Fourier Transform

$$F_N = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \dots & \omega^{(N-1)} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \dots & \omega^{2(N-1)} \\ \vdots & & & & & \\ 1 & \omega^{n-1} & \omega^{2(n-1)} & \dots & & \omega^{(N-1)(N-1)} \end{pmatrix}_{N \times N}$$

$$F_N = \begin{pmatrix} j \\ \hline \omega^{jk} \end{pmatrix} \quad k \text{ (index)} \quad \text{where } \omega = e^{2\pi i/N} \text{ and } \omega^N = 1$$

$$F_N = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \dots & \omega^{N-1} \\ \vdots & & & & \\ 1 & \omega^{n-1} & \dots & & \omega^{(N-1)^2} \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{n-1} \end{pmatrix} = \begin{pmatrix} \beta_0 \\ \beta_1 \\ \vdots \\ \beta_{n-1} \end{pmatrix}$$

$$O(N^2) \xrightarrow{\text{FFT}} O(N \log N)$$

↳ basis of digital signal processing

$n = \log N$

↳ • • • • •

n qubits

$$|j\rangle \xrightarrow{\text{QFT}} \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \omega^{jk} |k\rangle$$

QFT : $O(n^2)$ steps $= O(\log^2 N)$

↳ exponential speedup!

We get a quantum state over which we can perform sampling.

Fast Fourier Transform

Polynomial multiplication → naive $O(d^2)$ for multiplying 2 d-degree polys

$$A(x) = a_0 + a_1 x + \cdots + a_d x^d$$
$$B(x) = b_0 + b_1 x + \cdots + b_d x^d$$

Any polynomial of degree d can be represented using $(d+1)$ points

$$\{ (x_0, P(x_0)), \ldots, (x_d, P(x_d)) \}$$

$$P(x) = p_0 + p_1 x + p_2 x^2 + \cdots + p_d x^d$$

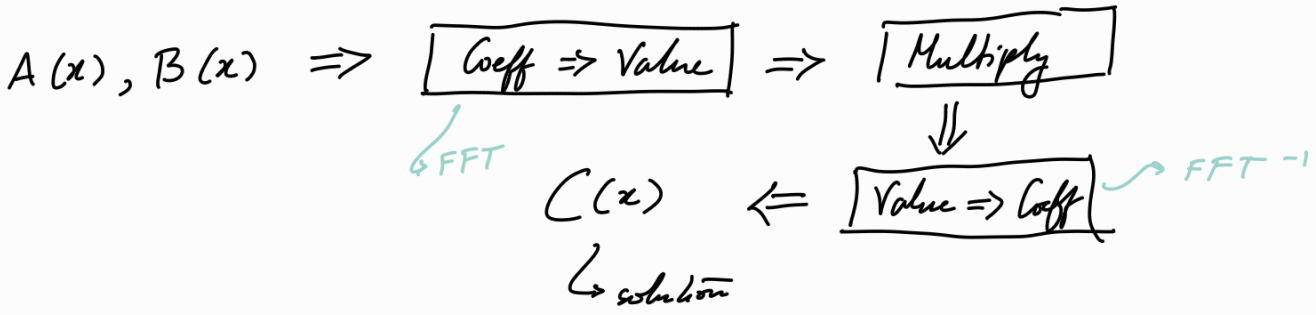
$$\begin{bmatrix} P(x_0) \\ P(x_1) \\ \vdots \\ P(x_d) \end{bmatrix} = \underbrace{\begin{bmatrix} 1 & x_0 & x_0^2 & \cdots & x_0^d \\ 1 & x_1 & x_1^2 & \cdots & x_1^d \\ \vdots & & & & \\ 1 & x_d & x_d^2 & \cdots & x_d^d \end{bmatrix}}_{M} \begin{bmatrix} p_0 \\ p_1 \\ \vdots \\ p_d \end{bmatrix}$$

M is invertible for unique $x_0, \ldots, x_d$

Two representations → coefficient and value representation

$A(x)$	$B(x)$	$C(x) = A(x) \cdot B(x)$ (has degree d)
$[(x_0, A(x_0)), \ldots]$	$[(x_0, B(x_0)), \ldots]$	$[(x_0, A(x_0) B(x_0)), \ldots]$
↓	↓	↓
$(d+1)$-points	$(d+1)$-points	$(d+1)$-points

$O(d)$ → current time complexity



Evaluation

$P(x) = P(-x)$ → even

$P(-x) = -P(x)$ → odd

$$\boxed{P(x) = P_e(x^2) + x\,P_o(x^2)}$$

$P(x)$: $[p_0, p_1, \cdots, p_{n-1}]$

$[\pm x_1, \pm x_2, \cdots, \pm x_{n/2}]$

$P(x) = P_e(x^2) + x\,P_o(x^2)$

$P_e(x^2)$: $[p_0, p_2, \cdots]$

$[x_1^2, x_2^2, \cdots, x_{n/2}^2]$

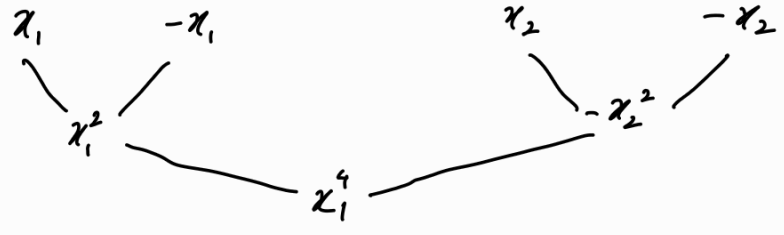
$P_o(x^2)$: $[p_1, p_3, \cdots]$

$[x_1^2, x_2^2, \cdots, x_{n/2}^2]$

Is it possible to make $[x_1^2, x_2^2, \cdots, x_{n/2}^2]$ ± paired?

Example

$$P(x) = x^3 + x^2 - x - 1$$



Here,

$x_1 = 1$,

$x_2 = i$

We basically solved the equation $x_1^4 = 1$

roots $1, i, -i, -1$

Also suppose you need $n = 6$ points $\longrightarrow$ make $n = 8$ (nearest power of 2)

Evaluate $P(x)$ at $[1, \omega, \omega^2, \ldots, \omega^{n-1}]$, $\omega = e^{2\pi i/n}$

$\Rightarrow$ Eval $P_e(x^2)$ and $P_o(x^2)$ at

$$[1, \omega^2, \omega^4, \ldots, \omega^{n-2}]$$

FFT : $P(x)$, $\omega = e^{2\pi i/N}$: $[\omega^0, \ldots, \omega^{n-1}]$

FFT : $P_e(x^2)$, $[\omega^0, \omega^2, \ldots, \omega^{n-2}]$

$y_e = [P_e(\omega^0), P_e(\omega^2), \ldots]$

FFT : $P_o(x^2)$, $[\omega^0, \omega^2, \ldots]$

$y_o = [P_o(\omega^0), \ldots]$

$$P(\omega^j) = y_e[j] + \omega^j y_o[j]$$

$$P(\omega^{j+n/2}) = y_e[j] - \omega^j y_o[j]$$

$$y = [P(\omega^0), P(\omega^1), \ldots, P(\omega^{n-1})]$$

Interpolation

$$\begin{bmatrix} P(\omega^0) \\ P(\omega^1) \\ \vdots \\ P(\omega^{n-1}) \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{n-1} \\ & & \ddots & & \end{bmatrix} \begin{bmatrix} p_0 \\ p_1 \\ \vdots \\ p_{n-1} \end{bmatrix}$$

$$FFT^{-1} = \frac{1}{n}\begin{bmatrix} 1 & 1 & 1 & 1 \cdots & 1 \\ 1 & \omega^{-1} & \omega^{-2} & \cdots & \omega^{-(n-1)} \\ & & \ddots & & \end{bmatrix}$$

