S.KIMMEL

Basic Algorithm:

1. Prepare $|0\rangle_A |0\rangle_B$

   A: N-dim, B: W-dim

2. Apply QFT_N to A

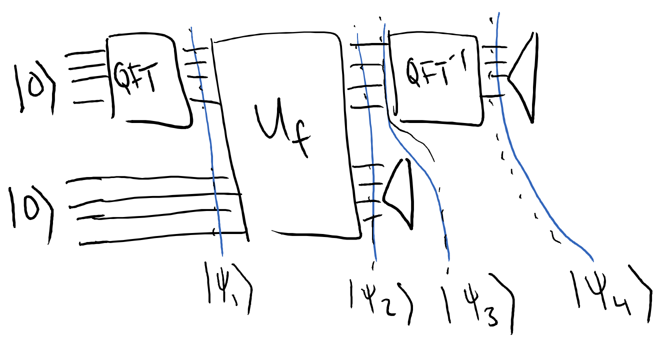
3. Apply U_f to A, B

4. Measure B in standard basis

5. Apply QFT_N^{-1} to A

6. Measure A in standard basis

Q: Write as circuit 



Total Algorithm

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

   Do classical postprocessing on y, y'. Outcome is pretty likely to be $r \rightarrow$ can check if outcome is correct

S. KIMMEL

QFT Tricks

y is integer

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

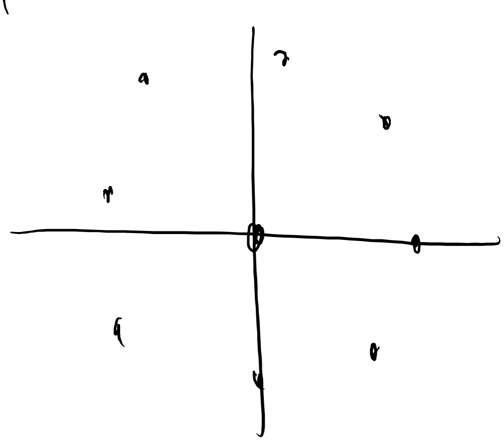
A) 0 B) 1 C) Depends on y D) t

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

y is integer

Q: What is $\sum_{k=0}^{t-1} e^{2\pi i k y/t}$ if $k \not\equiv 0 \mod t$?

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



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

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

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

If

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

$\Downarrow$ Distribute

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

amplitude of state $|j\rangle$

S.KIMMEL

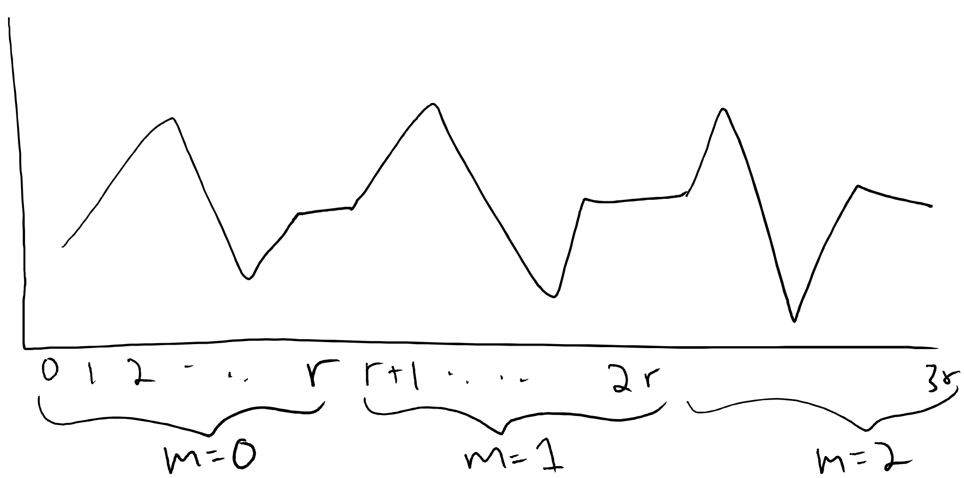
1. $$|\psi_1\rangle = \left(QFT\,|0\rangle\right)|0\rangle \underset{\substack{\uparrow \\ \text{from exercise}}}{=} \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle_A |0\rangle_B$$

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

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

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

S.KIMMEL

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

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.

To get outcome state, rewrite as

$$|\psi_2\rangle = \sum_i \alpha_i |\phi_i\rangle_A |i\rangle$$

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

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

$$\left(\frac{1}{a\sqrt{N}} \times \underbrace{a \sum_{m=0}^{m_b-1} |mr+b\rangle}_{} \right)$$

Q. What is a (approximately) to make this normalized

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 get outcome $|f(b) = s\rangle$. Let b^* be value s.t. $f(b^*) = s$

After Measurement, state is

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

We don't do anything else with B system, since tensor product, can just ignore from this point on

