FACTORING

Learning Goals

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

Announcements

- Check-In
- Project Proposal (grace period until Thurs) OH 12:30-1:30 Today; 12-1 Thurs.
- Participation: all but ~~3~~ 4 pset self assessments
- 11/13 exam ~~evening~~ in-class

- Winter Term:
  - 3 CS electives
  - Phil 1023 Ethics of AI and Alg.

Public Key Crypto (RSA)

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

Eve has access to: $\bar{m}$, K_{pub}, f, g $\rightarrow$ m

No direct access: m, K_{pri}

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

factoring a large number

$\underbrace{6701128736\ldots}_{617 \text{ digits}} = a \times b$

?

\$200K prize

\$100K for 308 digit

$\boxed{\checkmark}$ 250 digit

Quantum Computes Can Efficiently Factor

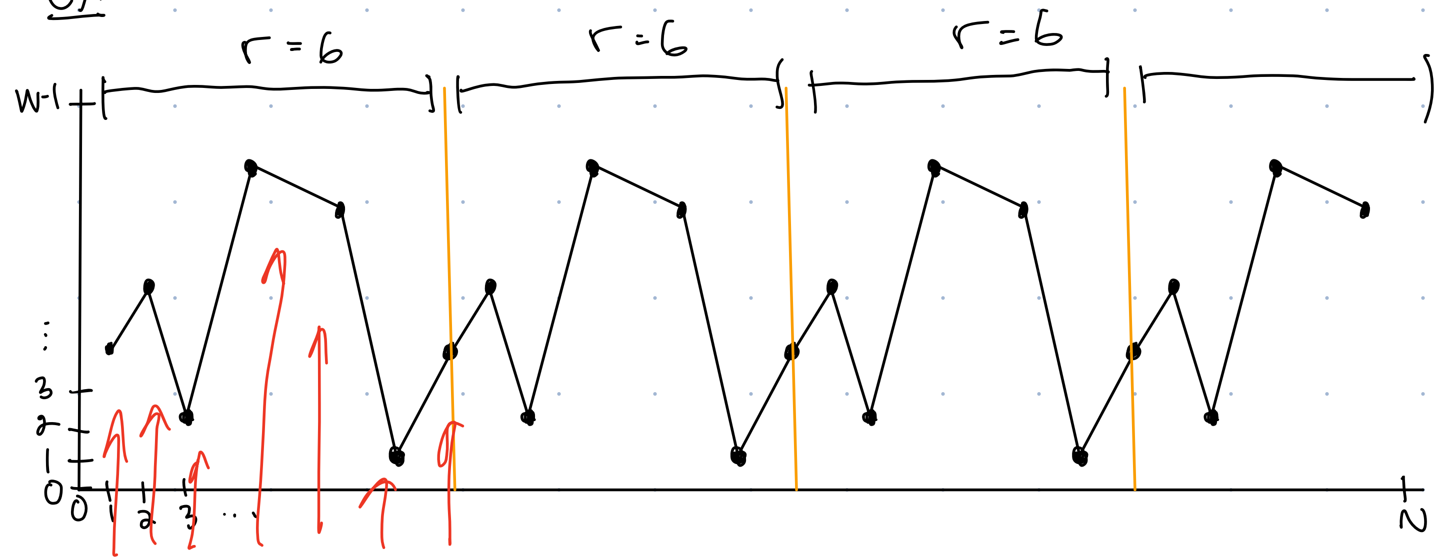
Factoring reduces (via number theory) to period finding:

Period Finding Problem

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

- 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:

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

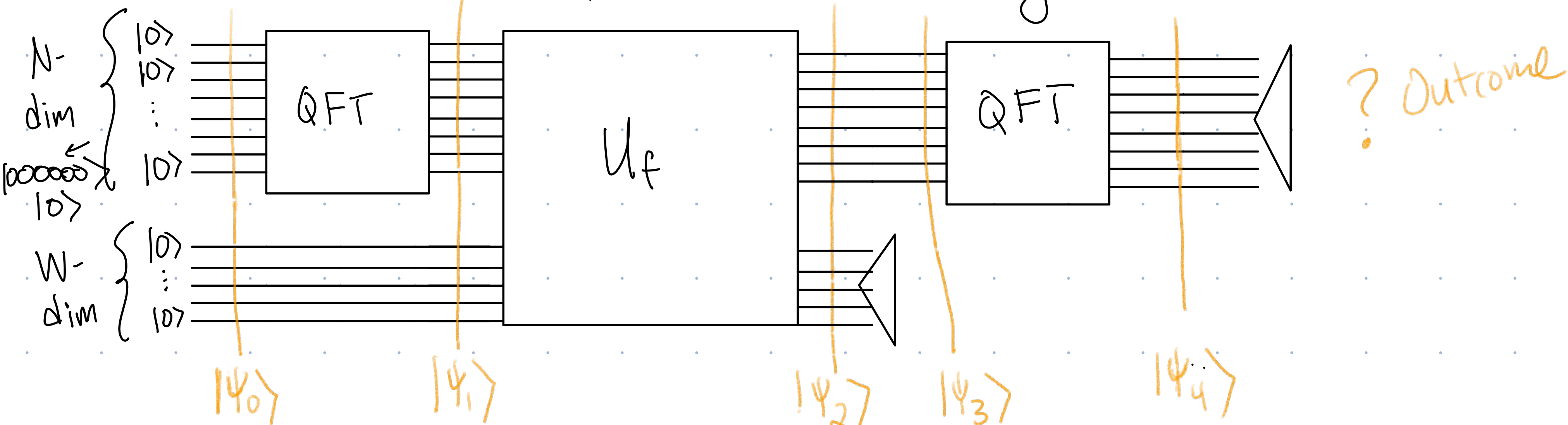
$|3\rangle \to |011\rangle$

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

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

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

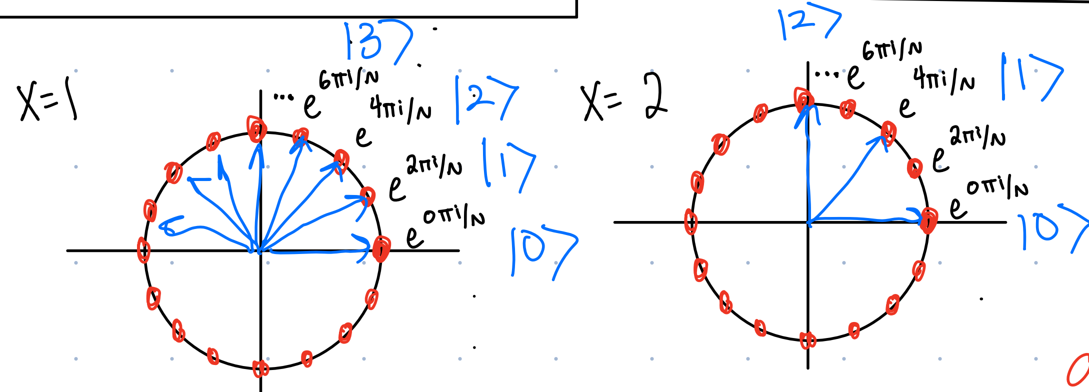
N-dim standard basis state

U_f:

