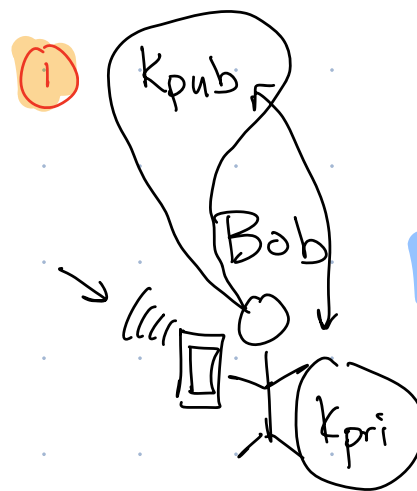
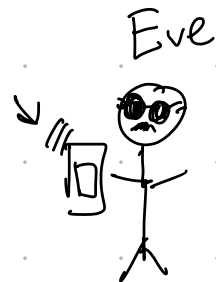


FACTORING

Learning Goals

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

Public Key Crypto (RSA)



④

$$m = g(\bar{m}, k_{pri})$$

⑥ Secret message
 $m \in \{0,1\}^n$

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

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

factoring a large number

6701128736....

617 digits

$$= a \times b$$

?

\$200K prize

\$100K for 308 digit



250 digit

Quantum Computers Can Efficiently Factor

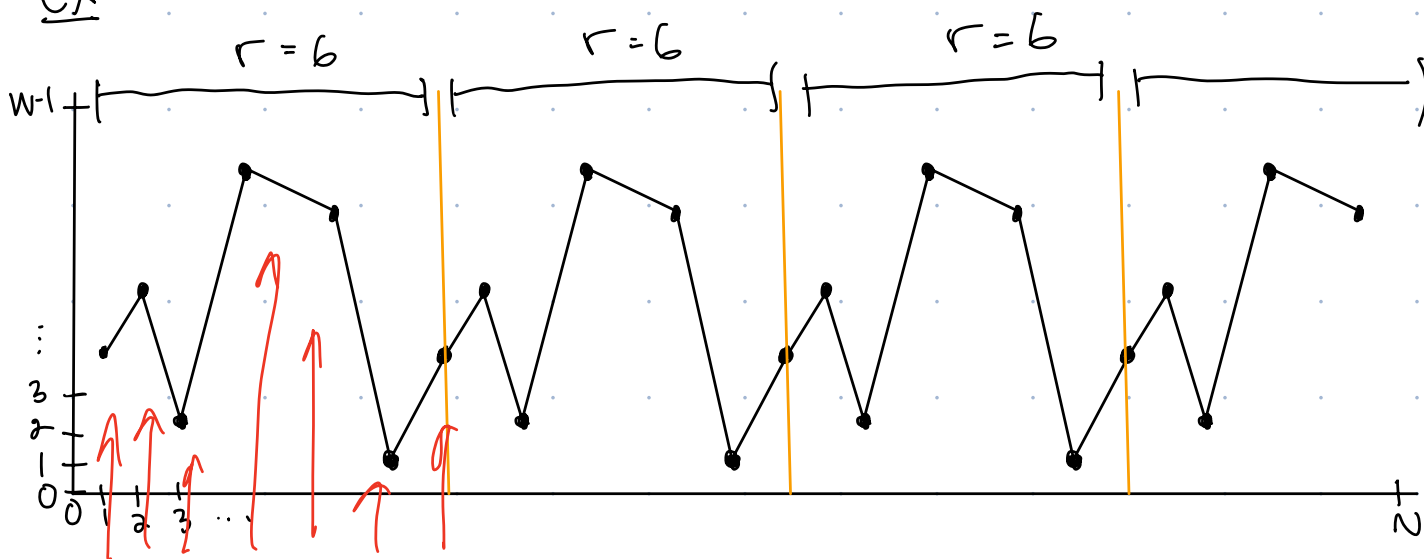
Factoring reduces (via number theory) to period finding:

Period Finding Problem

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

- 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:

$$011 \leftrightarrow 3$$

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

10011

2^4
↑
16-dimensional

Ambiguity:

$$|3\rangle \rightarrow |11\rangle$$

$$|3\rangle \rightarrow |011\rangle$$

$$|3\rangle \rightarrow |1000011\rangle$$

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

Standard Basis States:

