S. KIMMEL

Basic Algorithm:

1. Prepare $|0\rangle_A |0\rangle_B$ (A: N-dim, B: W-dim)

2. Apply QFT_N to A

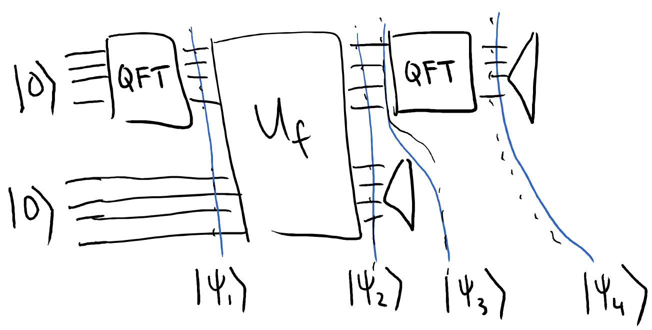
3. Apply U_f to A, B

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

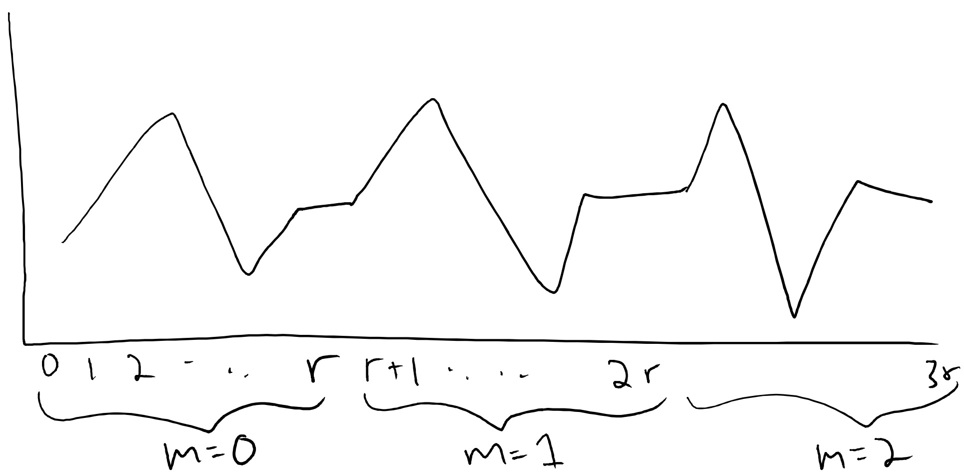
1. $|\psi_1\rangle = \left(QFT\,|0\rangle\right)|0\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle_A|0\rangle_B$

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 $\sum_m \sum_b$

S.KIMMEL

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

$\Downarrow$ 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

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

S. KIMMEL

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:

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

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.

S. KIMMEL

4. Now apply QFT_N to A:

Distribute!

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

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

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

Switch order of summation

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

Factor out $e^{2\pi i b^* y/N}$

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

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

5. Measure in standard basis:

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

(*)

$$= \left|\frac{1}{\sqrt{Nm_{b^*}}} e^{2\pi i b^* y/N}\right|^2 \left|\boxed{\sum_{m=0}^{m_{b^*}} e^{2\pi i mry/N}}\right|^2$$

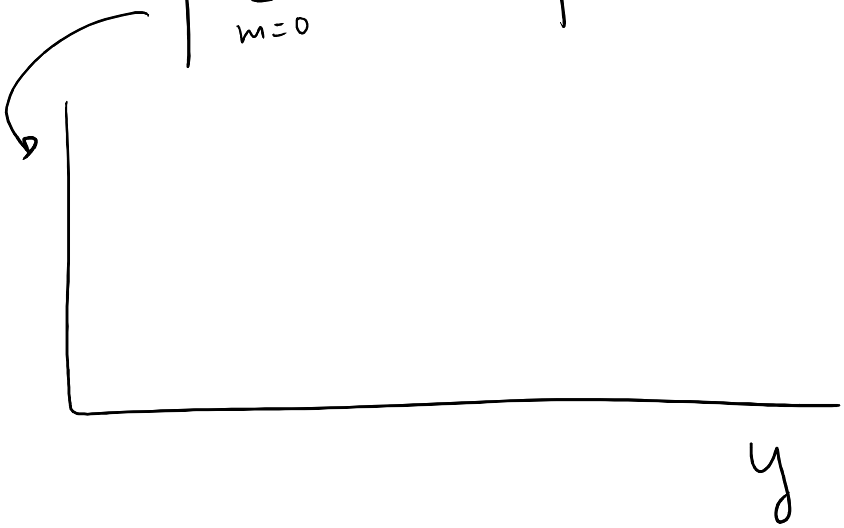
$$\downarrow \qquad\qquad \downarrow$$

$$\frac{1}{Nm_{b^*}} \approx \frac{1}{r} \qquad\qquad ?$$

S.KIMMEL

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

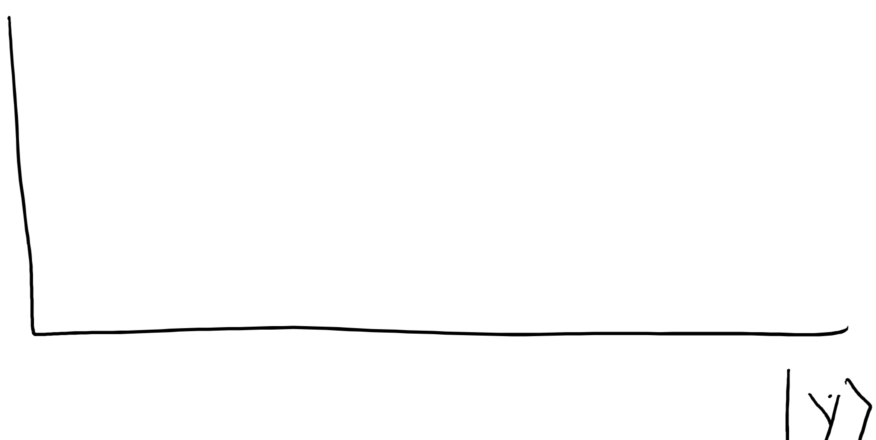
Probability of outcome $|y\rangle$



Q: Before QFT, we had

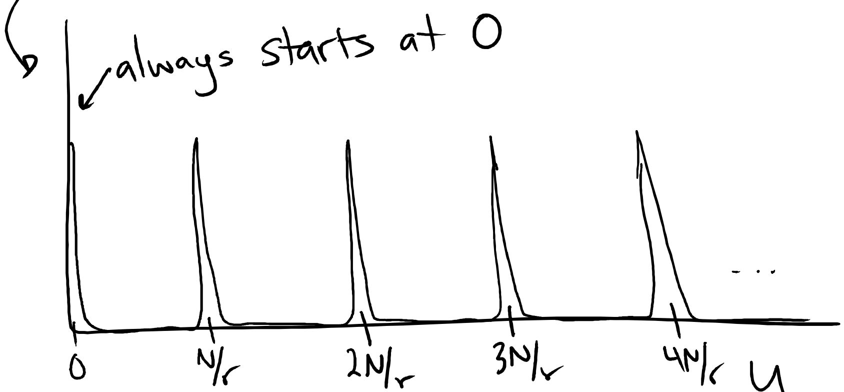
$$|\psi_3\rangle = \frac{1}{\sqrt{m_{b^*}}} \sum_{m=0}^{m_{b^*}-1} |mr + b^*\rangle$$

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



S.KIMMEL

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 $|y\rangle$

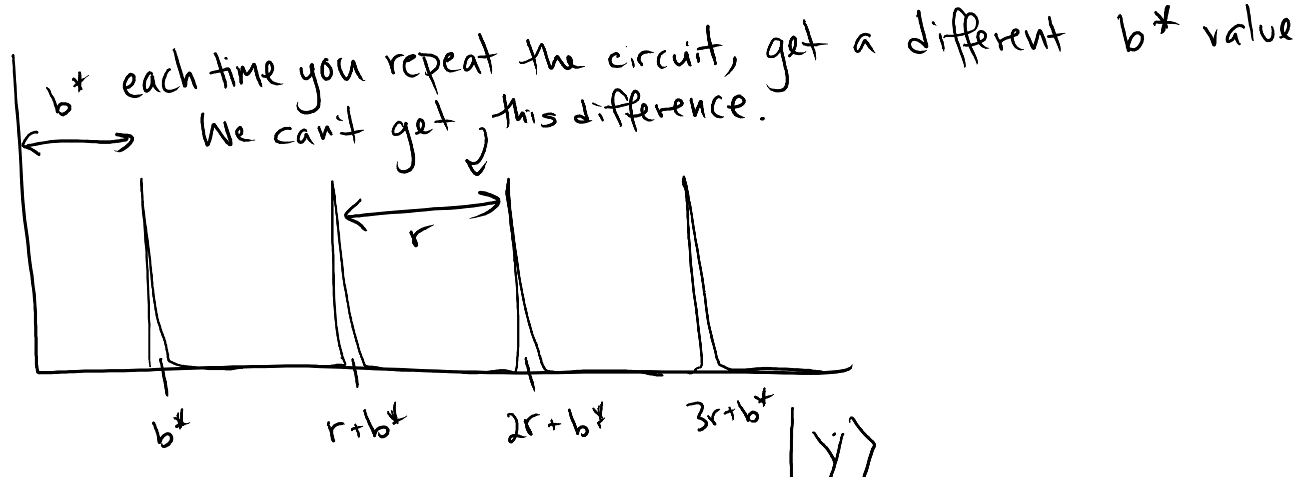
$$\sum_{m=0}^{m_{b^*}} \left(e^{2\pi i r y/N}\right)^m \quad \text{when } y = \frac{jN}{r} \text{ for } j \in \mathbb{Z}$$

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 $|y\rangle$.



S.KIMMEL

Classical Post Processing

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

$|y\rangle \xrightarrow{\text{continued fractions algorithm}} \frac{Nj}{r}$

(only one possible fraction nearby, since $r < \sqrt{N}$)

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

$$j = a \cdot j'$$

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

Solution
$\Longrightarrow$ Measure twice:

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

find least common multiple → very likely to be r → test $f(0) \stackrel{?}{=} f(r)$