Bernstein - Varizani algorithm

Input: $U_f : |x, y\rangle \longrightarrow |x, y \oplus f(x)\rangle$

$$f : \mathbb{B}^n \longrightarrow \mathbb{B}$$

$$x \longmapsto a \cdot x = a_1 x_1 + a_2 x_2 + \cdots + a_n x_n, \qquad a = a_1 \cdots a_n \in \mathbb{B}^n$$

Output: a

Algorithm:

$$|0^n\rangle |1\rangle$$

$$\xrightarrow{H^{\otimes (n+1)}} \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

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

$$\xrightarrow{H^{\otimes n} \otimes I} \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} \sum_{z=0}^{2^n-1} (-1)^{x \cdot z} |z\rangle |-\rangle$$

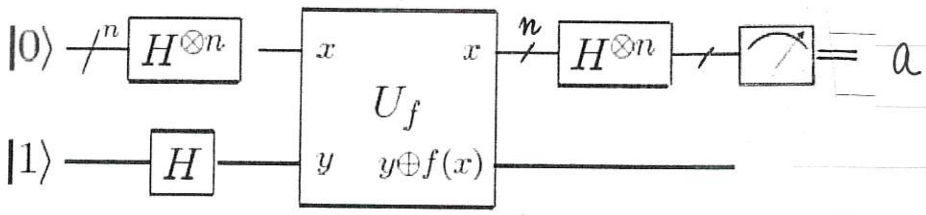
$$= \frac{1}{2^n} \sum_{z=0}^{2^n-1} \left(\sum_{x=0}^{2^n-1} (-1)^{x \cdot a + x \cdot z} \right) |z\rangle |-\rangle$$

$$\xrightarrow[\text{1st } n \text{ qubits}]{\text{measure}} a$$

說明
- $z = a$ 時, $x \cdot a + x \cdot z = x(a+z) = 0$, $\forall x \in \mathbb{B}^n$

  $Pr(\text{測得 } a) = 1$

- 思考: $z \neq a$?



Simon's algorithm

$a = 011$

x	$a \oplus x$	$f(x)$
000	011	010
001	011	101
100	111	110
101	110	001

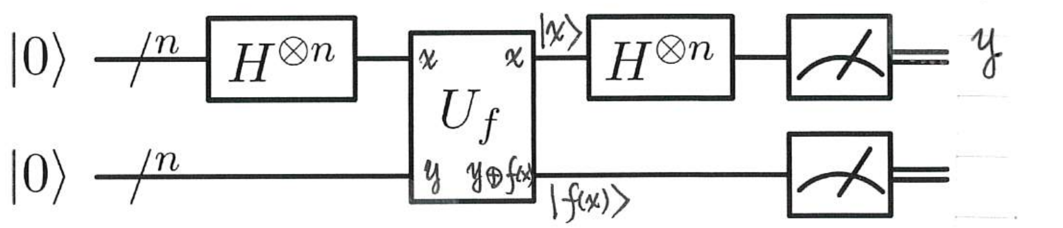
Input: $U_f \ |x, y\rangle \longrightarrow |x, y \oplus f(x)\rangle$

$f : \mathbb{B}^n \longrightarrow \mathbb{B}^n$

存在 $a \in \mathbb{B}^n$, $f(x) = f(x \oplus a)$

Output: a

Algorithm:



説明 $(n=3)$

$|000000\rangle$

$$\xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{8}}(|000000\rangle + |001000\rangle + |010000\rangle + |011000\rangle + |100000\rangle + |101000\rangle + |110000\rangle + |111000\rangle)$$

$$\xrightarrow{U_f} \frac{1}{\sqrt{8}}(|\underbrace{000}_{x}\underbrace{010}_{f(x)}\rangle + |001101\rangle + |010101\rangle + |011010\rangle + |100110\rangle + |101001\rangle + |110001\rangle + |111110\rangle)$$

$$\xrightarrow[\text{2nd } n \text{ qubits}]{\text{measure}} \frac{1}{\sqrt{8}}(\cancel{|000010\rangle} + \cancel{|001101\rangle} + \cancel{|010101\rangle} + \cancel{|011010\rangle} + |100\underline{110}\rangle + \cancel{|101001\rangle} + \cancel{|110001\rangle} + |111\underline{110}\rangle)$$

