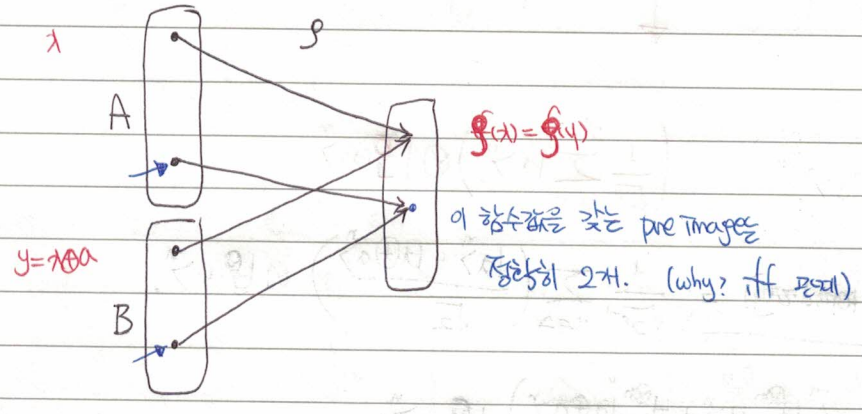
Simon's algorithm

Problem def

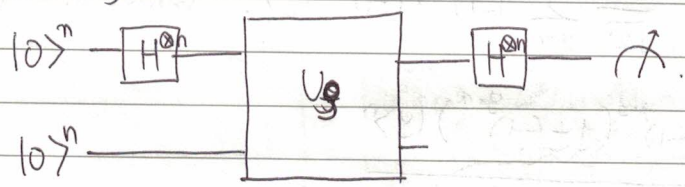
- a function $f : \{0,1\}^n \to \{0,1\}^n$ is $(\mathbb{Z}_2)^n$-periodic if $\exists\, a \neq 0$ s.t. (a called the period)

$$f(x) = f(y) \iff y = x \oplus a$$



- Given a $(\mathbb{Z}_2)^n$-periodic func f, find its period a
(Classically, need $\Omega(2^n)$ func calls.)

Simon's alg

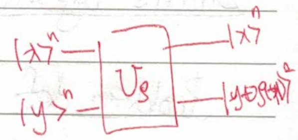


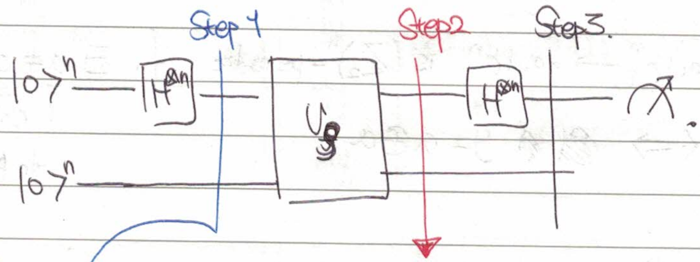
Recap of Hadamard's gate

$$|x\rangle \xrightarrow{H} \begin{cases} \frac{|0\rangle+|1\rangle}{\sqrt{2}} & \text{if } x=0 \\ \frac{|0\rangle-|1\rangle}{\sqrt{2}} & \text{if } x=1 \end{cases} \Rightarrow \frac{|0\rangle+(-1)^x|1\rangle}{\sqrt{2}} \Rightarrow \frac{1}{\sqrt{2}}\sum_{y=0}^{1}(-1)^{x\cdot y}|y\rangle.$$

$$\left.\begin{aligned} |x_1\rangle &\xrightarrow{H} \frac{1}{\sqrt{2}}\sum_{y_1=0}^{1}(-1)^{x_1\cdot y_1}|y_1\rangle \\ |x_0\rangle &\xrightarrow{H} \frac{1}{\sqrt{2}}\sum_{y_0=0}^{1}(-1)^{x_0\cdot y_0}|y_0\rangle \end{aligned}\right\} \frac{1}{\sqrt{2^2}}\sum_{y=0}^{3}(-1)^{x\cdot y}|y\rangle.$$

$$\Rightarrow H^{\otimes n}|x\rangle^n = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} (-1)^{x\cdot y} |y\rangle^n.$$





$$\left(\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle^n\right) \otimes |0\rangle^n.$$

