FACTORING

Learning Goals

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

Announcements

Post-quantum crypto

Participation
- PSets
- Exit Tickets if absent

Discussion Tuesday

Hype article unrelated to project part

Quantum Alg Learning Target = This! Practice!!!

BIG PICTURE → Crypto Important

↓

Factoring Breaks Crypto

↓

Period Finding Solves Factoring

Quant. Computers Solve Period Finding

Public Key Crypto (RSA)

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

Eve has access to: $\bar{m}$, K_{pub}, f, g — No direct access: m, K_{pri}

If she could solve a hard math problem $\Rightarrow m$

factoring a large number

$$\underbrace{67011287 36 \ldots}_{617 \text{ digits}} = a \times b$$

?

\$200K prize

\$100K for 308 digit

$\boxed{\checkmark}$ 250 digit

$\boxed{\text{Quantum Computes Can Efficiently Factor}}$

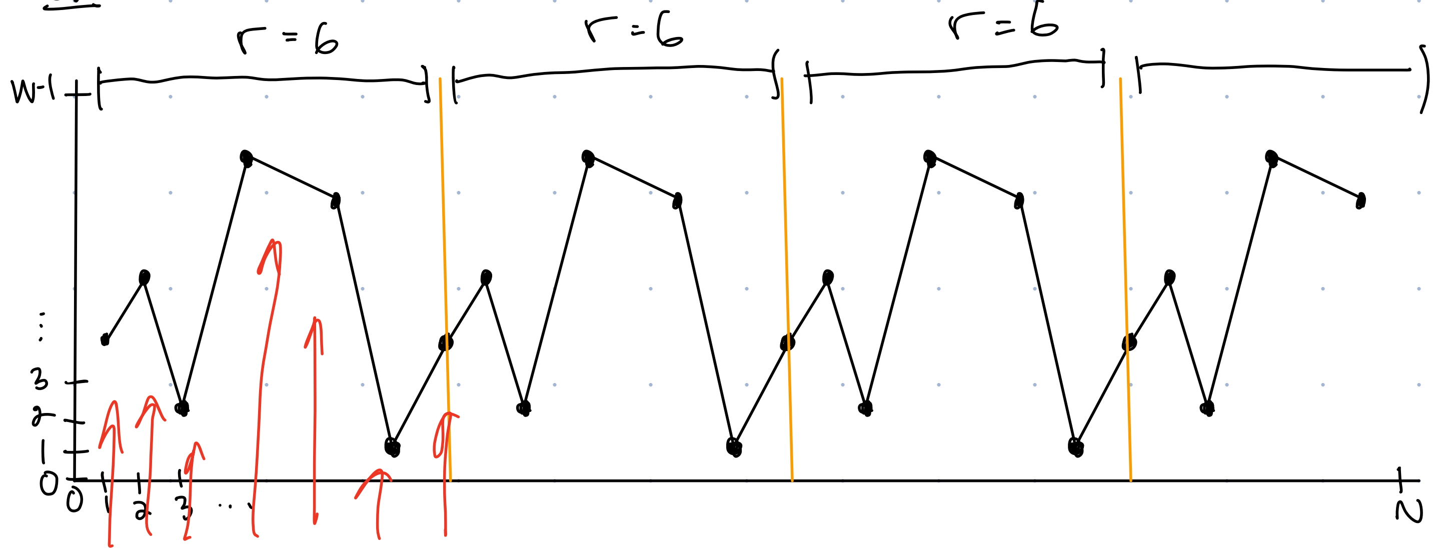
Factoring reduces (via number theory) to period finding:

Period Finding Problem

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

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

ex:



Output: r

What is the classical query complexity of ~~factoring~~ period finding?