$O(n \log n) \rightarrow$ Time Complexity

```
def FFT(P):
    # P = [p_0, p_1, ..., p_{n-1}]
    n = len(P)        # n = 2^k for some k
    if n == 1:
        return P
    ω = e^(2πi/n)
    P_e, P_o = P[0::2], P[1::2]
    y_e, y_o = FFT(P_e), FFT(P_o)
    y = [0] * n
    for j in range(n/2):
        y[j] = y_e[j] + ω^j y_o[j]
        y[j+n/2] = y_e[j] - ω^j y_o[j]
    return y
```

Properties of QFT

$$QFT = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{N-1} \\ \vdots & \vdots & \vdots & & \vdots \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \vdots \\ \alpha_{N-1} \end{pmatrix}$$

$$= \begin{pmatrix} \beta_0 \\ \beta_1 \\ \vdots \\ \beta_N \end{pmatrix}$$

$$F_N \left(\sum_j \alpha_j |j\rangle \right) = \sum_k \beta_k |k\rangle$$

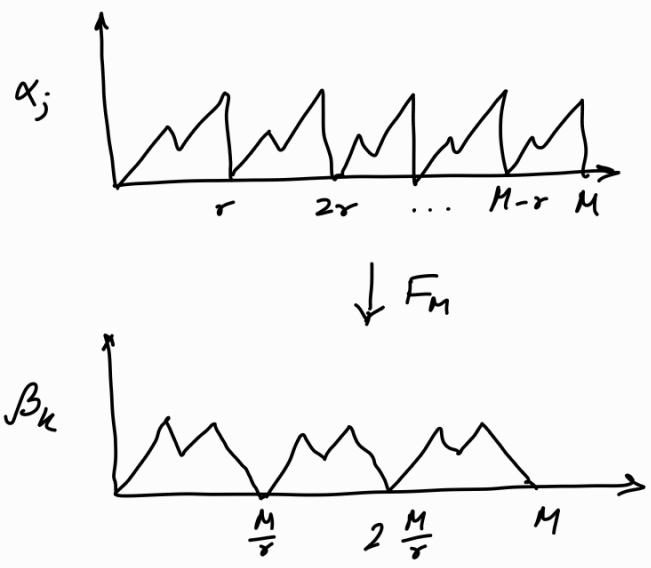
① Shift invariance

$$\frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & \cdots \\ 1 & \omega & \cdots \\ & \ddots & \end{pmatrix} \begin{pmatrix} \alpha_{N-1} \\ \alpha_0 \\ \vdots \\ \alpha_{N-2} \end{pmatrix} = \begin{pmatrix} 1 & \beta_0 \\ \omega & \beta_1 \\ & \vdots \\ \omega^{N-1} & \beta_{N-1} \end{pmatrix}$$

Doing a cyclic shift in the input doesn't change the output distribution.

Convolution - multiplication property of the Fourier Transform

② Periodicity is preserved



$$F_M \left(\sum_{j=0}^{M-1} \alpha_j |j\rangle \right)$$

$$= \sum_{k=0}^{M-1} \beta_k |k\rangle$$

Thus, if $\alpha_{j+r} = \alpha_j$

$\Rightarrow \beta_{k+\frac{M}{r}} = \beta_k$

Properties of QFT

Def: $|j\rangle \xrightarrow{QFT} \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \omega^{jk} |k\rangle$

① $\sum_j \alpha_j |j+s\rangle \xrightarrow{QFT} \sum_k \omega^{sk} \beta_k |k\rangle$

② $|\psi\rangle = \frac{1}{\sqrt{A}} \sum_{k=0}^{A-1} |kr\rangle$ (assume $r|N$, $A = \frac{N}{r}$)

$\downarrow$ QFT

$$\frac{1}{\sqrt{A}} \sum_{k=0}^{A-1} \frac{1}{\sqrt{N}} \sum_{l=0}^{N-1} \omega^{krl} |l\rangle$$

$$= \frac{1}{\sqrt{NA}} \sum_{k=0}^{A-1} \sum_{l=0}^{N-1} \omega^{krl} |l\rangle = \sum_{l=0}^{N-1} \alpha_l |l\rangle$$

where, $\alpha_l = \frac{1}{\sqrt{NA}} \sum_{k=0}^{A-1} (\omega^{rl})^k = \begin{cases} \sqrt{A/N} & \text{if } rl = 1 \\ \frac{1}{\sqrt{NA}} \frac{1-\omega^{rlA}}{1-\omega^{rl}} \end{cases}$

We know that $A = \frac{N}{r}$, what is the amplitude when $l = j\frac{N}{r}$?

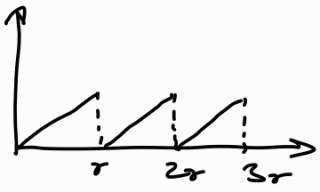
$$\sqrt{\frac{r}{N}} \sum_{k=0}^{N/r-1} |kr\rangle \xrightarrow{QFT} \sqrt{\frac{1}{r}} \sum_{j=0}^{r-1} |j\tfrac{N}{r}\rangle$$

Period Finding

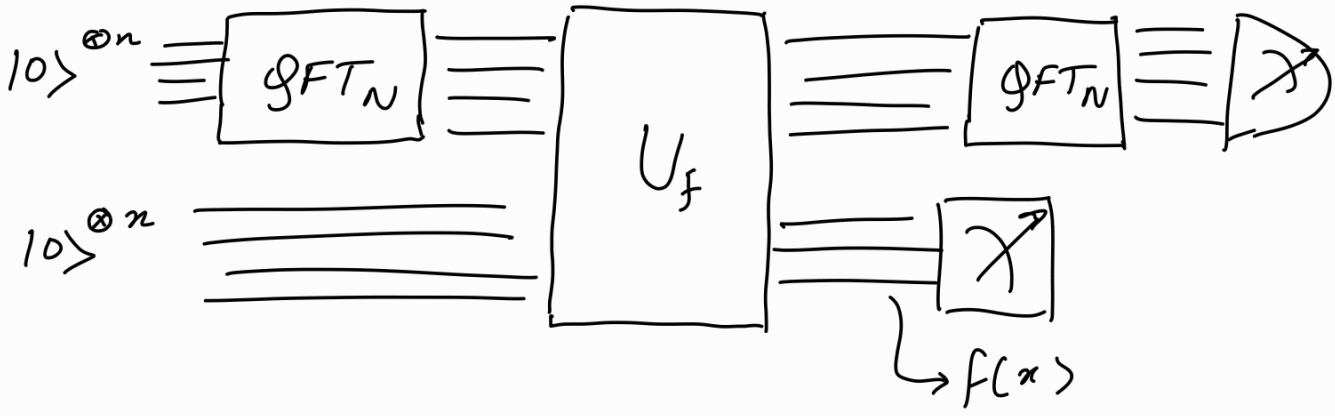
$f: \{0, 1, \ldots, N-1\} \to S$

f is periodic with period r/N

$f(x) = f((x + r) \bmod N)$



Given a black box C_f, determine r.



