Shor's Algorithm

Quantum Computation Basics (The Quantum Circuit Model)

Classical Circuits:

\[
\begin{align*}
\text{AND: } & \quad 00 \rightarrow 0 \quad 10 \rightarrow 0 \\
& \quad 01 \rightarrow 0 \quad 11 \rightarrow 1
\end{align*}
\]

Inputs are either 0 or 1, outputs are 0 or 1. These are called 'bits'. The 'speed' or 'runtime' is a measure of how many logic gates are used.

Quantum Circuits:

- Instead of bits, use 'qubits'. A qubit is \(\alpha|0\rangle + \beta|1\rangle \in \mathbb{C}\{|0\rangle, |1\rangle\}\)
  satisfying \(|\alpha|^2 + |\beta|^2 = 1\). Ortho-product (bits that are adjacent: \(|0\rangle \otimes |1\rangle = |01\rangle\).

- All quantum gates are reversible & have the same # of inputs & outputs. They can be thought of as unitary operators on \((\mathbb{C}^2)^\otimes n\).

- For us, a quantum computer can perform any unitary operation on one or two qubits. The runtime will measure the # of small gates.

Examples:

- Hadamard Gate: \(H: |0\rangle \rightarrow \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\), extend linearly. eg \(H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\).

- Controlled-NOT Gate (CNOT):
  - Classically, if \(x_1 = 1\), then \(y_2 = \bar{x}_2\); \(y_1 = x_1\) always.
  - Quantum, \(|10\rangle \rightarrow |10\rangle\), extend linearly. \(|11\rangle \rightarrow |11\rangle\), or partially collapses the state.

Entanglement & Measurement:

A two-qubit gate can entangle two qubits. Measurement of one qubit determines the other.

EPR Pair:

\[
\begin{align*}
\text{Output is } & \quad \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle \\
\text{Measurement of only one qubit determines the other one.}
\end{align*}
\]
Quantum Fourier Transform

First, let’s agree to not care about normalization too much.

The state $\sum_{x=0}^{2^n} |x\rangle |1\rangle$ is basically the same as $\left( \sum_{x=0}^{2^n} |x\rangle \right)^{\otimes n} \left( \sum_{x=0}^{2^n} |x\rangle \right)$.

Normally we’d represent a state as above, in the basis $\{|x\rangle : x \in \{0,1\}^n\}$ for $(\mathbb{C}^2)^\otimes n$. $(\mathbb{C}^2)^\otimes n$ can be thought of as the set of functions from $\{0,1\}^n$ to $\mathbb{C}$. Now think of $\{0,1\}^n$ as $\mathbb{Z}_N$ where $N = 2^n$, by identifying an integer in $[0, ..., N-1]$ with its binary representation.

Another basis for this vector space is the set of characters on $\mathbb{Z}_N$:

(A character is a homomorphism $\mathbb{Z}_N \to \mathbb{C}^\times$. So if $\chi$ is one then $\chi(0) = 1$, $\chi(1) = \chi(1)^n$, so (since $N = 0$) $\chi(1)$ is an $N^{th}$ root of unity.)

$\{\chi_x : x \in \mathbb{Z}_N\}$ where $\chi_x(x) = \omega^{x \cdot x}$, where $\omega = e^{2\pi i / N}$ is a primitive $N^{th}$ root of unity.

Theorem: $\{\chi_x : x \in \mathbb{Z}_N\}$ is an orthonormal basis for $\mathbb{C}^{\mathbb{Z}_N}$.

Proof: $\langle \chi_x | \chi_y \rangle = \sum_{x \in \mathbb{Z}_N} \chi_x(x)^* \chi_y(x) = \sum_{x \in \mathbb{Z}_N} \omega^{x \cdot y} = \begin{cases} N & \text{if } y = 0 \\ 0 & \text{if not} \end{cases}$.

So we can normalize by $\frac{1}{\sqrt{N}}$ to get a real ONB.

A state $g : \mathbb{Z}_N \to \mathbb{C}$ can be viewed as $\sum_{x \in \mathbb{Z}_N} g(x) |1\rangle |x\rangle$. It also has a representation $\sum_{x \in \mathbb{Z}_N} \hat{g}(y) |\chi_y\rangle$ (this defines $\hat{g}$).

The QFT takes $g \mapsto \hat{g}$. i.e., $\sum_{x \in \mathbb{Z}_N} g(x) |1\rangle = \sum_{y \in \mathbb{Z}_N} \hat{g}(y) |\chi_y\rangle \mapsto \sum_{y \in \mathbb{Z}_N} \hat{g}(y) |1\rangle$.

