_2) \Leftrightarrow a^{x_1} b^{x_2} = a^{y_1} b^{y_2} \Leftrightarrow a^{x_1 - y_1} b^{x_2 - y_2} = 1 \Leftrightarrow a^{x_1 - y_1} a^{k(x_2 - y_2)} = 1$$

$$\Leftrightarrow x_1 - y_1 = -k(x_2 - y_2) \text{ in } Z_r \Leftrightarrow (x_1, x_2) - (y_1, y_2) \in \{(-kt, t) : t \in Z_r\}$$

Therefore, $f(x_1, x_2) = f(y_1, y_2)$ **if and only if**

(x_1, x_2) **and** (y_1, y_2) **are in the same coset of the hidden subgroup**

$$K = \langle(-k, 1)\rangle \subset Z_r \times Z_r$$

Thus, DLP is also a special case of HSP.

[Appendix 3] Hidden Subgroup Problem

$$G = \bigcup_{i=0}^{\frac{|G|}{|K|}-1} x_i K \quad \text{for some } x_i \in G, \; x_0 = 1(\text{identity})$$

General Strategy for solving HSP

(0) $f : G \to X$ a function such that $f(g) = f(g'), g, g' \in xK$
$f(g) \neq f(g'), g \in xK, g' \in x'K, xK \neq x'K$

where K : unknown subgroup of G

(1) Construct superposition of over all elements of G $\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle$

(2) Apply $U_f : |x\rangle|y\rangle \mapsto |x\rangle|y \oplus f(x)\rangle$ with $|g\rangle|0\rangle$ then $\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle|f(g)\rangle$

In fact, $$\boxed{\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle|f(g)\rangle = \frac{\sqrt{|K|}}{\sqrt{|G|}} \sum_{i=0}^{\frac{|G|}{|K|}-1} \left(\frac{1}{\sqrt{|K|}} \sum_{g \in K} |x_i g\rangle \right) |f(x_i)\rangle}$$

Coset sampling

(3) (Conceptually) Measure second register. Then $\frac{1}{\sqrt{|K|}} \sum_{g \in K} |x_0 g\rangle$

(4) Find the subgroup K using various methods(e.g. QFT for OFA)