LECTURE - 6.

Today :

* Hadamard transform as a change of basis.
* Fourier transform over $\mathbb{Z}_N$
* Simon's algorithm over $\mathbb{Z}_N$
  (i.e. period-finding, precursor to Shor)

Announcements

HW1 out next week (Mon / Tues)

TODAY : NEW PERSPECTIVE.

$$g : \{0,1\}^n \to \mathbb{C}$$

We can write g
$$\begin{bmatrix} g(0^n) \\ g(0^{n-1}1) \\ \vdots \\ \vdots \\ g(1^n) \end{bmatrix}$$

$$|g\rangle = \sum_{x\in\{0,1\}^n} \frac{g(x)\,|x\rangle}{\sqrt{g(0^n)^2 + g(0^{n-1}1)^2 + \cdots}}$$

(upto normalization)

$$= g(0^n)\begin{bmatrix} 1 \\ 0 \\ \vdots \\ \vdots \\ 0 \end{bmatrix} + g(0^{n-1}1)\begin{bmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ \vdots \\ 0 \end{bmatrix} + \cdots g(1^n)\begin{bmatrix} 0 \\ \vdots \\ \vdots \\ \vdots \\ 1 \end{bmatrix}$$

"computational basis vectors".

$\{\chi_s\}_{s \in \{0,1\}^n}$ is an orthonormal basis.

$$\chi_s = \frac{1}{2^{n/2}} \begin{bmatrix} \chi_s(0^n) \\ \chi_s(0^{n-1}1) \\ \vdots \\ \chi_s(1^n) \end{bmatrix}$$

where for any x,

$$\chi_s(x) = (-1)^{s.x}$$

$$|g\rangle = \sum_s \hat{g}(s) \underbrace{|\chi_s\rangle}_{\text{Fourier basis}}$$

What is $\hat{g}(s)$? → amplitude on vector $|\chi_s\rangle$

$$\hat{g}(s) = \langle \chi_s | g \rangle$$

$$= \begin{bmatrix} (\chi_s(0^n))^* & \cdots\cdots & (\chi_s(1^n))^* \end{bmatrix} \begin{bmatrix} g(0^n) \\ \vdots \\ g(1^n) \end{bmatrix}$$

$$= \sum_{x \in \{0,1\}^n} \chi_s(x)\, g(x) \quad \text{(upto normalization)}$$

$$= \mathbb{E}_{x \leftarrow \{0,1\}^n}\left[\chi_s(x)\, g(x)\right]$$

$$\hat{g}(0) = \mathbb{E}_{x \leftarrow \{0,1\}^n}\left[g(x) \right]$$

Lets go back to DJ

$$\sum_x |x\rangle \longrightarrow \boxed{\begin{array}{c} U_f \\ \text{(balanced or constant)} \end{array}} \longrightarrow \sum_x (-1)^{f(x)} |x\rangle$$

$$= \sum_x g(x) |x\rangle$$

Lets say $(-1)^{f(x)} \equiv g(x)$

$$|g\rangle = \sum_x g(x) |x\rangle$$

equivalently

$$= \sum_s \hat{g}(s) |\chi_s\rangle$$

where $\hat{g}(s) = \mathbb{E}_x \left[\chi_s(x) g(x)\right]$

$$\hat{g}(0) = \mathbb{E}_x[g(x)]$$

Case I.

f is constant, say $\forall x\; f(x) = b$

$$\hat{g}(0^n) = \mathbb{E}_x\left[(-1)^b\right] = \pm 1$$

$\rightarrow$ amplitude on $|x_{0^n}\rangle$

that means

$$|g\rangle = \pm 1\, |x_{0^n}\rangle$$

Case II.

f is balanced

$$\hat{g}(0^n) = \mathbb{E}_x[g(x)]$$

$$= \mathbb{E}_x\left[(-1)^{f(x)}\right]$$

$$= \frac{1}{2^n}\left[2^{n/2} - 2^{n/2}\right] = 0.$$

$$|g\rangle = 0\,|x_{0^n}\rangle + \overbrace{\qquad\qquad\qquad}^{\text{non-zero amplitudes}}$$

Claim.

$$H^{\otimes n}\left(\sum_s \hat{g}(s)|\chi_s\rangle\right) \to \sum_s \hat{g}(s)|s\rangle.$$

[Remark: this means $H^{\otimes n}(|g\rangle) \to$

① $\pm 1\,|0^n\rangle$ for constant f

② 0 amplitude on $|0^n\rangle$ for balanced f.]

