9: Factoring

Friday, April 16, 2021 12:23 PM

Public Key Cryptography:

Step 3

Publicly agreed on function

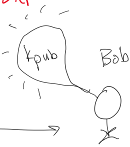
$f(m, K_{pub}) = \overline{m}$

encoded

Alice has message m to send to Bob

Eve learns $\overline{m}$, but can't decode without factoring

Step 2:



Bob

Kprivate

Step 1: Create Kpub, Kprivate

public, private keys

have a special relationship

Step 4:

Bob does

$g(\overline{m}, K_{private}) \Rightarrow m$

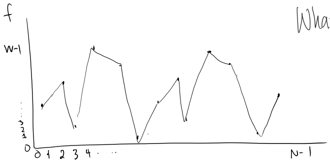
Factoring: 15? ⇒ 3, 5

Takes ~exponential time for large #'s.

Factoring reduces (via some number theory) to period finding

Period Finding Problem

- $f: \{0,1,2,\dots,N-1\} \to \{0,1,2,\dots,W-1\}$
- f has (unknown) period r. $f(x) = f(x+r)$ $\forall x \leq N-1-r$
- No repeats within a period $(f(i) \neq f(j)$ if $|i-j| < r)$
- $N > r^2$ (many repeats)



What is r?

times need to evaluate f(x) for some x

What is classical query complexity of period finding?

A. $O(\log r)$ B. $O(r)$ C. $O(r^2)$ $O(N)$

$\uparrow$ Brute force search

Bits to Digits

Classically, when designing algorithms, we don't write everything in base 2, even though computer is made of bits.

$011 \to 3$

$$|011\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\0\\0\\1\\0\\0\\0\\0\end{pmatrix} \to |3\rangle$$

$$\frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle + |11\rangle\right) \to \frac{1}{2}\left(|0\rangle + |1\rangle + |2\rangle + |3\rangle\right)$$
$$= \frac{1}{4} \sum_{i=0}^{3} |i\rangle$$

U_f's action on standard basis states:

$$U_f \underset{\substack{\uparrow \\ \text{N-dimensional} \\ \text{standard basis state} \\ \text{(could create with} \\ \log_2 N \text{ qubits)}}}{|x\rangle} \underset{\substack{\nwarrow \\ \text{W-dim. vector} \\ \text{s.b. state}}}{|y\rangle} = |x\rangle |y + f(x) \bmod W\rangle$$

Q: If $N = 100$, $W = 50$, what is the size (dimension) of the vector space that U_f acts on?

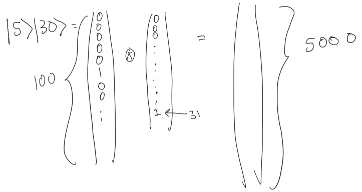
A) 150   B) 5000   C) $2^{100} \cdot 2^{50}$ D) 2^{5000}

Q: If $N = 100$, $W = 50$, $f(5) = 23$, what is

$U_f |5\rangle |30\rangle$

A) $|5\rangle|2\rangle$ B) $|5\rangle|3\rangle$ C) $|28\rangle|30\rangle$

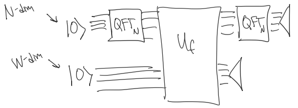
D) Not enough information



Standard Basis Measurement : $\{|0\rangle, |1\rangle, |2\rangle, \dots |t-1\rangle\}$

$|\psi\rangle = \sum_{x=0}^{t-1} a_x |x\rangle$ Measure $|\psi\rangle$ in standard basis → outcome $|j\rangle$ with probability $|a_j|^2$

Quantum Circuit For Factoring



Alg. For Factoring

Run circuit twice. Get outcomes y, y'

Do classical post-processing on y, y' → get r with high probability. Check by querying $f(0), f(r)$.

QFT

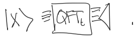
QFT_t is a $t \times t$ matrix (acts on t-dimensional vector space, $\log_2 t$ qubits)

For standard basis state $|x\rangle$: ← base 10

← regular multiplication $x \cdot y$

$$QFT_t |x\rangle = \frac{1}{\sqrt{t}} \sum_{y=0}^{t-1} e^{\frac{2\pi i x y}{t}} |y\rangle$$

Q:



.

What is probability of outcome $|y\rangle$?

