Quantum Fourier Transform.

Discrete Fourier Transform.

Polynomial: $p(x) = a_0 + a_1 x^1 + a_2 \cdot x^2 + \cdots + a_{n-1} x^{n-1}$

$$g(x) = b_0 + b_1 x^2 + b_2 x^2 + \cdots + b_{n-1} x^{n-1}$$

What is $p(x) \cdot g(x) = f(x) = c_0 + c_1 x^2 + \cdots + c_{2n-1} x^{2n-2}$

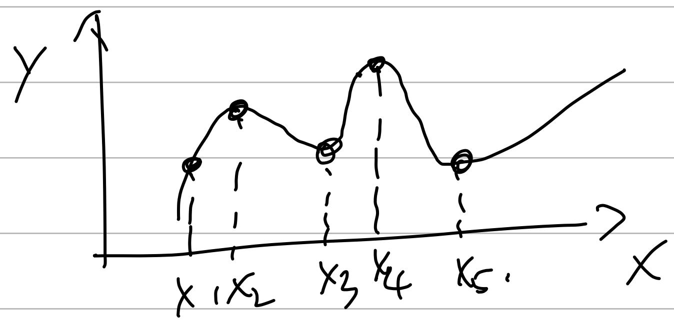
Naive approach needs $O(n^2)$ complexity.

Every n distinct points fix a degree-$(n-1)$ poly.

$\{(x_0, y_0) \cdots (x_{n-1}, y_{n-1})\} \longrightarrow$ polynomial

$\downarrow$

Lagrange Interpolation



If $\begin{cases} p(x_1) = y_1, \\ g(x_1) = y_2', \end{cases} \Rightarrow \boxed{f(x_1) = y_1 \cdot y_1'}$

$\vdots$

$$\begin{cases} p(x_{2n-1}) = y_{2n-1}, \\ g(x_{2n-1}) = y'_{2n-1}, \end{cases} \Rightarrow \boxed{f(x_{2n-1}) = y_{2n-1} y'_{2n-1}}$$

$\Downarrow$ Lagrange Inter...

recover $f(x) = c_0 + c_1 x^1 + \dots + c_{2n-2} x^{2n-2}$

Story:

Given $\begin{cases} (x_1, y_1) \cdots (x_{2n-1}, y_{2n-1}) \\ (x_1, y'_1) \cdots (x_{2n-1}, y'_{2n-1}) \end{cases}$

it take $\underline{O(n)}$ to compute $\begin{cases} (x_1, y_1 y'_1) \\ (x_2, y_2 y'_2) \\ \vdots \\ (x_{2n-1}, y'_{2n-1}) \end{cases}$

Question: How to get.

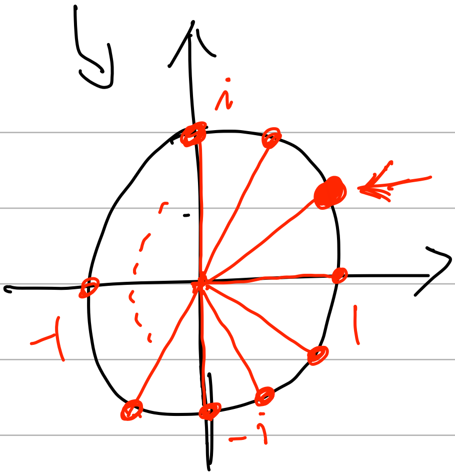
Naive: Eval. $p(x)$ for $2n-1$ times.

$\Rightarrow O(n^2)$ computation.

n-th roots of unity: (i.e. the solution to)

$x^n = 1$ (in complex field)

$|$



complex plane.

principal n-th root of unity.