Proof. $|\chi_s\rangle = \sum_y (-1)^{s\cdot y}|y\rangle$

$$H^{\otimes n}\left(\sum_s \hat{g}(s)|\chi_s\rangle\right)$$

$$= H^{\otimes n}\left(\sum_s \hat{g}(s)\sum_y (-1)^{s\cdot y}|y\rangle\right)$$

$$= \sum_s \hat{g}(s)\sum_y (-1)^{s\cdot y}\left(H^{\otimes n}|y\rangle\right)$$

$$H^{\otimes n}|y\rangle = \sum_z (-1)^{y\cdot z}|z\rangle$$

$$= \sum_s \hat{g}(s) \sum_y (-1)^{s\cdot y} \sum_z (-1)^{y\cdot z} |z\rangle$$

$$= \sum_s \hat{g}(s) \sum_{y,z} (-1)^{y\cdot(s\oplus z)} |z\rangle$$

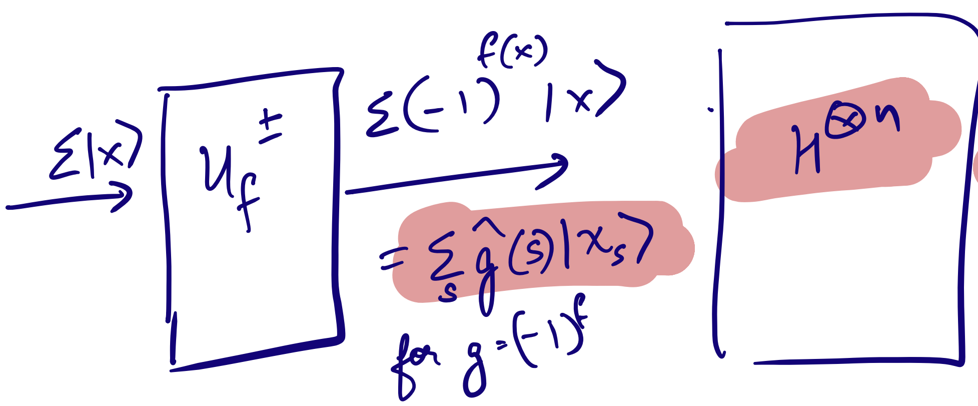
$$\sum_z \sum_y (-1)^{y\cdot(s\oplus z)} |z\rangle$$

$$= \sum_{z:z=s} |z\rangle = |s\rangle.$$

$s = z$ then $\sum_y (-1)^{y(s\oplus z)} = 2^n$

$s \neq z$ then $\sum_y (-1)^{y(s\oplus z)} = 0$

$$= \sum_s \hat{g}(s) |s\rangle$$



$\sum_s \hat{g}(s)|s\rangle$

constant : $\hat{g}(\vec{0}) = \pm 1$

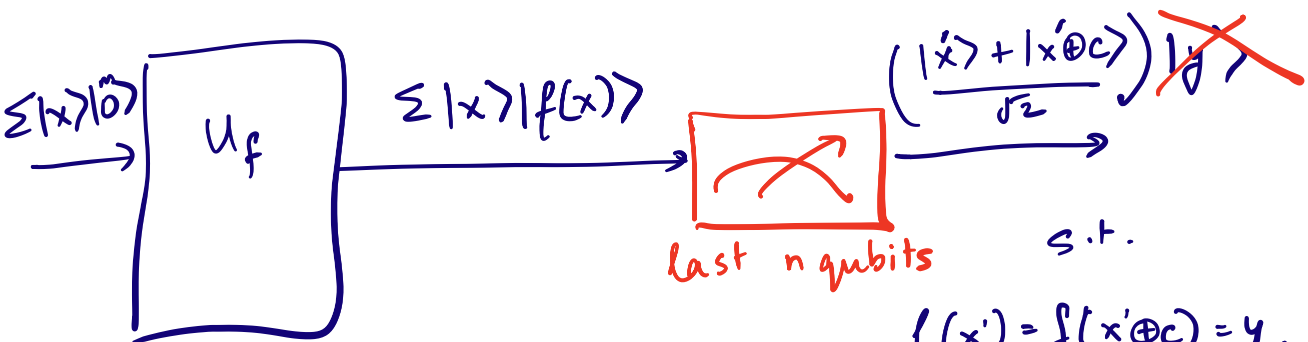
$\Rightarrow$ c.b. measurement always returns 0^n.

balanced : $\hat{g}(\vec{0}) = 0. \Rightarrow$ " never returns 0^n.