A) $\frac{1}{t}$ B) $\frac{1}{\sqrt{t}}$ C) $\frac{xy}{t}$ d $\frac{y}{t}$

$$QFT_t|x\rangle = \frac{1}{\sqrt{t}} \sum_{y=0}^{t-1} e^{2\pi i xy/t} |y\rangle$$

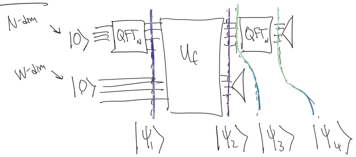
Probability of outcome $|y\rangle$: $\left| \frac{1}{\sqrt{t}} e^{2\pi i xy/t} \right|^2$

$$= \frac{1}{\sqrt{t}} e^{2\pi i xy/t} \cdot \frac{1}{\sqrt{t}} e^{-2\pi i xy/t}$$

$$= \frac{1}{t}$$

All outcomes equally likely.

Analyze!

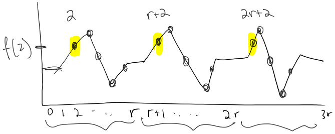


$$\star\ |\psi_1\rangle = (QFT_N|0\rangle)|0\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{t-1} e^{\overset{\swarrow e^0=1}{2\pi i y\cdot 0/t}} |y\rangle|0\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{t-1} |y\rangle|0\rangle \quad \text{(change } y \text{ to } x\text{)}$$

$$\star\ |\psi_2\rangle = U_f \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle|0\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} U_f|x\rangle|0\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle_A |f(x)\rangle_B$$

Next: Measure B in standard basis. Partial Measurement

⇒ Group standard basis states.



$$(|2\rangle + |r+2\rangle + |2r+2\rangle + \cdots)_A |f(2)\rangle_B$$

$$|\psi_2\rangle = \frac{1}{\sqrt{N}} \sum_{b=0}^{r-1} \sum_{m=0}^{m_b-1} |mr+b\rangle_A |f(b)\rangle_B$$

m_b = # of iterations in which b appears

Now B is grouped by standard basis states!

⇒ Normalize

$$|\psi_2\rangle = \frac{\alpha_b}{\sqrt{N}} \sum_{b=0}^{r-1} \left(\frac{1}{\alpha_b} \sum_{m=0}^{m_b-1} |mr+b\rangle_A \right) |f(b)\rangle_B$$

Q: What is α_b (approximately)?

A): $\sqrt{\frac{1}{b}}$ B) $\sqrt{\frac{1}{m}}$ C) $\sqrt{\frac{N}{r}}$ D) $\sqrt{\frac{N}{br}}$

$$\frac{1}{\alpha_b}\sum_{m=0}^{m_b}|mr+b\rangle = \sum_{m=0}^{m_b-1}\frac{1}{\alpha_b}|mr+b\rangle.$$

Normalization $\frac{m_b-1}{|\alpha_b|^2} = 1 \rightarrow \alpha_b = \sqrt{m_b}$

m_b is number of times value $f(b)$ appears in f.
This is $\frac{N}{r}$ (rounded up or down to integer). $\alpha_b \approx \sqrt{\frac{N}{r}}$

for now, won't worry about rounding

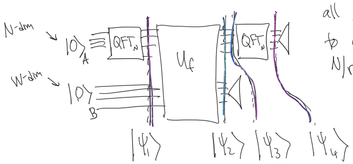
$$|\psi_2\rangle = \frac{\alpha_b}{\sqrt{N}} \sum_{b=0}^{r-1} \left(\frac{1}{\alpha_b} \sum_{m=0}^{m_b-1} |mr+b\rangle_A \right) |f(b)\rangle_B$$

$$|\psi_2\rangle \approx \frac{1}{\sqrt{r}} \sum_{b=0}^{r-1} \left(\sqrt{\frac{r}{N}} \sum_{m=0}^{N/r-1} |mr+b\rangle \right) |f(b)\rangle$$

Measure B: get every element of range of f with equal probability (1/r). A collapses to

☆ $|\psi_3\rangle = \sqrt{\frac{r}{N}} \sum_{m=0}^{N/r-1} |mr+b^*\rangle$ if outcome $|f(b^*)\rangle$ is measured.

Went from a superposition of all N standard basis states to a superposition of only N/r standard basis states



☆ $|\psi_4\rangle = QFT_N \sqrt{\frac{r}{N}} \sum_{m=0}^{N/r-1} |mr+b^*\rangle = \sqrt{\frac{r}{N}} \sum_{m=0}^{N/r-1} QFT_N |mr+b^*\rangle$

$= \sqrt{\frac{r}{N}} \frac{1}{\sqrt{N}} \sum_{m=0}^{N/r-1} \sum_{y=0}^{N-1} e^{2\pi i y(mr+b^*)/N} |y\rangle$

Need amplitude of $|y\rangle$ to analyze measurement

Switch order of summations

$= \frac{\sqrt{r}}{N} \sum_{y=0}^{N-1} \sum_{m=0}^{N/r-1} e^{2\pi i y(mr+b^*)/N} |y\rangle$

Amplitude of $|y\rangle \Rightarrow \frac{\sqrt{r}}{N} \sum_{m=0}^{N/r-1} e^{2\pi i y(mr+b^*)/N}$

$= \frac{\sqrt{r}}{N} \sum_{m=0}^{N/r-1} e^{2\pi i y mr/N} \boxed{e^{2\pi i y b^*/N}}$

↑ No m, can factor

$= e^{2\pi i y b^*/N} \frac{\sqrt{r}}{N} \sum_{m=0}^{N/r-1} e^{2\pi i y mr/N}$

☆ Prob of outcome $|y\rangle = \left| e^{2\pi i y b^*/N} \frac{\sqrt{r}}{N} \sum_{m=0}^{N/r-1} e^{2\pi i y mr/N} \right|^2$

$= \frac{r}{N^2} \left| \sum_{m=0}^{N/r-1} e^{2\pi i y mr/N} \right|^2$

$= \frac{r}{N^2} \left| \boxed{\sum_{m=0}^{N/r-1} \left(e^{2\pi i y r/N}\right)^m} \right|^2$

b^* goes away! Works for any b^*

Use geometric series formula:

$$\boxed{\sum_{m=0}^{t-1} a^m} = \begin{cases} \frac{1-a^t}{1-a} & \text{if } a \neq 1 \\ t & \text{if } a = 1 \end{cases}$$

$a = e^{2\pi i y r/N} = 1 \longleftrightarrow yr = \overset{\text{integer}}{k} N \rightarrow \frac{N}{r}$

$a = e^{2\pi i y r/N} \neq 1 \longleftrightarrow yr \neq kN \rightarrow \frac{1 - \left(e^{2\pi i y r/N}\right)^{N/r}}{1 - e^{2\pi i y r/N}} = \frac{1 - e^{2\pi i y}}{1 - e^{2\pi i y r/N}} = 0$

$$\text{Prob of outcome } |y\rangle = \begin{cases} \frac{r}{N^2} \cdot \left(\frac{N}{r}\right)^2 = \frac{1}{r} & \text{if } y = kN/r \\ 0 & \text{else} \end{cases}$$

What does it mean?

If learn $\frac{Nk}{r}$, $\frac{Nk'}{r}$ for some $k, k' \in \mathbb{Z}$, can learn r w.h.p. (see pset).

Query Complexity

- Quantum: $O(1)$
- Classical: $O(r)$ Wrong: $O(\sqrt{r})$

Time Complexity of Factoring

To factor n, set $N = n$

- QFT_N: $O(\log_2^2 N)$ gates
- U_f (for factoring): $O(\log_2 N)$ gates

$\}$ $O((\log_2 N)^2)$ time

Classical, Best Alg. → $e^{O((\log_2 N)^{1/3})}$ number field sieve algorithm

Nearly exponential speed-up!

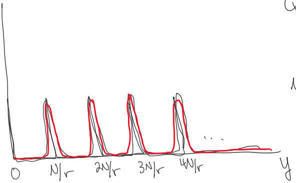
Some details: What if N/r is not an integer!

$$\frac{1}{N}\left\lceil\frac{r}{N}\right\rceil \cancel{\frac{r}{N^2}} \left| \sum_{m=0}^{\lceil N/r \rceil -1} e^{2\pi i y m r/N} \right|^2 \Rightarrow \frac{r}{N^2}\cdot\frac{N^2}{r^2} = \frac{1}{r} \quad \text{if } y = gN/r$$

$$\downarrow$$

$$\sum_{m=0}^{\lceil N/r \rceil -1} \left(e^{2\pi i y r/N}\right)^m = \begin{cases} \approx N/r & \text{if } y = gN/r \text{ for integer } g \\ \approx \dfrac{1-\left(e^{2\pi i y r/N}\right)^{N/r}}{1-e^{2\pi i y r/N}} = \dfrac{1-e^{2\pi i y}}{1-e^{2\pi i y r/N}} = 0 & \text{else} \end{cases}$$

$$\frac{r}{N^2}\cdot\frac{N^2}{r} = \frac{1}{r} \quad \text{if } y = gN/r$$



Not a standard basis state... not even a possible outcome!

Query twice, get outcomes

$|g_1 N/r\rangle, |g_2 N/r\rangle \Leftarrow$ very close to multiples of N/r.

Method to get r... see Pset.

See Pset