Order Finding - page 1

Tuesday, November 13, 2018 6:29 PM

In this lecture we will give a quantum algorithm to solve Order Finding:

Input: integers x + N such that $\gcd(x,N)=1$.
Output: smallest r such that $x^r \equiv 1 \mod N$.

Next lecture we will show: r always exists.
+ poly time alg for Order Finding $\Longrightarrow$ poly time alg for Factoring.

Note the number of bits required to specify N is: $\lceil \log_2 N \rceil$

So the "size" of the input is $O(\log N)$

We want an algorithm that is polynomial in $\log(N)$ e.g. $O((\log N)^k)$.

(not $O(N^k)$)

For crypto protocols N is ~ 200 digits.

$$N \sim 10^{200}$$

$\log_2 N = \underbrace{\log_2 10}_{\text{const.}} \log_{10} N$

Note # bits to specify $N = \lceil \log_2 N \rceil$
digits to specify $N = \lceil \log_{10} N \rceil$ $\Big\}$ $O(\log N)$.

Order Finding - page 2

Tuesday, November 13, 2018 6:46 PM

Addition and Multiplication mod N can be done in time $O(\log^2 N)$.

What about $x^y \bmod N$? $x, y \le N$.

Can't afford.

```
prod = x
for k = 2 to y
    prod = prod · x mod N.
Return (prod).
```

Instead:

s: $\overset{-}{x}$ $\overset{1}{x^2}$ $\overset{2}{x^{2^2}}$ $\overset{3}{x^{2^3}}$ ...

$p = 1$ (partial result).
$s = x$ (current x^{2^k})
$r = y$ (used to get binary expansion of y.

```
While (r > 0)
    if (r mod 2 = 1)
        p = p·s mod N.
    s = s·s
    r = r DIV 2.
End.
Return (p).
```

$x^{13} = x^{2^3} \cdot x^{2^2} \cdot x^{2^0}$

$13 = (1101)_2$.

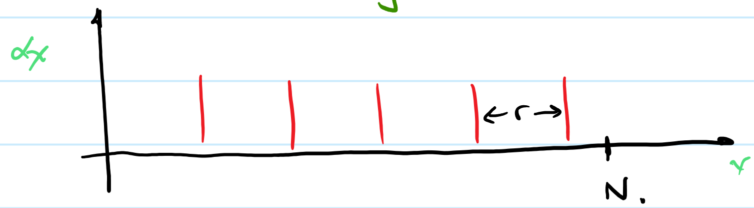
Each iteration $O(\log^2 N)$.
#iterations $O(\log y) = O(\log N)$.

Order Finding - page 3

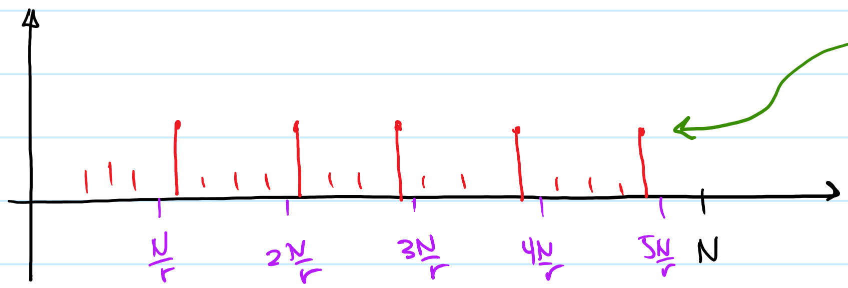
Tuesday, November 13, 2018 6:57 PM

Here's what we'll need from the last lecture:

Start with $|\Phi_r\rangle = \sum_{j=0}^{s-1} \frac{1}{\sqrt{s}} |kr+\ell\rangle$ $0 \le \ell \le r-1$, $s = \lfloor \frac{N}{r} \rfloor$



Now apply DFT_N: $\cancel{DFT_N} |\Phi_r\rangle = \sum_{a=0}^{N-1} \hat{\alpha}_a |a\rangle$



amplitude at least $\frac{1}{2\sqrt{2}\sqrt{r}}$

We showed that if we measure with probability $\ge \frac{c}{\log\log r}$ we get a value for "a"

such that ① $|ar - kN| \le r/2$ for some k $\rightarrow$ $|a - k\frac{N}{r}| \le 1/2.$

② $\gcd(k,r) = 1.$

We will show that this is sufficient information to recover r.