$\Downarrow$

(1st n qubits): $\frac{1}{\sqrt{2}}(\underset{z}{|100\rangle} + \underset{z \oplus a}{|111\rangle})$

$(0-1)(0+1)(0+1)$
$(0-1)(0-1)(0-1)$

$$\xrightarrow{H^{\otimes n}} \frac{1}{4}(|000\rangle + |001\rangle + |010\rangle + |011\rangle - |100\rangle - |101\rangle - |110\rangle - |111\rangle$$
$$+ |000\rangle - |001\rangle - |010\rangle + |011\rangle - |100\rangle + \underbrace{|101\rangle}_{a \cdot y = 1} + |110\rangle - \underbrace{|111\rangle}_{a \cdot y = 0})$$

$$= \underline{\frac{1}{2}(|000\rangle + |011\rangle - |100\rangle - |111\rangle)}$$

$$
\begin{aligned}
&H^{\otimes n}\left[\frac{1}{\sqrt{2}}\left|z\right\rangle+\frac{1}{\sqrt{2}}\left|z\oplus a\right\rangle\right]\\
=&\frac{1}{\sqrt{2}}H^{\otimes n}\left|z\right\rangle+\frac{1}{\sqrt{2}}H^{\otimes n}\left|z\oplus a\right\rangle\\
=&\frac{1}{\sqrt{2}}\left[\frac{1}{\sqrt{2^n}}\sum_{y\in\{0,1\}^n}(-1)^{z\cdot y}\left|y\right\rangle\right]+\frac{1}{\sqrt{2}}\left[\frac{1}{\sqrt{2^n}}\sum_{y\in\{0,1\}^n}(-1)^{(z\oplus a)\cdot y}\left|y\right\rangle\right]\\
=&\frac{1}{\sqrt{2^{n+1}}}\sum_{y\in\{0,1\}^n}\left[(-1)^{z\cdot y}+(-1)^{(z\oplus a)\cdot y}\right]\left|y\right\rangle\\
=&\frac{1}{\sqrt{2^{n+1}}}\sum_{y\in\{0,1\}^n}\left[(-1)^{z\cdot y}+(-1)^{(z\cdot y)\oplus(a\cdot y)}\right]\left|y\right\rangle\\
=&\frac{1}{\sqrt{2^{n+1}}}\sum_{y\in\{0,1\}^n}(-1)^{z\cdot y}\left[1+(-1)^{a\cdot y}\right]\left|y\right\rangle
\end{aligned}
$$

$a=011$, $a\cdot y=a_1y_1+a_2y_2+a_3y_3=0 \pmod 2$

方程式 (2^{n-1}個)

$$
y=\begin{cases}
000 & \\
011 & a_2+a_3=0\\
100 & a_1=0\\
111 & a_1+a_2+a_3=0
\end{cases}
$$

Black box Oracle.