$$|0\rangle^{\otimes n}\,|0\rangle^{\otimes n} \xrightarrow{QFT_N \otimes I} \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} |k\rangle\,|0\rangle^{\otimes n}$$

$$= \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} |k\rangle\,|f(k)\rangle$$

$|f(k)\rangle$ ↓ measured

$$\frac{|k\rangle + |k+r\rangle + \ldots + |k+N-r\rangle}{\sqrt{\frac{r}{N}}}$$

$$\sqrt{\frac{r}{N}} \sum_{k=0}^{N/r-1} |jr + k\rangle \xrightarrow{QFT} \left| \frac{1}{\sqrt{r}} \sum_{\ell=0}^{r-1} |\ell \tfrac{N}{r} + k\rangle \right|$$

We get random multiples of $\frac{N}{r}$ times, repeat to get more random multiple and get GCD

↳ $\frac{N}{r}$ is obtained.

$\Rightarrow$ r we get since we know N

Shor's Algorithm

n bit number → Classical : $\exp(O(\sqrt{n}))$

→ Quantum : $O(n^3)$, $O(n^2)$ circuit complexity

① $x \neq \pm 1 \pmod N$ but $x^2 = 1 \pmod N$

$\Rightarrow N \mid (x+1)(x-1)$

but $N \nmid (x+1)$, $N \nmid (x-1)$

$\Rightarrow N = \underbrace{\gcd(x+1, N)}_{p} \underbrace{\gcd(x-1, N)}_{q}$

② $X \pmod N$

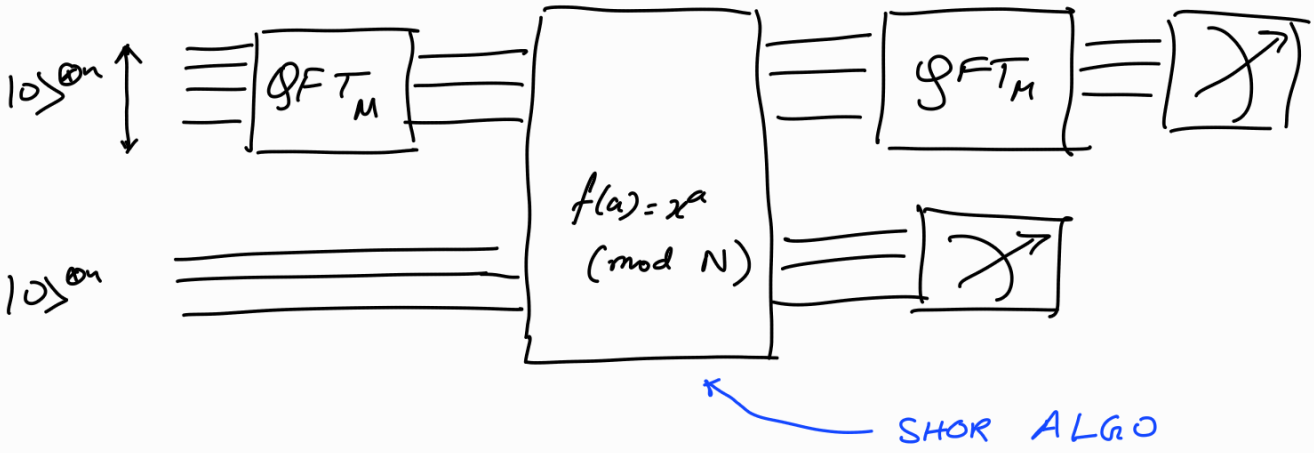
↳ $1 = x^r \pmod N$

here, r = order of x, r = even (with prob $1/2$) and $y = x^{r/2} \neq \pm 1 \pmod N$

