LECTURE 7: PERIOD-FINDING, SHOR'S ALGORITHM.

[HW1 will be out by midnight today, due midnight 02/18]

TODAY: Simon's algorithm over $\mathbb{Z}_N$, use it to factor M s.t. $|M| = n$ in time poly(n). Shor's algorithm.

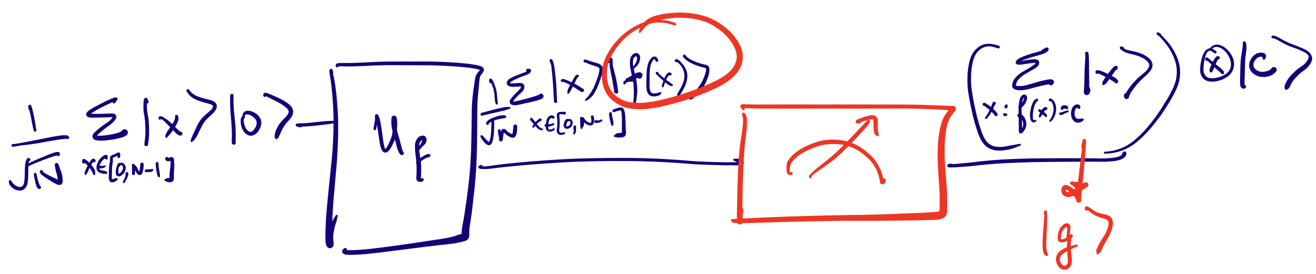
RECALL from last lecture:

Given a function $f : \mathbb{Z}_N \to Y$.
s.t. $\exists s \; \forall x$, $f(x) = f(x+s) = f(x+2s) \ldots\ldots$
otherwise distinct i.e. $f(x) = f(y) \Rightarrow |(y-x)|$ is a multiple of s.

Example | R | G | B | Y | M | R | G | B | Y | M | . . . . | $(s \mid N)$

$|\leftarrow s = 5 \rightarrow|$

Last time: Finding s with $O(\log N)$ quantum queries.



$$|g\rangle = |x'\rangle + |x'+s\rangle + |x'+2s\rangle \ldots\ldots \quad \left(\frac{N}{s} \text{ terms}\right).$$

QFT over $\mathbb{Z}_N$.

$$|g\rangle \equiv \sum_{\sigma \in N} \hat{g}(\sigma)\,|x_\sigma\rangle$$

where $\hat{g}(\sigma) = \underset{x}{\mathbb{E}}\left[(\chi_\sigma(x))^* g(x) \right]$ $\quad \chi_\sigma(x) = \omega^{\sigma x}$

$$= \underset{x}{\mathbb{E}}\left[\omega^{-\sigma x} g(x) \right]$$

$$= \underset{k}{\mathbb{E}}\left[\omega^{-\sigma(x'+ks)} \right]$$

$$= \omega^{\overset{\text{mod } N}{\uparrow}{-(\sigma . x')}} + \omega^{\overset{\text{mod } N}{\uparrow}{-\sigma(x'+s)}} + \omega^{-\sigma(x'+2s)} + \ldots\ldots\ \omega^{-\sigma(x'+(\frac{N}{s}-1)s)}$$

(for $x' < s$).

$\hat{g}(\sigma) = 0$ for σ s.t. $\sigma s \neq 0$, $\hat{g}(\sigma) = 1$ for σ s.t. $\sigma s = 0$.

Case 1. $\sigma s = 0 \mod N$.

$$= \omega^{-\sigma x'} + \omega^{-\sigma x'} + \ldots \qquad \left(\frac{N}{s} \text{ times}\right)$$

$$= \omega^{-\sigma x'}$$

Case 2. $\sigma s \neq 0 \mod N$

$$= \omega^{-\sigma x'}\left(1 + \omega^{-\sigma s} + \omega^{-\sigma 2s} + \ldots\ldots\ \omega^{-\sigma(\frac{N}{s}-1)s}\right)$$

$$= \omega^{-\sigma x'} \cdot \left(1 + \beta + \beta^2 + \ldots\ \beta^{(\frac{N}{s})-1}\right).$$

$$= \frac{\beta^{\frac{N}{s}} - 1}{\beta - 1}$$

$1 - 1 = 0$

$$= \omega^{-\sigma x'} \cdot \frac{\left[(\omega^{-\sigma \cancel{s}})^{(\frac{N}{\cancel{s}})} - 1\right]}{\omega^{-\sigma s} - 1} = \omega^{-\sigma x'} \cdot \frac{(\omega^N)^{\sigma} - 1}{\omega^{-\sigma s} - 1}$$

$$= 0.$$

QFT.

$$|g\rangle = \sum \hat{g}(\sigma)\, |x_\sigma\rangle = \sum_{\sigma : \sigma s = 0} |x_\sigma\rangle \quad \text{(upto normalization)}$$

$$\downarrow \text{QFT} \qquad\qquad \downarrow \text{QFT circuit}$$

$$\sum \hat{g}(\sigma)\, |\sigma\rangle \qquad\qquad \sum_{\sigma : \sigma s = 0} |\sigma\rangle .$$

Measure $QFT(|g\rangle) \to$ uniform σ s.t. $\sigma s = 0$

$\sigma s = 0$, or $\sigma s = N$, or $\sigma s = 2N$, ... $\sigma s = (s-1) N$.