Order Finding - page 4

Tuesday, November 13, 2018 7:16 PM

r smallest $x^r \equiv 1 \mod N$.

$x^l \equiv x^{l+r} = x^{l+2r} = \cdots$
$x^l \cdot x^r$

Algorithm for Order Finding:

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

Q is a large power of 2 $Q \gg N^2$ $Q = 2^q$.

We will use two registers: $|\text{———}\rangle|\text{———}\rangle$
\# mod Q — q qubits; \# mod N — $\lceil \log N \rceil$ qubits

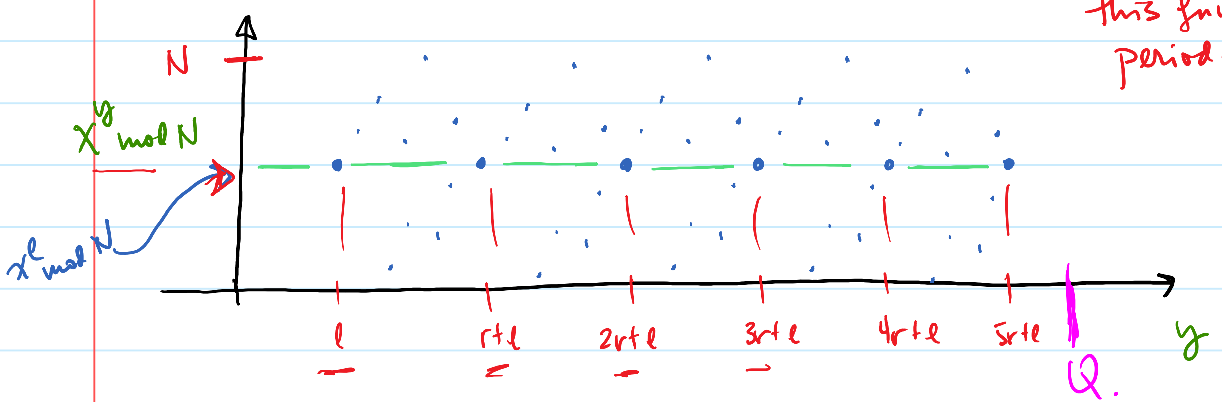
(1) Start with $|0 \cdots 0\rangle \otimes |0 \cdots 0\rangle$

(2) $H^{\otimes q}$ on register 1 to get: $\frac{1}{\sqrt{Q}} \sum_{y=0}^{Q-1} |y\rangle|0\rangle$

(3) Compute $x^y \mod N$ $\frac{1}{\sqrt{Q}} \sum_{y=0}^{Q-1} |y\rangle|x^y \mod N\rangle$

x^l

this function is periodic in r!



(4) Measure 2nd register. If 2nd register $\equiv x^l \mod N$
1st register is an even superposition of
$|jr+l\rangle$ $0 \le j \le \left\lfloor \frac{N}{r} \right\rfloor - 1$.

$\frac{1}{\sqrt{s}} \sum_{j=0}^{s-1} |jr+l\rangle|x^l \mod N\rangle$ $s = \left\lfloor \frac{Q}{r} \right\rfloor$

Order Finding - page 5

Tuesday, November 13, 2018 7:30 PM

$$\Rightarrow \frac{1}{\sqrt{s}} \sum_{j=0}^{s-1} |jr+\ell\rangle \cancel{|x^\ell \bmod N\rangle} \qquad s = \left\lfloor \frac{Q}{r} \right\rfloor$$

(5) Ignore 2^{nd} register and apply QFT (mod Q) to the first register.

With probability $\geq \frac{c}{\lg\lg r}$ will get a such that

$$\frac{|ar - kQ|}{rQ} \leq \frac{r/2}{rQ} \quad \text{where } \gcd(k,r) = 1.$$

(6) Use a, Q to find k + r

$$\left| \frac{a}{Q} - \frac{k}{r} \right| \leq \frac{1}{2Q} \leq \frac{1}{2r^2} \qquad Q \gg N^2 \gg r^2.$$

We will use continued fractions to find k + r.

This is why it's important that $\gcd(k,r) = 1$.

All we have is an estimate of k/r.

For example if $k = 4$ and $r = 14$ $\quad \frac{k}{r} = \frac{4}{14} = \frac{2}{7}$

would recover 2 + 7 (not 4 + 14).

Order Finding - page 6

Tuesday, November 13, 2018 7:41 PM

Let $\gamma = a/N$. Have $\left|\gamma - \frac{k}{r}\right| \leq \frac{1}{2r^2}$.

Use continued fraction representation of γ to get a series of rational approximations to γ. One of those approximations will be k/r.

A real number γ can be approximated by a sequence of integers $a_0, a_1, a_2, \ldots, a_n$ as:

$$\gamma \approx a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots \frac{1}{a_n}}}}$$

Order Finding - page 7

Tuesday, November 13, 2018 7:47 PM

Best illustrated with an example $\gamma = 7.27$

$$7 + \frac{27}{100} = 7 + \frac{1}{100/27} = 7 + \frac{1}{3 + \frac{19}{27}}$$

$$= 7 + \frac{1}{3 + 1/(27/19)} = \frac{1}{3 + \frac{1}{1 + \frac{8}{19}}}$$

$$= 7 + \frac{1}{3 + \frac{1}{1 + 1/(19/8)}} = 7 + \frac{1}{3 + \frac{1}{1 + \frac{1}{2 + 3/8}}}$$

$$= 7 + \frac{1}{3 + \frac{1}{1 + \frac{1}{2 + \frac{1}{2 + 2/3}}}}$$

$$= \underset{a_0}{7} + \frac{1}{\underset{a_1}{3} + \frac{1}{\underset{a_2}{1} + \frac{1}{\underset{a_3}{2} + \frac{1}{\underset{a_4}{2} + \frac{1}{\underset{a_5}{1} + \frac{1}{\underset{a_6}{2}}}}}}} = \frac{727}{100}$$

$P_0 = 7$

$Q_0 = 1$

Could have stopped at a_3 to get:

$$7 + \frac{1}{3 + \frac{1}{1 + \frac{1}{2}}} = \frac{80}{11} \approx 7.27$$

$80 = P_3$

$11 = Q_3$

Order Finding - page 8

Tuesday, November 13, 2018 8:07 PM

$(a_0, a_1, \ldots, a_n)$

$\frac{P_0}{Q_0} = \frac{a_0}{1}$ $\frac{P_1}{Q_1} = a_0 + \frac{1}{a_1}$

We get a series of approximations to γ.

$$\frac{P_0}{Q_0} \quad \frac{P_1}{Q_1} \quad \frac{P_2}{Q_2} \quad \cdots \quad \frac{P_n}{Q_n} = \gamma.$$

$$Q_0 < Q_1 < Q_2 < \cdots < Q_n$$

Smallest

$x^{Q_j} \equiv 1 \bmod N$.

Two important facts:

- If γ is rational, eventually $\frac{P_n}{Q_n} = \gamma$.
- $\frac{P_j}{Q_j}$ is the best approximation to γ by any fraction whose denominator is $\leq Q_j$.

Theorem (Proven in appendix of Nielsen and Chuang)

If $\left|\gamma - \frac{k}{r}\right| \leq \frac{1}{2r^2}$ then $k = P_j$ for some j
$r = Q_j$

Can test if $x^{Q_j} \bmod N = 1$

pick the smallest Q_j for which this holds.