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

$$\text{(by periodicity)} = \frac{1}{\sqrt{2^{n-1}}} \sum_{x\in A} \left(\frac{|x\rangle^n + |x\oplus a\rangle^n}{\sqrt{2}}\right) \otimes |f(x)\rangle^n.$$

Step 3: $\displaystyle \frac{1}{\sqrt{2^{n-1}}} \sum_{x\in A} \left(\frac{\text{"}H^{\otimes n}\text{"}|x\rangle^n + \text{"}H^{\otimes n}\text{"}|x\oplus a\rangle^n}{\sqrt{2}}\right) |f(x)\rangle^n.$

$(x_1\oplus a_1)\cdot y_1$

Note: $\displaystyle H^{\otimes n}|x\oplus a\rangle^n = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} (-1)^{(x\oplus a)\cdot y} |y\rangle^n$

$$= \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} (-1)^{x\cdot y}\cdot(-1)^{y\cdot a} |y\rangle^n. \quad (\text{since } (-1)^{(x\oplus a)\cdot y} = (-1)^{(x+a)\cdot y}).$$

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

If $y\cdot a = 0 \pmod 2$ → 2 (Σ 하나씩 남음), o/w, 0

$$\frac{1}{\sqrt{2^{n-1}}} \sum_{x\in A} \frac{1}{\sqrt{2^{n-1}}} \sum_{y\cdot a=0 \,(\mathrm{mod}\, 2)} (-1)^{x\cdot y} |y\rangle^n.$$

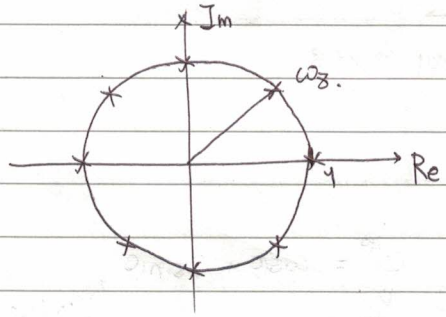
⇒ measure를 하면 a와 orthogonal 한 y만 얻음!

⇒ 이 quantum circuit을 ~~[illegible]~~ n+T 번 수행하면 whp lin indep, orthogonal to a인 것을 n-1개 얻을 수 있음. 그러면 마지막 a를 특정할 수 있음.

in poly(n) time!

Discrete Fourier transform

Nth Roots of Unity $\omega_N := e^{\frac{2\pi i}{N}}$.



- $\omega_N^N = 1$.

DFT: $\mathbb{C}^N \to \mathbb{C}^N$ s.t.

$$\frac{1}{\sqrt{N}} \begin{bmatrix} 1 & 1 & 1 \cdots & 1 \\ 1 & \omega & \omega^2 & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \omega^{2(N-1)} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \omega^{(N-1)(N-1)} \end{bmatrix}$$

- Normally, ω^{-jk}...

Given $f \in \mathbb{C}^N$,

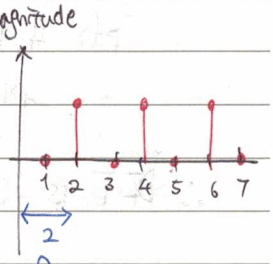
$$\hat{f}_j := \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} f_k \cdot \omega^{jk} \quad \text{for } j = 0, \cdots, N-1.$$