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

$011 \longleftrightarrow 3$

$|011\rangle \longleftrightarrow |3\rangle$

$|0011\rangle$ ← 2^4 ← 16-dimensional

Standard Basis States:

$\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$

$\updownarrow \quad \updownarrow \quad \updownarrow$

$\underbrace{\{|0\rangle, |1\rangle, |2\rangle, |3\rangle, \dots |N-1\rangle\}}_{\text{N-dimensional system}}$

$$\sum_{i \in \{0,1\}^m} |i\rangle \longleftrightarrow \sum_{j=0}^{2^m-1} |j\rangle$$

Ambiguity:

$|3\rangle \to |11\rangle$

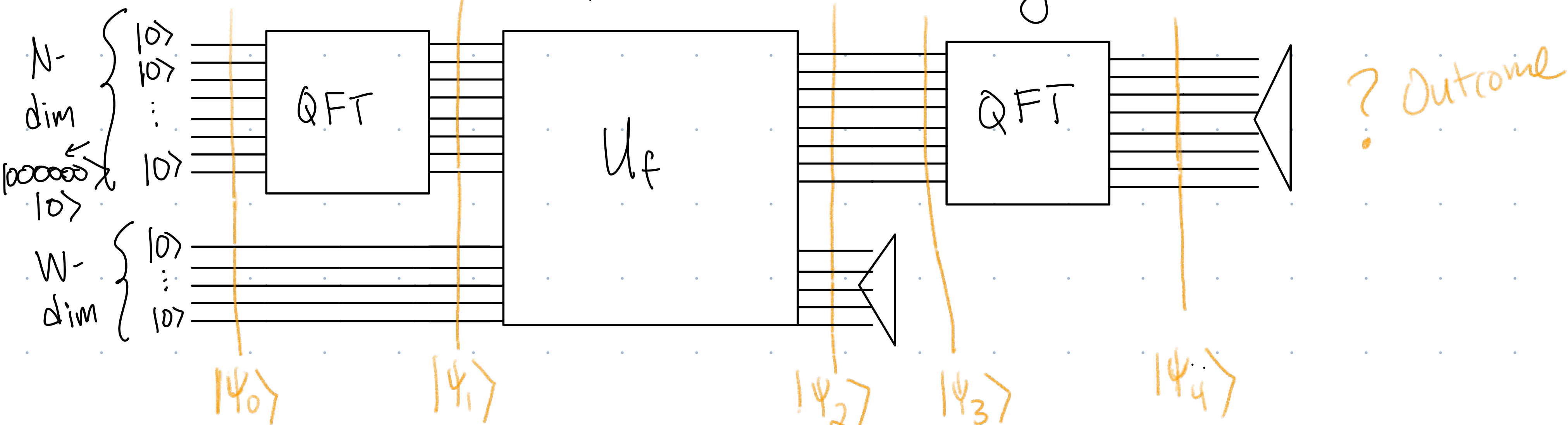
$|3\rangle \to |011\rangle$

$|3\rangle \to |000011\rangle$

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

A) $\lceil \log_2 3 \rceil$ B) 3 C) $\lceil \log_2 N \rceil$ D) N

Quantum Circuit for Period Finding



QFT: Quantum Forier Transform

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

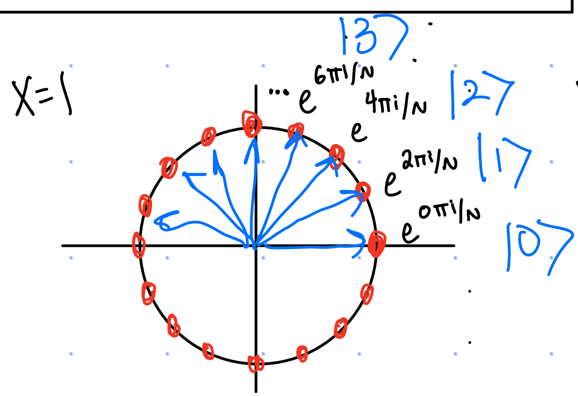
N-dim standard basis state

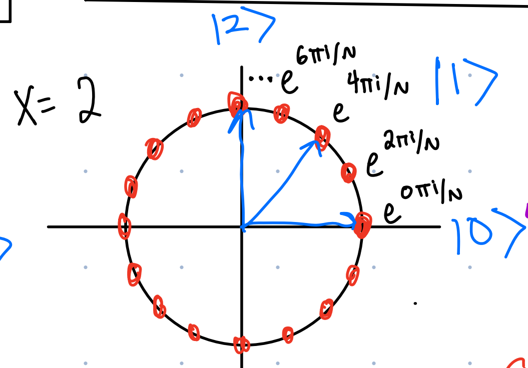
U_f:

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

N-dim W-dim s.b. states

Phase of each s.b. state in superposition



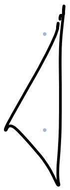


$$\boxed{QFT|0\rangle = ?}$$

$$= \sum_{i=0}^{N-1} \frac{1}{\sqrt{N}} |y\rangle$$

go/fourier-transform

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

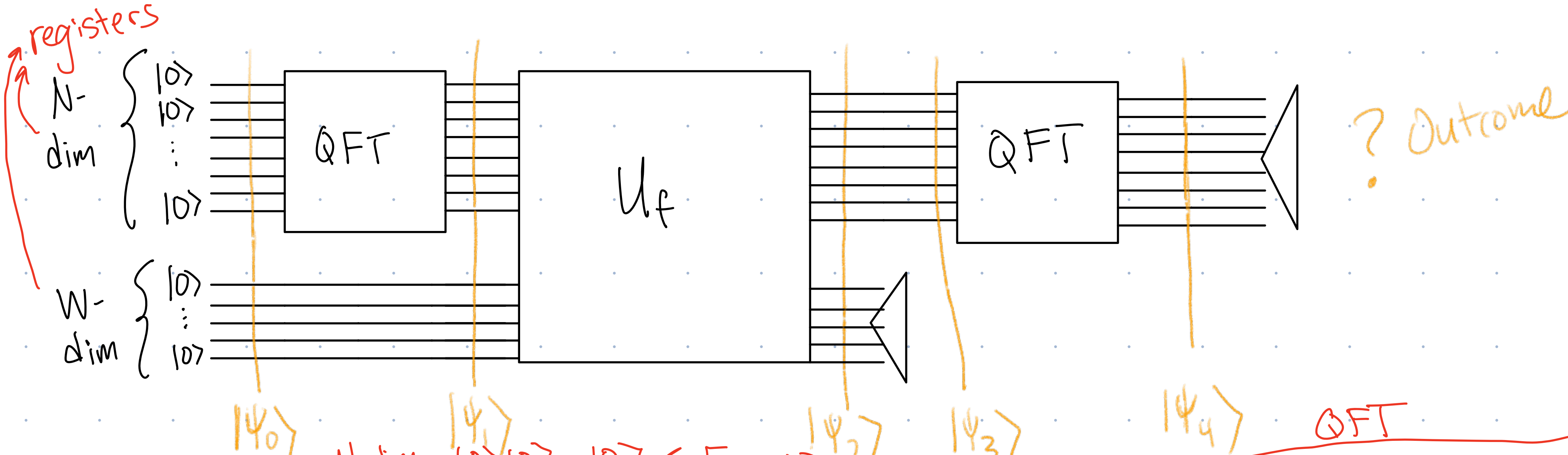
 = Standard basis measurement

- Measure entire state:

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

- Partial measurement (B system)
  - Factor standard basis states of measured register
  - Collapse + renormalize

Group Excercise: Analyze!



N-dim

$|0\rangle|0\rangle\cdots|0\rangle \leftarrow \lceil \log_2 N\rceil$ qubits

W-dim

$$|\psi_0\rangle = |0\rangle|0\rangle$$

QFT

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

$$|\psi_1\rangle = (QFT\otimes I)|0\rangle|0\rangle = (QFT|0\rangle)\otimes|0\rangle$$

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

U_f

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

$$|\psi_2\rangle = U_f\left[\left(\frac{1}{\sqrt{N}}\sum_{y=0}^{N-1}|y\rangle\right)\otimes|0\rangle\right]$$

$$= \frac{U_f}{\sqrt{N}}\left[(|0\rangle+|1\rangle+|2\rangle+\cdots|N-1\rangle)|0\rangle\right]$$

$$= U_f \frac{1}{\sqrt{N}} \left(|0\rangle|0\rangle + |1\rangle|0\rangle + |2\rangle|0\rangle + \cdots |N-1\rangle|0\rangle \right)$$

$$= U_f \frac{1}{\sqrt{N}} \left(\sum_{y=0}^{N-1} |y\rangle|0\rangle \right)$$

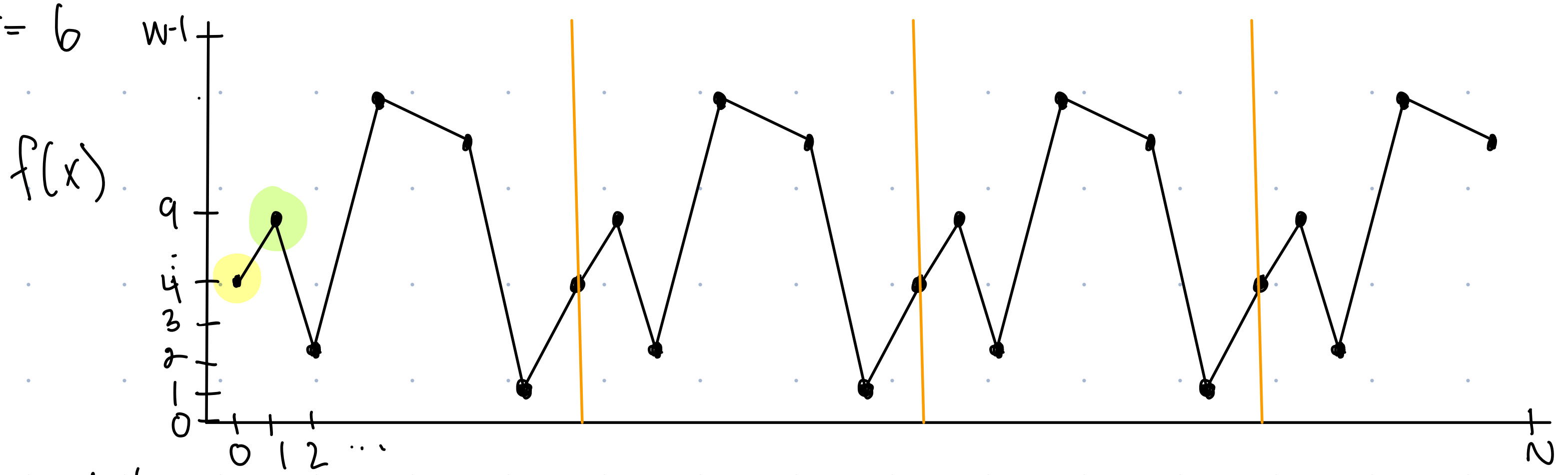
$$= \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} U_f |x\rangle|0\rangle$$

$$= \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle|0 + f(x) \bmod w\rangle$$

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

ex:

$r = 6$



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

$$\frac{1}{\sqrt{N}} \Big(|0\rangle_A |4\rangle_B + |1\rangle_A |9\rangle_B + |2\rangle_A |2\rangle_B + |3\rangle|13\rangle + |4\rangle|12\rangle + |5\rangle|1\rangle +$$
$$|6\rangle|4\rangle + |7\rangle|9\rangle + |8\rangle|2\rangle + |9\rangle|13\rangle + |10\rangle|12\rangle + |11\rangle|1\rangle +$$
$$|12\rangle|4\rangle + |13\rangle|9\rangle + |14\rangle|2\rangle + |15\rangle|13\rangle + |16\rangle|12\rangle + |17\rangle|1\rangle + \cdots$$

measure $|9\rangle$ collapse

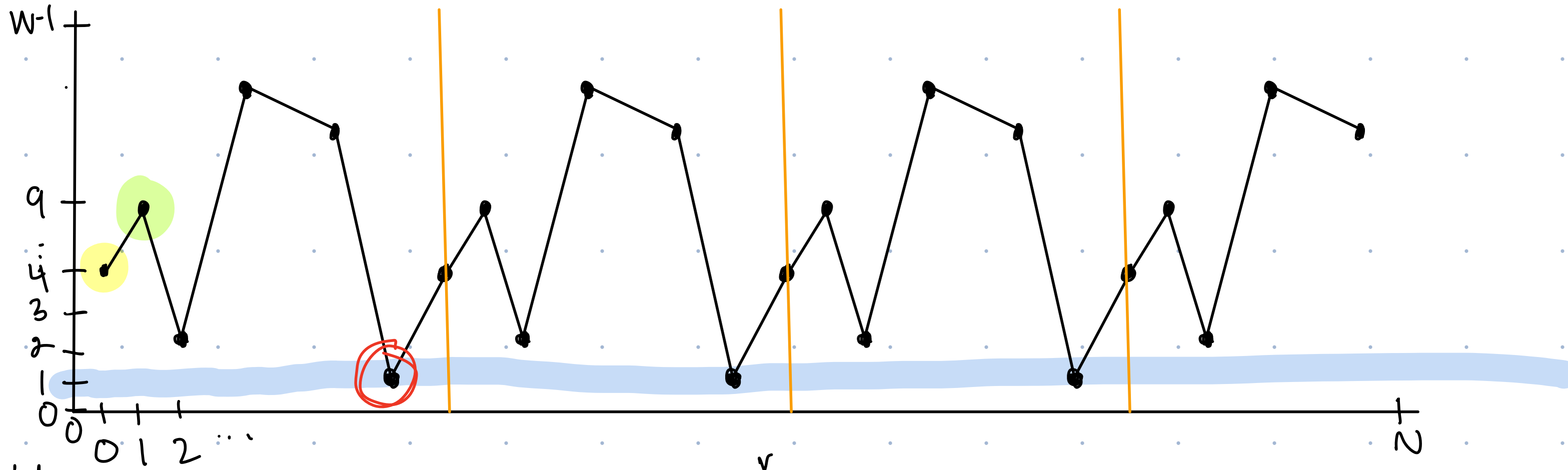
measure $|13\rangle$ collapse

$$\frac{1}{\sqrt{p(9)}} \left(\frac{1}{\sqrt{N}} |1\rangle + \frac{1}{\sqrt{N}} |7\rangle + \frac{1}{\sqrt{N}} |13\rangle + \cdots \right) |9\rangle$$

$$\frac{1}{\sqrt{p(13)}} \left(\frac{1}{\sqrt{N}} |3\rangle + \frac{1}{\sqrt{N}} |9\rangle + \frac{1}{\sqrt{N}} |15\rangle + \cdots \right) |13\rangle$$

HOW TO REPRESENT THE COLLAPSED STATE?

r = 6



After U_f:

$$\frac{1}{\sqrt{N}}\Big(|0\rangle_A|4\rangle_B + |1\rangle_A|9\rangle_B + |2\rangle_A|2\rangle_B + |3\rangle|13\rangle + |4\rangle|12\rangle + |5\rangle|1\rangle +$$
$$|6\rangle|4\rangle + |7\rangle|9\rangle + |8\rangle|2\rangle + |9\rangle|13\rangle + |10\rangle|12\rangle + |11\rangle|1\rangle +$$
$$|12\rangle|4\rangle + |13\rangle|9\rangle + |14\rangle|2\rangle + |15\rangle|13\rangle + |16\rangle|12\rangle + |17\rangle|1\rangle + \cdots$$

If measure outcome $|y\rangle$ in 2nd register, let b^* be the value such that:

- $f(b^*) = y$
- b^* is in the first period.

} define b^*

If outcome is $|1\rangle$, what is b^* for above f?

A) 0 B) 1 C) 5 D) No b^* exists.

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

$$\frac{1}{\sqrt{N}} \Big(|0\rangle_A |4\rangle_B + |1\rangle_A |9\rangle_B + |2\rangle_A |2\rangle_B + |3\rangle|13\rangle + |4\rangle|12\rangle + |5\rangle|1\rangle +$$
$$|6\rangle|4\rangle + |7\rangle|9\rangle + |8\rangle|2\rangle + |9\rangle|13\rangle + |10\rangle|12\rangle + |11\rangle|1\rangle +$$
$$|12\rangle|4\rangle + |13\rangle|9\rangle + |14\rangle|2\rangle + |15\rangle|13\rangle + |16\rangle|12\rangle + |17\rangle|1\rangle + \cdots$$

measure $|9\rangle$ collapse

measure $|13\rangle$ collapse

b^* $\quad b^*+r \quad b^*+2r$

$$\frac{1}{\sqrt{p(9)}} \left(\frac{1}{\sqrt{N}} |1\rangle + \frac{1}{\sqrt{N}} |7\rangle + \frac{1}{\sqrt{N}} |13\rangle + \cdots \right) |9\rangle$$

$$\frac{1}{\sqrt{p(13)}} \left(\frac{1}{\sqrt{N}} |3\rangle + \frac{1}{\sqrt{N}} |9\rangle + \frac{1}{\sqrt{N}} |15\rangle + \cdots \right) |13\rangle$$

$$\frac{1}{\sqrt{p(f(b^*))}} \frac{1}{\sqrt{N}} \sum_{m=0}^{\frac{N}{r}-1} |b^* + m \underbrace{r}_{\text{period}}\rangle |\cancel{f(b^*)}\rangle$$

ignore

$\frac{N}{r}$ = # of repeats of periods

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

$$\frac{1}{\sqrt{N}} \Big(|0\rangle_A |4\rangle_B + |1\rangle_A |9\rangle_B + |2\rangle_A |2\rangle_B + |3\rangle|13\rangle + |4\rangle|12\rangle + |5\rangle|1\rangle +$$
$$|6\rangle|4\rangle + |7\rangle|9\rangle + |8\rangle|2\rangle + |9\rangle|13\rangle + |10\rangle|12\rangle + |11\rangle|1\rangle +$$
$$|12\rangle|4\rangle + |13\rangle|9\rangle + |14\rangle|2\rangle + |15\rangle|13\rangle + |16\rangle|12\rangle + |17\rangle|1\rangle + \cdots$$

measure $|9\rangle$ collapse

$$\frac{1}{\sqrt{p(9)}} \left(\frac{1}{\sqrt{N}} |1\rangle + \frac{1}{\sqrt{N}} |7\rangle + \frac{1}{\sqrt{N}} |13\rangle + \cdots \right) |9\rangle$$

measure $|13\rangle$ collapse

$$\frac{1}{\sqrt{p(13)}} \left(\frac{1}{\sqrt{N}} |3\rangle + \frac{1}{\sqrt{N}} |9\rangle + \frac{1}{\sqrt{N}} |15\rangle + \cdots \right) |13\rangle$$

Generally: $\dfrac{1}{\sqrt{p(f(b^*))}} \dfrac{1}{\sqrt{N}} \displaystyle\sum_{m=0}^{N/r-1} |b^* + mr\rangle \cancel{|f(b^*)\rangle}$

Add abs squared of amplitudes in this part

$$= \left|\frac{1}{\sqrt{N}}\right|^2 + \left|\frac{1}{\sqrt{N}}\right|^2 + \cdots \left|\frac{1}{\sqrt{N}}\right|^2 = (\#) \cdot \frac{1}{N} = \frac{N}{r} \cdot \frac{1}{N} = \frac{1}{r}$$

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

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

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

$$|\psi_4\rangle = \sqrt{\frac{r}{N}} \sum_{m=0}^{\frac{N}{r}-1} \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi i y (b^* + mr)/N} |y\rangle$$

$$\underbrace{\omega|0\rangle + \omega|1\rangle + \omega|2\rangle + \ldots \omega|N-1\rangle}_{m=0} + \underbrace{\xi|0\rangle + \xi|1\rangle + \ldots + \xi|N-1\rangle}_{m=1} + \underbrace{\_\_\_\_}_{m=2}$$

Switch order of summation:

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

$$e^{2\pi i y b^*/N} \; e^{2\pi i y mr/N}$$

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

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

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

Pull m out of exponent

Prob. of outcome y: $\left| \frac{\sqrt{r}}{N} e^{2\pi i b^* y/N} \boxed{\sum_{m=0}^{\frac{N}{r}-1} \left(e^{2\pi i y r/N} \right)^m} \right|^2$

