CS6846 – Quantum Algorithms and Cryptography

Shor's Algorithm

Instructor: Shweta Agrawal, IIT Madras
Email: shweta@cse.iitm.ac.in

Discrete log

G, g generator. Given $h = g^a \bmod p$.

Want: a.

$$f(x, y) = g^x h^{-y} = g^{x-ay}$$

$$f(x+a, y+1) = g^{x+a} h^{-y-1}$$

$$= g^{x+a-ay-a}$$

$$= g^{x-ay}.$$

Period is $(a, 1)$.

Factoring:

Given $N = p \cdot q$, want p and q

Order Finding:

Input: integers x & N, $\gcd(x, N) = 1$

Output: smallest r s.t. $x^r \equiv 1 \ (N)$.

Claim: Factoring reduces to order finding.

To prove this, we show some lemmas.

Lemma: Given N & x s.t. x is a nontrivial square root of 1 mod N, can find factors of N.

↓ $x \not\equiv \pm 1 \mod N$ & $x^2 \equiv 1 \mod N$

Proof: $x^2 \equiv 1 \bmod N \Rightarrow x^2 - 1 \equiv 0 \bmod N$

$(x+1)(x-1) \equiv 0 \bmod N$. But $x \not\equiv \pm 1 \,(N)$.

Hence $1 < x < N-1$,

$\gcd(x-1, N)$ or $\gcd(x+1, N)$

give a non-trivial factor of N.

Lemma: Let p be an odd prime & x uniformly chosen in $\mathbb{Z}_p^*$ i.e. $\{1, \ldots, p-1\}$.

Then $\text{ord}(x)$ is even w.p. $\geq \frac{1}{2}$.

Proof: By Fermat's little theorem

$$x^{p-1} \equiv 1 \bmod p.$$

Can write $x = g^k$ for some k.

$\Pr(k \text{ is odd}) = \frac{1}{2}$. Assume k is odd.

Let r denote order of x.

$x^r \equiv 1 \bmod p$, $g^{kr} \equiv 1 \bmod p$.

$\Rightarrow p-1 \mid kr \Rightarrow r$ is even.

($p-1$: even, k: odd)

Lemma: $N = p \cdot q$, where p & q are odd primes. Let $x \leftarrow \mathbb{Z}_N^*$. If $\gcd(x, N) = 1$ then with prob $\geq \frac{3}{8}$, ord(x) is even and $x^{\frac{r}{2}} \not\equiv \pm 1 \mod N$.

$x^r \equiv 1 \mod N$, $(x^{r/2})^2 \equiv 1 \mod N$

& we are saying $x^{r/2} \not\equiv \pm 1 \mod N$

non trivial sq root of 1 mod N.

Proof: Apply CRT.

Choosing $x \leftarrow \mathbb{Z}_N^*$ is equivalent to choosing $x_1 \leftarrow \mathbb{Z}_p^*$ & $x_2 \leftarrow \mathbb{Z}_q^*$.

Let $r_1 \triangleq ord(x_1)$ & $r_2 \triangleq ord(x_2)$.

By previous lemma, since x_1 & x_2 are chosen randomly & p & q are odd primes,

$$Pr(r_i \text{ is even}) \geq \frac{1}{2} \text{ for } i \in \{1,2\}.$$

$$\therefore Pr(r_1 \text{ and } r_2 \text{ are both odd}) < \frac{1}{4}.$$

$$\therefore Pr(r_1 \text{ or } r_2 \text{ is even}) \geq \frac{3}{4}$$

Note that r is even when r_1 or r_2 is even.

$$\therefore Pr(r \text{ is even}) \geq \frac{3}{4}.$$

Since r is even, consider $x^{r/2}$

$(x^{r/2})^2 \equiv 1 \bmod N$. So $x^{r/2}$ is a square root of 1 mod N.

The only sq roots of 1 mod N are $(1,1)$, $(-1,-1)$, $(1,-1)$, $(-1,1)$

$\Pr(x^{r/2} \not\equiv \pm 1 \bmod N) \geq \frac{1}{2}$.

$f_x(a) = x^a \bmod N$.

Shor's Algorithm: (ord(x) = r)

Simple Case.

Let $\underline{\underline{Q}} \gg \underline{\underline{N^2}}$. Assume $r \mid Q$.

Read : $r \nmid Q$.

① Registers $|0\rangle \otimes |0\rangle$
sufficiently long

② Prepare i/p superposition.

$$\frac{1}{\sqrt{Q}} \sum_{a=0}^{Q-1} |a\rangle |0\rangle$$

3. $f_x(a) = x^a \bmod N$. (Remember $\mathrm{ord}(x) = r$)

Note that f is distinct on $[0, \ldots, r-1]$

since otherwise $\mathrm{ord}(x)$ would be smaller.

Apply function oracle to get

$$\frac{1}{\sqrt{Q}} \sum_{a=0}^{Q-1} |a\rangle |f(a)\rangle.$$

4. Measure 2nd register.

$$\frac{1}{\sqrt{Q/r}} \sum_{j=0}^{\frac{Q}{r}-1} |jr + l\rangle |f(l)\rangle.$$

5. Apply QFT. (Drops ℓ)

$$\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \omega^{k\ell} \left| k \cdot \frac{q}{r} \right\rangle.$$

6. Measure. Get $k\frac{q}{r}$.

$\gcd(k, \frac{q}{r}) = 1$ with good prob.

Then computing $\gcd(q, \frac{kq}{r}) \Rightarrow \frac{q}{r} \Rightarrow r$

General Case: Need to analyze $\lfloor \frac{q}{r} \rfloor$.

Can show that we get "constructive interference" at pts that are close to multiples of $\frac{q}{r}$.