FACTORING

Learning Goals

- Analyze a multi-qubit algorithm
- Become familiar with Shor's factoring algorithm (most famous q. alg)

Project!

Exit Tickets

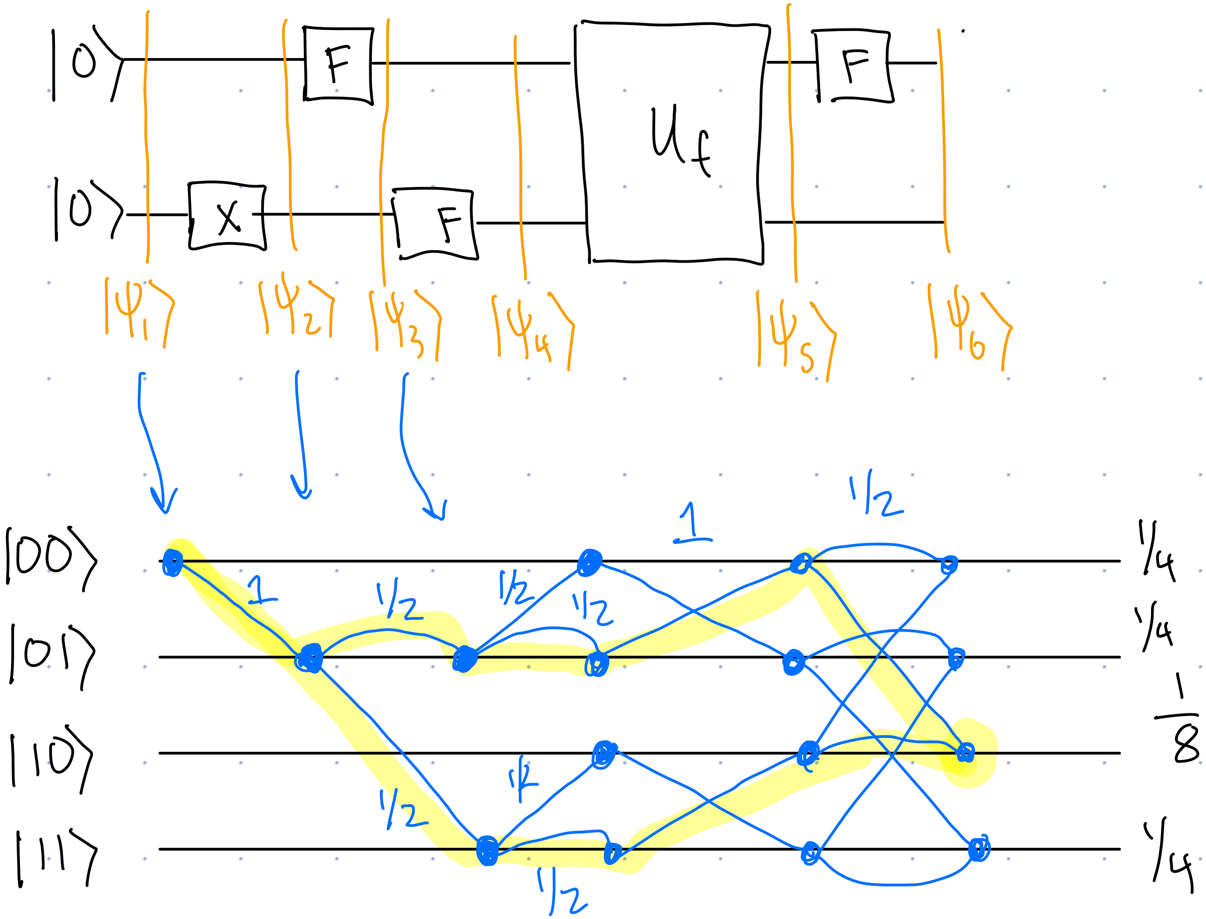
What is QFT and why do we use it?

Discrete periodic function

$|b^* + mr\rangle$ s.b?

Does this probabilistic alg. solve Deutsch's Problem?

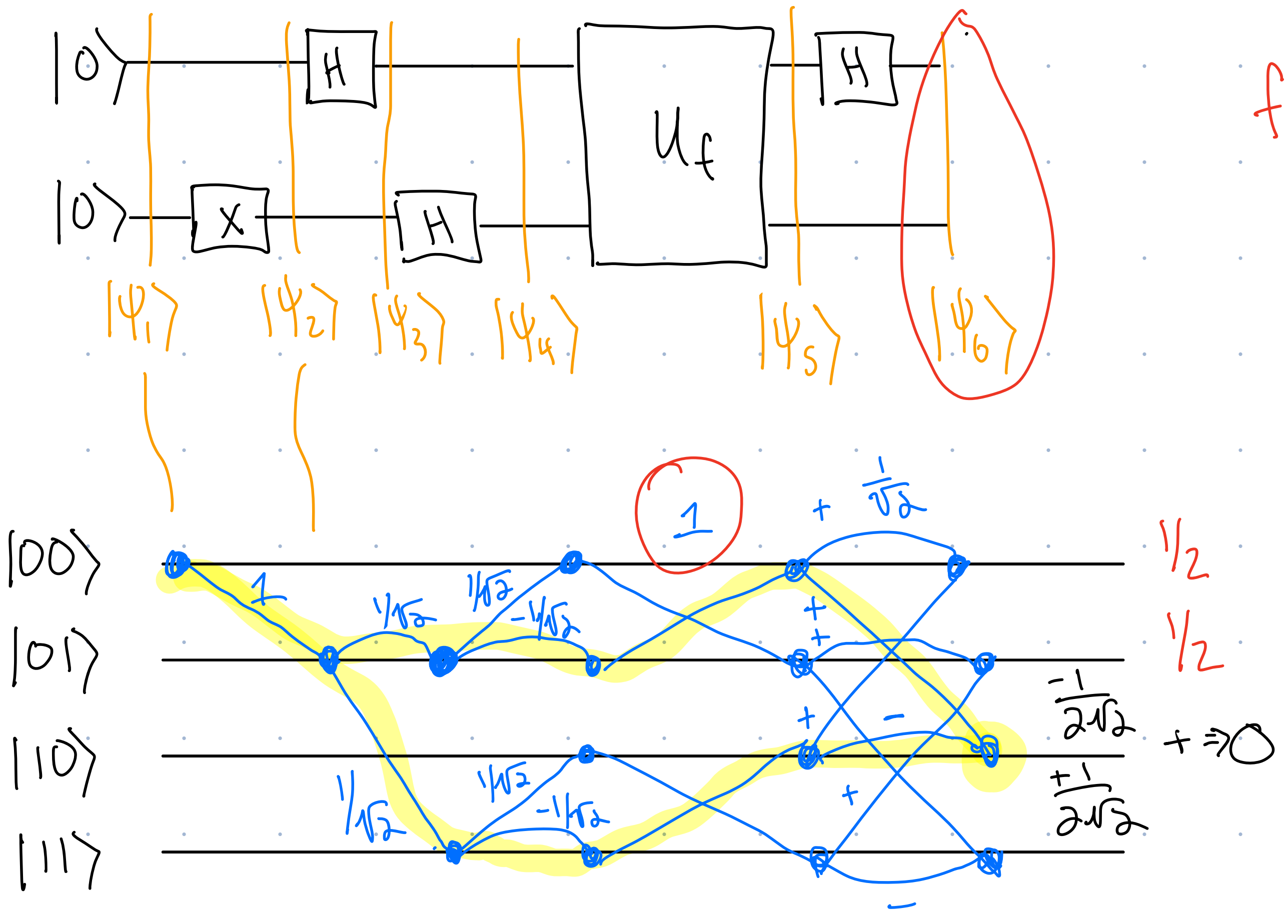
A) YES B) NO (why?)