Geometric Series:

$$\sum_{m=0}^{t-1} a^m$$

In our case:

- $a = e^{2\pi i y r/N}$
- $t = N/r$

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

<u>Case 1</u>

$$a \neq 1 \leftrightarrow e^{2\pi i yr/N} \neq 1$$

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

$$= \frac{1-\cancelto{1}{e^{2\pi i y}}}{1-e^{2\pi i yr/N}}$$

$$=0$$

<u>Case 2</u>

$$a=1 \leftrightarrow e^{2\pi i yr/N}=1$$

$$\leftrightarrow \frac{yr}{N} = k \in \mathbb{Z}$$

$$\leftrightarrow y = \frac{kr}{N} \text{ for } k\in\mathbb{Z}$$

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

Prob. of outcome y: $\left| \frac{\sqrt{r}}{N} e^{2\pi i b^* y/N} \boxed{\sum_{m=0}^{\frac{N}{r}-1} \left(e^{2\pi i y r/N}\right)^m} \right|^2$

Plugging in:

Case 1

$$\left| \frac{\sqrt{r}}{N} e^{2\pi i b^* y/N} \cdot 0 \right|^2 = 0$$

Case 2

$$\left| \frac{\sqrt{r}}{N} e^{2\pi i b^* y/N} \frac{N}{r} \right|^2$$

$$= \cancelto{1}{\left| e^{2\pi i b^* y/N} \right|^2} \frac{1}{r}$$

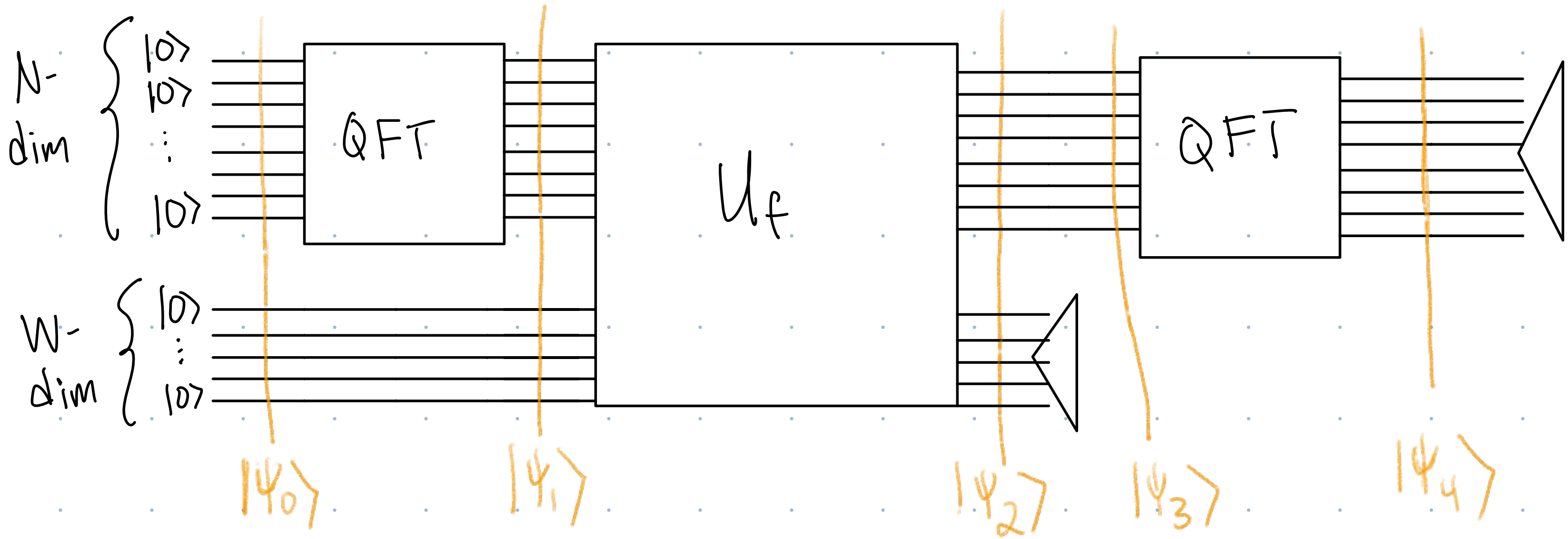
$$= \frac{1}{r}$$

End result: Final measurement of first register will always result in a multiple of $\frac{N}{r}$

$$\Rightarrow y = \frac{kN}{r} \text{ for } k \in \mathbb{Z}$$

Period Finding Algorithm (Shor's Algorithm)