This is a unitary transformation since it takes one ONB to another. The QFT can be implemented with $(N+1) = n^2$ gates. It is denoted like this:

```
\[
x_n \xrightarrow{J} y_n \\
x_1 \\
\]
```
Given $M$, factor it: first, check if it's prime (this can be done quickly)

- find $r$, a nontrivial square root of 1 mod $M$ (this might not exist if $M$ is a power of an odd prime) (i.e. $r^2 \equiv 1 \pmod{M}$ but $r \not\equiv \pm 1 \pmod{M}$).
- Then $(r+1)(r-1) \equiv 0 \pmod{M}$, but $r+1, r-1 \not\equiv 0 \pmod{M}$. So both $r+1$ & $r-1$ share a factor with $M$. Let $c = \gcd(r-1, M)$. (GCD can be computed quickly).
- factor $c$ and $\frac{M}{c}$, return all prime factors. There will be about $\log M$ total recursive calls because $M$ has about $\log M$ prime factors.

How do we find $r$?

- pick a random $A \in \mathbb{Z}_M$. Compute $\gcd(A, M)$. if it's not 1, then it's a nontrivial factor of $M$ so we've made our algorithm a little faster. if it is 1, then $A \in \mathbb{Z}_M^\times$
- find the order $s$ of $A \in \mathbb{Z}_M^\times$. i.e., $A^s = 1$ but $A^k \not\equiv 1 \pmod{M}$ for some $k < s$.
- Suppose we are lucky and $s$ is even. Then $A^{s/2}$ is a square root of 1.
- Suppose we are even more lucky and $A^{s/2} \not\equiv 1$. Then let $r = A^{s/2}$.

**Lemma:** Suppose $M$ has $\geq 2$ distinct odd prime factors. Then if we pick $A \in \mathbb{Z}_M^\times$ uniformly at random, $\Pr(\text{ord}(A)\text{ is even } \& A^s \equiv 1) \geq \frac{1}{2}$.

So if we try many times and do not find such an $A$, we can be reasonably sure that $M$ is a power of an odd prime (needless to say $M$ is not even). So we can now binary-search for the $k^{th}$ root of $M$ (which takes $\log M$ time) where $k \in \{1, 2, \ldots, \log M\}$, so in total this will take $(\log M)^2$ time.

But how do we find $s = \text{ord}(A)$ quickly?
Problem: Given $f: \mathbb{Z}_N \rightarrow \{1, \ldots, 2^m\}$ = "colors" with the promise

That $f$ is periodic -- $\exists s \in \mathbb{Z}_N \setminus \{0\}$ s.t. $f(x) = f(x+s)$ $\forall x \in \mathbb{Z}_N$, AND $f(x) \neq f(y)$ whenever $x - y$ is not a multiple of $s$.

Find this $s$.

Solution Algorithm: Let $O$ be an oracle for $f: |X\rangle|0^m\rangle \rightarrow |X\rangle|f(x)\rangle$

- prepare the state $\frac{1}{\sqrt{N}} \sum_{x \in \mathbb{Z}_N} |x\rangle$, which can be done with lots of Hadamard gates:

- attach $10^m\rangle$ to get $\frac{1}{\sqrt{N}} \sum_{x \in \mathbb{Z}_N} |x\rangle \otimes 10^m\rangle$.

- apply the oracle to the state, obtaining $\frac{1}{\sqrt{N}} \sum_{x \in \mathbb{Z}_N} |x\rangle \otimes |f(x)\rangle$.

- measure the last $m$ qubits. You'll get a certain color $c$.

The overall state will collapse to a state $\sum_{x \in \mathbb{Z}_N} |x\rangle \otimes |c\rangle$ normalized.

The normalizing constant is $\sqrt{\frac{N}{s}}$ since there are $\frac{N}{s}$ preimages of $c$.

We can write this state as $\sum_{x \in \mathbb{Z}_N} \left( \sum_{f(x)=c} \frac{1}{\sqrt{N}} |x\rangle \right) \otimes |c\rangle$ where $f_c(x) = \left\{ \begin{array}{ll} 1 & \text{if } f(x) = c \\ 0 & \text{otherwise} \end{array} \right.$

- apply the QFT to the first $n$ qubits, which currently store $f_c \in \mathbb{Z}^{\mathbb{Z}_N}$.

Now, let $t$ be the first element of $\mathbb{Z}_N$ for which $f(t) = c \& f_c(t) \neq 0$.