$\frac{1}{8}$ per path × 2 path : 1/4

Is this quantum algorithm deterministic?

A) YES B) NO C) sort of



$f(0) = f(1) = 1$

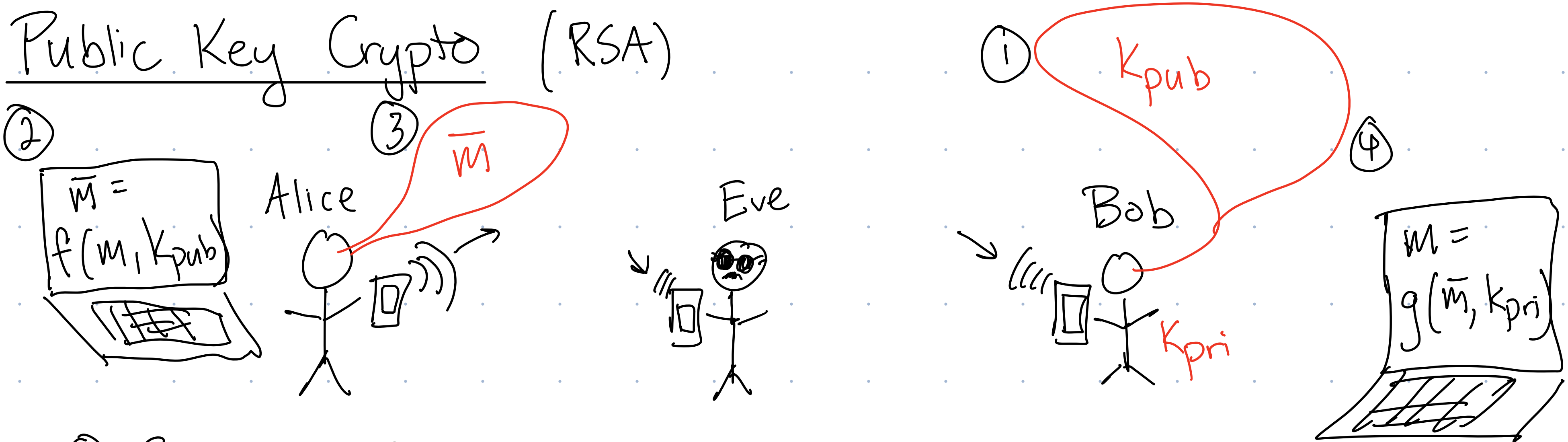
1/2

1/2

$f(0) = 1$

$f(1) = 0$

Public Key Crypto (RSA)



⓪ Secret message

$m \in \{0,1\}^n$

Eve has K_{pub}, $f(m, K_{pub}) = \bar{m}$

If could solve $\underbrace{\text{hard math problem}}_{\text{factoring a large number}}$ → could learn m

$$\underbrace{67011287\,3\,6\ldots}_{617 \text{ digits}} = a \times b$$

\$200,000

\$100K 308 digits

X 250 digit

Period Finding

Factoring reduces to period finding (number theory)