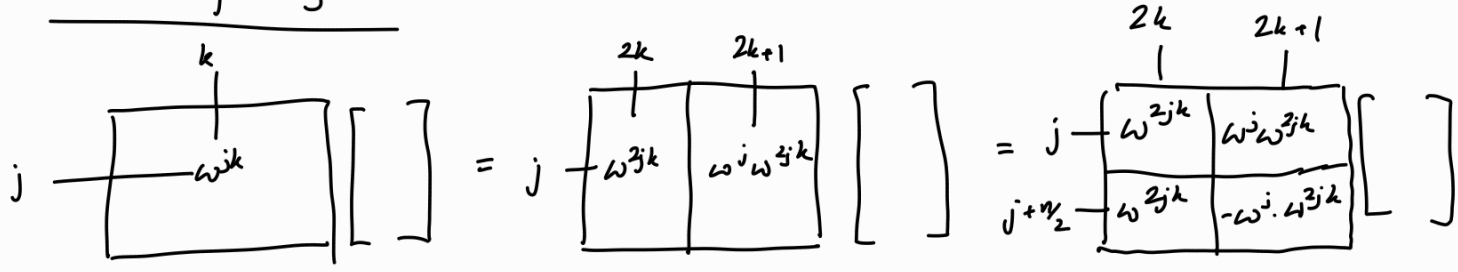
but $x^r = 1 \pmod N$

Finding order of x

order of x = period of $f(a) = x^a \pmod N$

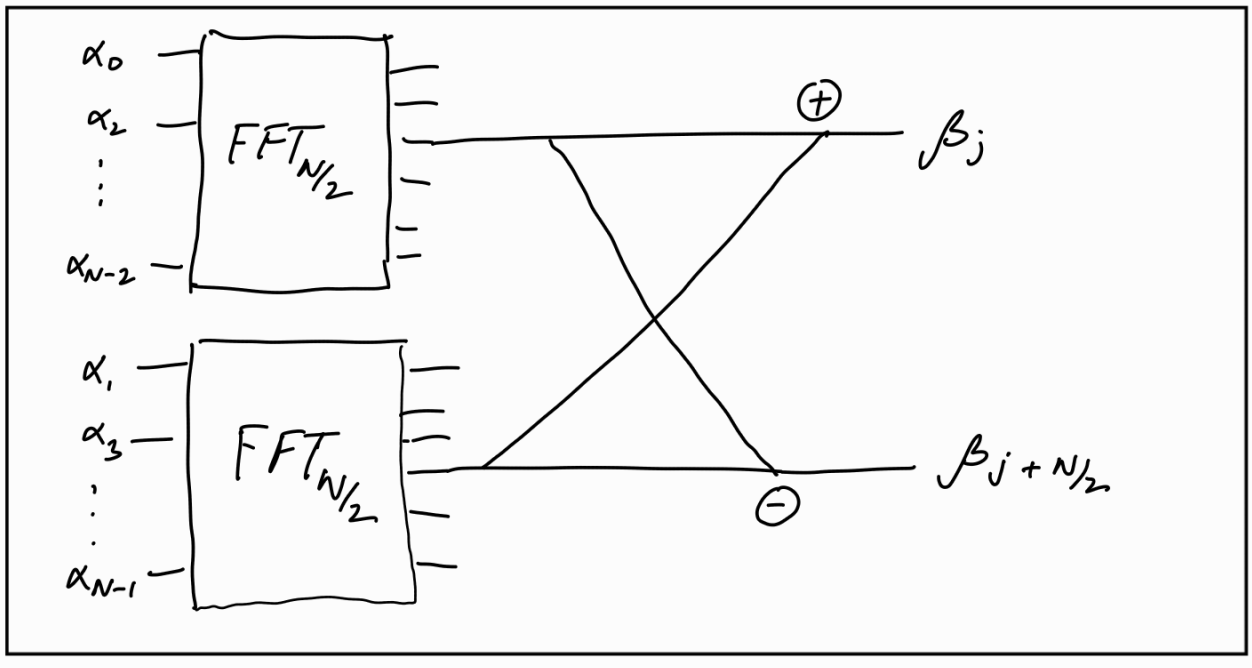


Circuit for QFT



$$F_N = \begin{array}{|c|c|} \hline F_{N/2} & \omega^j F_{N/2} \\ \hline F_{N/2} & -\omega^j F_{N/2} \\ \hline \end{array}$$

$$H_N = \begin{array}{|c|c|} \hline H_{N/2} & H_{N/2} \\ \hline H_{N/2} & -H_{N/2} \\ \hline \end{array}$$



FFT_N

Circuit for QFT

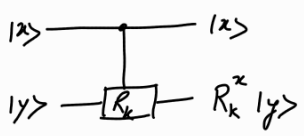
$$QFT(|j\rangle) = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \omega^{jk} |k\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{\frac{2\pi i jk}{2^n}} |k\rangle$$

$$j = j_1 j_2 \cdots j_n = j_1 2^{n-1} + j_2 2^{n-2} + \cdots + j_n 2^0$$

$$\frac{j}{2} = \frac{j_1 2^{n-1}}{2} + \frac{j_2 2^{n-2}}{2} + \cdots + \frac{j_n 2^0}{2}$$

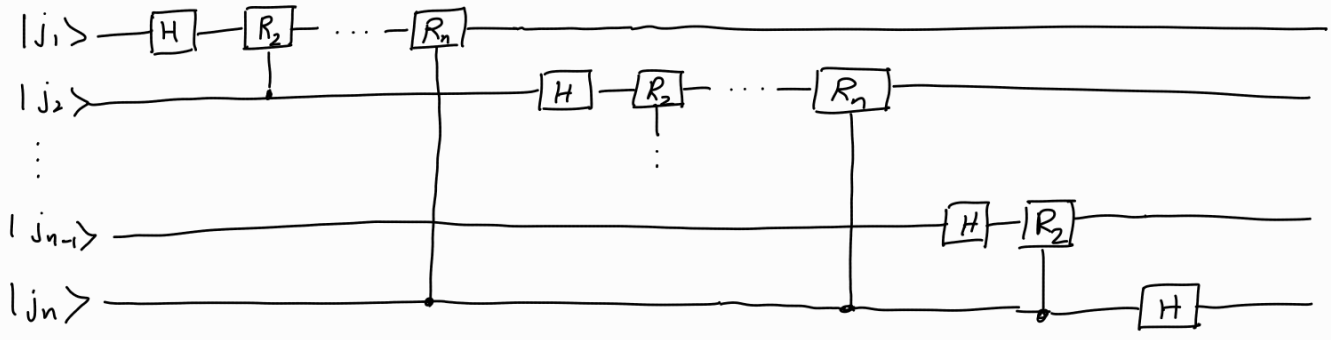
$$\Rightarrow e^{2i\pi j/2} = e^{2i\pi\, 0.j_n}$$

$$\Rightarrow e^{2i\pi j/2^n} = e^{2i\pi\, 0.j_1 j_2 j_3 \cdots j_n}$$



$$R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{i2\pi/2^k} \end{pmatrix}$$

$$C\text{-}R_k |1\rangle |z\rangle = e^{i 2\pi z/2^k} |z\rangle$$



↳ this circuit + $n/2$ swap gates (QFT)

Complexity: $O(n^2) = O(\log^2 N) \longrightarrow$ QFT

$O(n^3) = O(\log^3 N) \longrightarrow$ SHOR

$$|j\rangle \xrightarrow{QFT_n} \frac{1}{\sqrt{N}} \bigotimes_{l=1}^{n} \sum_{k_l=0}^{1} e^{i2\pi j k_l 2^{-l}} |k_l\rangle$$

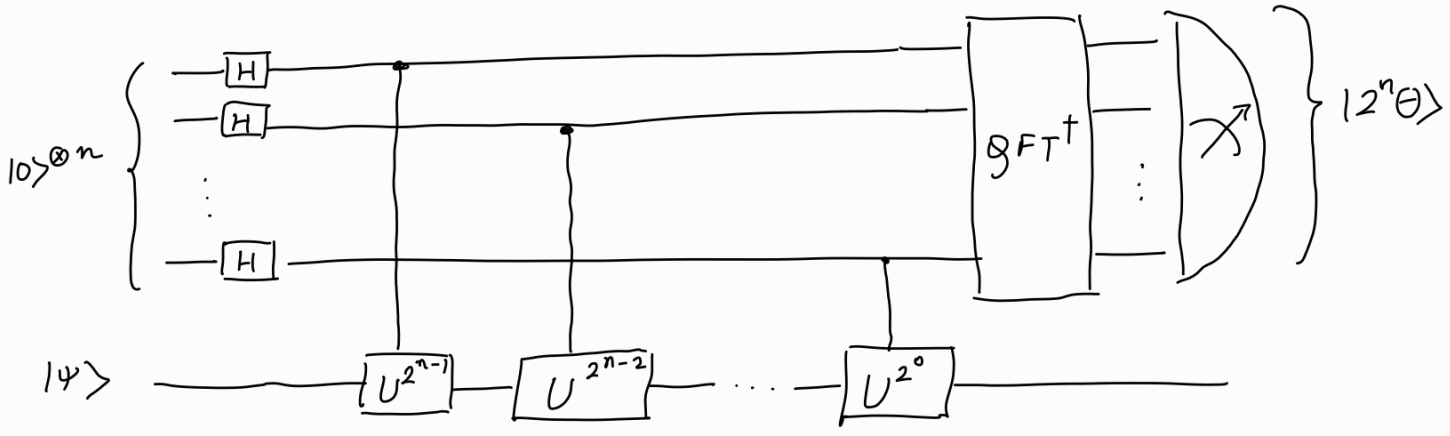
$$= \frac{1}{\sqrt{N}} \left[(|0\rangle + e^{i2\pi j/2} |1\rangle)(|0\rangle + e^{i2\pi j/2^2} |1\rangle) \cdots (|0\rangle + e^{i2\pi j/2^n} |1\rangle) \right]$$

$$= \frac{1}{\sqrt{N}} \left[(|0\rangle + e^{i2\pi\, 0.j_n} |1\rangle)(|0\rangle + e^{i2\pi\, 0.j_{n-1} j_n} |1\rangle) \cdots (|0\rangle + e^{i2\pi\, 0.j_1 j_2 \cdots j_n} |1\rangle) \right]$$