S. KIMMEL

4. Now apply QFT_N^{-1} to A:

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

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

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

Switch order of summation

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

Distributive property

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

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

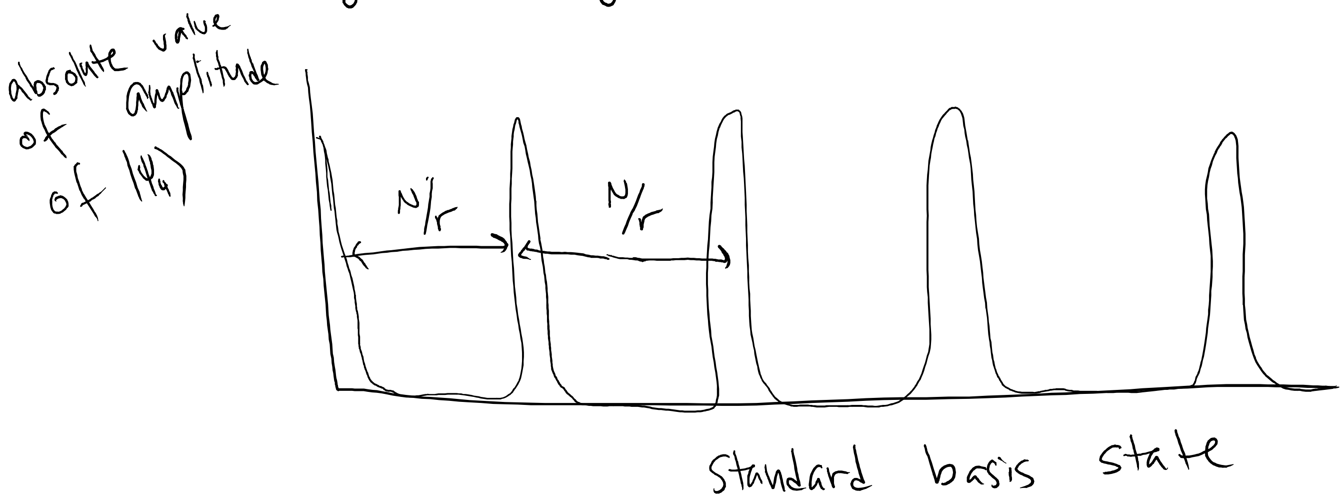
5. Measure in standard basis.

$$\mathrm{Prob}(y) = \underbrace{\left| \frac{1}{\sqrt{Nm_{b^*}}} e^{2\pi i b^* y/N} \right|^2}_{\frac{1}{Nm_{b^*}}} \underbrace{\left| \overset{(*)}{\sum_{m=0}^{m_{b^*}} e^{-2\pi i mry/N}} \right|}_{?}$$

S.KIMMEL

Claim 1:

(*) Is large when y is close to a multiple of $\frac{N}{r}$



This means if measure in standard basis, get y: $y \approx \frac{jN}{r}$, or $\frac{y}{N} \approx \frac{j}{r}$. Bunch of math:

$$\text{Prob}\left(\left|\frac{y}{N} - \frac{j}{r}\right| \le \frac{1}{2N} \text{ for some } j\right) \ge \frac{4}{\pi^2}$$

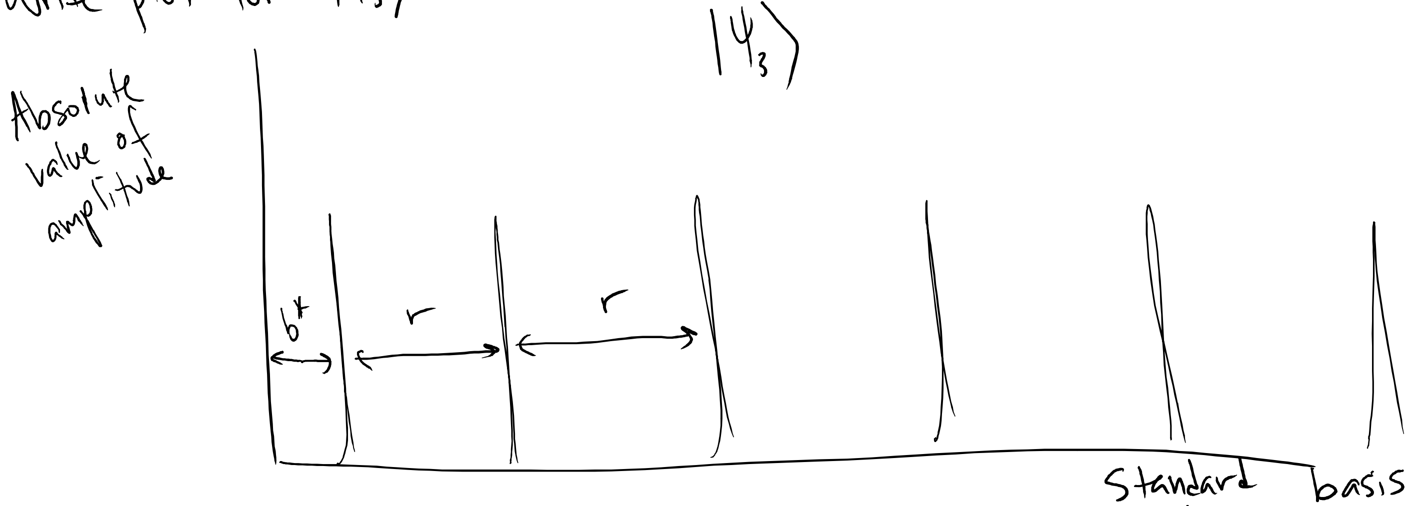
"Good y"