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

N-dim W-dim s.b. states

Phase of each s.b. state in superposition

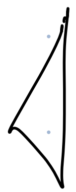


$$\boxed{QFT|0\rangle = ?}$$

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

go/fourier-transform

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

 = Standard basis measurement

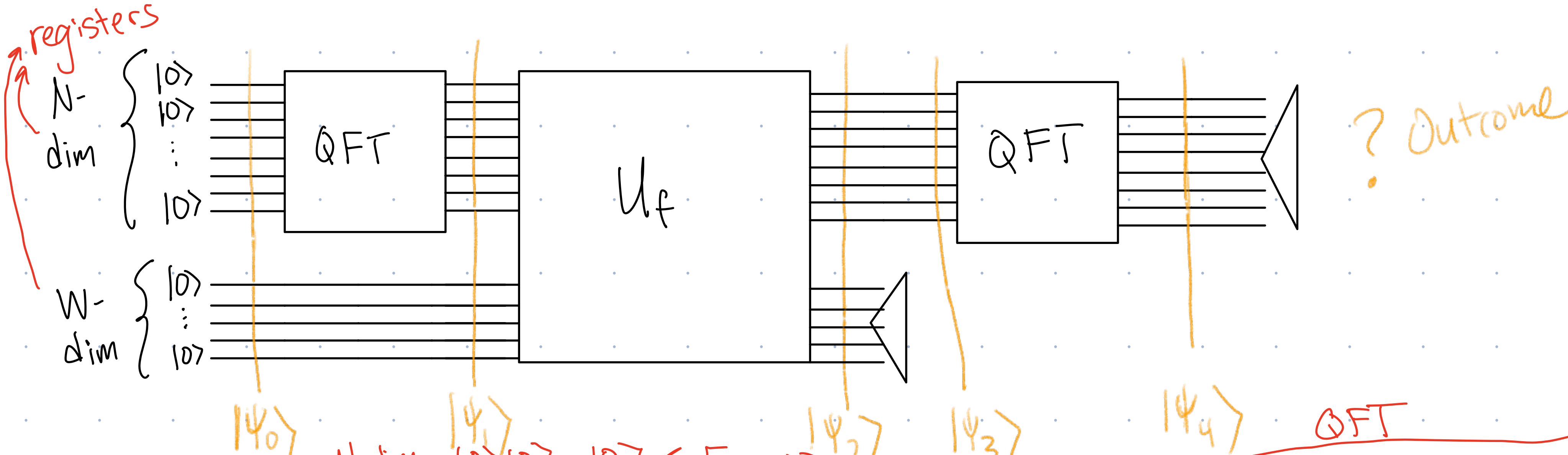
- Measure entire state:

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

- Partial measurement (B system)

  - Factor standard basis states of measured register
  - Collapse + renormalize

Group Excercise: Analyze!



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

W-dim

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

QFT

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

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

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

U_f

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

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

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

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

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

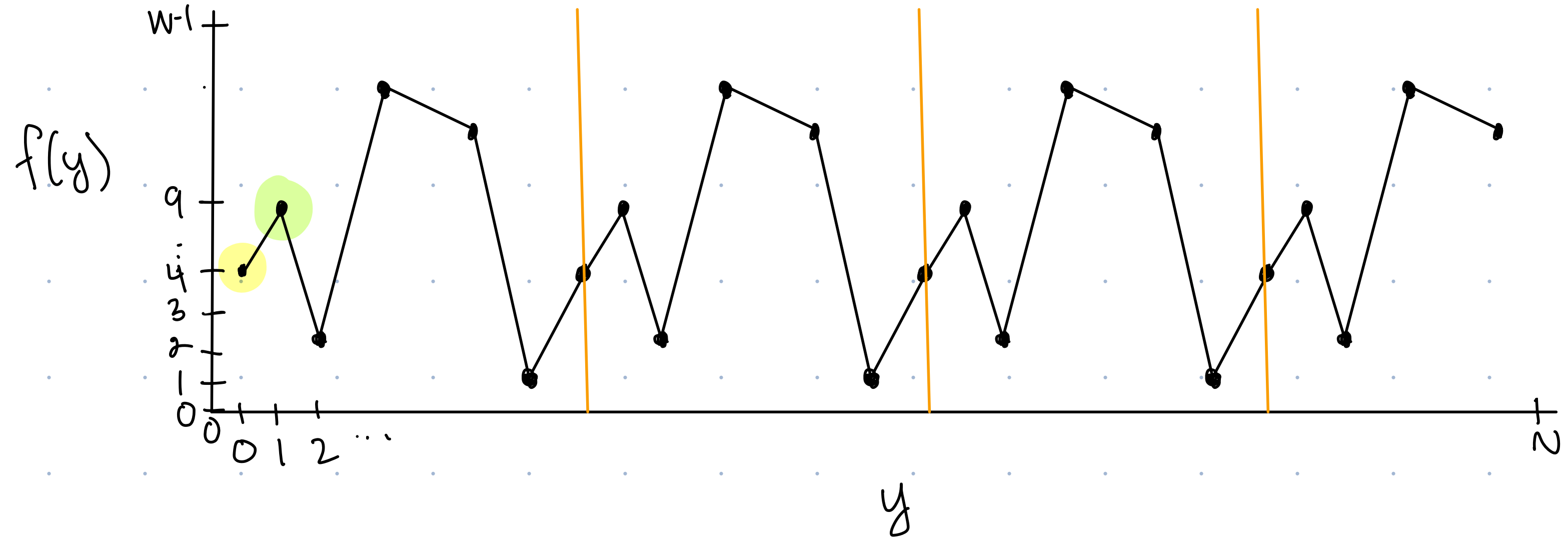
$$= \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} U_f |x\rangle|0\rangle$$