Examples $N=8$

$$\begin{bmatrix} & & & & & & & \\ & & & & & & & \\ & & & & & & & \\ & & & & & & & \\ & & & & & & & \\ & & & & & & & \\ & & & & & & & \\ & & & & & & & \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \omega^3 + \omega^7 = \omega^3(1+\omega^4) = 0 \\ \omega^6 + \omega^{14} = \omega^6(1+\omega^8) = 2\omega^6 = -2i \\ 0 \\ 2i \\ 0 \\ -2i \\ 0 \end{bmatrix}$$

$= \omega^9 + \omega^{21} = \omega^9(1+\omega^{12})$

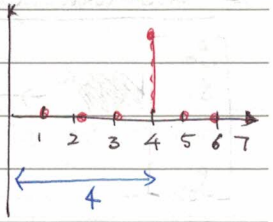
↳ period = 4



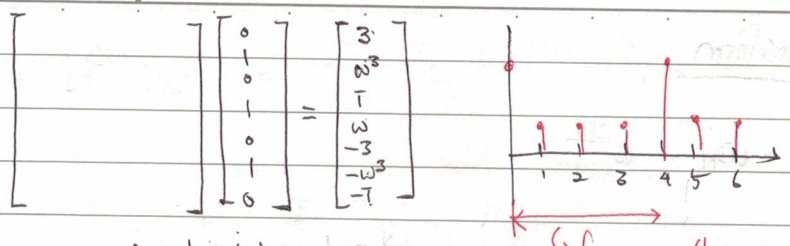
frequency = 2.

$$\begin{bmatrix} & & & & & & & \\ & & & & & & & \\ & & & & & & & \\ & & & & & & & \\ & & & & & & & \\ & & & & & & & \\ & & & & & & & \\ & & & & & & & \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \omega + \omega^3 + \omega^5 + \omega^7 = 0 \\ \omega^2 + \omega^6 + \omega^{10} + \omega^{14} = 0 \\ \omega^3 + \omega^9 + \omega^{15} + \omega^{21} = \omega^3 + \omega - \omega^3 - \omega = 0 \\ \omega^4 + \omega^{12} + \omega^{20} + \omega^{28} = -4. \\ \vdots \\ \vdots \\ \vdots \end{bmatrix}$$

↳ period = 2



frequency = 4



period: 지점 2

↳ frequency 4이내 존재.

Proposition. DFT is unitary!

$$DFT^{\dagger} = \frac{1}{\sqrt{N}} \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega^{-1} & & & \omega^{-(N-1)} \\ 1 & \omega^{-2} & & & \\ \vdots & \vdots & & & \\ 1 & \omega^{-(N-1)} & & & \omega^{-(N-1)(N-1)} \end{bmatrix}$$

Since $e^{i\theta} = \cos\theta + i\sin\theta$ ↔ $e^{-i\theta} = \cos\theta - i\sin\theta$ (conjugate)

then,

$$DFT^{\dagger} \cdot DFT = \frac{1}{N} \begin{bmatrix} 1 & \omega^{-j} & \omega^{-2j} & \cdots & \omega^{-j(N-1)} \end{bmatrix} \begin{bmatrix} 1 \\ \omega^{k} \\ \omega^{2k} \\ \vdots \\ \omega^{k(N-1)} \end{bmatrix} = I.$$

(k)

Claim: $\sum_{l=0}^{N-1} \omega^{(k-j)l} = \begin{cases} N & \text{if } k=j \pmod N \\ 0 & \text{if } k \neq j \pmod N \end{cases}$

pf) If $k=j$, easy to see. Otw, $\omega^{k-j} \neq 1$ is a N^{th} root of unity.

$$x^N - 1 = (x-1)(x^{N-1} + x^{N-2} + \cdots + x + 1) = 0.$$

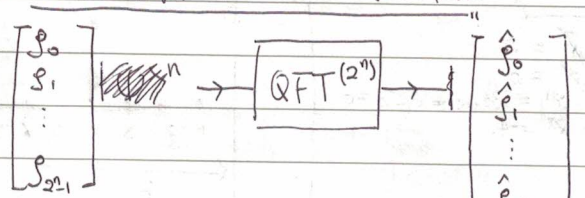
$=0$.