Simon's algorithm.

$f(x) = f(x \oplus c)$

Find c.



s.t.

$f(x') = f(x' \oplus c) = y.$

$$|g\rangle = \frac{|x'\rangle + |x' \oplus c\rangle}{\sqrt{2}}$$

$$|g\rangle = 0|0^n\rangle + 0|0^{n-1}1\rangle \ldots + \frac{1}{\sqrt{2}}|x'\rangle + \overset{\text{zeroes}}{\ldots} + \frac{1}{\sqrt{2}}|x' \oplus c\rangle$$

$$+ \overset{\text{zeroes}}{\ldots}$$

$$|g\rangle = \sum_s \hat{g}(s)\,|\chi_s\rangle$$

$$\hat{g}(s) = \mathop{\mathbb{E}}_x\left[\chi_s(x)\, g(x)\right]$$

$$= \chi_s(x') + \chi_s(x' \oplus c)$$

$$= (-1)^{s.x'} + (-1)^{s.(x' \oplus c)} = (-1)^{s.x'}\left[1 + (-1)^{s.c}\right]$$

$(-1)^{s.c} = -1$ when $s \not\perp c$

$(-1)^{s.c} = 1$ when $s \perp c$

When $s \not\perp c$, $\hat{g}(s) = 0$. When $s \perp c$, $\hat{g}(s) \neq 0$.

$$|g\rangle = \sum_s \hat{g}(s)\,|\chi_s\rangle.$$

But we know that $\hat{g}(s)$ is non-zero iff $s \perp c$.
ie $s.c = 0$

$$|g\rangle = \sum_s \hat{g}(s)\,|\chi_s\rangle$$ with non-zero $\hat{g}(s) \Leftrightarrow s \perp c$.

$$\left(H^{\otimes n}|g\rangle\right) = \sum_s \hat{g}(s)\,|s\rangle$$ with non-zero $\hat{g}(s) \Leftrightarrow s \perp c$.

$\Rightarrow$ measuring $\left(H^{\otimes n}|g\rangle\right)$ in computational basis will ONLY give outcomes "s" s.t. $s \perp c$.

(over $\mathbb{Z}_2^n$)

Fourier transform over $\mathbb{Z}_N$

Integers mod N

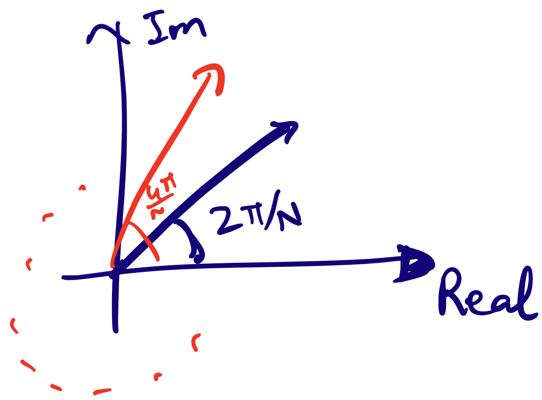
$\{\chi_0, \chi_1, \ldots, \chi_{N-1}\}$ $N = 2^n$.

$[0, N-1]$ $[0, N-1]$ multiplication over integers

$$\chi_\sigma(x) = \omega^{(\sigma . x)} \qquad \sigma \in [0, N-1]$$

$$\omega = e^{\frac{2\pi i}{N}} = \cos\frac{2\pi}{N} + i \sin\frac{2\pi}{N}$$

ω is the N^{th} root of unity



$$\omega^2 = e^{\frac{4\pi i}{N}}$$

$$\omega^N = e^{\frac{2\pi i}{\cancel{N}}\cdot\cancel{N}} = e^{2\pi i} = 1.$$

$$\chi_s = \begin{bmatrix} \chi_s(0) \\ \vdots \\ \chi_s(N-1) \end{bmatrix} = \begin{bmatrix} \omega^{s.0} \\ \vdots \\ \omega^{s.N-1} \end{bmatrix}$$

FACTS.