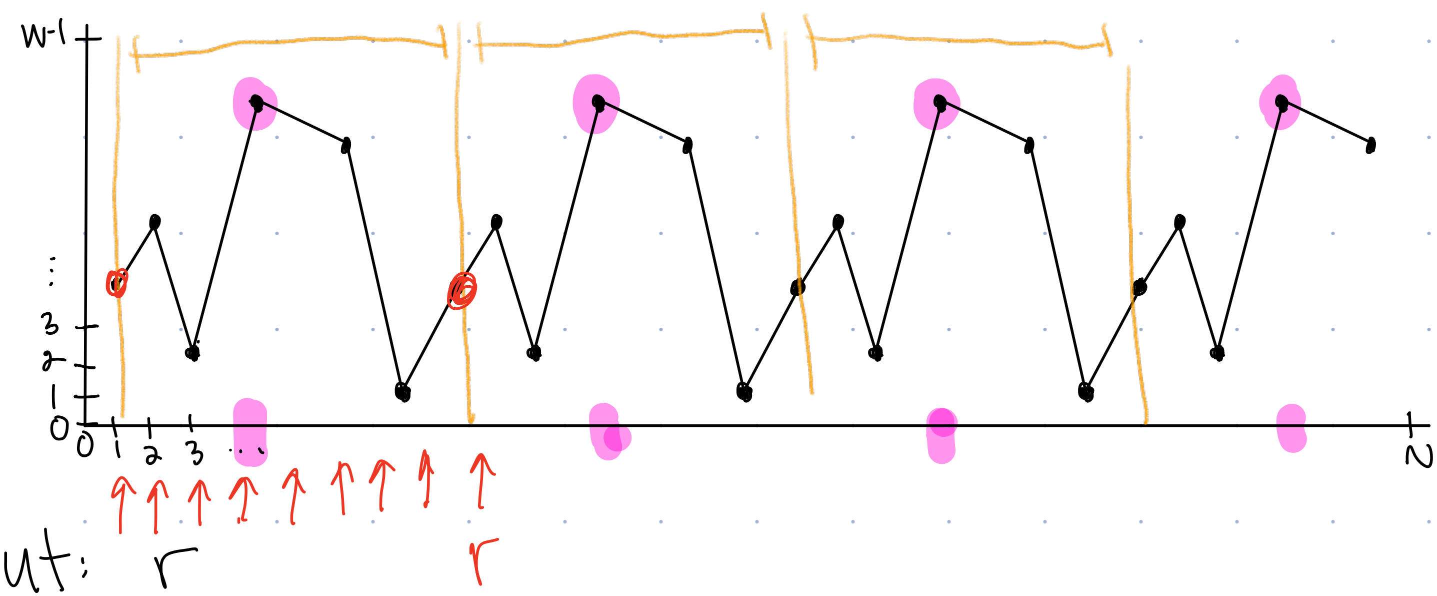
Period Finding Problem

Input: Query access to $f: \{0,1,2,\dots,N-1\} \to \{0,1,2,\dots,W-1\}$

- f has unknown period r
- no repeated values within a period
- $N > r^2$ (many repeats)

$f(x) = f(x+r)$

ex: f $r=6$



Output: r

What is the classical query complexity of period finding?

Birthday

$\boxed{\text{A) } O(\sqrt{r})}$

Paradox

Brute Force

$\boxed{\text{B) } O(r)}$

C) $O(r^2)$

D) $O(N)$

Bits to Digits

Classically, we code using base 10, not binary. We'll do same:

If there N possible Standard Basis States

$$\{|0\rangle, |1\rangle, |2\rangle, |3\rangle, \dots |N-1\rangle\}$$

"N-dimensional state"

$$011 \leftrightarrow 3$$

$$|011\rangle \leftrightarrow |3\rangle$$

Ambiguity:

$$|3\rangle \leftrightarrow |11\rangle$$

$$|3\rangle \leftrightarrow |011\rangle$$

$$|3\rangle \leftrightarrow |0000000011\rangle$$

If $|3\rangle$ is an N-dimensional state, how many qubits are in the system?

$2^{\#\text{ qubits}} = \#$ standard b.s.

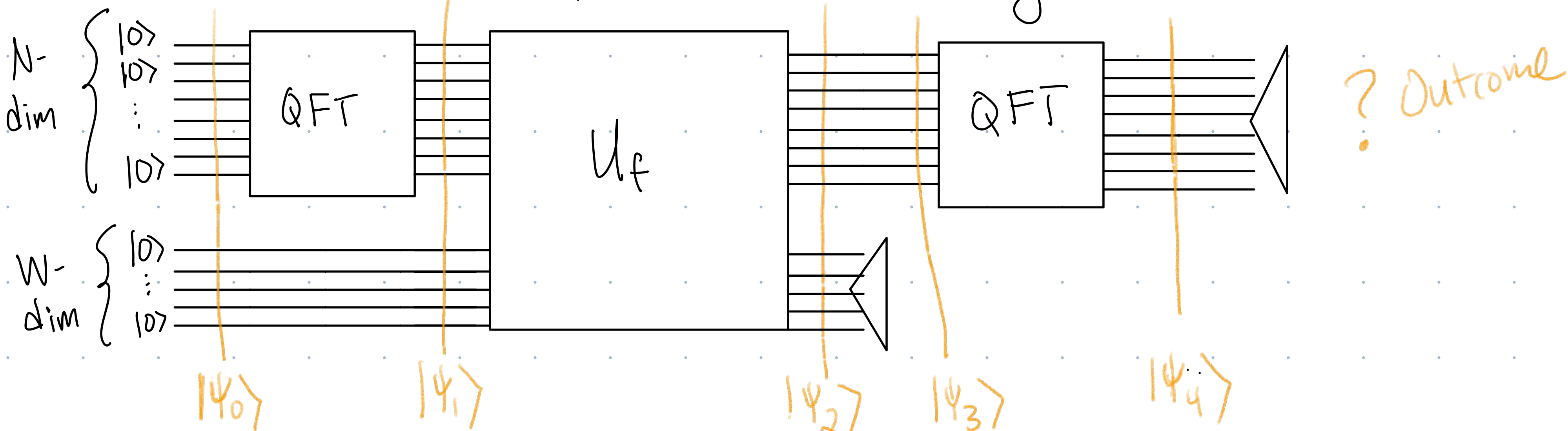
A) $O(1)$ $\quad$ $\boxed{\text{B) } O(\log N)}$ $\quad$ C) $O(N)$ $\quad$ D) $O(2^N)$

$|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, \dots \quad |111\rangle$

$|0\rangle \quad |1\rangle \quad |2\rangle \quad |3\rangle \quad |4\rangle, \dots \quad |7\rangle$

Quantum Circuit for Period Finding

$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$



QFT: Quantum Fourier Transform

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

N-dim standard basis state

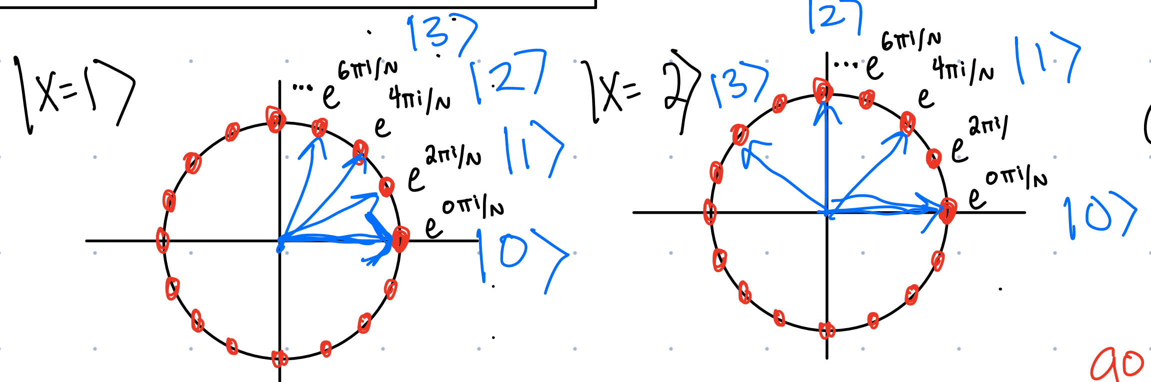
U_f:

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

N-dim W-dim

s.b. states

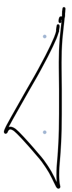
Phase of each s.b. state in superposition



$QFT|0\rangle = ?$

go/fourier-transform

Reminder: $U\left(\sum_i a_i |i\rangle\right) = \sum a_i U|i\rangle$

 = Standard basis measurement

- Measure entire state:

$$|\psi\rangle = \sum_{x=0}^{N-1} a_x |x\rangle \Rightarrow \text{Prob of outcome } |x^*\rangle \text{ is } |a_{x^*}|^2$$

- Partial measurement (B system)

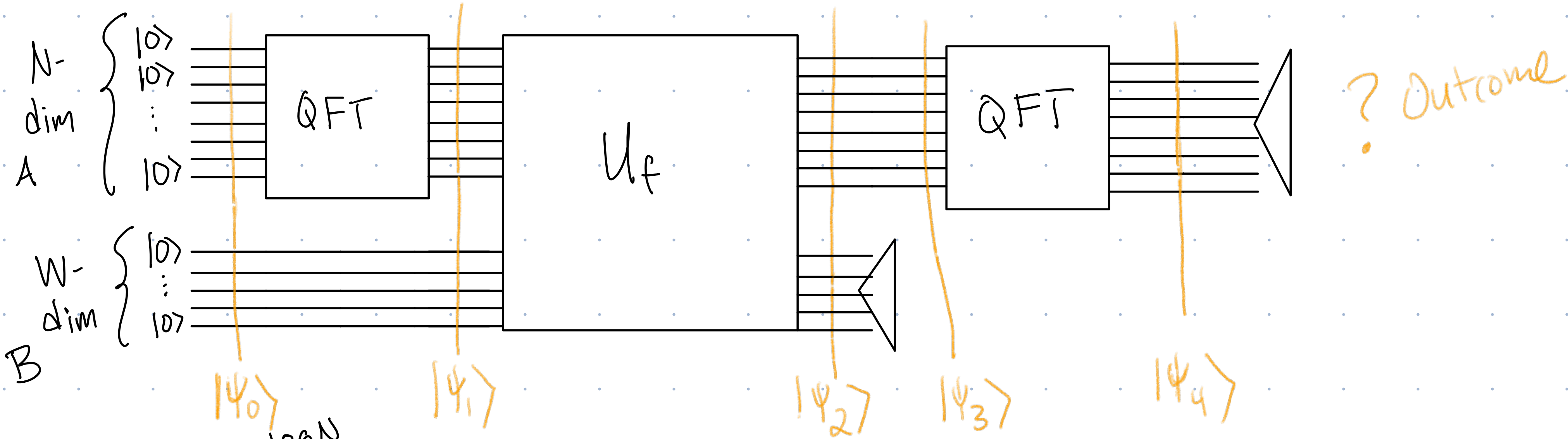
10

$$|\psi\rangle_{AB} = \sum_{x=0}^{N-1}\sum_{y=0}^{W-1} a_{xy} |x\rangle_A |y\rangle_B \Rightarrow \text{Prob of outcome } |y^*\rangle \text{ is}$$

$$P(|y^*\rangle) = \sum_{x=0}^{N-1} |a_{xy^*}|^2$$

$$\Rightarrow \text{Collapse to } \frac{1}{\sqrt{P(|y^*\rangle)}} \sum_{x=0}^{N-1} a_{xy^*} |x\rangle |y^*\rangle$$

Group Excercise: Analyze!



$$|\psi_0\rangle = |\overbrace{000\cdots 0}^{\log N}\rangle_A |000\cdots 0\rangle = |0\rangle_A |0\rangle_B$$

$\boxed{|x\rangle \to \text{ so } x = 0}$

$$|\psi_1\rangle = (QFT_A \otimes I_B)|0\rangle_A |0\rangle_B = \left(QFT|0\rangle_A\right) \otimes I|0\rangle_B$$

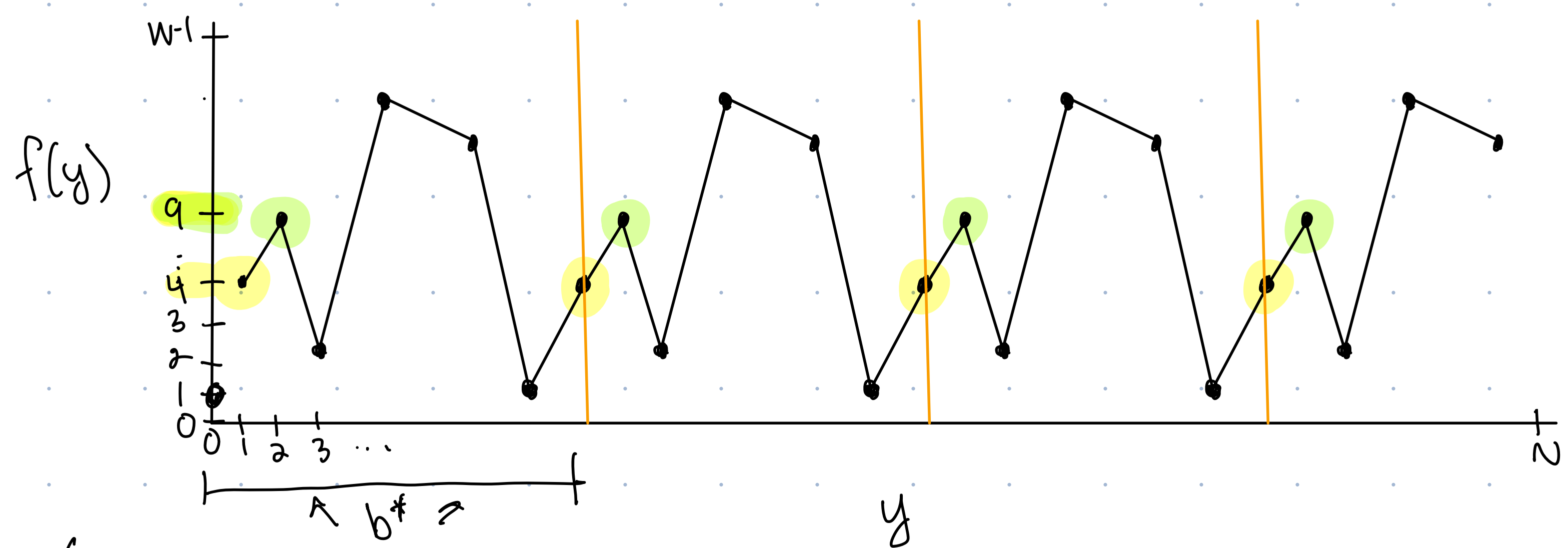
$$= \left(\frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi i \cdot 0 \cdot y/N} |y\rangle\right)_A \otimes |0\rangle_B = \left(\sum_{y=0}^{N-1} \frac{1}{\sqrt{N}} |y\rangle\right)_A \otimes |0\rangle_B$$

$$|\psi_2\rangle = U_f\left(\frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \left(|y\rangle|0\rangle\right)\right) = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} U_f \underset{x \to y}{|y\rangle} \underset{y \to 0}{|0\rangle} = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} |y\rangle |f(y) + 0 \bmod W\rangle$$

$$= \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} |y\rangle_A |f(y)\rangle_B$$

For the following example, what does state collapse to if outcome is $|4\rangle$? If outcome is $|9\rangle$? What is pattern if get outcome $|f(b^*)\rangle$

$r = 6$



$$\frac{1}{\sqrt{N}}\Big(|0\rangle|1\rangle + |1\rangle|4\rangle + |2\rangle|9\rangle + |3\rangle|15\rangle + |4\rangle|11\rangle + |5\rangle|2\rangle + |6\rangle|1\rangle$$

$$+|6\rangle|4\rangle + |7\rangle|9\rangle + |8\rangle|15\rangle + |9\rangle|11\rangle + \cdots$$

$$= \frac{1}{\sqrt{N}}\Big[(|0\rangle + |6\rangle + |12\rangle + \cdots)|1\rangle + (|1\rangle + |7\rangle + |13\rangle + \cdots)|4\rangle$$

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

$$\frac{1}{\alpha}\left(|0\rangle + |5\rangle + |10\rangle + |15\rangle \cdots\right) \qquad \frac{1}{\alpha}\left(|1\rangle + |6\rangle + |11\rangle + \cdots\right)$$

(outcome $|1\rangle$) (outcome $|4\rangle$)

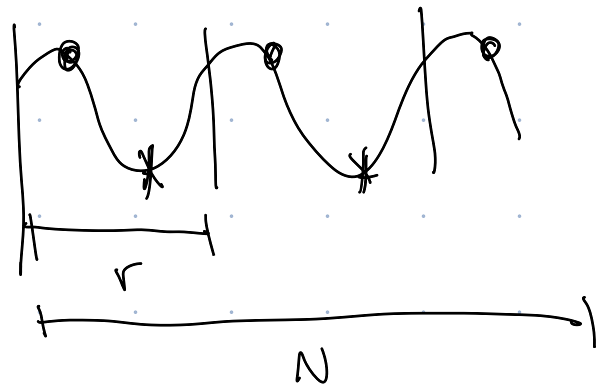
$$\frac{1}{\sqrt{N}}\left(|b^*\rangle + |b^*+r\rangle + |b^*+2r\rangle + |b^*+3r\rangle + \cdots\right)|f(b^*)\rangle$$

$\downarrow$

outcome $f(b^*)$

$$\boxed{|\psi_3\rangle = \sqrt{\frac{r}{N}} \sum_{m=0}^{\sim\frac{N}{r}-1} |b^*+mr\rangle|f(b^*)\rangle}$$

$$\frac{1}{\sqrt{P(f(b^*))}} \qquad \overbrace{\frac{1}{\sqrt{\frac{1}{r}}} \cdot \frac{1}{\sqrt{N}}}$$



$$\Pr(f(b^*)) = \frac{N}{r}\left|\frac{1}{\sqrt{N}}\right|^2 = \frac{1}{r}$$

$$\left\lfloor \frac{N}{r} \right\rfloor \text{ or } \left\lfloor \frac{N}{r} \right\rfloor - 1$$

Suppose measure outcome $|f(b^*)\rangle$:

$$\boxed{|\psi_3\rangle = \sqrt{\frac{r}{N}} \sum_{m=0}^{\sim\frac{N}{r}-1} |b^* + mr\rangle_A \cancel{|f(b^*)\rangle_B}}$$

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

$$|\psi_4\rangle = QFT|\psi_3\rangle = QFT\left(\sqrt{\frac{r}{N}} \sum_{m=0}^{\sim\frac{N}{r}-1} |b^* + mr\rangle\right)$$

$$= \sqrt{\frac{r}{N}} \sum_{m=0}^{\sim\frac{N}{r}-1} QFT|b^* + mr\rangle$$

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

$m=0$ $\qquad\qquad\qquad\qquad$ $m=1$ $\qquad\qquad\qquad$ $m=2$

$|z=0\rangle + |z=1\rangle + |z=2\rangle \cdots |z=N-1\rangle + |0\rangle + |1\rangle + |2\rangle + \cdots |N-1\rangle + |0\rangle + |1\rangle$

Rewriting by grouping amplitudes

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

$$\Pr(|z^*\rangle)=\left|\sqrt{\frac{r}{N}}\cdot\frac{1}{\sqrt{N}}\sum_{m=0}^{\sim\frac{N}{r}-1}\underbrace{e^{2\pi i(b^*+mr)z^*/N}}_{e^{2\pi i b^* z^*/N}\cdot e^{2\pi i m r z^*/N}}\right|^2$$

$w\in\mathbb{R}$

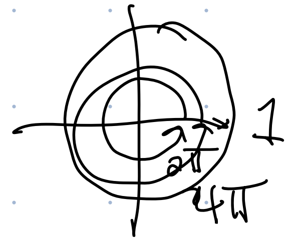
$$\left|e^{iw}\right|=1$$

$$\Pr(|z^*\rangle)=\Bigg|\underbrace{\sqrt{\frac{r}{N}}\frac{1}{\sqrt{N}}\,e^{\cancel{2\pi i b^* z^*/N}}}_{c}\Bigg|^2\cdot\Bigg|\underbrace{\sum_{m=0}^{\sim N/r-1}\left(e^{2\pi i r z^*/N}\right)^m}_{d}\Bigg|^2$$

$$\frac{r}{N^2}$$

$$|c\cdot d|^2$$
$$=|c|^2|d|^2$$

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



$$\boxed{\begin{array}{c} a = e^{2\pi i r z^*/N} \\ a = 1 \end{array}}$$

$t = \sim N/r$

Sum: $\dfrac{N}{r}$

$$P(|z^*\rangle) = \frac{r}{N^2} \cdot \left(\frac{N}{r}\right)^2 = \frac{1}{r}$$

$a \neq 1$

$$\frac{1 - e^{2\pi i r z^*/N \cdot \frac{N}{r}}}{1 - e^{2\pi i r z^*/N}} = 1 - \overset{1}{\cancel{e^{2\pi i z^*}}}$$

$$= 0$$

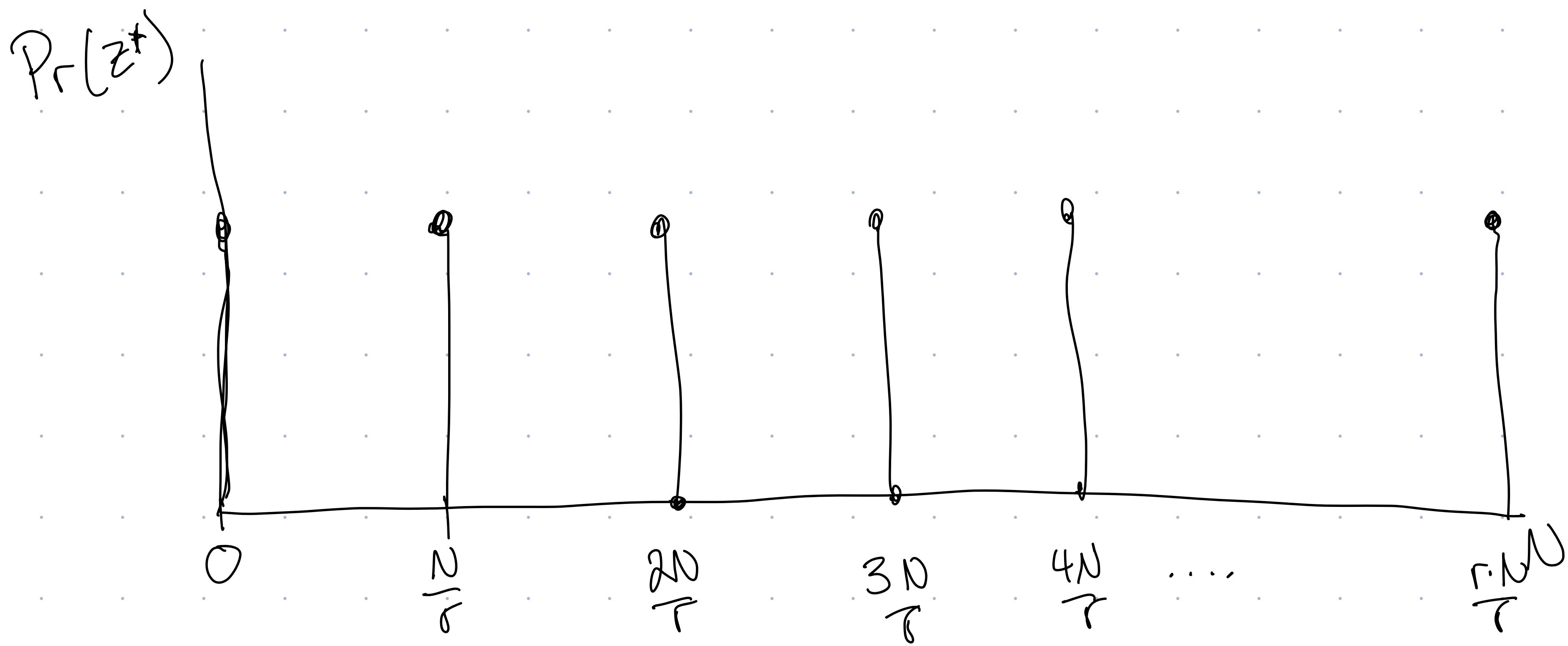
When does

$$e^{2\pi i r z^*/N} = 1 \iff 2\pi i r z^*/N = 2\pi i k \text{ for } k \in \mathbb{Z}$$

$$z^* = \frac{kN}{r} \text{ for some } k \in \mathbb{Z}$$

Geomtric Series Formula:

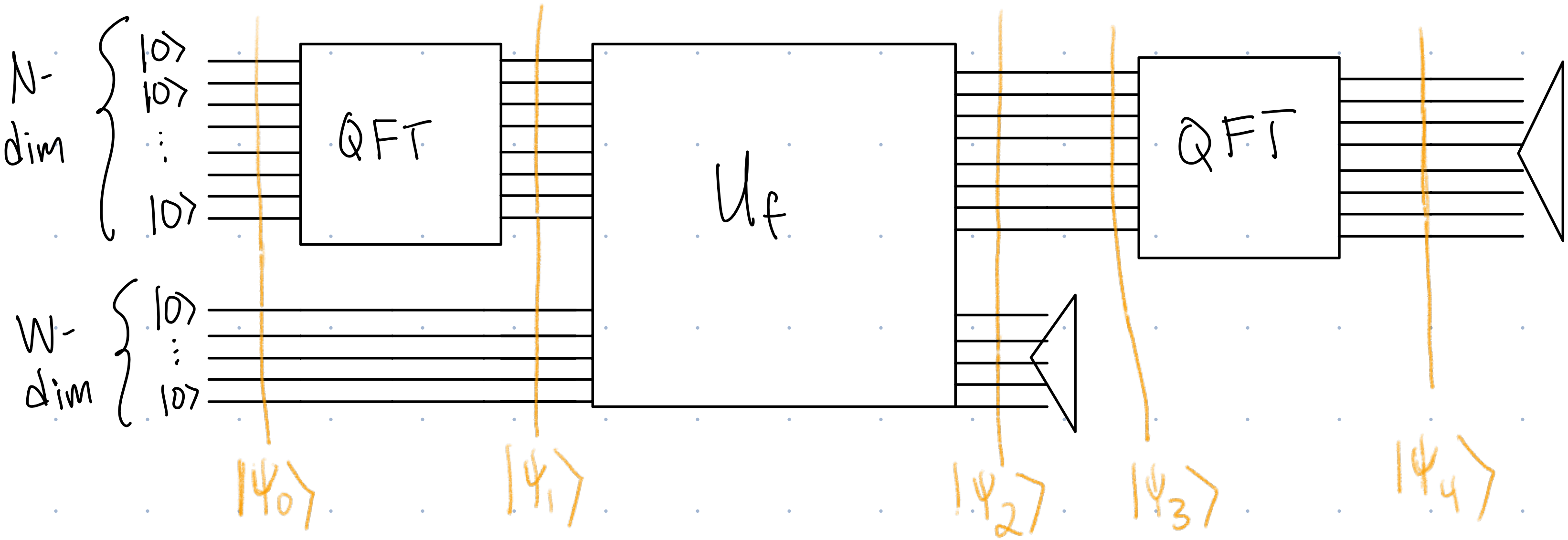
$$\sum_{m=0}^{t-1} a^m = \begin{cases} t & \text{if } a = 1 \\ \dfrac{1-a^t}{1-a} & \text{if } a \neq 1 \end{cases}$$



Period Finding Algorithm (Shor's Algorithm)

$\boxed{2r}$

① Run 2 times:



$$z_1 = \frac{k_1 N}{r}$$

$$z_2 = \frac{k_2 N}{r}$$

② Run greatest common divisor alg (Euclid alg)

$$\gcd\left(\frac{k_1 N}{r}, \frac{k_2 N}{r}\right) \rightarrow \tilde{r}$$

③ Check $f(0) = f(\tilde{r}) \Rightarrow$ Conclude $\tilde{r}$ = period

Query Compexity of Period Finding

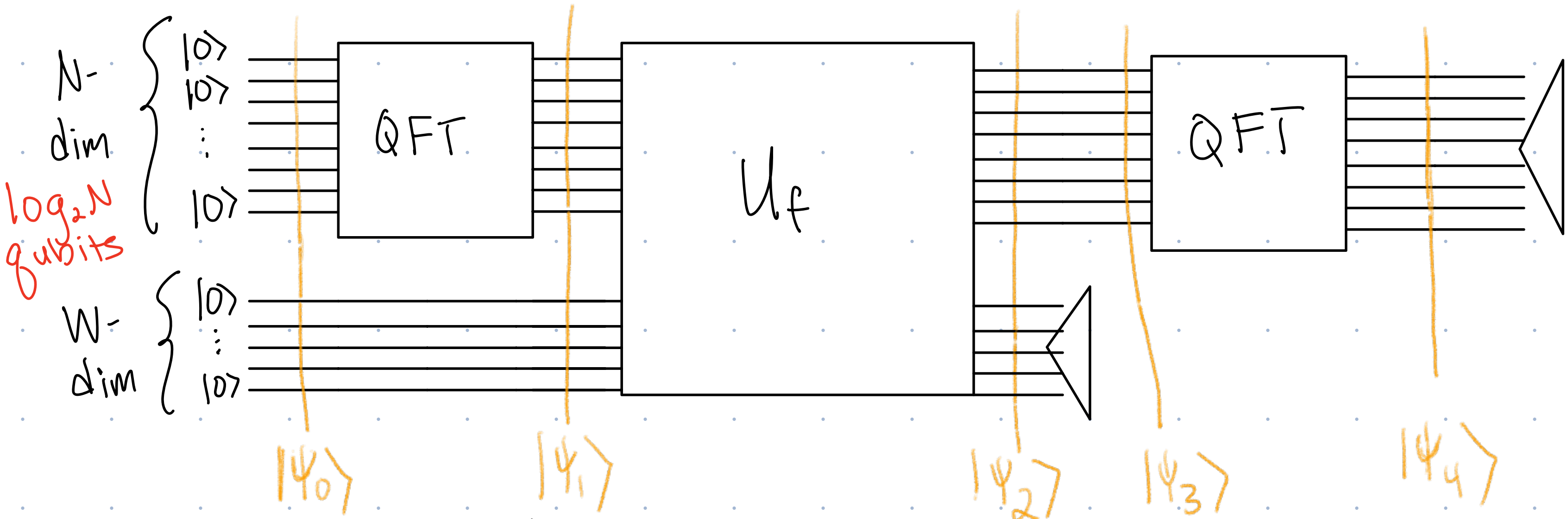
Classical: $O(\sqrt{r})$

Quantum: $O(1)$

Time Complexity of Factoring

Quantum: $O(\log^2(N))$

Circuit used to factor N.