$\therefore$ DFT is unitary! □

$$|\psi\rangle^n = \sum_{x=0}^{2^n-1} f_x |x\rangle^n$$

$$QFT|\psi\rangle^n = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} f_x \cdot \omega^{xy} |y\rangle^n.$$

Quantum Fourier transform

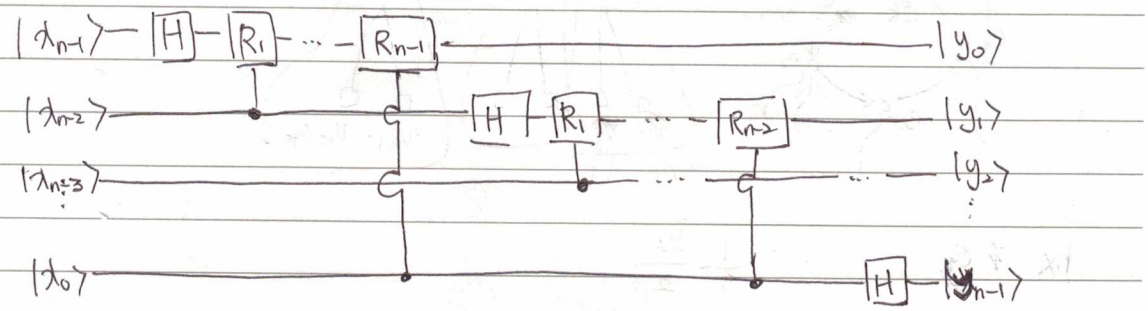


(If $|\psi\rangle^n = f_x$, $[QFT|\psi\rangle^n]_y = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} f_x \cdot \omega^{xy}$)

or equivalently, $QFT|x\rangle^n := \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} \omega^{xy} |y\rangle^n$. for $x \in \{0, \cdots, 2^n-1\}$.

"linearity" of

QFT circuit



where $R_k := \begin{bmatrix} 1 & 0 \\ 0 & \omega^{2^{n-k-1}} \end{bmatrix}$. $\Rightarrow$ $O(n^2)$ gates.

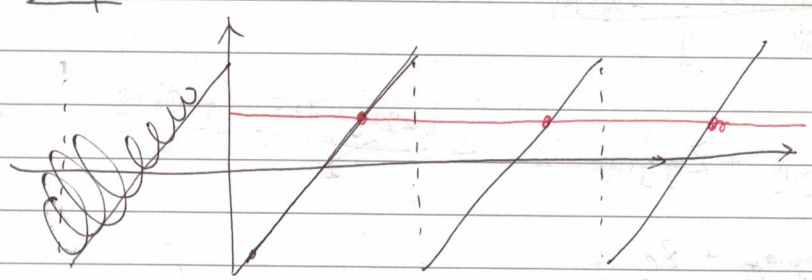
- Cannot directly compare DFT & QFT.

Shor's period finding.

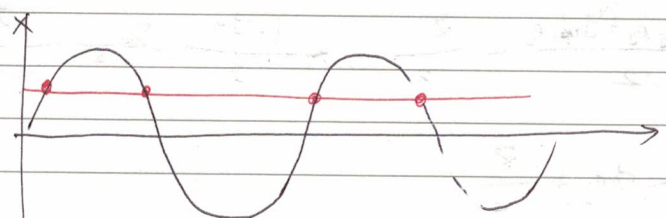
A function $f: \mathbb{Z}_M \to S$ (for $S \subseteq \mathbb{Z}_M$) is called periodic injective if $\exists\ a \in \mathbb{Z}_M$ (called the period) s.t. $\forall x \neq y$, we have

$f(x) = f(y)$ iff $y = x + ka$ for some int k.

Examples



periodic injective



periodic, not injective.

Problem def: Given a periodic injective f, find its period.

↳ alg: