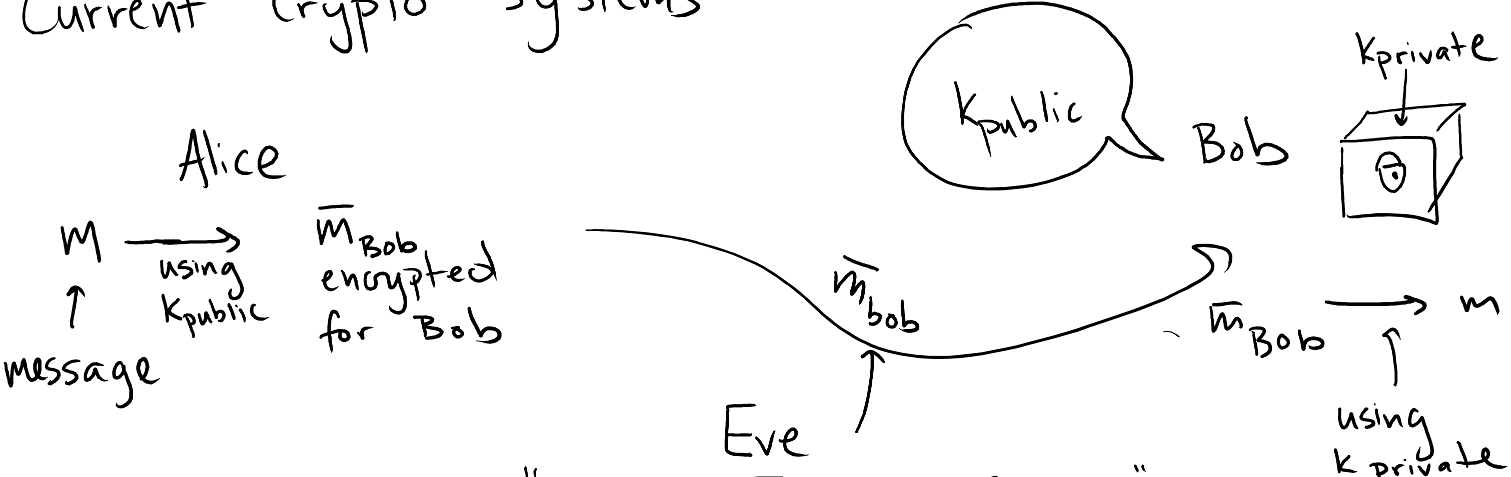
S.KIMMEL

Current Crypto Systems

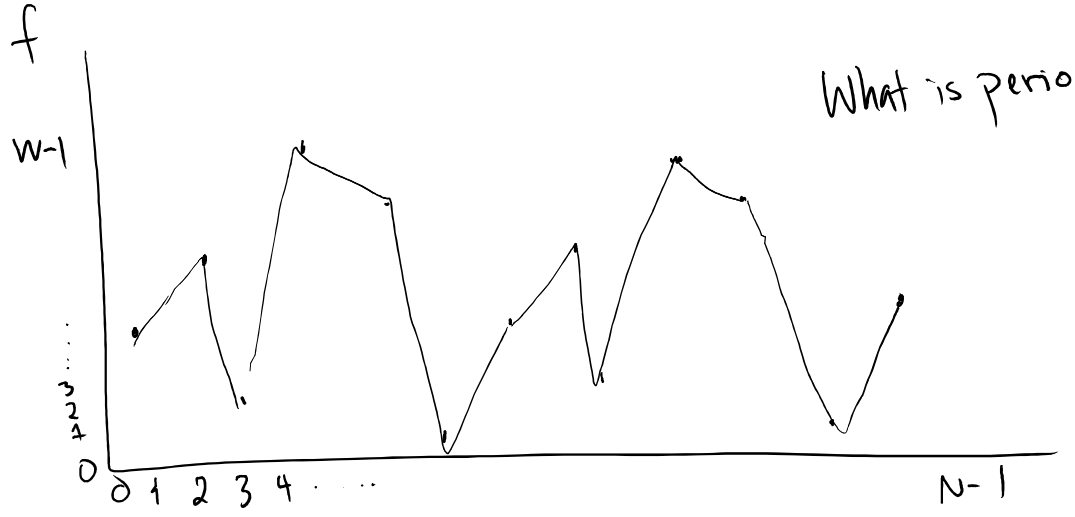


"If only I could factor..."

If you can find the period of a specific function, then can factor, then can break crypto systems

Period Finding Problem

- f has domain $[N]$. Notation: $[N] = \{0,1,2,\dots N-1\}$
- Range of f is $[W]$, In other words: $f:[N]\rightarrow[w]$
- f periodic period $r \Rightarrow f(x) = f(x+r)$
- no repeats within a period: $(f(i) \neq f(j) \text{ if } |i-j| < r)$
- $N > r^2$



What is period?

What is classical query complexity of period finding?

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

- Let U_f act on $N \times R$ dimensional quantum system

$$U_f|x\rangle|y\rangle = |x\rangle|y+f(x) \bmod W\rangle$$

$$\underset{N\text{-dim}}{\uparrow} \quad \underset{W\text{-dim}}{\uparrow}$$

✻ Changing standard basis labels:

$$\begin{array}{ccccccc}
 & & \text{Old Label} & \text{Vector} & \text{New Label} & & \\
 & & |00\rangle = & \begin{pmatrix}1\\0\\0\\0\end{pmatrix} & = |0\rangle & & \\
\text{Binary Rep} & \Rightarrow & |01\rangle = & \begin{pmatrix}0\\1\\0\\0\end{pmatrix} & = |1\rangle & \Leftarrow & \text{Base 10 Rep} \\
 & & |10\rangle = & \begin{pmatrix}0\\0\\1\\0\end{pmatrix} & = |2\rangle & &
\end{array}$$

What is classical query complexity of period finding?

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

$\Uparrow$

Ask $f(1), f(2), f(3)\ldots$ until get a repeat value. Need to look at r values

- Let U_f act on $N \times R$ dimensional quantum system

$$U_f \underset{\substack{\uparrow \\ N\text{-dim}}}{|x\rangle} \underset{\substack{\uparrow \\ W\text{-dim}}}{|y\rangle} = |x\rangle |y + f(x) \bmod W\rangle$$

✲ Changing standard basis labels:

	Old Label	Vector	New Label	
	$\lvert 00\rangle =$	$\begin{pmatrix}1\\0\\0\\0\end{pmatrix}$	$= \lvert 0\rangle$	
Binary Rep $\Rightarrow$	$\lvert 01\rangle =$	$\begin{pmatrix}0\\1\\0\\0\end{pmatrix}$	$= \lvert 1\rangle$	$\Leftarrow$ Base 10 Rep
	$\lvert 10\rangle =$	$\begin{pmatrix}0\\0\\1\\0\end{pmatrix}$	$= \lvert 2\rangle$	

$$f:\underset{\underset{\text{domain}}{\uparrow}}{[100]} \to \underset{\underset{\text{range}}{\uparrow}}{[50]} \qquad \text{Suppose } f(5)=23$$

$$U_f|5\rangle|30\rangle = |5\rangle|30+23 \mod 50\rangle$$

$$= |5\rangle|3\rangle$$

$$= \text{length } 100 \rightarrow \begin{pmatrix}0\\0\\0\\0\\1\\0\\\vdots\end{pmatrix} \otimes \begin{pmatrix}0\\0\\1\\0\\0\\\vdots\end{pmatrix} \leftarrow \text{length } 50$$

Basic Algorithm:

1. Prepare $|0\rangle_A |0\rangle_B$ ← N-dim ← W-dim

2. Apply QFT_N to A

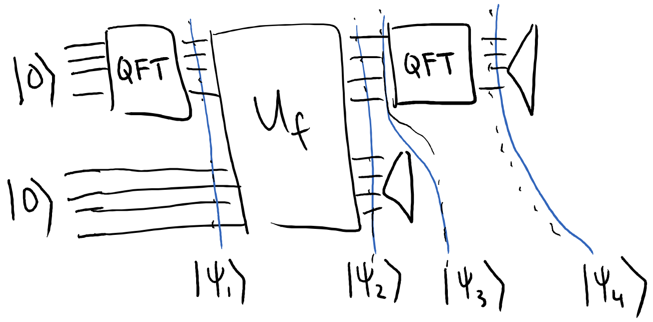
3. Apply U_f to A, B

4. Measure B in standard basis

5. Apply QFT_N to A

6. Measure A in standard basis

Q: Write as circuit -



Full Algorithm

1. Run basic algorithm twice. Get outcomes y, y'. Do Classical postprocessing on y, y'. Outcome of postprocessing is r with high probability. Check by querying $f(1)$ and $f(r+1)$

S.KIMMEL

Important Unitary: Quantum Fourier Transform for Period Finding

QFT_t is an $t \times t$ unitary

For standard basis state $|x\rangle$:

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

Q: If apply QFT_t to a standard basis state $|x\rangle$ and then measure in standard basis, what is the probability of getting outcome y:

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

Important Unitary: Quantum Fourier Transform for Period Finding

QFT_t is an $t \times t$ unitary

For standard basis state $|x\rangle$:

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

Q: If apply QFT_t to a standard basis state $|x\rangle$ and then measure in standard basis, what is the probability of getting outcome y:

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

Because $\left|\frac{e^{\frac{2\pi i x y}{t}}}{\sqrt{t}}\right|^2 = \left|\frac{1}{\sqrt{t}}\right|^2 \left|e^{2\pi i x y/t}\right|^2 = \frac{1}{t}$

S.KIMMEL

QFT Tricks

y is integr integer n

Q: What is $\sum_{k=0}^{t-1} e^{2\pi i k y/t}$ if $y = n \cdot t$

A) 0 B) 1 C) Depends on y D) t

y is integr integer n

Q: What is $\sum_{k=0}^{t-1} e^{2\pi i k y/t}$ if $y \neq n t$.

A) 0 B) 1 C) Depends on y D) t

S.KiMMEL

QFT Tricks

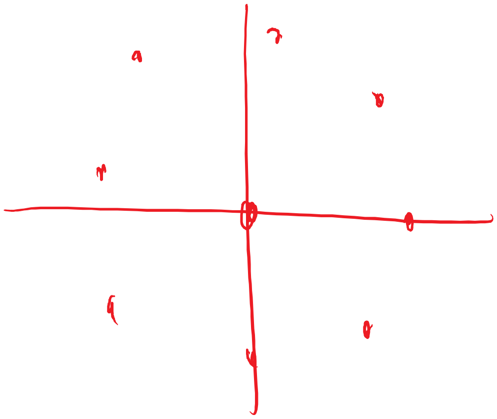
Q: What is $\sum_{k=0}^{t-1} e^{2\pi i k \overset{\swarrow y \text{ is integer}}{y}/t}$ if $y = \overset{\swarrow \text{integer } n}{n}\cdot t$

A) 0 B) 1 C) Depends on y [✓ D) t]

$$\sum_{k=0}^{t-1} e^{2\pi i m t y/t} = \sum_{k=0}^{t-1}\left(e^{2\pi i}\right)^{my} = \sum_{k=0}^{t-1}(1)^{my} = \sum_{k=0}^{t-1} 1 = t$$

Q: What is $\sum_{k=0}^{t-1} e^{2\pi i k \overset{\swarrow y \text{ is integer}}{y}/t}$ if $y \neq \overset{\swarrow \text{integer } n}{n}.t$

[✓ A) 0] B) 1 C) Depends on y D) t



Math Tricks

- $$\sum_{k=0}^{t-1} e^{\frac{2\pi i k y}{t}} = \sum_{k=0}^{t-1} \left(e^{\frac{2\pi i y}{t}}\right)^{k}$$

Geometric Series: $$\sum_{k=0}^{t-1} r^{k} = \frac{1-r^{k+1}}{1-r} \quad (r\neq 1)$$

$$= \frac{1-e^{\frac{2\pi i t y}{t}}}{1-e^{\frac{2\pi i y}{t}}} = \frac{1-\boxed{e^{2\pi i y}}}{1-e^{2\pi i y/t}} = 0$$

- $$\sum_{k=0}^{t-1} a_k \left(\sum_{j=0}^{t-1} b_j |j\rangle\right)$$

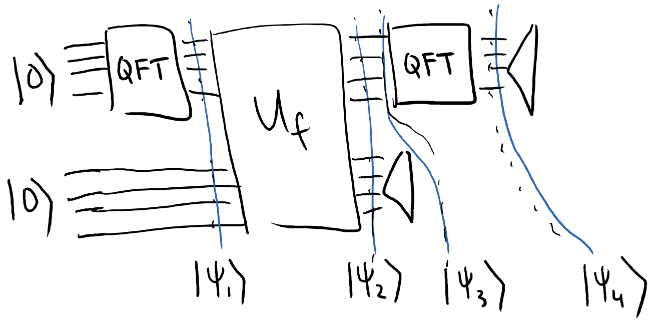
$$\Downarrow \text{ Distribute}$$

$$\sum_{k=0}^{t-1}\sum_{j=0}^{t-1} a_k b_j |j\rangle \xrightarrow[\text{Swap order}]{} \sum_{j=0}^{t-1} \overbrace{\left(\sum_{k=0}^{t-1} a_k b_j\right)}^{\text{amplitude of state } |j\rangle} |j\rangle$$

Basic Algorithm:

1. Prepare $\underset{\text{N-dim}}{|0\rangle_A}\underset{\text{W-dim}}{|0\rangle_B}$
2. Apply QFT_N to A
3. Apply U_f to A, B
4. Measure B in standard basis
5. Apply QFT_N to A
6. Measure A in standard basis

Q: Write as circuit -



Full Algorithm

1. Run basic algorithm twice. Get outcomes y, y'. Do Classical postprocessing on y, y'. Outcome of postprocessing is r with high probability. Check by querying $f(1)$ and $f(r+1)$

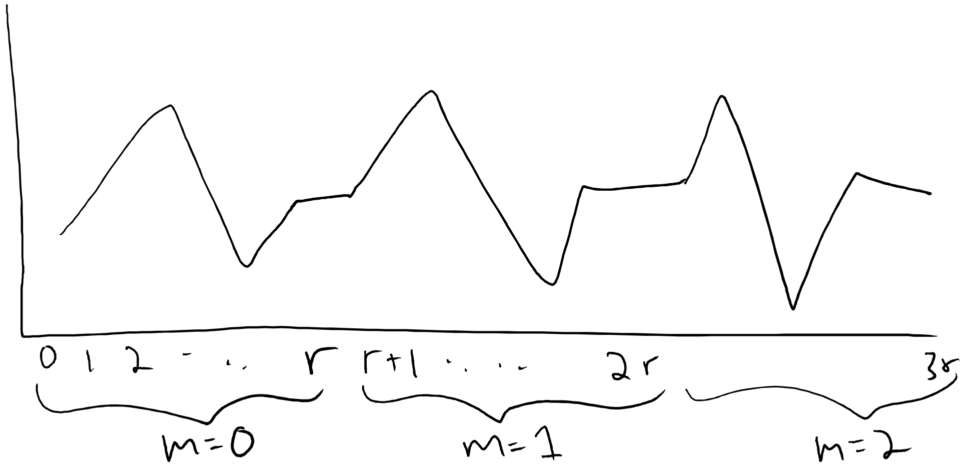
1. $|\psi_1\rangle = \left(QFT\,|0\rangle\right)|0\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle_A |0\rangle_B$

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

Recall: f(x) is periodic. Let's write $x = m\underset{\uparrow \text{period}}{r} + b$

Q: What is f(mr+b) equal to?

A) $f(r)$ B) $f(m)$ $\boxed{\text{C) } f(b)}$ D) $f(mr)$



$b \in [r]$

$m \in \left[\frac{N}{r}\right]$

$m=i$, $b=j$ corresponds to j^{th} element of i^{th} block of r

Rewrite x as $x = mr+b$. $\sum_x$ becomes $\sum_m \sum_b$

$$|\psi_2\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle|f(x)\rangle$$

$$\Big\Downarrow \text{ with change of variables}$$

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

m_b is # blocks where b occurs. If r does not divide N evenly, some values of b will not occur in last block

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

3. Measure B register in standard basis.

Use partial measurement to analyze:

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

standard basis states, different for each b by assumption that values are unique within a period

$$|\psi_2\rangle = \sum_{b=0}^{r-1} \underbrace{\frac{1}{\alpha\sqrt{N}}}_{\text{Related to probability of outcome}} \underbrace{\left(\alpha\sum_{m=0}^{m_b-1}|mr+b\rangle\right)_A}_{\text{Want this to be normalized}} |f(b)\rangle_B$$

Q. What is the (approximate) value of α?

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

Because $m_b = \frac{N}{r}$ or $\frac{N}{r}-1$

Suppose we get outcome $|s\rangle$. Let b^* be value such that $f(b^*)=s$. Then after measurement, state collapses to:

$$|\psi_3\rangle = \left(\frac{1}{\sqrt{m_{b^*}}}\sum_{m=0}^{m_{b^*}-1}|mr+b^*\rangle\right)_A |f(b^*)\rangle_B$$

We never do anything else with B system. Since partial measurement leaves us in tensor state of A & B, we can ignore B from here on.

4. Now apply QFT_N to A:

Distribute!

$$|\psi_4\rangle = QFT_N \frac{1}{\sqrt{m_{b^*}}}\sum_{m=0}^{m_{b^*}-1}|mr+b^*\rangle = \frac{1}{\sqrt{m_b^*}}\sum_{m=0}^{m_{b^*}-1} QFT_N|mr+b^*\rangle$$

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

$$= \frac{1}{\sqrt{Nm_{b^*}}}\sum_{m=0}^{m_{b^*}-1}\left(\sum_{y=0}^{N-1} e^{\frac{2\pi imry}{N}} e^{\frac{2\pi ib^*y}{N}}|y\rangle\right)$$

Switch order of summation ↗

$$= \frac{1}{\sqrt{Nm_{b^*}}}\sum_{y=0}^{N-1}\left(\sum_{m=0}^{m_{b^*}-1} e^{\frac{2\pi ib^*y}{N}} e^{\frac{2\pi imry}{N}}|y\rangle\right)$$

Factor out $e^{2\pi i b^* y/N}$ ↗

$$= \frac{1}{\sqrt{Nm_{b^*}}}\sum_{y=0}^{N-1} e^{\frac{2\pi ib^*y}{N}}\left(\sum_{m=0}^{m_{b^*}-1} e^{\frac{2\pi imry}{N}}\right)|y\rangle$$

$$|\psi_4\rangle = \sum_{y=0}^{N-1}\frac{1}{\sqrt{Nm_{b^*}}} e^{2\pi ib^*y/N}\left(\sum_{m=0}^{m_{b^*}-1} e^{2\pi imry/N}\right)|y\rangle$$

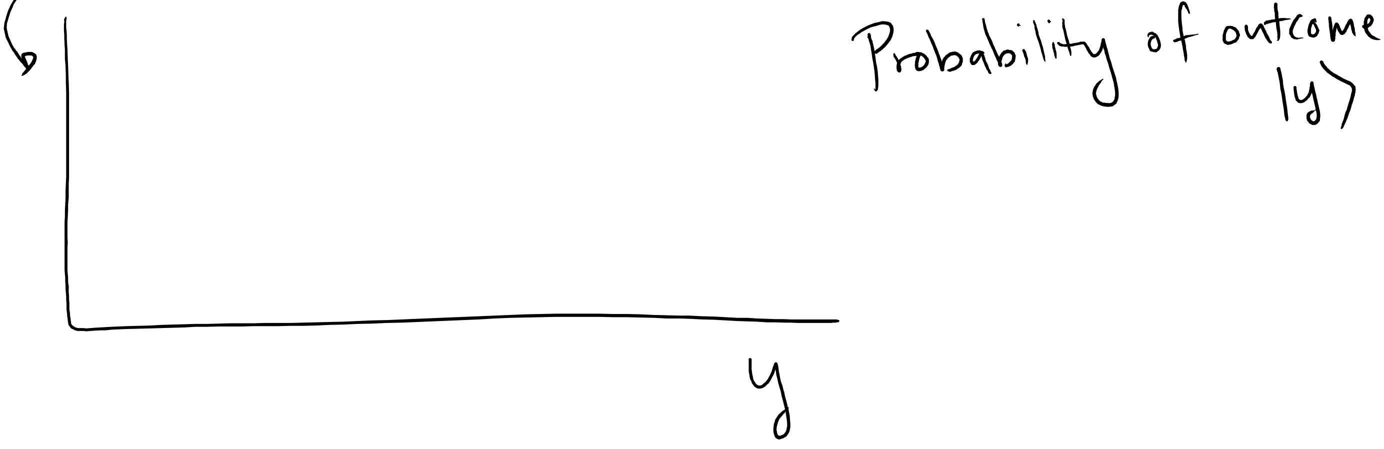
5. Measure in standard basis:

$$Pr(\text{outcome } |y\rangle) = \left|\frac{1}{\sqrt{nm_{b^*}}} e^{2\pi ib^*y/N}\cdot\sum_{m=0}^{m_{b^*}-1} e^{2\pi imry/N}\right|^2$$

$$= \left|\frac{1}{\sqrt{Nm_{b^*}}} e^{2\pi ib^*y/N}\right|^2 \left|\underbrace{\boxed{\sum_{m=0}^{m_{b^*}-1} e^{2\pi imry/N}}}_{?}\right|^2 \quad (*)$$

$$\downarrow \quad \boxed{\frac{1}{Nm_{b^*}} \approx \frac{r}{N^2}}$$

Q: Plot $\left|\sum_{m=0}^{m_{b^*}} e^{2\pi i m r y/N}\right|^2$ as a function of y

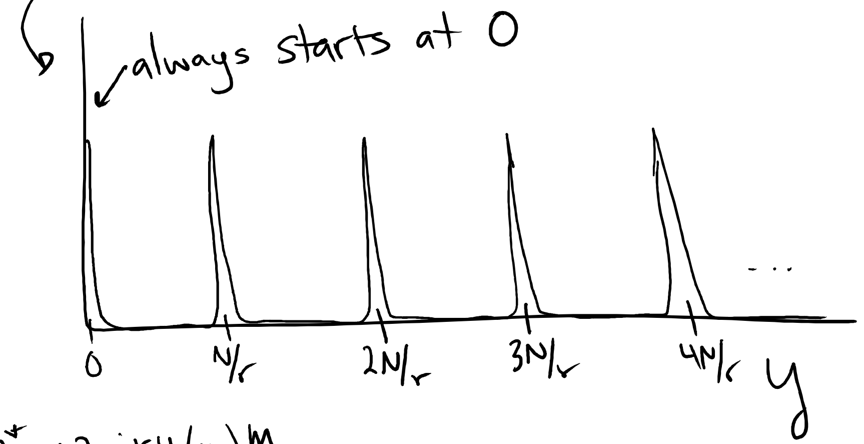


Q: Before QFT, we had

$$|\psi_3\rangle = \frac{1}{\sqrt{m_{b^*}}}\sum_{m=0}^{m_{b^*}-1}|mr+b^*\rangle$$

Why not measure $|\psi_3\rangle$? Plot probability of outcome $|y\rangle$

Q: Plot $\left| \sum_{m=0}^{m_{b^*}} e^{2\pi i m r y/N} \right|^2$ as a function of y



Probability of outcome $|y\rangle$

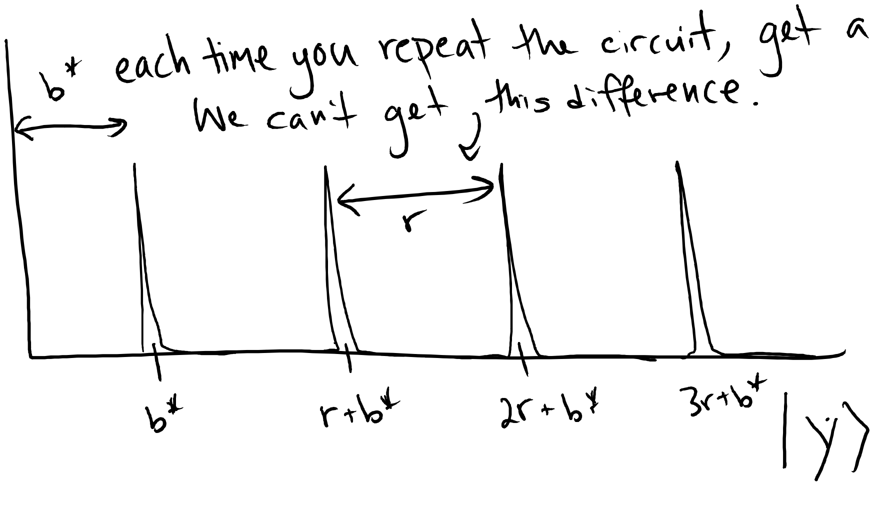
$$\sum_{m=0}^{m_{b^*}} \left(e^{2\pi i r y/N}\right)^m$$ when $y = \frac{jN}{r}$ for $j \in \mathbb{Z}$

Repeat twice, get $\frac{jN}{r}$, $\frac{j'N}{r}$... some math... learn r with high probability!

Q: Before QFT, we had

$$|\psi_3\rangle = \frac{1}{\sqrt{m_{b^*}}} \sum_{m=0}^{m_{b^*}-1} |mr + b^*\rangle$$

Why not measure $|\psi_3\rangle$? Plot probability of outcome $|y\rangle$.



each time you repeat the circuit, get a different b^* value. We can't get this difference.

Classical Post Processing

continued fractions algorithm

1.
- $\frac{Nj}{r}$ might not be an integer
- $|y\rangle$ must be an integer

$$\left.\begin{array}{l}\frac{Nj}{r} \text{ might not be an integer} \\ |y\rangle \text{ must be an integer}\end{array}\right\} \quad |y\rangle \rightarrow \frac{Nj}{\boxed{r}} \leftarrow \text{get a guess for } r$$

2. If not prime $(r = a \cdot b)$

$$j = a \cdot j'$$

$$\frac{Nj}{r} = \frac{Nj'}{b} \leftarrow \text{looks like period is } b.$$

Solution $\Longrightarrow$ Measure twice:

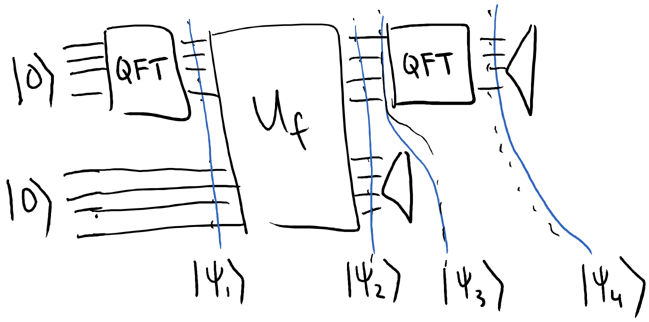
$$\frac{Nj'}{b}, \quad \frac{Nj''}{c}$$

find least common multiple

very likely to be r

test $f(0) \overset{?}{=} f(r)$

Basic Algorithm:



Full Algorithm

Run basic algorithm twice. Get outcomes y, y'.

Do Classical postprocessing on y, y'. Outcome of postprocessing is r with high probability. Check by querying $f(1)$ and $f(r+1)$

Quantum Query Complexity: $O(1)$

Classical Query Complexity: $O(r)$

☆ But this is for period finding... what about factoring?

☆ What about time complexity? (We care about time to implement QFT.

Time Complexity of factoring

Comparison to Classical

domain of f

- If want to factor number n, set $N = n$.

  ↳ Use $O(\log(n))$ qubits.

- QFT_N: $O((\log_2 N)^2)$ single + 2 qubit gates
- U_f: For factoring application: $O(\log_2 N)$ gates

$\Rightarrow$ $O((\log_2 N)^2)$ time for Quantum

$\Rightarrow$ $e^{O((\log_2 N)^{1/3})}$ for classical

⇓

number field sieve algorithm

Sub-exponential in $\log_2 N$ (almost exponential)

polynomial in $\log_2 N$

"Exponential Speed-up"