Quantum Phase Estimation

Given an unitary operator U, estimate θ such that

$$U = e^{2\pi i \theta} |\psi\rangle$$



Mathematical formulation lies as follows:

$$|\psi_0\rangle = |0\rangle^{\otimes n} |\psi\rangle$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2^n}} (|0\rangle + |1\rangle)^{\otimes n} |\psi\rangle$$

$$|\psi_2\rangle = \frac{}{\sqrt{2^n}} (|0\rangle + e^{2i\pi 2^{n-1}\theta} |1\rangle)$$
$$(|0\rangle + e^{2i\pi 2^{n-2}\theta} |1\rangle) \dots (|0\rangle + e^{2i\pi 2^0 \theta} |1\rangle)$$

$$= \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i \theta k} |k\rangle \otimes |\psi\rangle$$

where k denotes the integer representation of n-bit binary numbers.

$$QFT^\dagger \left(\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i \theta k} |k\rangle \right) \otimes |\psi\rangle$$

$$= \frac{1}{2^n} \sum_{k=0}^{2^n-1} \sum_{x=0}^{2^n-1} e^{-\frac{2i\pi k}{2^n}(x - 2^n\theta)} |x\rangle \otimes |\psi\rangle$$

The above expression peaks near $x = 2^n\theta$ when $2^n\theta$ is an integer meaning in the computational basis gives the phase in auxiliary with a high probability.

$$|\psi_4\rangle = |2^n\theta\rangle \otimes |\psi\rangle$$

When $2^n\theta$ is not an integer, it can be shown that still the exp peaks near $2^n\theta = x$ with prob $> \frac{4}{\pi^2} \approx 40\%$.

$$2^n\theta = a + 2^n\delta$$

$$Pr(a) = \begin{cases} 1 \longrightarrow & \delta = 0 \\ \frac{1}{2^{2n}} \left| \sum_{k=0}^{2^n-1} e^{2\pi i \delta k} \right| = \frac{1}{2^{2n}} \left| \frac{1 - e^{2\pi i 2^n \delta}}{1 - e^{2\pi i \delta}} \right|^2 \longrightarrow & \delta \neq 0 \end{cases}$$

$$= \frac{1}{2^{2n}} \left| \frac{2\sin(\pi 2^n \delta)}{2\sin(\pi\delta)} \right|^2$$

$$> \frac{1}{2^{2n}} \left| \frac{\sin(\pi 2^n \delta)}{\pi\delta} \right|^2$$

$$> \frac{1}{2^{2n}} \left(\frac{2 \cdot 2^n \delta}{\pi\delta} \right)^2 = \frac{4}{\pi^2} \approx 40\%$$