- $\chi_0 = \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix}$ $\qquad \underset{x}{E}\left[\chi_0(x)\right] = 1.$

- $\chi_s(x) = \chi_x(s) = \omega^{s.x} = \omega^{x.s}$

- $\underset{x \leftarrow Z_N}{\mathbb{E}}\left[\chi_s(x)\right] = 0$ for $s \neq 0$.
  $= 1$ for $s = 0$.

$$= \frac{1}{N} \sum_{x \in [0, N-1]} \omega^{s.x}$$

$$= \frac{1}{N}\left(\omega^0 + \omega^s + \omega^{2s} + \dots + \omega^{s(N-1)}\right)$$

numerator $= 0$

$$= \frac{1}{N}\left(\frac{\omega^{sN} - 1}{\omega^s - 1}\right) = 0. \text{ when } s \neq 0.$$

$\omega^N = 1. \Rightarrow \omega^{sN} = 1.$

denominator $\neq 0$

- $\chi_s(x)\,\chi_r(x) = \chi_{s+r}(x)$
- $(\chi_r(x))^* = \omega^{-rx} = \chi_{-r}(x) = \chi_r(-x)$

  $\hookrightarrow \omega = e^{\frac{2\pi i}{N}}$
- orthonormal

$$\langle \chi_s | \chi_r \rangle = \mathop{\mathbb{E}}_{x}\left[(\chi_s(x))^* (\chi_r(x))\right]$$
$$= \mathop{\mathbb{E}}_{x}\left[\chi_{r-s}(x)\right]$$

$$\mathbb{E}\left[\chi_{r-s}(x)\right] = 0 \quad \text{when} \quad r \neq s$$
$$= 1 \quad \text{when} \quad r = s.$$

- Form a basis for $\mathbb{C}^N$.

As before, we can write

$$|g\rangle = \sum_{s \in \mathbb{Z}_N} \hat{g}(s)\, |\chi_s\rangle$$

$$\hat{g}(s) = \langle \chi_s | g \rangle = \mathop{\mathbb{E}}_{x}\left[\underline{\chi_{-s}(x)}\, g(x)\right]$$

We will see there is a quantum circuit C with polylog N gates that implements the transform

$$\sum_s \hat{g}(s) |\chi_s\rangle \xrightarrow{C} \sum_s \hat{g}(s) |s\rangle$$

Period - finding

$$f : \mathbb{Z}_N \to S.$$

"Promise" : f is periodic, i.e.

$\exists\, s$ s.t. $\forall x$, $f(x) = f(x+s) = f(x+2s) \dots$
otherwise distinct $f(x) = f(y) \Rightarrow |(y-x)|$ is a multiple of s

R	G	B	Y	M	R	G	B	Y	M	R	.....

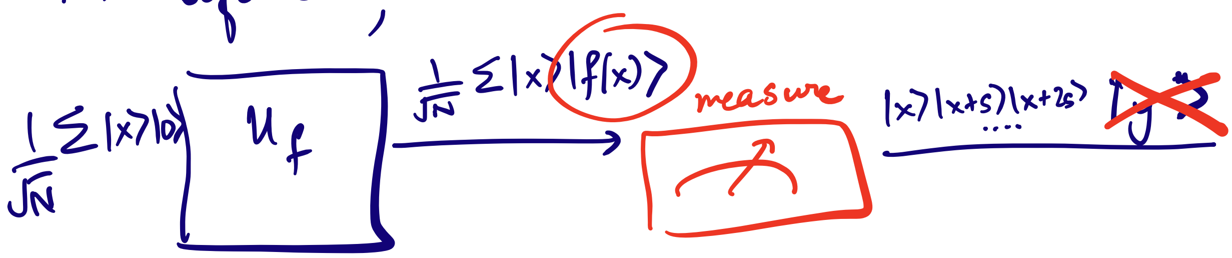
Right now, this promise means s must divide N.

If $N = 2^n$ and $s \mid N \Rightarrow s = \underbrace{\{1, 2, 4, 8 \dots 2^n\}}_{n \text{ possibilities for } s.}$

then there is a simple classical algorithm that with $O(n)$ queries finds s (simply by checking for all n possibilities).

Still, for now we will develop a quantum algorithm to solve this problem. The quantum algorithm will even apply to a relaxed setting, but the classical one will not.

As before,



$$|g\rangle = |x\rangle + |x+s\rangle + |x+2s\rangle \dots$$

$$= \sum \hat{g}(\sigma)\,|x_\sigma\rangle \qquad \boxed{\xrightarrow{\text{circuit}} \sum \hat{g}(\sigma)\,|\sigma\rangle.}$$

What should $\hat{g}(\sigma)$ be?

(Next time...)