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

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

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 $|f(b^*)\rangle$

$r = 6$



Group!
- Name
- Pronouns (optional)
- 1 stressor
- 1 joy

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

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

$|f(b^*)\rangle$

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

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

Suppose measure outcome $|f(b^*)\rangle$: b^* is input that gives us $f(b^*)$, where b^* is in first period

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

N/r repeats

$$P(|f(b^*)\rangle) = \underbrace{\left|\frac{1}{\sqrt{N}}\right|^2 + \left|\frac{1}{\sqrt{N}}\right|^2 + \cdots \left|\frac{1}{\sqrt{N}}\right|^2}_{\frac{N}{r}} = \frac{N}{r} \cdot \frac{1}{N} = \frac{1}{r}$$

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

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

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

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

Plugging In:

$|\psi_4\rangle =$

$|\psi_5\rangle =$

$=$

$=$

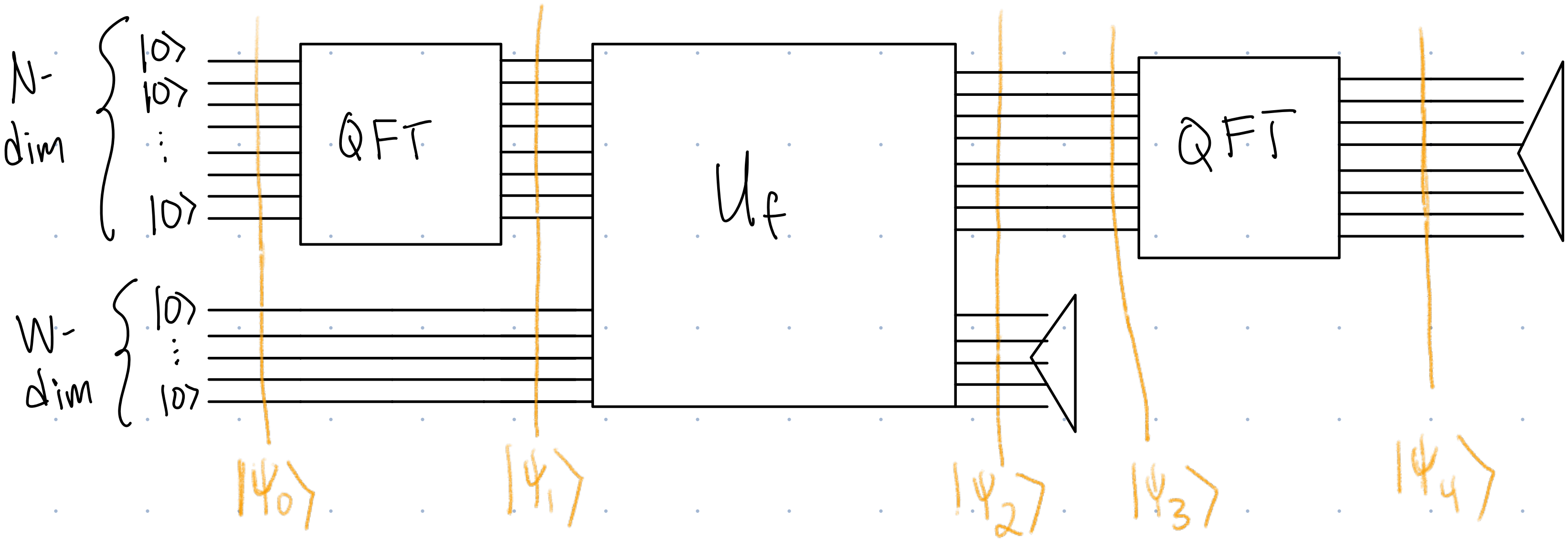
Probability of Outcome $|z^*\rangle \rightarrow |\text{amplitude of } |z^*\rangle|^2$