$$U_f : |x, y\rangle \longrightarrow |x, y \oplus f(x)\rangle$$

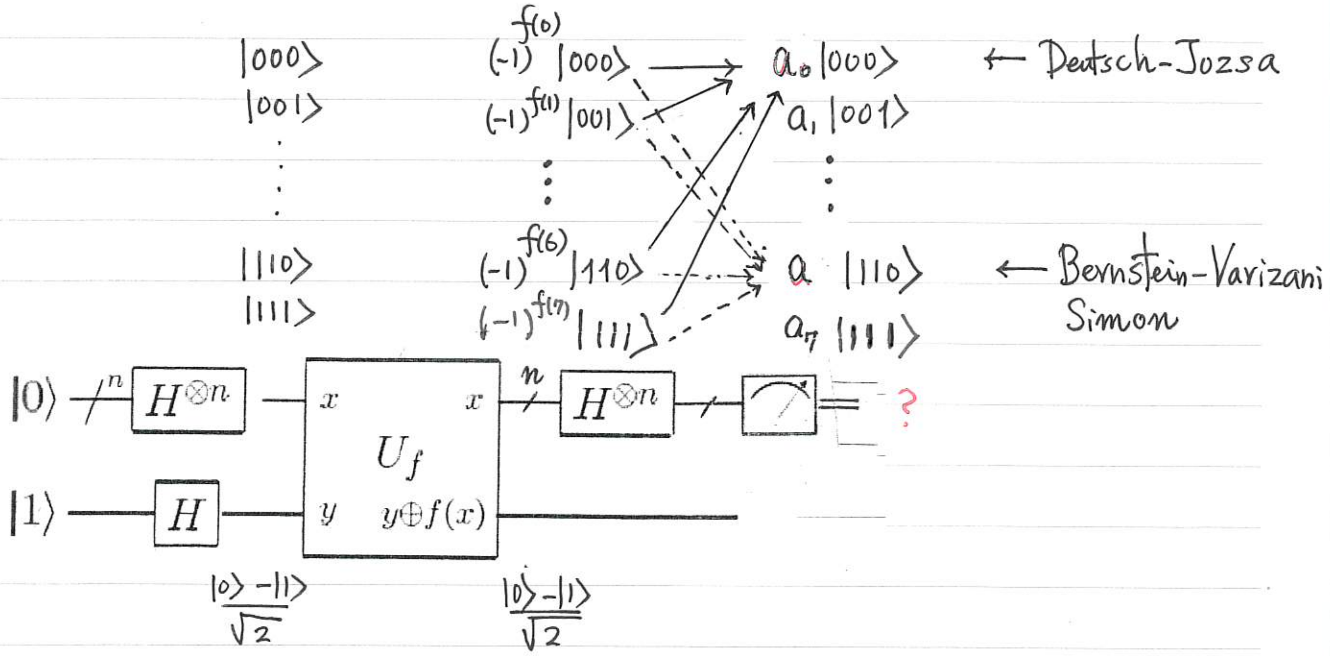
(1) Deutsch-Jozsa : $f : \mathbb{B}^n \to \mathbb{B}$, f : constant/balanced?

(2) Bernstein-Varizani : $\to \mathbb{B}$, $f(x) = a \cdot x$, $a = ?$

(3) Simon : $\to \mathbb{B}^n$, $f(x) = f(x \oplus a)$, $a = ?$

(4) Grover : $\to \mathbb{B}$, $f(x_0) = 1$, $x_0 = ?$

$$|110\rangle \to (|0\rangle - |1\rangle)(|0\rangle - |1\rangle)(|0\rangle + |1\rangle)$$



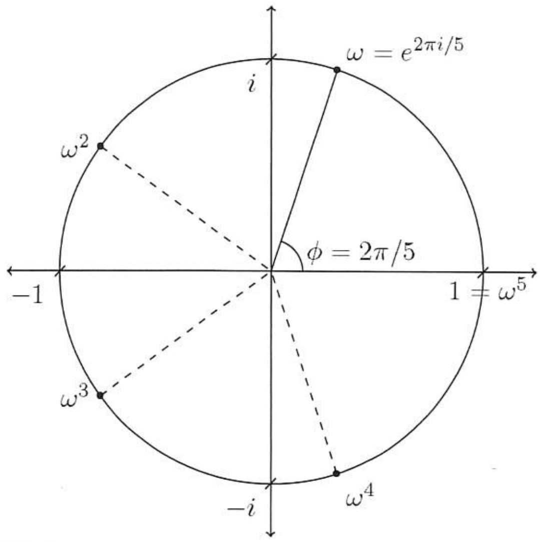
復習：單位根 (roots of unity)

(1)

$$\omega = \cos\theta + i\sin\theta = e^{i\theta}$$

$$\omega\overline{\omega} = 1$$

$$\omega^{-1} = \overline{\omega} = \cos\theta - i\sin\theta = e^{-i\theta}$$



(2) $x^N - 1 = 0$, $\quad x = e^{\frac{2\pi i}{N}k}$, $\quad 0 \le k \le N-1$

$\qquad = \omega_N^k$

(3) $x^5 - 1 = 0$

$(x-1)(x^4 + x^3 + x^2 + x + 1) = 0$

$x = 1, \omega, \omega^2, \omega^3, \omega^4$. $\quad \omega = e^{\frac{2\pi}{5}i}$

(i) $\alpha^5 = 1$, $\quad \alpha = 1, \omega, \omega^2, \omega^3, \omega^4$

(ii) $\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1 = 0$, $\quad \alpha = \omega, \omega^2, \omega^3, \omega^4$