$\Rightarrow \sigma = 0$ or $\frac{N}{s}$ or $\frac{2N}{s}$ or ..... $\frac{(s-1)N}{s}$.

Let $p = \frac{N}{s}$.

$\sigma = 0$ or p or $2p$ or ...... $(s-1)\, p$.

$GCD(ap, bp) = p$ when $GCD(a, b) = 1$.

So if you obtain any ap, bp s.t. $GCD(a, b) = 1$
GCD is computable in time (classically) poly(n)
This can be done in $O(\log N)$ attempts.

FACTORING (Shor's algorithm).

PROBLEM.

$M = pq$ find (p, q)

(p, q n-bit long)

Claim 1.

It suffices to find $r \neq \pm 1 \pmod{M}$,

such that $r^2 = 1 \bmod M$.

$\Leftrightarrow r^2 - 1 = 0 \bmod M$

$\Leftrightarrow (r-1)(r+1) = 0 \bmod M$

$= kM$ for some $k \neq 0$.

$(r-1)$ and $(r+1)$ are both.

1) non-zero mod M.

2) are factors of kM.

$\mathrm{GCD}(r-1, M)$ or $\mathrm{GCD}(r+1, M)$

must be a prime factor of M

Claim.

$\mathrm{GCD}(r-1, M) \neq 1$ or $\mathrm{GCD}(r+1, M) \neq 1$.

Proof.

$\mathrm{GCD}(r-1, kM) = (r-1)$. Suppose $\mathrm{GCD}(r-1, M) = 1$.

$\Rightarrow \mathrm{GCD}(r-1, k) = r-1$. --- (1)

$GCD(r+1, kM) = (r+1)$. Suppose $GCD(r+1, M) = 1$

$\Rightarrow GCD(r+1, k) = r+1$. ---②.

Both ① and ② cannot be true simultaneously.

Given M,

How to find r s.t. $r^2 = 1 \mod M$.

Sample $A \leftarrow \mathbb{Z}_M$

find smallest s such that $A^s = 1 \mod M$.

(order of A in $\mathbb{Z}_M$.)

If s happens to be even,

then set $r = A^{\frac{s}{2}}$. $r^2 = \left(A^{\frac{s}{2}}\right)^2 = 1 \mod M$.

For random A,

$Pr[\, s \text{ is even} \,] \geq \frac{1}{2}$.

Factorizing M reduces to:

Given A, M each n bits long,

find s s.t. $A^s = 1 \mod M$.

$$A^0 = 1,\ A^1 = A,\ A^2,\ A^3 \ldots\ldots \underset{=1}{A^s},\ \underset{=A}{A^{s+1}},\ A^{2}\ldots\ldots$$

1) Find $N \gg M$, $|N| = \cancel{\text{poly}(n)}\ n$.

2) Define $f : \{0, 1, \dots N-1\} \to \{0, 1, \dots M-1\}$

$$f(x) = A^x \bmod M.$$

f :

x	$f(x)$
0	1
1	$A \bmod M$
2	$A^2 \bmod M$
$\vdots$	
$s-1$	$A^{s-1} \bmod M$
s	1
	A
	$\vdots$

1	A	A^2	....	1	A	....

$s \nmid N$.

1) Start with $\frac{1}{\sqrt{N}} \sum_{x \in [0, N-1]} |x\rangle |0^n\rangle$.

2) $U_f \to \frac{1}{\sqrt{N}} \sum_x |x\rangle |f(x)\rangle$.

3) Measure register containing $f(x)$ to get

$$\Big(\sum_{x: f(x)=c} |x\rangle\Big) \otimes |c\rangle$$

$$|g\rangle = |x'\rangle + |x'+s\rangle + |x'+2s\rangle \ldots\ldots \left(\left\lfloor \tfrac{N}{s} \right\rfloor - 1\right) \text{ terms.}$$

$\left(\left\lceil \tfrac{N}{s} \right\rceil - 1\right)$ terms.