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)

① Run 2 times:



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

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

②

③

Query Compexity of Period Finding

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

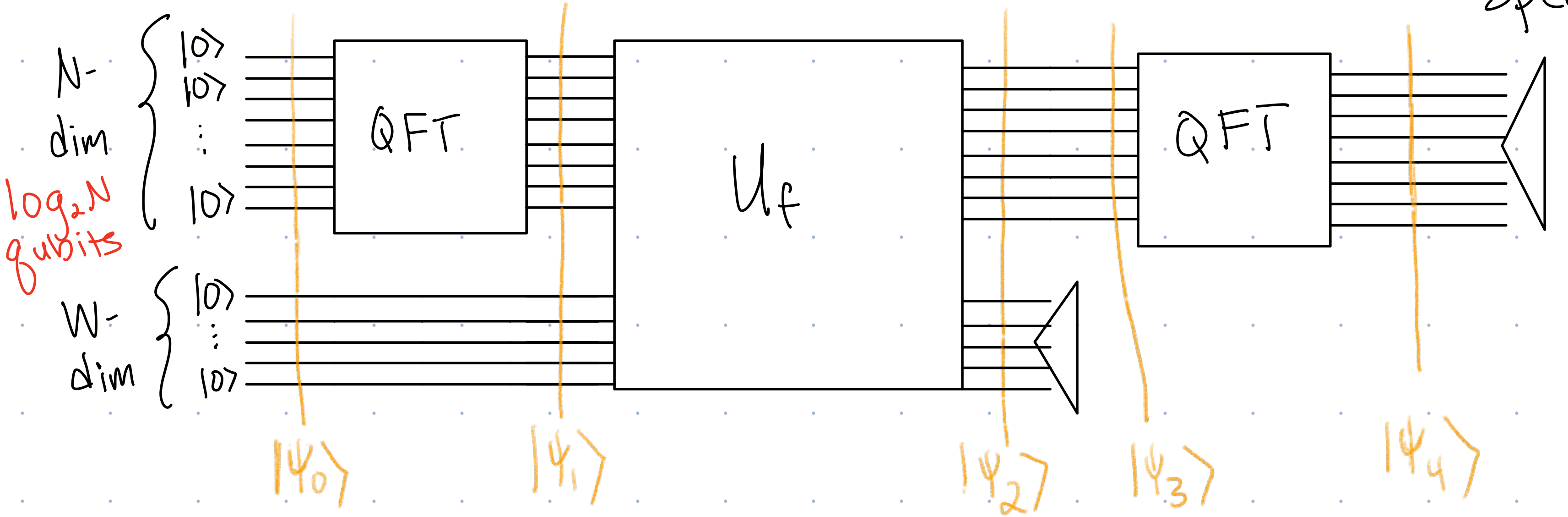
Quantum: $O(1)$

Time Complexity of Factoring

Quantum: $O(\log_2 N)$

Nearly Exponential Speedup!

Circuit used to factor N.



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

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

Pesky Detail:

We looked at prob of: $z^* = \frac{KN}{r}$

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