(4) $x^{12} - 1 = 0$, $\quad x = \omega_{12}^k$, $\quad 0 \le k \le N-1$

(i) $\alpha^{12} = 1$, $\quad \alpha = 1, \omega, \omega^2, \cdots, \omega^{11}$

(ii) $1 + \alpha + \alpha^2 + \cdots + \alpha^{11} = 0$, $\quad \alpha = \omega, \omega^2, \cdots, \omega^{11}$

(iii) $1 + \omega^2 + \omega^4 + \omega^6 + \omega^8 + \omega^{10} = 0$

$(1 + \omega_6 + \omega_6^2 + \omega_6^3 + \omega_6^4 + \omega_6^5 = 0)$

$1 + \omega^3 + \omega^6 + \omega^9 = 0$

$(1 + \omega_4 + \omega_4^2 + \omega_4^3 = 0)$

Quantum Fourier Transform

No.
Date:

$$\mathbb{C}^N \longrightarrow \mathbb{C}^N$$

$$\mathrm{QFT}_N = \frac{1}{\sqrt{N}}\begin{array}{c} \begin{array}{cccccc} & & j\downarrow & & & \end{array} \\ \begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \cdots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \cdots & \omega^{2(N-1)} \\ 1 & \omega^3 & \omega^6 & \omega^9 & \cdots & \omega^{3(N-1)} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \omega^{3(N-1)} & \cdots & \omega^{(N-1)(N-1)} \end{bmatrix}\end{array} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{N-1} \end{bmatrix} \longmapsto \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ \vdots \\ c_{N-1} \end{bmatrix} \begin{array}{c} |0\rangle \\ |1\rangle \\ |2\rangle \\ \vdots \\ |N-1\rangle \end{array}$$

$$\sum_{k=0}^{N-1} a_k |k\rangle \longrightarrow \sum_{k=0}^{N-1} c_k |k\rangle$$

(1) $\mathrm{QFT}_N = \frac{1}{\sqrt{N}}\left[\omega^{kj}\right]_{0\le k, j \le N-1}, \quad \omega = e^{\frac{2\pi}{N}i}$

(2) $c_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \omega^{kj} a_j$

(3) $|j\rangle \longrightarrow \frac{1}{\sqrt{N}}\begin{bmatrix} 1 \\ \omega^j \\ \omega^{2j} \\ \vdots \\ \omega^{(N-1)j}\end{bmatrix}\begin{array}{c} |0\rangle \\ |1\rangle \\ |2\rangle \\ \vdots \\ |N-1\rangle \end{array} = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \omega^{kj}|k\rangle$

$N=2^n$ ⇓ 2進位

$$|j_{n-1},\cdots,j_0\rangle \xrightarrow{\mathrm{QFT}} \frac{1}{\sqrt{2^n}} \sum_{k_{n-1}\cdots k_0 \in \mathbb{B}^n} e^{\frac{2\pi i}{2^n}(k_{n-1}2^{n-1}+k_{n-2}2^{n-2}+\cdots+k_1 2+k_0)(j_{n-1}2^{n-1}+j_{n-2}2^{n-2}+\cdots+j_1 2+j_0)} \underbrace{}_{}|k_{n-1}\cdots k_0\rangle$$

$$\left(e^{2\pi i k}=1\right) \quad = \frac{1}{\sqrt{2^n}}\sum_{k_{n-1}=0}^{1}\cdots\sum_{k_0=0}^{1} e^{2\pi i k_{n-1}\frac{j_0}{2}}\cdot e^{2\pi i k_{n-2}\left(\frac{j_1}{2}+\frac{j_0}{2^2}\right)}\cdots e^{2\pi i k_0\left(\frac{j_{n-1}}{2}+\frac{j_{n-2}}{2^2}+\cdots+\frac{j_0}{2^n}\right)} |k_{n-1}\rangle\otimes\cdots\otimes|k_0\rangle$$

$$= \frac{1}{\sqrt{2^n}}\sum_{k_{n-1}=0}^{1} e^{2\pi i k_{n-1}\frac{j_0}{2}}|k_{n-1}\rangle \otimes \sum_{k_{n-2}=0}^{1} e^{2\pi i k_{n-2}\left(\frac{j_1}{2}+\frac{j_0}{2^2}\right)}|k_{n-2}\rangle\otimes\cdots$$
$$\otimes \sum_{k_0=0}^{1} e^{2\pi i k_0\left(\frac{j_{n-1}}{2}+\frac{j_{n-2}}{2^2}+\cdots+\frac{j_0}{2^n}\right)}|k_0\rangle$$