Wants to use roots of unity to represent the polynomial:

(w_n is the principal n-th root of unity)

$$\begin{cases} (w_n^0, \; p(w_n^0)) \\ (w_n^2, \; p(w_n^2)) \\ \quad \vdots \\ (w_n^{n-1}, \; p(w_n^{n-1})) \end{cases}$$

$$\Leftrightarrow \begin{bmatrix} (w_n^0)^0 & (w_n^0)^1 & \cdots & (w_n^0)^{n-1} \\ (w_n^2)^0 & (w_n^2)^2 & \cdots & (w_n^2)^{n-1} \\ \vdots & \vdots & & \vdots \\ (w_n^{n-1})^0 & (w_n^{n-1})^1 & \cdots & (w_n^{n-1})^{n-1} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix}$$

(can prove)

$$= \begin{bmatrix} p(w_n^0) \\ p(w_n^2) \\ \vdots \\ p(w_n^{n-1}) \end{bmatrix} = \begin{bmatrix} \sum_{k=1}^{n-1} w_n^{0 \cdot k} \cdot a_k \\ \sum_{k=1}^{n-1} w_n^{2 \cdot k} \cdot a_k \\ \vdots \\ \sum_{k=1}^{n-1} w_n^{(n-1) \cdot k} a_k \end{bmatrix}$$

Main take-away:

The structure of the $[\omega_n^{ij}]$ matrix allows $\boxed{\text{some Divide-and-conquer idea}}$, to decrease the above matrix-vector multiplication to $O(n\log n)$ computation.

aka. Fast Fourier Transform

In general, $\forall j \in \{0, 1, \dots, n-1\}$

$$y_j = \boxed{\underbrace{p(\omega_n^j)}_{x_j} = \sum_{k=1}^{n-1} \omega_n^{j\cdot k}\cdot a_k}$$

Quantum Fourier Transform (QFT)

$\forall\ |x\rangle \in \{|0\rangle, |1\rangle, \dots |N-1\rangle\}$

$$F_N : |x\rangle \longmapsto \frac{1}{\sqrt{N}} \cdot \sum_{y=0}^{N-1} \omega_N^{x\cdot y} |y\rangle,$$

where ω_N is the principal N-th. root of unity.

$\hookrightarrow W_N = e^{\frac{2\pi i}{N}} = \cos(\frac{2\pi}{N}) + i\sin(\frac{2\pi}{N})$

Remark:

① F_N is unitary. ✓

②
$$\begin{cases} |0\rangle \xrightarrow{F_N} \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} W_N^{0\cdot y} |y\rangle = |\tilde{0}\rangle \\ |1\rangle \longrightarrow \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} W_N^{1\cdot y} |y\rangle = |\tilde{1}\rangle \\ \vdots \\ |N-1\rangle \longrightarrow \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} W_N^{(N-1)\cdot y} |y\rangle = |\widetilde{N-1}\rangle \end{cases}$$

rename

$$\begin{cases} \forall\ j \in \{|1\rangle, |2\rangle \cdots |N-1\rangle\}. \\ |j\rangle \xmapsto{F_N} |\tilde{j}\rangle \end{cases}$$

$\sim$ tilde

$$\underbrace{\{|\tilde{j}\rangle\}_{j=0}^{N-1} := \{|\tilde{0}\rangle, |\tilde{1}\rangle, \cdots, |\widetilde{N-1}\rangle\}}$$

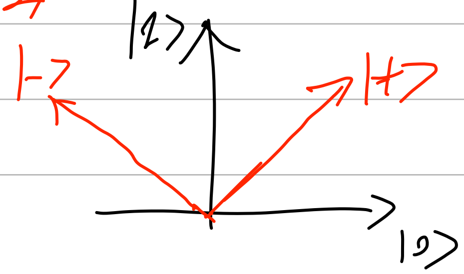
Fourier Basis

Form a orthonormal basis

2-D analog: $(H = F_2)$

$|0\rangle \xmapsto{H} |+\rangle$

$|1\rangle \longmapsto |-\rangle$



③ The inverse of QFT:

$\forall |x\rangle \in \{|0\rangle, |1\rangle, \cdots |N-1\rangle\}$

$$F_N^{-1} : |x\rangle \longmapsto \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \omega_n^{-x\cdot y} |y\rangle$$

Thm 1: let $N = 2^n$, it holds that

$\forall |x\rangle \in \{|0\rangle, |1\rangle, \cdots, |N-1\rangle\}$

$$|x\rangle \xmapsto{F_N} \frac{1}{\sqrt{2^n}} (|0\rangle + e^{2\pi i\, 0.x_n} |1\rangle) \otimes$$

$$\boxed{x = x_1 \cdot 2^{n-1} + x_2 \cdot 2^{n-2} + \cdots x_n \cdot 2^{n-n}} \qquad (|0\rangle + e^{2\pi i\, 0.x_{n-1}x_n} |1\rangle) \otimes$$

$$([x]_2 = x_1 x_2 \cdots x_n) \qquad \cdots\cdots$$

$$(|0\rangle + e^{2\pi i \cdot 0.x_1 x_2 \cdots x_n} |1\rangle)$$

$$\left(= \frac{1}{\sqrt{2^n}} \cdot \sum_{y=0}^{N-1} \omega_n^{x\cdot y} |y\rangle \right)$$

Proof follows from:

① def of $\omega_{2^n} := e^{2\pi i / 2^n}$

② Binary expansion:

$$0.x_1 x_2 \cdots x_n = \frac{x_1}{2^1} + \frac{x_2}{2^2} + \cdots + \frac{x_n}{2^n}$$

③ standard Dirac-notion linear algebra

Phase Estimation:

Problem: Given a controlled version of U^K for $K=1,2,\dots$

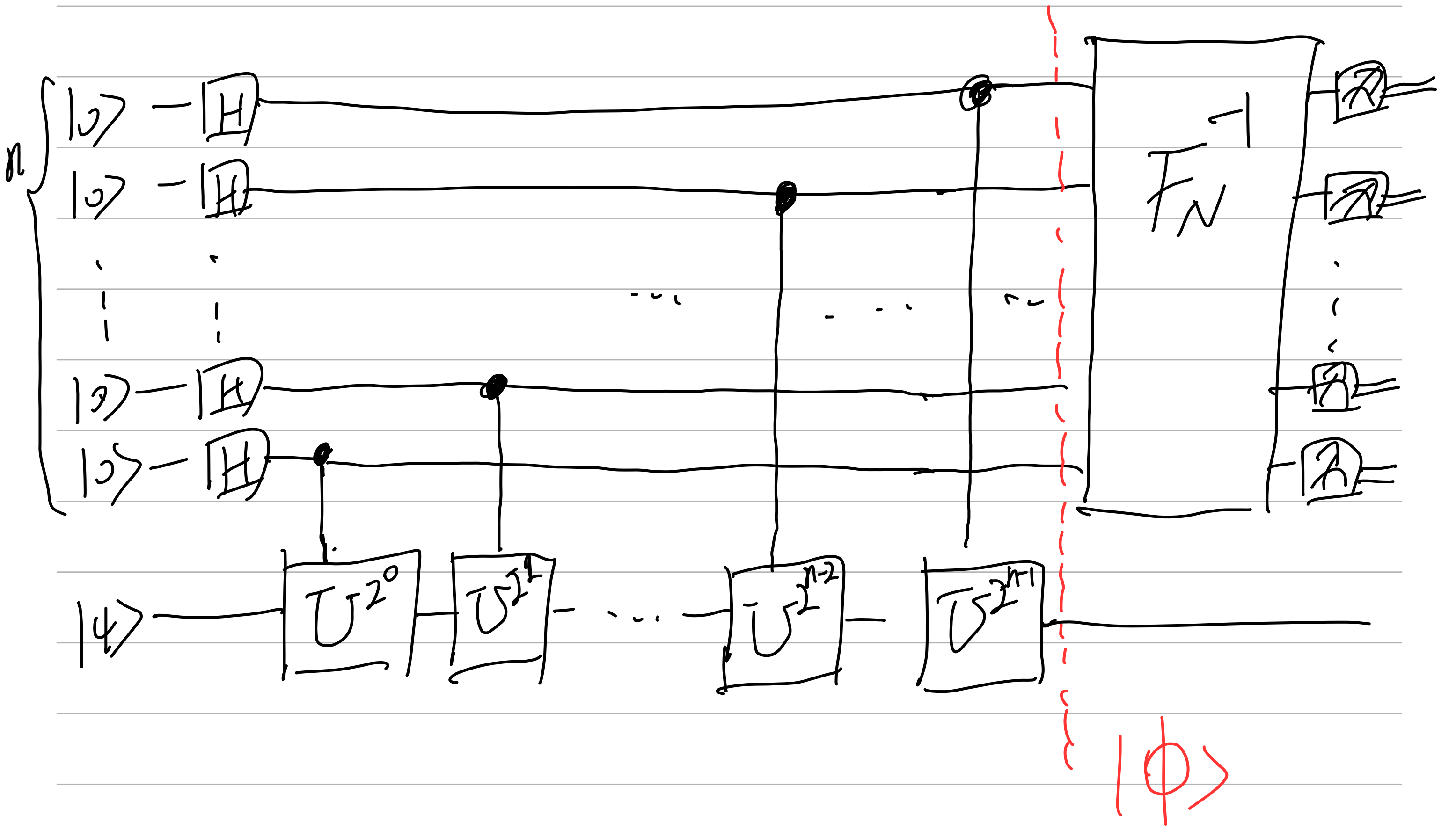
$$ctrl\text{-}U^K\,|b\rangle|\phi\rangle := \begin{cases} |0\rangle|\phi\rangle \\ |1\rangle\left(U^K|\phi\rangle\right) \end{cases}$$