Then $f_c(x) = \left\{ \begin{array}{ll} 1 & \text{if } f(t) = c \& f_c(t) \neq 0 \\ 0 & \text{otherwise} \end{array} \right.$

- $f_c(x) = \sum_{y \in \mathbb{Z}_N} \frac{1}{\sqrt{N}} \sum_{s \in \mathbb{Z}_N} \chi_{N}^{y}(x-s) \rightarrow \sum_{y \in \mathbb{Z}_N} \frac{e^{-i \omega x y}}{\sqrt{N}} |y\rangle$ QFT

Measuring this state yields some $y \in \mathbb{Z}_N$, and each $y$ has probability $\left| \frac{e^{-i \omega x y}}{\sqrt{N}} \right|^2 = \frac{1}{N}$ of occurring (this is completely ind. of $c$).

- we can sample from this to obtain a few multiples of $\frac{N}{s}$, then take their GCD. $\gcd(aN, bN) = \gcd(a, b) \cdot N$, so we'll get $\frac{N}{s}$ if $a$ $b$ are coprime. And the probability of this happening goes to $\frac{1}{\pi s^2}$ as $N$ gets large, so for large enough $N$ we don't have to sample too many times. Having $\frac{N}{s}$, divide $N$ by it to get $s$. 

Order-Finding Algorithm

Problem: Given $m$-bit $M$ and $A$, find $\text{ord}(A)$ in this group.

Solution Algorithm: let $\text{poly}(m)$ be a large polynomial like $m^{10}$. Let $N = 2^{\text{poly}(m)}$.

Define $f: \{0, \ldots, N-1\} \rightarrow \mathbb{Z}_N$ by $f(x) = A^x \mod M$. $A^0 = A^s = 1$ and all powers in between are distinct, so $f$ is almost $s$-periodic.

We don't have $s \mid N$, so we modify the period-finding algorithm to fix this.

Start as before: $\frac{1}{\sqrt{N}} \sum_0^{N-1} |x\rangle \otimes |0\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_0^{N-1} |x\rangle \otimes (A^x \mod M) \rightarrow$ measure & collapse.

We measure a color $c$, let $D$ be the number of times $c$ occurs, either $[N/s]$ or $[N/s]$.

The collapsed state is $\frac{1}{\sqrt{D}} \sum_{j=0}^{D-1} |x+s\cdot j\rangle \otimes |c\rangle$ where $b$ is minimal s.t. $A^b \equiv c \mod M$.

Apply the QFT. Note that $|1\rangle = 1 \frac{1}{\sqrt{N}} \sum_0^{N-1} \chi_y(x) \chi_y \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \omega^{-y\cdot x} |y\rangle$.

So our collapsed state becomes $\frac{1}{\sqrt{D}} \sum_{j=0}^{D-1} \sum_{y=0}^{N-1} \frac{1}{\sqrt{N}} \omega^{-y\cdot s\cdot j} |y\rangle$, so the probability of measuring a particular $y$ from this state is $\frac{1}{DN} \left| \sum_{j=0}^{D-1} \omega^{-y\cdot s\cdot j} \right|^2 = \frac{1}{DN} \left| \sum_{j=0}^{D-1} \omega^{-y\cdot s\cdot j} \right|^2$.

We'd like to get a $y$ such that $y_s$ is small mod $N$. Specifically, if $-\frac{S}{2} \leq y_s \mod N \leq \frac{S}{2}$ then $|y_s - kN| \leq \frac{S}{2}$ for some $k$.

Equivalently, $\left| \frac{y}{N} - \frac{k}{S} \right| \leq \frac{1}{2N}$. So $\frac{y}{N}$ is a good approximation to $\frac{k}{S}$ (better if we take $N$ and $\text{poly}(m)$ to be larger).

Now $k$ was chosen randomly in $\{0, \ldots, S-1\}$, so with probability at least $\frac{1}{\log S} > \frac{1}{m}$, $k$ and $s$ are coprime. So by computing $\frac{k}{S}$ using Euclid's algorithm and stopping when the remainder is small, not 0, i.e. expanding $\frac{k}{S}$ into a continued fraction & stopping early) we can find $S$.

(to be sure we have the right $S$, find two $k$ and $k'$ that give $s_2$ and $s_1$ co-prime).

The probability of finding such a $y$ is positive, at least $\frac{1}{10}$.

Intuitively, if $y$ is small then all of $\omega^{-y\cdot s\cdot j}$ will be close to 1, so they will add positively & not cancel each other out too much.