Claim 2:

If learn $y \approx \frac{jN}{r}$, $y' \approx \frac{j'N}{r}$ for 2 randomly chosen j, j', can learn r with probability $1/2$. (Using "Classical Post Processing")

S.KIMMEL

Q: Write plot for $|\psi_3\rangle$:



Q. Why is $|\psi_4\rangle$ better than $|\psi_3\rangle$ for learning r? (Think about making a measurement on $|\psi_3\rangle$)

A. We don't know value of b^*. We only know $f(b^*)$. If measure $|\psi_3\rangle$ in standard basis, get $|mr+b^*\rangle$ for some unknown m and b^*, so can't figure out r. But what if create $|\psi_3\rangle$ again. Value of b^* changes! If measure in standard basis, get $|m'r+b^{*\prime}\rangle$ for some unknown m' and $b^{*\prime}$! With $|\psi_4\rangle$, period always starts at origin, so if measure in standard basis, get $|kN/r\rangle$ for some k, can figure out r.

S.KIMMEL

Claim 2: Given $y \in \{0, \dots N-1\}$ such that

$$\left|\frac{y}{N} - \frac{j}{r}\right| \le \frac{1}{2N} \quad \text{for } j \in \{0, 1, \dots, r-1\},$$

we can learn r with high probability.

Claim 2a: There is a unique fraction j'/r' with $r' \in \{0, 1, \dots \sqrt{N}-1\}$, $j' \in \{0, 1, \dots r'-1\}$ such that

$$\left|\frac{y}{N} - \frac{j'}{r'}\right| \le \frac{1}{2N}$$

In our case we assumed $r < \sqrt{N}$ (This is why that assumption mattered!)

So given y, there is only one possible fraction j'/r' that is close to y, and has small denominator.

S.KIMMEL

To find j/r', take continued fraction of c:

$$c = \frac{853}{2048} = \frac{1}{\frac{2048}{853}} = \frac{1}{2+\frac{342}{853}} = \frac{1}{2+\frac{1}{\frac{853}{342}}} = \frac{1}{2+\frac{1}{2+\frac{169}{342}}}$$

$$= \frac{1}{2+\frac{1}{2+\frac{1}{\frac{342}{169}}}} = \frac{1}{2+\frac{1}{2+\frac{1}{2+\frac{4}{169}}}} = \frac{1}{\ddots\, \frac{1}{2+\frac{1}{\frac{169}{4}}}}$$

$$= \frac{1}{\ddots\, \frac{1}{2+\frac{1}{42+\frac{1}{4}}}}$$

continue until all numerators are 1

"Convergents" are values without the final fraction:

- $\frac{1}{2+\cancel{\frac{342}{853}}} \rightarrow \frac{1}{2}$
- $\frac{1}{2+\frac{1}{2+\cancel{\frac{169}{342}}}} \rightarrow \frac{1}{2+\frac{1}{2}} = \frac{2}{5}$
- $\frac{1}{2+\frac{1}{2+\frac{1}{2+\cancel{\frac{4}{169}}}}} \longrightarrow \frac{1}{2+\frac{1}{2+\frac{1}{2}}} = \frac{5}{12}$
- $\longrightarrow \frac{212}{509}$

S.KIMMEL

__Thm__: If z is a rational number and $a, b \in \mathbb{Z}$, such that

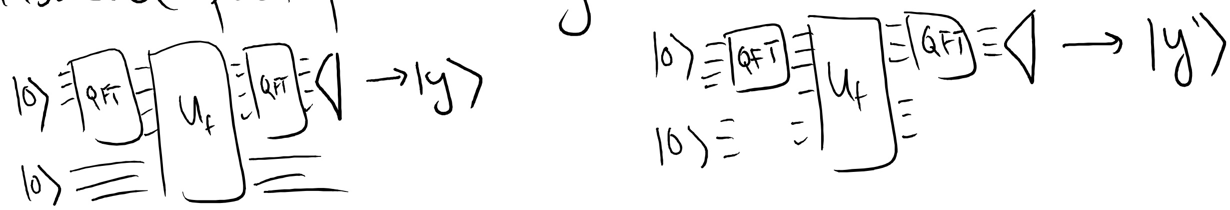
$$\left| z - \frac{a}{b} \right| < \frac{1}{2b^2},$$

then $\frac{a}{b}$ is a convergent of the continued fraction of z.

Q. Put it all together:

7. Classical post processing of final measurement

Do twice



Take continued fraction of $\frac{y}{N}$, and look at convergents.
There will be only one convergent $\frac{a}{b}$ with denominator $< \sqrt{N}$ such that $\left| \frac{a}{b} - \frac{y}{N} \right| \leq \frac{1}{2N}$. If y is good, b will either equal r, or will be a factor of r.

Test if have correct r by checking if $f(x) = f(x+b)$.
Otherwise repeat and get out b'. Test if correct r.
If not find Least Common Multiple(b, b'), and test if correct r.