Also,
Given an eigenstate $|\psi\rangle$ of U:

$$U|\psi\rangle = e^{2\pi i\theta}\cdot|\psi\rangle \qquad \theta\in[0,1]$$

$(\cos(x)=\cos(x+2\pi))$

Goal: Find θ.



Analysis:

Claim:

$\forall k$, $\text{ctrl-}U^{2^k} |+\rangle |\psi\rangle = \frac{1}{\sqrt{2}} (|0\rangle + e^{2\pi i \theta \cdot 2^k} |1\rangle) |\psi\rangle$ ... ①

Since $\theta \in [0, 1]$

$[\theta] = 0.\theta_1 \theta_2 \cdots \theta_n = \underbrace{\frac{\theta_1}{2^1} + \frac{\theta_2}{2^2} + \cdots + \frac{\theta_n}{2^n}}$ ... ②

Binary.

$\Rightarrow$ ① $= \frac{1}{\sqrt{2}} (|0\rangle + e^{2\pi i (\frac{\theta_1}{2^1} + \frac{\theta_2}{2^2} + \cdots + \frac{\theta_k}{2^k} + \frac{\theta_{k+1}}{2^{k+1}} + \cdots + \frac{\theta_n}{2^n}) \cdot 2^k} |1\rangle) |\psi\rangle$

notice: $e^{2\pi i (\frac{\theta_1}{2^1} + \cdots + \frac{\theta_k}{2^k}) \cdot 2^k} = 1$

$\Rightarrow$ ① $= \frac{1}{\sqrt{2}} (|0\rangle + e^{2\pi i (\frac{\theta_{k+1}}{2^{k+1}} + \cdots + \frac{\theta_n}{2^n}) \cdot 2^k} |1\rangle) |\psi\rangle$

$= \frac{1}{\sqrt{2}} (|0\rangle + e^{2\pi i \cdot 0.\theta_{k+1} \theta_{k+2} \cdots \theta_n} |1\rangle) |\psi\rangle$ ... ③

Summary:

$\text{ctrl-}U^{2^k} \cdot |+\rangle |\psi\rangle =$

$\Rightarrow |\phi\rangle = \frac{1}{\sqrt{2^n}} (|0\rangle + e^{2\pi i \cdot 0.\theta_n} |1\rangle) \otimes$

$(|0\rangle + e^{2\pi i \cdot 0.\theta_{n-1} \theta_n} |1\rangle) \otimes$

$(|0\rangle + e^{2\pi i \cdot 0.\theta_{n-2} \theta_{n-1} \theta_n} |1\rangle) \otimes$

...

$$\underbrace{\left(|0\rangle + e^{2\pi i \cdot 0.\theta_1\theta_2\cdots\theta_n}|1\rangle\right)}\otimes\underbrace{|\psi\rangle}$$

$$\Rightarrow \left(F_N^{-1} \otimes \underbrace{I}\right)|\phi\rangle = |\theta\rangle|\psi\rangle$$

↳ Follows from Thm 1

on the $|\psi\rangle$'s register

Caveats:

① Can't compute the exact θ if θ has more than n digits. But a good estimate.

② U^{2^n} requires exponential complexity?

— (Answer: repeat squaring Algo.)

Summary:

QPE is an Algo that given ctrl-U^{2^k}'s and a eigenvector $|\psi\rangle$ of U:

$$|0^n\rangle|\psi\rangle \xmapsto{QPE} |\theta\rangle|\psi\rangle$$

where θ is the θ in $U|\psi\rangle = e^{2\pi i\theta}|\psi\rangle$

Kitaev's Factoring:

Problem: give $N = \underbrace{p \cdot q}_{\text{two prime numbers } p, q}$.

$$|[p]_2| = n = |[q]_2|$$

Goal: Find p.

Two Steps:

nothing quantum.
Pure number-theory stuff

Step-1: covert Factoring to another problem called "Order Finding"

Step-2: Solve "order Finding" using QPE.

our focus.

Order Finding:

Problem: Give positive integer N and ~~x~~ x

such that:

$$\begin{cases} ① \ 1 \leq x < N \\ ② \ \gcd(N, x) = 1 \end{cases}$$

Goal: Find the smallest positive integer r

such that $x^r = 1 \pmod N$

(We call "r" as the "order" of x)

"The" U for Order Finding:

$\forall$ computational basis $|y\rangle \in \{|0\rangle, |1\rangle, \cdots |N\rangle\}$.

$$U_x : |y\rangle \longmapsto |x \cdot y \bmod N\rangle$$

(Claim: U_x is a unitary.)

Thm 2: Let r denote the order of x.

(i.e. $x^r = 1 \bmod N$). Then, for all

$s \in \{0, 1, \dots, r\}$, def a state:

$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} w_r^{-sk} \, |x^k \bmod N\rangle$$

w_r is the principal r-th root of unity (i.e. $e^{\frac{2\pi i}{r}}$)

Then: $U_x \cdot |u_s\rangle = w_r^{s} |u_s\rangle = e^{2\pi i \frac{s}{r}} |u_s\rangle$

Attempt 1:

Run QPE with U_x and $|u_s\rangle$

$$|0^n\rangle|u_s\rangle \xrightarrow{QPE} \underbrace{|\tfrac{s}{r}\rangle}|u_s\rangle$$

continued Fraction Algo

$\downarrow$

r.

Caveat: We don't know how to prepare $|u_s\rangle$.

Solution:

Claim 1: It holds that $\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}|u_s\rangle = |1\rangle$

Run QPE in the following way.

$$QPE\cdot(|0^n\rangle|1\rangle) = QPE\cdot\left(\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}|0^n\rangle|u_s\rangle\right)$$

$$= \underbrace{\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}\left|\frac{s}{r}\right\rangle_{reg1}|u_s\rangle_{reg2}}$$

$\downarrow$ measure register 1:

output the following state for a random "s"

$$= \left|\frac{s}{r}\right\rangle|u_s\rangle.$$