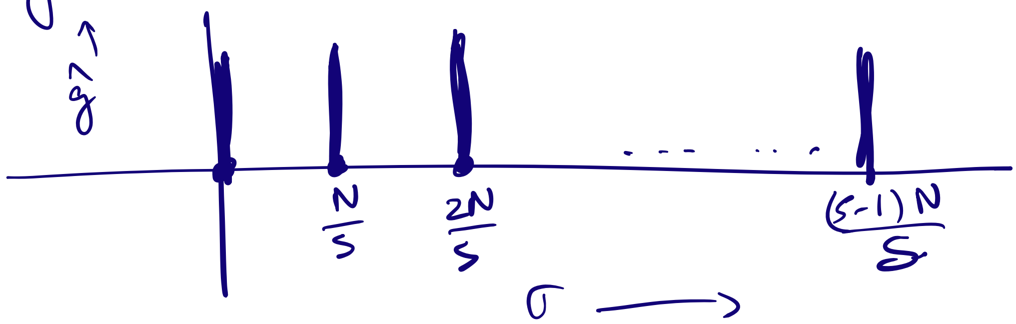
$\forall\, \sigma$ s.t. $\sigma . s = 0 \mod N$

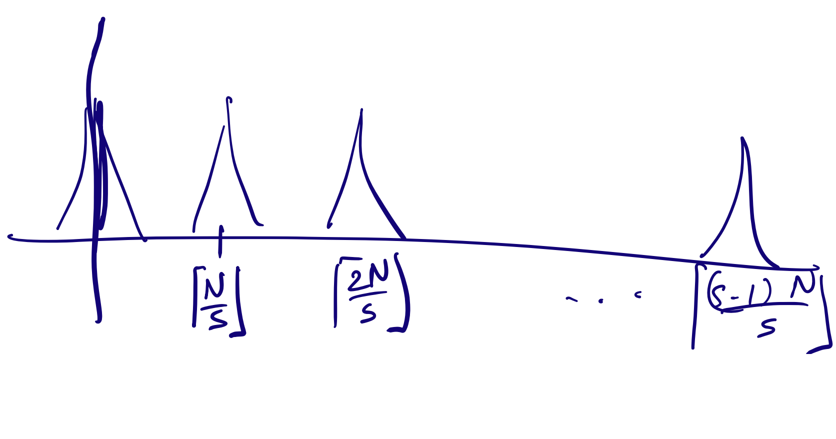
$$\hat{g}(\sigma) \neq 0.$$

$\forall\, \sigma$ s.t. $\sigma s \neq 0 \mod N$

$$\hat{g}(\sigma) = 0.$$

If $s | N$





$$QFT(|g\rangle) \to \sum \hat{g}(\sigma)\,|\sigma\rangle.$$

Measurement results in $\left\lceil \frac{kN}{s} \right\rfloor$ for some k

w.p. $\gtrsim 0.4$

Some more number theory s.t.

Given $\gamma = \left\lceil \frac{kN}{s} \right\rfloor$ $\quad \frac{\gamma}{N} = \frac{k}{s}$ for integers k and S.

(Euclid + continued fractions).

Gives us k, S.

Hidden Subgroup Problem

$$f : G \longrightarrow S$$

G is an additive group.

Given there is a subgroup $H \subset G$ s.t.

$\forall x \in G, \forall h \in H, \quad f(x+h) = f(x).$

and $\quad f(x) \neq f(y)$ if $(x-y) \notin H$.

Problem: Find H.

① Simon's algorithm.

$G = \mathbb{Z}_2^n$ or $\mathbb{Z}_N$ $\quad H = \{0, s\}$ for $s \neq 0$.

② Discrete logarithm

Fix prime p, $g \in \mathbb{Z}_p^*$ $\quad x \in \mathbb{Z}_{p-1}$

find s given (g, h) where $h = g^s \bmod p$.

$f(x) = (g^a h^{-b}) \bmod p$. for $(x = (a,b))$

$G = \mathbb{Z}_p^2 \quad H = \{(s,1)\}$.

$$f((a,b) + (s,1)) = g^{a+s} h^{-(b+1)} \bmod p$$

$$= g^a \overset{=h}{\cancel{g^s}} h^{-b} \cancel{h^{-1}} \bmod p.$$

$$= f(a,b)$$

How to implement QFT over $\mathbb{Z}_N$.

$$|g\rangle = \sum_{x \in [0,N-1]} g_x |x\rangle$$

$$\boxed{\begin{array}{c} \displaystyle = \sum_{\sigma \in [0,N-1]} \hat{g}(\sigma) |\chi_\sigma\rangle \\ \big\downarrow \text{ Q ckt.} \\ \displaystyle \sum_{\sigma \in [0,N-1]} \hat{g}(\sigma) |\sigma\rangle . \end{array}}$$

We want to implement:

$$\forall x, \quad |x\rangle \longrightarrow \frac{1}{\sqrt{N}} \sum_{\sigma \in \mathbb{Z}_N} \underbrace{\left(\chi_\sigma(x)\right)^*}_{= \omega^{-\sigma x}} |\sigma\rangle$$

Example: $N = 16$, $n = \lg_2 N = 4$.

$$|x\rangle \to \frac{1}{4}\left(\sum_{\sigma \in \mathbb{Z}_N} \omega^{-\sigma x} |\sigma\rangle \right)$$

$$= \frac{1}{4}\left(|0000\rangle + \omega^{-x}|0001\rangle + \omega^{-2x}|0010\rangle + \omega^{-3x}|0011\rangle \cdots\cdots + \omega^{-15x}|1111\rangle \right).$$

[Next time...]