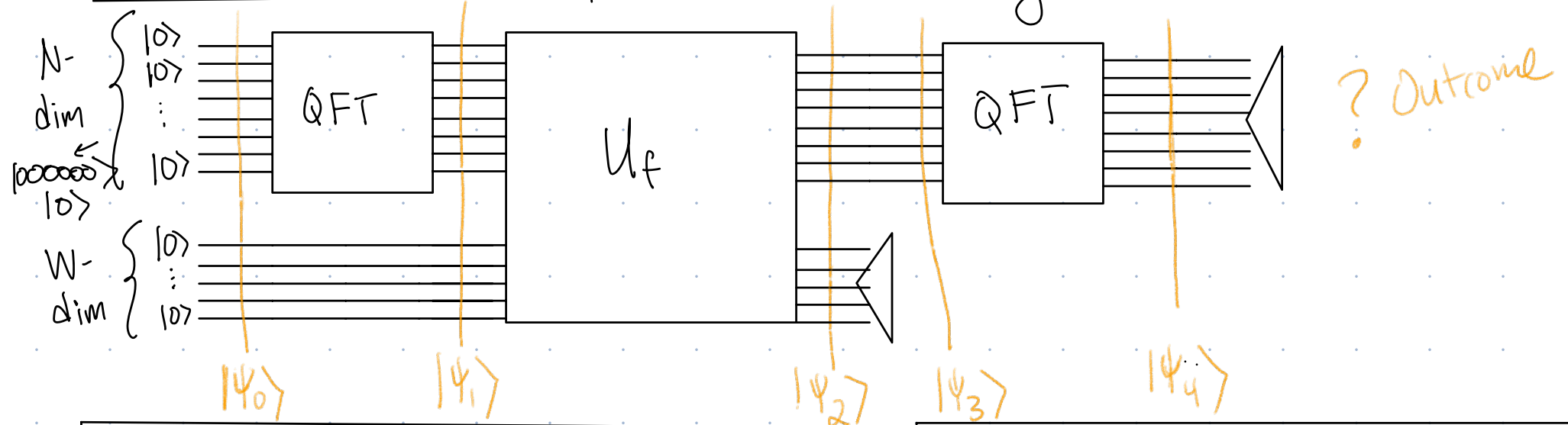
$$\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$$

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

N -dimensional system

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

Quantum Circuit for Period Finding



QFT: Quantum Fourier Transform

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

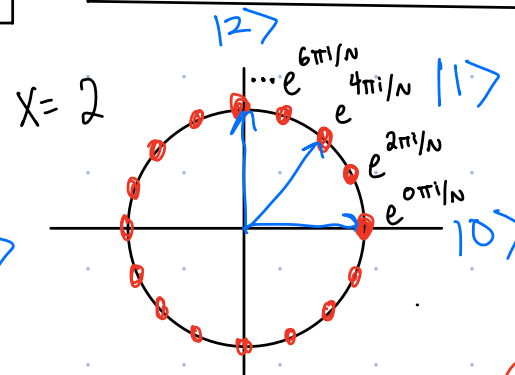
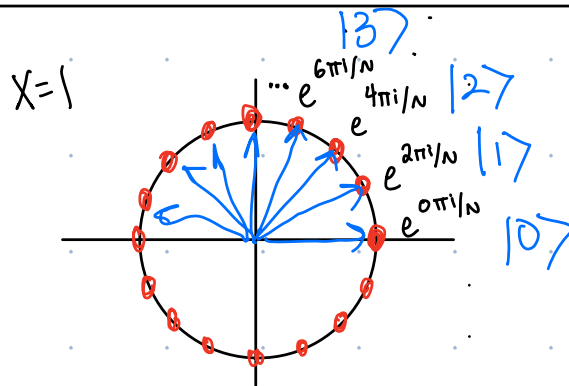
$\uparrow$
N-dim
standard basis state

U_f :