Grover Search Algorithm

Given $f: \{0, 1, \ldots, N-1\} \longrightarrow \{0, 1\}$

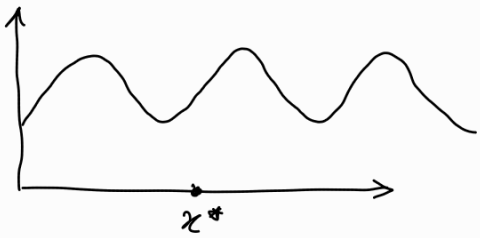
find x such that $f(x) = 1$

$\exists$ exactly one x s.t. $f(x) = 1$ → hardest case

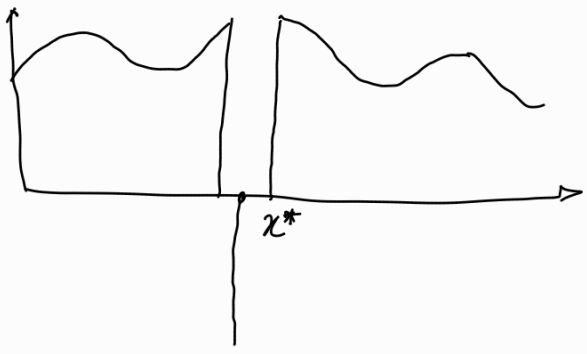
Phase inversion

$$f(x^*) = 1$$

$$\sum_{\forall x} \alpha_x |x\rangle$$

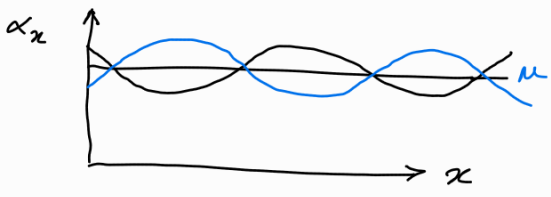


Phase inversion



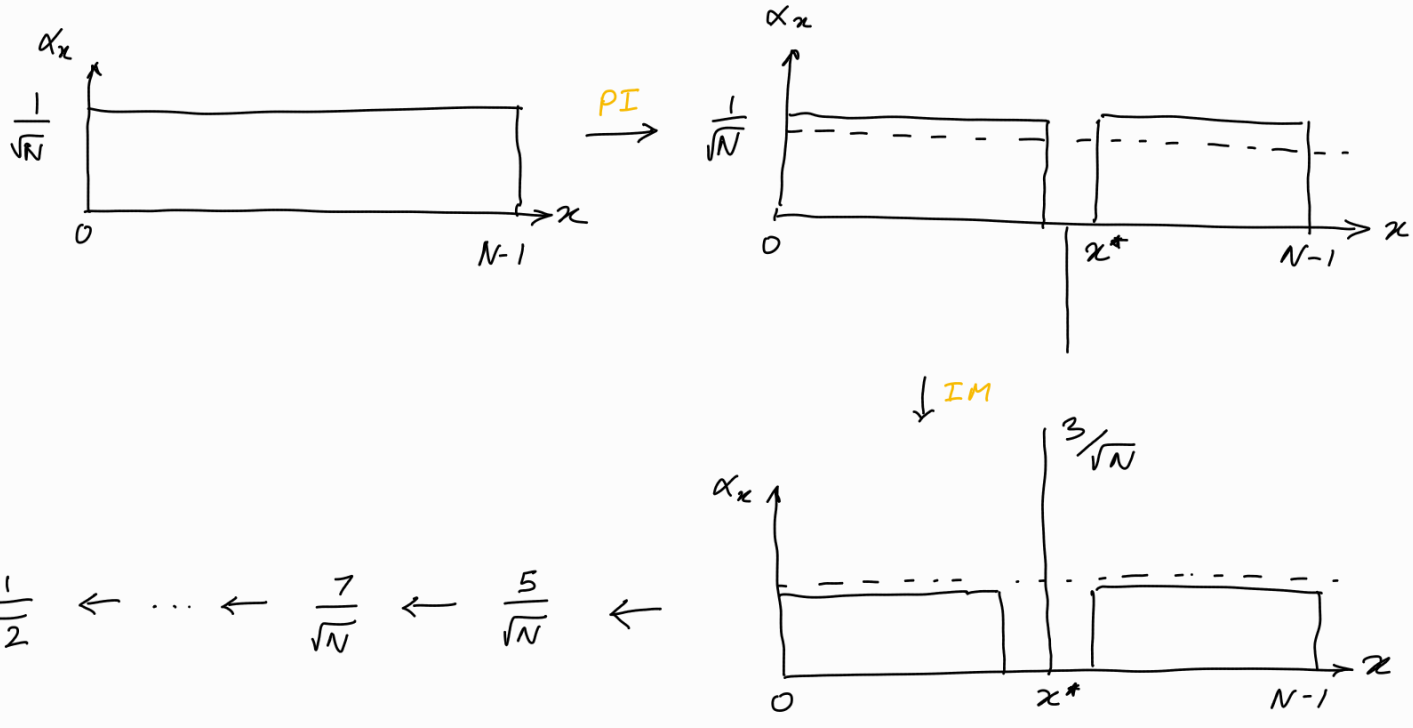
Inversion about the mean

$$\sum_{x} \alpha_x |x\rangle$$



$$\sum_{x} (2\mu - \alpha_x) |x\rangle$$

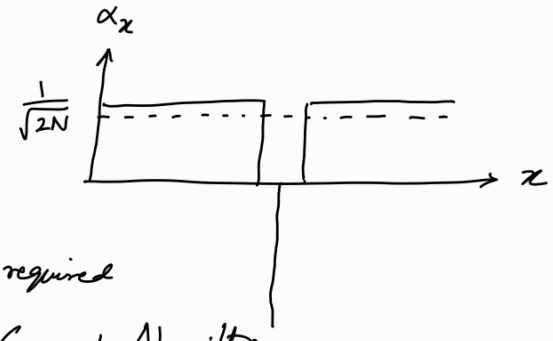
Grover's Algorithm



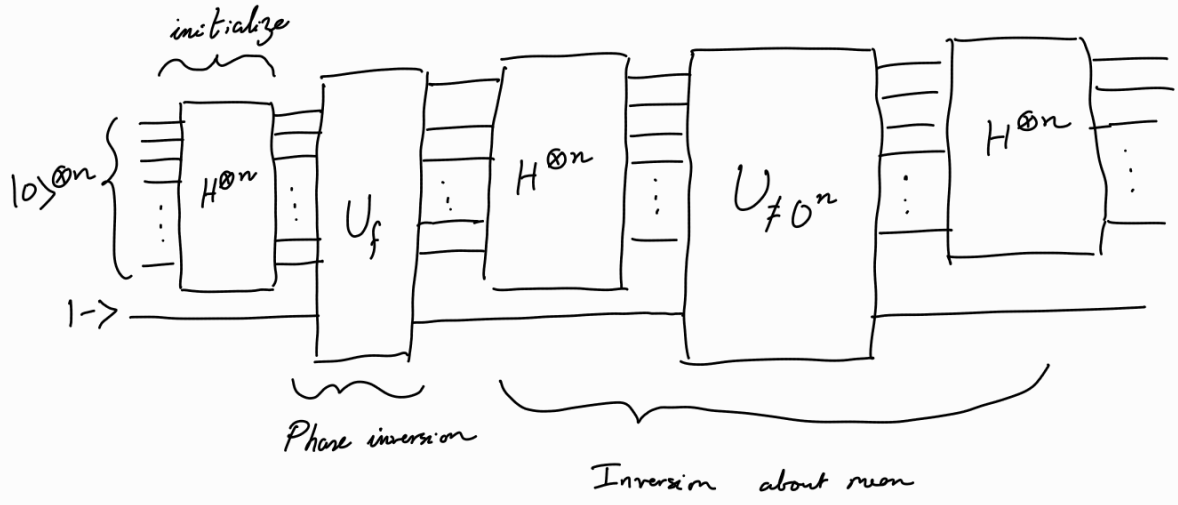
$$\frac{1}{\sqrt{2}} \leftarrow \cdots \leftarrow \frac{7}{\sqrt{N}} \leftarrow \frac{5}{\sqrt{N}} \leftarrow$$

What is the amplitude of rest when needle has $\frac{1}{\sqrt{2}}$? $\frac{1}{\sqrt{2N}}$

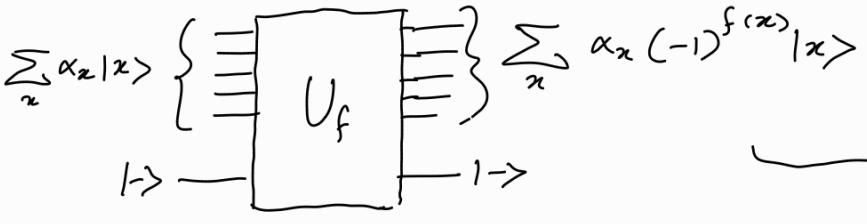
How much improvement are we making per step? $2 \times \frac{1}{\sqrt{2N}} = \sqrt{\frac{2}{N}}$



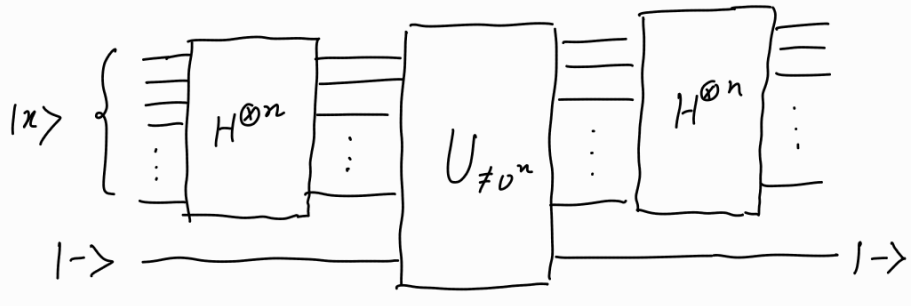
$\frac{1/\sqrt{2}}{\sqrt{2}/\sqrt{N}} = \frac{\sqrt{N}}{2}$ ⇝ upper bound on the number of steps required in Grover's Algorithm



Implementation



↪ Phase inversion



$$g(x) = \begin{cases} 0 & \text{if } x = 0^n \\ 1 & \text{otherwise} \end{cases}$$

↳ Reflection about mean is same as reflection about $|u\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle$

$$H^{\otimes n} \begin{pmatrix} 1 & 0 & 0 & \cdots \\ 0 & -1 & & \\ 0 & & -1 & \\ \vdots & & & \ddots \\ 0 & & & & -1 \end{pmatrix} H^{\otimes n}$$

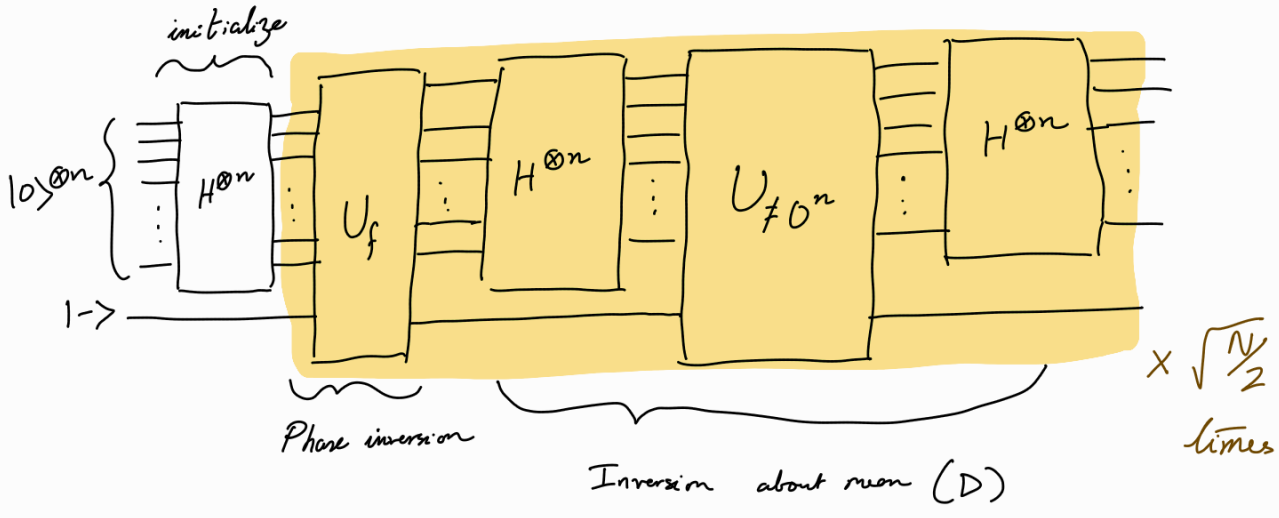
$$= H^{\otimes n} \begin{pmatrix} 2 & \cdots \\ \vdots & 0 & \ddots \\ & & & 0 \end{pmatrix} H^{\otimes n} - H^{\otimes n} H^{\otimes n}$$

$$= H^{\otimes n} \begin{pmatrix} 2 & 0 & \ddots \\ & & & 0 \end{pmatrix} H^{\otimes n} - I$$

$$= \begin{pmatrix} \frac{2}{N}-1 & \frac{2}{N} & \cdots & \frac{2}{N} \\ \vdots & \frac{2}{N}-1 & \ddots & \vdots \\ \frac{2}{N} & \cdots & & \frac{2}{N}-1 \end{pmatrix}$$

$$\begin{pmatrix} \frac{2}{N}-1 & \frac{2}{N} & \cdots \\ \vdots & \ddots & \vdots \\ \frac{2}{N} & \cdots & \frac{2}{N}-1 \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \vdots \\ \alpha_{N-1} \end{pmatrix} = \begin{pmatrix} 2\mu - \alpha_0 \\ 2\mu - \alpha_1 \\ \vdots \\ 2\mu - \alpha_{N-1} \end{pmatrix}$$

$$\sum_x \alpha_x |x\rangle \longrightarrow \sum_x (2\mu - \alpha_x)|x\rangle$$



Then measure and with prob $> \frac{1}{2}$ you find the needle.

(make sure you don't uncompute)

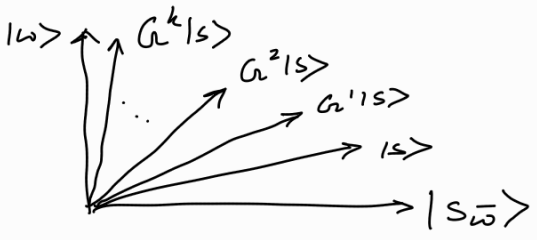
D is the diffuser now, $D = H^{\otimes n}\left(2|0^n\rangle\langle 0^n| - \mathbb{I}\right) H^{\otimes n}$

$= 2|s\rangle\langle s| - \mathbb{I}$

The Grover iterate: $G_r = D U_f^{\pm}$

$$|s\rangle = \cos\left(\frac{\theta}{2}\right)|s_{\bar{\omega}}\rangle + \sin\left(\frac{\theta}{2}\right)|\omega\rangle$$

G_r rotates $|s\rangle$ gradually to $|\omega\rangle$.



Find k such that $|\langle\omega| G_r^k |\omega\rangle|^2 \approx 1$

$$G_r = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

$$G_r^k|s\rangle = \cos\left(\frac{(2k+1)\theta}{2}\right)|s_{\bar{\omega}}\rangle + \sin\left(\frac{(2k+1)\theta}{2}\right)|\omega\rangle$$

$$\boxed{k = \frac{\pi}{4}\sqrt{N/M} - 1/2 \Rightarrow G_r^k|s\rangle = |\omega\rangle}$$

But what if we donot know M? (M → no. of x^*s in database)

$$\boxed{\sin\theta/2 = \sqrt{M/N}}$$

① Randomized Quantum Search

(Grover with $\frac{\pi}{4}\sqrt{N/M}$ iterations

with $M = 2, 4, 8, \ldots, 2^{\log_2 N}$)

② Quantum Counting (estimate M using phase estimation)

Inequalities

① Triangle Ineq :

$$\|x+y\| \leq \|x\| + \|y\|$$

$$\big|\,\|x\| - \|y\|\,\big| \leq \|x-y\|$$

② Cauchy Schwarz :

$$|\langle u, v\rangle|^2 \leq \langle u, u\rangle \langle v, v\rangle$$

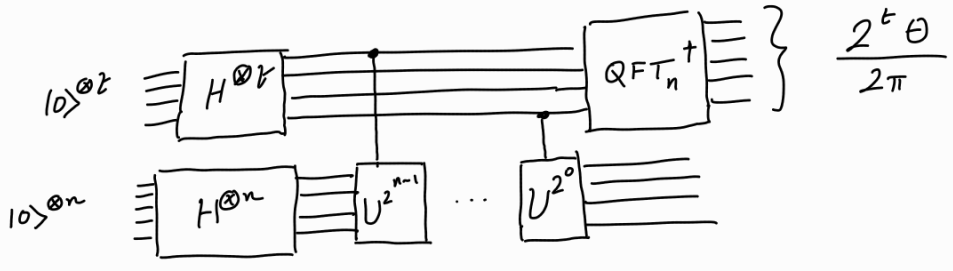
Quantum Counting

$$U = G_2 = D U_f^{\pm}$$

$$G_2 = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

has eigenvectors $\begin{bmatrix} -i \\ 1 \end{bmatrix}$ and $\begin{bmatrix} i \\ 1 \end{bmatrix}$

with eigenvalues $e^{\pm i\theta}$



↳ estimate θ to find concerned M given N

↓

no. of x s.t. $f(x) = 1$

Optimality of Quantum Search

$$|\psi_T^\omega\rangle = U_T U_\omega U_{T-1} U_\omega \cdots U_1 U_\omega |s\rangle$$

$$|\psi_T\rangle = U_T U_{T-1} \cdots U_1 |s\rangle$$

$$D_T = \sum_{\omega \in \{0,1\}^n} \| \psi_T^\omega - \psi_T \|$$

↳ don't want distance to be biased

Properties :

① After T iterations, $D_T \leq 4T^2$

② In order to enquire $|\langle \omega | \psi_T^\omega \rangle|^2 \geq 1/2$

for any $\omega \in \{0,1\}^n$, $D_T = \Omega(N)$

Together claim (1) and (2) $\Rightarrow T \geq cN$

$\Rightarrow$ Grover search is optimal.

Quantum Amplitude Amplification

$$U|0\rangle^{\otimes n} = \sqrt{p}\,|\psi_{good}\rangle + \sqrt{1-p}\,|\psi_{bad}\rangle$$

my algorithm succeeds with prob p,

and $|\psi_{good}\rangle \perp |\psi_{bad}\rangle$

$$\| \pi_{good} |\psi_0\rangle \|^2 = p, \quad \pi_{good} = |\psi_{good}\rangle\langle\psi_{good}|$$

The classical algorithm requires $\frac{1}{p}$ iterations.