① Run 2 times:



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

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

② Continued Fractions $\quad y_1 \to \frac{s_1}{j_1} = \frac{k_1 N}{r} \qquad y_2 \to \frac{s_2}{j_2} = \frac{k_2 N}{r}$

ⓘ j_1 or j_2 will be r ⓘⓘ j_1, j_2 are factors of $r \to$ l.c.m.$(j_1, j_2) \Rightarrow r$

③ Check $f(0) \stackrel{?}{=} f(r)$

Successful with prob. $\geq 2/3$

Query Compexity of Period Finding

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

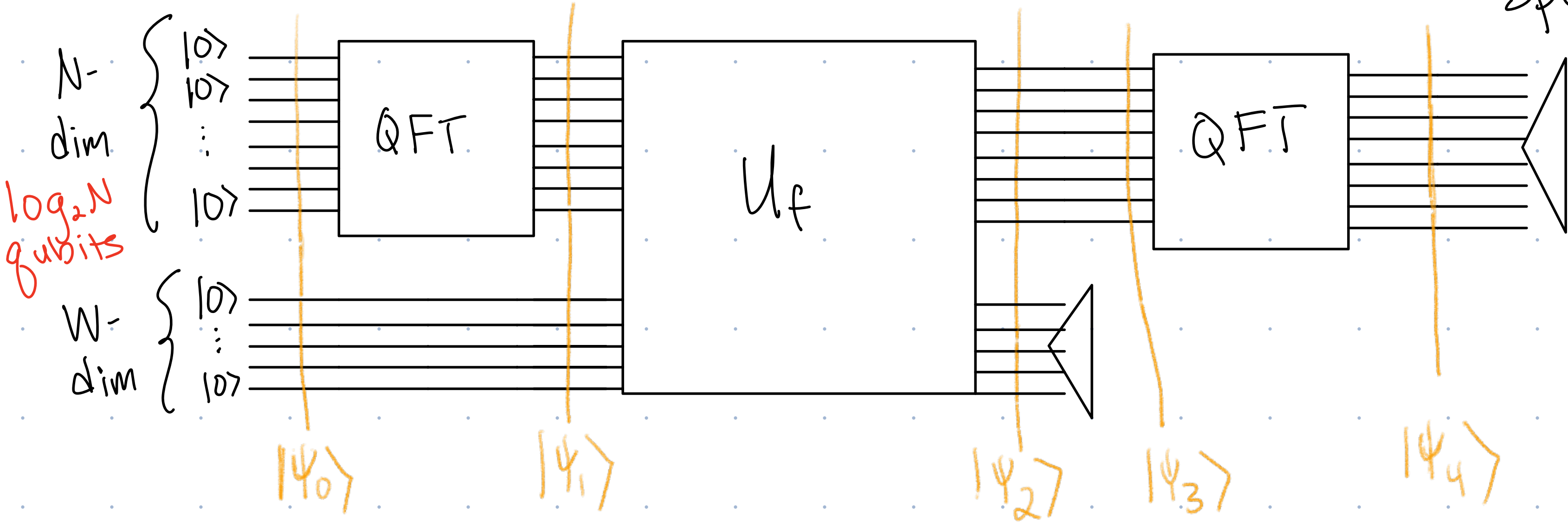
Quantum: $O(1)$

Time Complexity of Factoring

Quantum: $O(\log_2 N)$

Nearly Exponential Speedup!

Circuit used to factor N.



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

Classical: $e^{O(\log_2^{1/3} N)}$ $\quad$ Number Field Sieve

Pesky Detail:

We looked at prob of: $y = \frac{KN}{r}$

But if $\frac{N}{r} \notin \mathbb{N}$, y is a fraction... see pset.