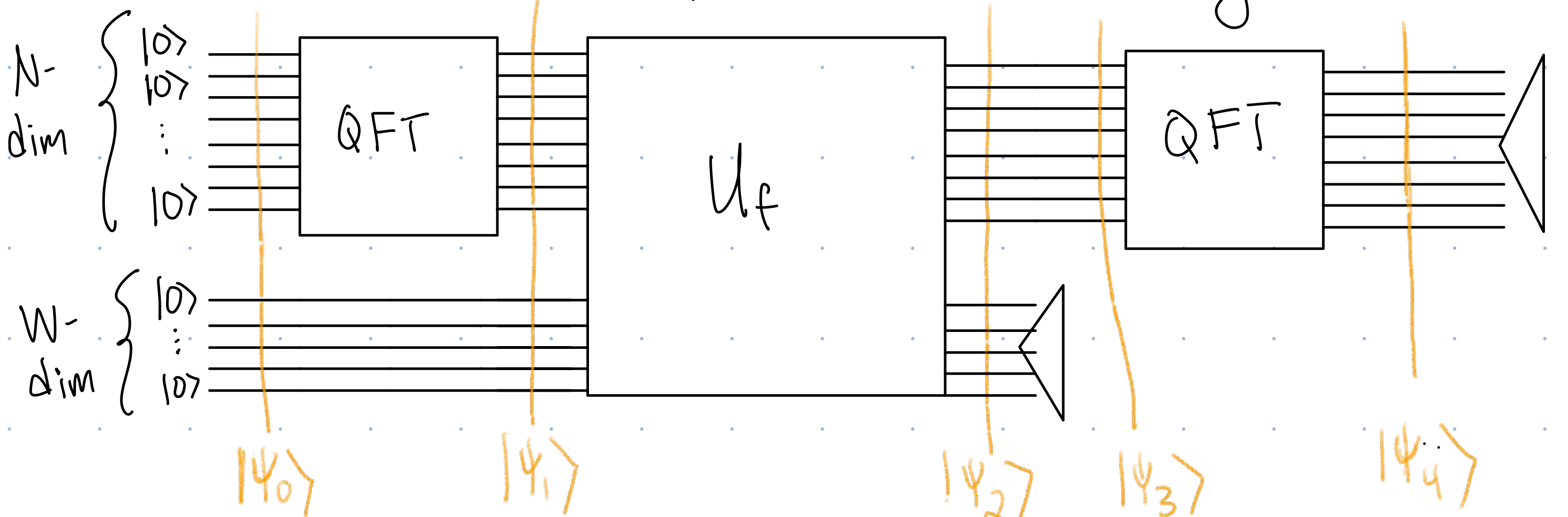
$O(\log_2^2 N)$ $O(\log_2 N)$ $O(\log_2^2 N)$

Classical: $e^{O(\log_2^{1/3} N)}$ ~ quasi exponential in $\log N$

Pesky Detail: $z^* = \frac{kN}{r} \in \mathbb{N}$ $\frac{N}{r} \in \mathbb{N}$

Quantum Circuit for Period Finding

GROUP WORK Version



? Outcome

QFT: Quantum Forier Transform

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

N-dim standard basis state

U_f:

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

N-dim   W-dim

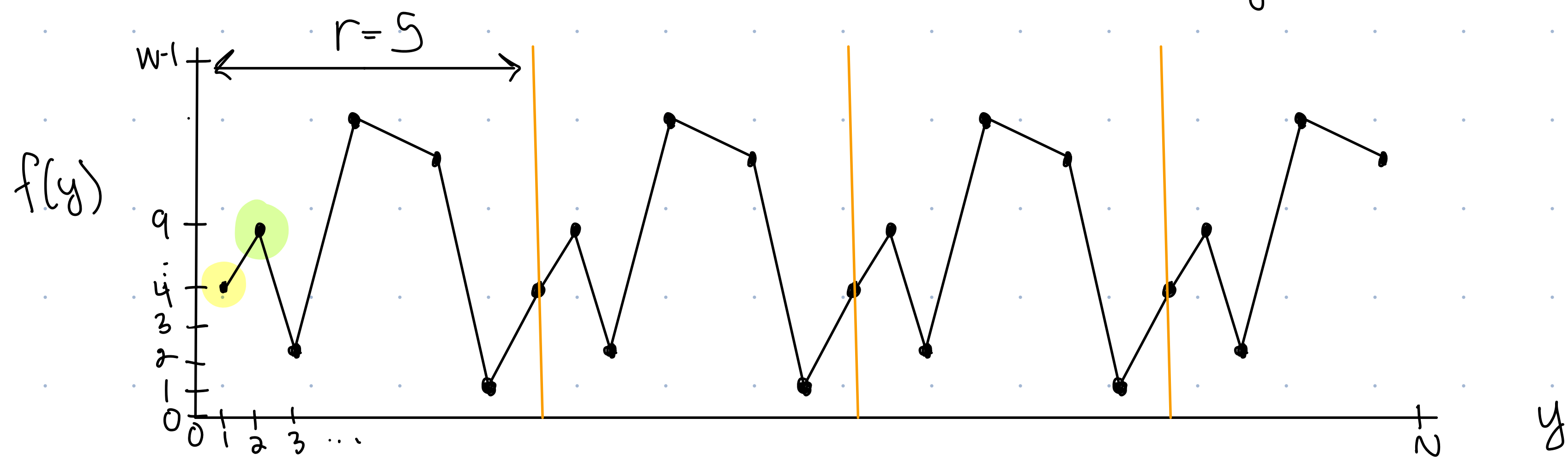
standard basis state

$|\psi_0\rangle =$

$|\psi_1\rangle =$

$|\psi_2\rangle =$

For the following example, what does state $|\psi_3\rangle$ collapse to if outcome is $|4\rangle$? If outcome is $|9\rangle$? What is pattern if get outcome $|f(b^*)\rangle$

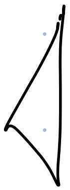


(outcome $f(b^*)$) $\quad |\psi_3\rangle = \boxed{} \sum_{m=0}^{\boxed{}} |b^* \boxed{}\rangle$

Geomtric Series Formula:

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

Reminder: $U\left(\sum_i a_i |i\rangle\right) = \sum_i a_i U|i\rangle$

 = Standard basis measurement

- Measure entire state:

$$|\psi\rangle = \sum_{x=0}^{N-1} a_x |x\rangle \implies \text{Prob of outcome } |x\rangle \text{ is } |a_x|^2$$

- Partial measurement (B system)

$$|\psi\rangle_{AB} = \sum_{x=0}^{N-1}\sum_{y=0}^{W-1} a_{xy}|x\rangle|y\rangle \Rightarrow \text{Prob of outcome } |y\rangle \text{ is}$$

$$p(|y\rangle) = \sum_{x=0}^{N-1} |a_{xy}|^2$$

$\Rightarrow$ Collapse to $\frac{1}{\sqrt{p(|y\rangle)}} \sum_{x=0}^{N-1} a_{xy}|x\rangle \cancel{|y\rangle}$ Destroyed

only terms with that specific $|y\rangle$

⋮