Claim : $\exists$ a quantum algorithm that outputs $|\psi_{good}\rangle$ with a high probability in $O(\frac{1}{\sqrt{p}})$

Grover's Algorithm

① $U = H^{\otimes n}$

$|\psi_0\rangle = |s\rangle$, $\sqrt{p} = \sqrt{\frac{M}{N}}$

② $U_f^{\pm} \rightarrow$ oracle $\begin{cases} -x_0, & \text{if } f(x_0)=1 \\ x_0, & \text{if } f(x_0)=0 \end{cases}$

$= U_f^{\pm} |x_0\rangle$

$U_f^{\pm} |\omega\rangle = |\omega\rangle$

$U_f^{\pm} |s_{\bar{\omega}}\rangle = |s_{\bar{\omega}}\rangle$

$\Rightarrow U_\omega = \mathbb{I} - 2|\omega\rangle\langle\omega|$

③ $D = H^{\otimes n}(2|0^n\rangle\langle 0^n| - \mathbb{I}) H^{\otimes n}$

$= U_s$ (let)

④ Algo: $(U_s U_\omega)^k H^{\otimes n} |0\rangle^{\otimes n}$

for $k = \frac{\pi}{4}\sqrt{\frac{N}{M}} - \frac{1}{2}$

$\downarrow$

$O(\sqrt{\frac{1}{p}})$

Quantum Amplitude Amplification

① U : any quantum algorithm

② We will consider the 2-D invariant subspace spanned by

$\{|\psi_{good}\rangle, |\psi_{bad}\rangle\}$

$U_{\psi_{good}} = \mathbb{I} - 2|\psi_{good}\rangle\langle\psi_{good}|$

③ $U_{\psi_0} = U(2|0^n\rangle\langle 0^n| - \mathbb{I})U^\dagger$

$= 2|\psi_0\rangle\langle\psi_0| - \mathbb{I}$

④ Algo: $(U_{\psi_0} U_{\psi_{good}})^k U |0\rangle^{\otimes n}$

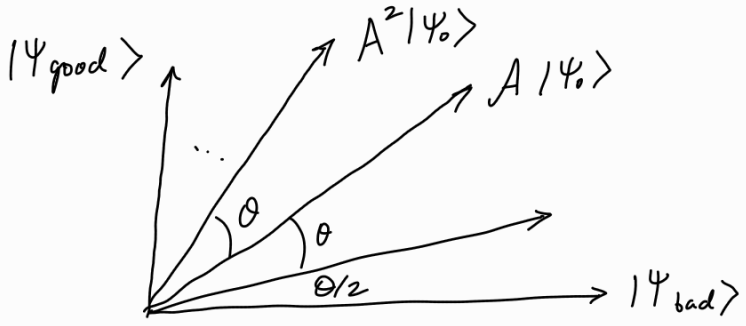
$\approx |\psi_{good}\rangle$

for $k = O(\sqrt{\frac{1}{p}})$

For QAA we have $U_{\psi_{good}} = \mathbb{I} - 2|\psi_{good}\rangle\langle\psi_{good}|$

$U_{\psi_0} = 2|\psi_0\rangle\langle\psi_0| - \mathbb{I}$

$|\psi_0\rangle = \sin(\frac{\theta}{2})|\psi_{good}\rangle + \cos(\frac{\theta}{2})|\psi_{bad}\rangle$



$$U_{\Psi_0} = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix} = \text{reflection about } |\Psi_0\rangle$$

$$U_{\Psi_{good}} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \text{reflection about } x\text{-axis}$$

$$\mathcal{A} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} = \text{rotation by theta}$$

Needed $\frac{2k+1}{2}\theta = \pi/2 \Rightarrow \theta = \frac{\pi}{2k+1}$

For $\sqrt{p} \ll 1$, $\sin\left(\frac{\theta}{2}\right) \approx \frac{\theta}{2} = \sqrt{p} \Rightarrow \theta = 2\sqrt{p}$

$$\Rightarrow 2\sqrt{p} = \frac{\pi}{2k+1} \Rightarrow 2k+1 = \frac{\pi}{2\sqrt{p}} \Rightarrow 2k = \frac{\pi}{2\sqrt{p}} - 1$$

$$\Rightarrow k = \frac{\pi}{4\sqrt{p}} - \frac{1}{2}$$

We only need $O\left(\frac{1}{\sqrt{p}}\right)$ queries to U.

$O\left(\frac{T_U}{\sqrt{p}}\right) \rightarrow$ overall complexity (given implementing U requires time T_U)

$$QAA = O\left(\frac{T_U}{\sqrt{p}}\right)$$

Constructing $U_{\psi_{good}}$

→ Let's modify U by adding ancilla qubits.

→ The mindful quantum algorithmist would design U in this manner if they want to use QAA afterwards.

$$U|0\rangle^{\otimes n}|0\rangle^{\otimes m} = \sqrt{p}\,|\psi_{good}\rangle|0\rangle^{m} + \sqrt{1-p}\,\underbrace{|\psi_{bad}\rangle|1\rangle^{m}}_{|\phi\rangle}$$

HHL algorithm : $U_{QPE}\,(U_b \otimes \mathbb{I})\,|0\rangle^{\otimes n}|0\rangle = \sqrt{p_0}\,|\tilde{x}\rangle|0\rangle + \sqrt{1-p_0}\,|\phi\rangle^{\perp}$

$$\| |\tilde{x}\rangle - |x\rangle \| \leq \epsilon \quad \text{where} \quad |x\rangle = \frac{\sum_j c_j/\lambda_j\,|v_j\rangle}{\left|\sum_j c_j/\lambda_j\,|v_j\rangle\right|^2}$$

We have $U|0\rangle^{n}|0\rangle^{m} = \sqrt{p}\,\underbrace{|\psi_g\rangle|0\rangle^{m}}_{|\psi_{good}\rangle \text{ new}} + \sqrt{1-p}\,\underbrace{|\phi\rangle}_{\hookrightarrow |\psi}$

$$(\mathbb{I} \otimes |0^m\rangle\langle 0^m|)\,|\phi\rangle = 0$$

$$\rightarrow \boxed{U_{\psi_{good}} = \mathbb{I}_n \otimes (\mathbb{I} - 2|0^m\rangle\langle 0^m|)}$$

① $U_{\psi_{good}}|\psi_{good}\rangle = -|\psi_g\rangle|0\rangle^{m}$

↳ flipping the phase

② $U_{\psi_{good}}|\phi\rangle = |\psi_b\rangle$ for $\phi \perp \psi_g$

Thus, $(U_{\psi_0} U_{good})^k |\psi_0\rangle \approx |\psi_{good}\rangle$ where $k = O(\frac{1}{\sqrt{p}})$

Complexity: $O(\frac{T_u}{\sqrt{p}})$

Complexity of HHL

$$\sqrt{p_0} \sim \frac{1}{\kappa}$$

$$\boxed{T_{HHL} = O\left(\frac{\kappa^2}{\epsilon}\right)}$$