$$= \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i \overbrace{\frac{j_0}{2}}^{0.j_0}}|1\rangle\right)\otimes\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\overbrace{\left(\frac{j_1}{2}+\frac{j_0}{2^2}\right)}^{0.j_1j_0}}|1\rangle\right)\otimes\cdots$$
$$\otimes\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\overbrace{\left(\frac{j_{n-1}}{2}+\frac{j_{n-2}}{2^2}+\cdots+\frac{j_0}{2^n}\right)}^{0.j_{n-1}\cdots j_0}}|1\rangle\right)$$

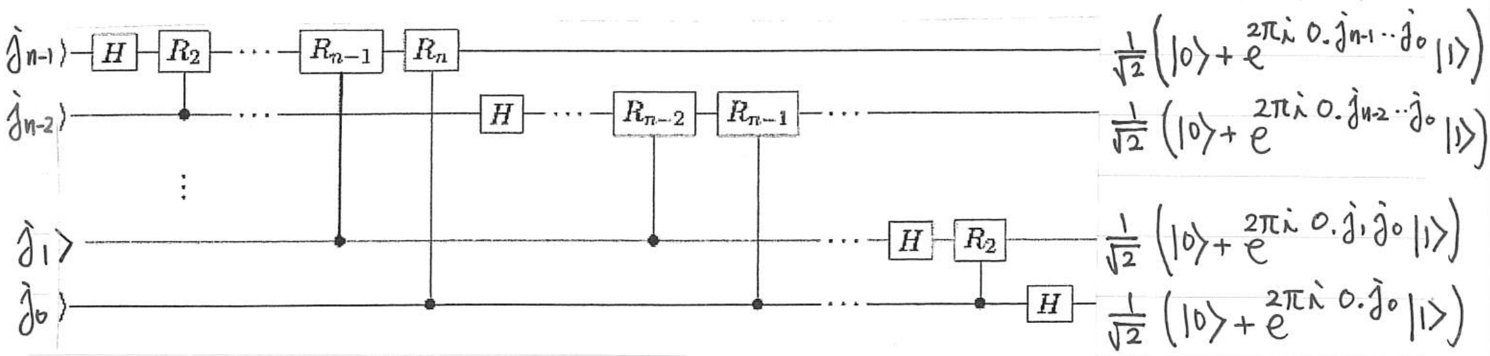
$$= \frac{1}{\sqrt{2}}\left(|0\rangle+(-1)^{j_0}|1\rangle\right)\otimes\frac{1}{\sqrt{2}}\left(|0\rangle+(-1)^{j_1}e^{2\pi i\frac{j_0}{2^2}}|1\rangle\right)\otimes\cdots$$
$$\otimes\frac{1}{\sqrt{2}}\left(|0\rangle+(-1)^{j_{n-1}}e^{2\pi i\left(\frac{j_{n-2}}{2^2}+\cdots+\frac{j_0}{2^n}\right)}|1\rangle\right)$$

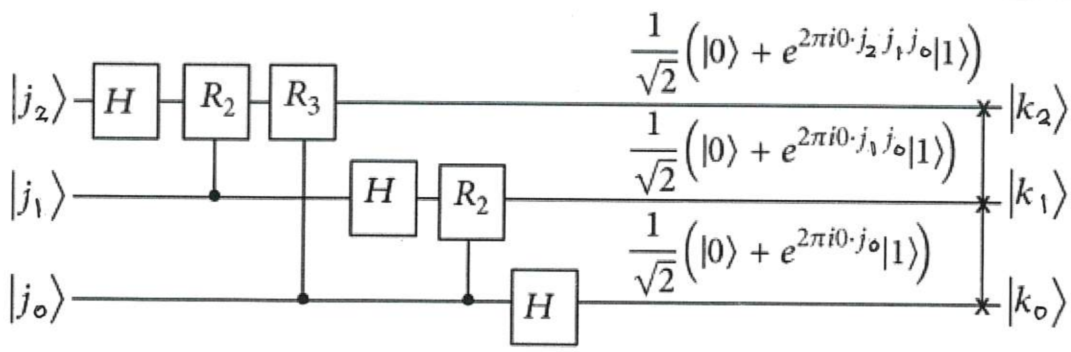
Quantumn Circuit

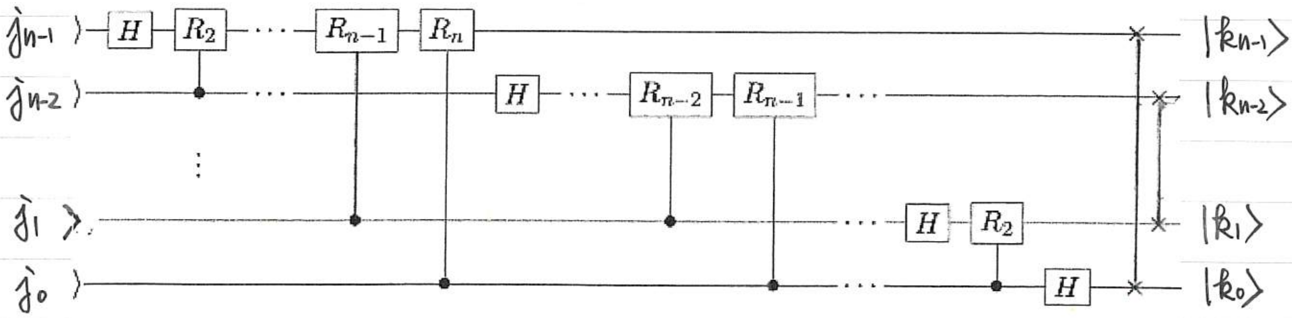
Phase shift $R_\theta = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix}$ $\begin{cases} |0\rangle \rightarrow |0\rangle \\ |1\rangle \rightarrow e^{i\theta}|1\rangle \end{cases}$

No.
Date: / /

$R_n = R_{\frac{2\pi}{2^n}}$







$\overline{\omega} = \omega^{-1}$

$\omega = e^{\frac{2\pi}{5} i}$

$$QFT_5 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 \\ 1 & \omega^2 & \omega^4 & \omega^6 & \omega^8 \\ 1 & \omega^3 & \omega^6 & \omega^9 & \omega^{12} \\ 1 & \omega^4 & \omega^8 & \omega^{12} & \omega^{16} \end{bmatrix}_{5\times 5}$$

QFT 性質：

(1) QFT : unitary

$QFT^{-1} = QFT^* = [\overline{\omega}^{jk}] = [\omega^{-jk}]$

pf : $F_j^* F_k \overset{N=5}{=\!=} \frac{1}{\sqrt{5}} [1 \ \omega^{-j} \ \omega^{-2j} \ \omega^{-3j} \ \omega^{-4j}] \frac{1}{\sqrt{5}} \begin{bmatrix} 1 \\ \omega^k \\ \omega^{2k} \\ \omega^{3k} \\ \omega^{4k} \end{bmatrix}$

$$= \begin{cases} 1 & j=k \\ \frac{1}{5}\left(1+\omega^3+\omega^6+\omega^9+\omega^{12}\right) = 0 & j=1,\ k=4 \end{cases}$$

(2) Linear shift

$N=4$

$\omega^4 = 1$

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 \\ 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega^9 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix} = \begin{bmatrix} a+b+c+d \\ a+\omega b+\omega^2 c+\omega^3 d \\ a+\omega^2 b+\omega^4 c+\omega^6 d \\ a+\omega^3 b+\omega^6 c+\omega^9 d \end{bmatrix} = \begin{bmatrix} a' \\ b' \\ c' \\ d' \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 \\ 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega^9 \end{bmatrix} \begin{bmatrix} d \\ a \\ b \\ c \end{bmatrix} = \begin{bmatrix} d+a+b+c \\ d+\omega a+\omega^2 b+\omega^3 c \\ d+\omega^2 a+\omega^4 b+\omega^6 c \\ d+\omega^3 a+\omega^6 b+\omega^9 c \end{bmatrix} = \begin{bmatrix} a' \\ \omega b' \\ \omega^2 c' \\ \omega^3 d' \end{bmatrix}$$

$$\begin{bmatrix} \ \end{bmatrix} \begin{bmatrix} c \\ d \\ a \\ b \end{bmatrix} = \begin{bmatrix} c+d+a+b \\ c+\omega d+\omega^2 a+\omega^3 b \\ c+\omega^2 d+\omega^4 a+\omega^6 b \\ c+\omega^3 d+\omega^6 a+\omega^9 b \end{bmatrix} = \begin{bmatrix} a' \\ \omega^2 b' \\ \omega^4 b' \\ \omega^6 c' \end{bmatrix}$$

No.
Date: / /

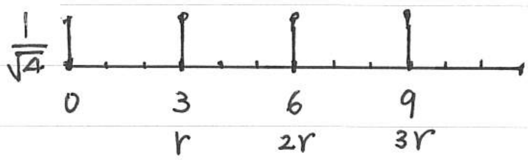
(3) Period / Wavelength

$$\frac{1}{\sqrt{N/r}}\left(|0\rangle+|r\rangle+|2r\rangle+\cdots+|(\tfrac{N}{r}-1)r\rangle\right) \xrightarrow{QFT_N} \frac{1}{\sqrt{r}}\left(|0\rangle+|\tfrac{N}{r}\rangle+|2\tfrac{N}{r}\rangle+\cdots+|(r-1)\tfrac{N}{r}\rangle\right)$$

$\begin{cases} \text{period} = r \\ \frac{N}{r} \text{ copies} \end{cases}$ period $= \frac{N}{r}$, r copies

例 $N=12$, $\begin{cases} r = 3 \\ N/r = 4 \end{cases}$

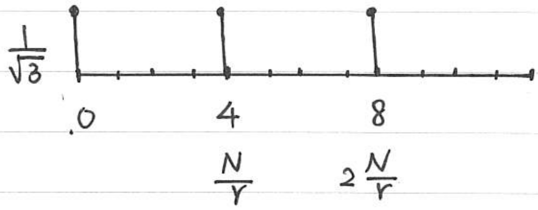
- $\frac{1}{\sqrt{4}}\left(|0\rangle+|3\rangle+|6\rangle+|9\rangle\right)$



($\frac{N}{r}$ copies)

$\downarrow QFT_{12}$

$\frac{1}{\sqrt{3}}\left(|0\rangle+|4\rangle+|8\rangle\right)$



(r copies)

$$\begin{array}{c} \quad 0 \qquad\qquad\quad 3 \quad 6 \quad 9 \\ \downarrow \qquad\qquad\quad \downarrow \quad \downarrow \quad \downarrow \end{array}$$

$$\frac{1}{\sqrt{12}}\begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & w & w^2 & w^3 & & w^{11} \\ 1 & w^2 & w^4 & w^6 & & w^{22} \\ 1 & w^3 & w^6 & w^9 & & w^{33} \\ 1 & w^4 & w^8 & w^{12} & & w^{41} \\ \vdots & & & & & \\ 1 & w^{11} & w^{22} & w^{33} & \cdots & w^{121} \end{bmatrix} \frac{1}{\sqrt{4}}\begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{12}\sqrt{4}}\begin{bmatrix} 1+1+1+1 \\ 1+w^3+w^6+w^9 \\ 1+w^{2\cdot3}+w^{2\cdot6}+w^{2\cdot9} \\ 1+w^{3\cdot3}+w^{3\cdot6}+w^{3\cdot9} \\ 1+w^{4\cdot3}+w^{4\cdot6}+w^{4\cdot9} \\ 1+w^{5\cdot3}+w^{5\cdot6}+w^{5\cdot9} \\ \\ \\ 1+w^{8\cdot3}+w^{8\cdot6}+w^{8\cdot9} \\ \\ \\ \\ \end{bmatrix} = \frac{1}{\sqrt{3}}\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

$$w^{k\cdot0}+w^{k\cdot3}+w^{k\cdot6}+w^{k\cdot9} \qquad k = 4j,\ 4j+1,\ 4j+2,\ 4j+3$$

- $\frac{1}{\sqrt{4}}\left(|1\rangle+|4\rangle+|7\rangle+|10\rangle\right)$

$\longrightarrow \frac{1}{\sqrt{3}}\left(|0\rangle+w^4|4\rangle+w^8|8\rangle\right)$