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

$\uparrow$ $\uparrow$
N-dim W-dim
s.b. states

Phase of
each s.b.
state in
superposition



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

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

go/fourier-transform

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

$\triangleleft$ = Standard
basis
measurement

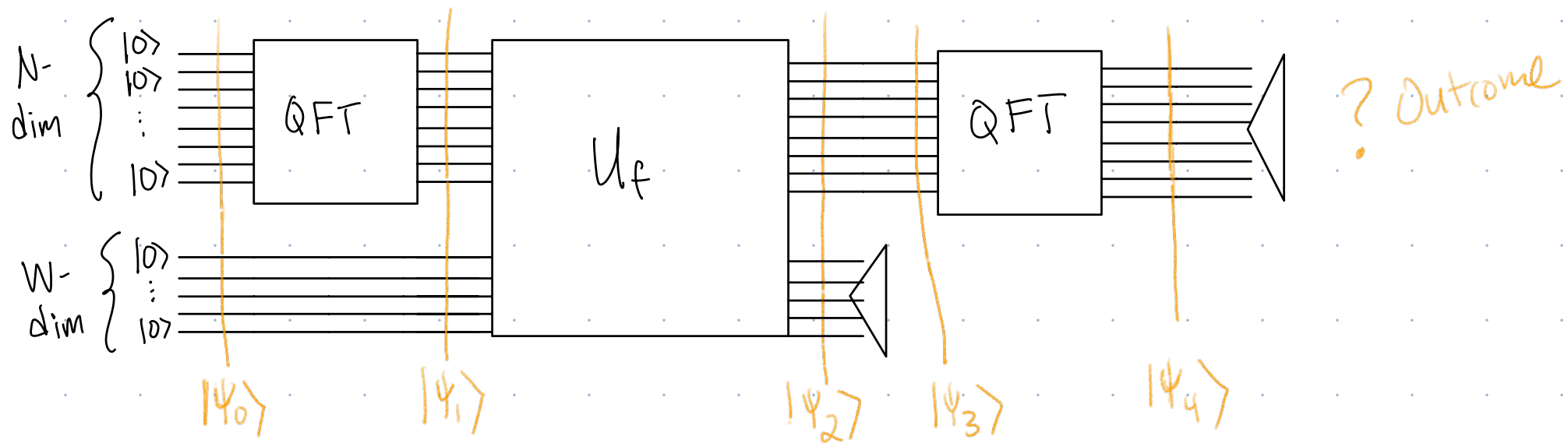
- Measure entire state:

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

- Partial measurement (B system)

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

Group Exercise: Analyze!



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

$$|\psi_1\rangle =$$

=

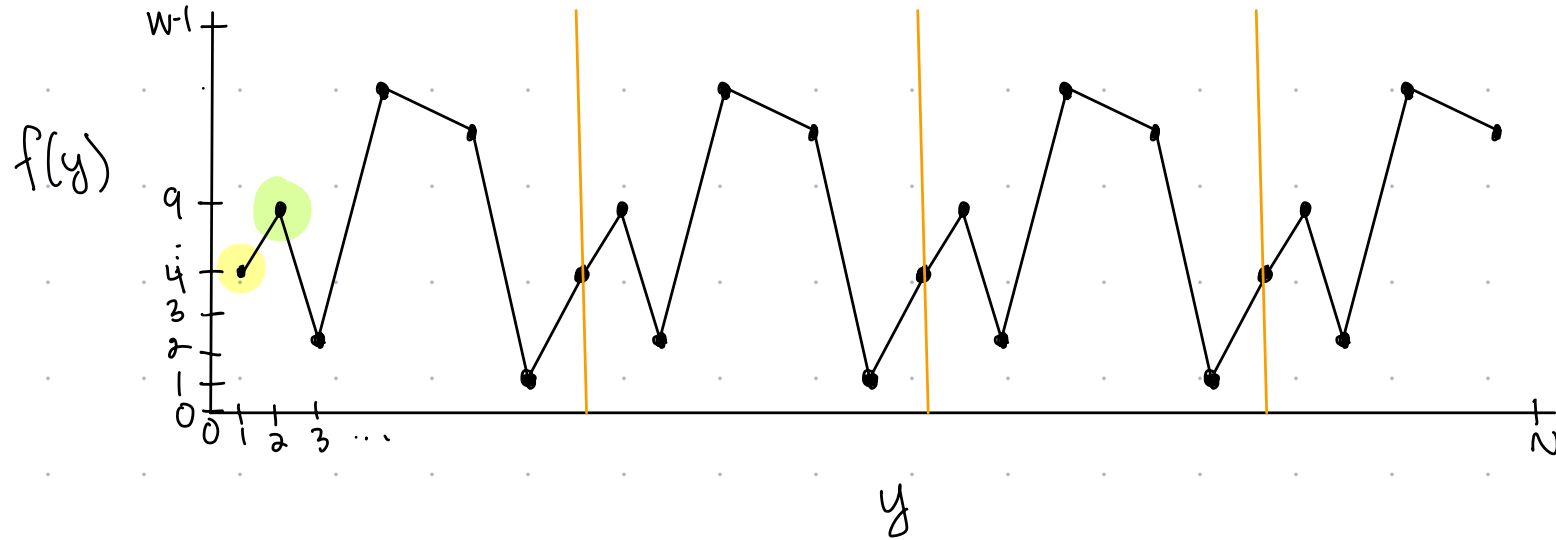
$$|\psi_2\rangle =$$

$$|\psi_3\rangle = \boxed{} \sum_{m=0}^{\boxed{}} |b^* + \boxed{}\rangle$$

(outcome of partial measurement is $f(b^*)$)

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 $|f(b^*)\rangle$?

$r=5$



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

$$|\psi_4\rangle =$$

$$=$$

Plugging In:

$$|\psi_4\rangle =$$

$$|\psi_5\rangle =$$

"

"

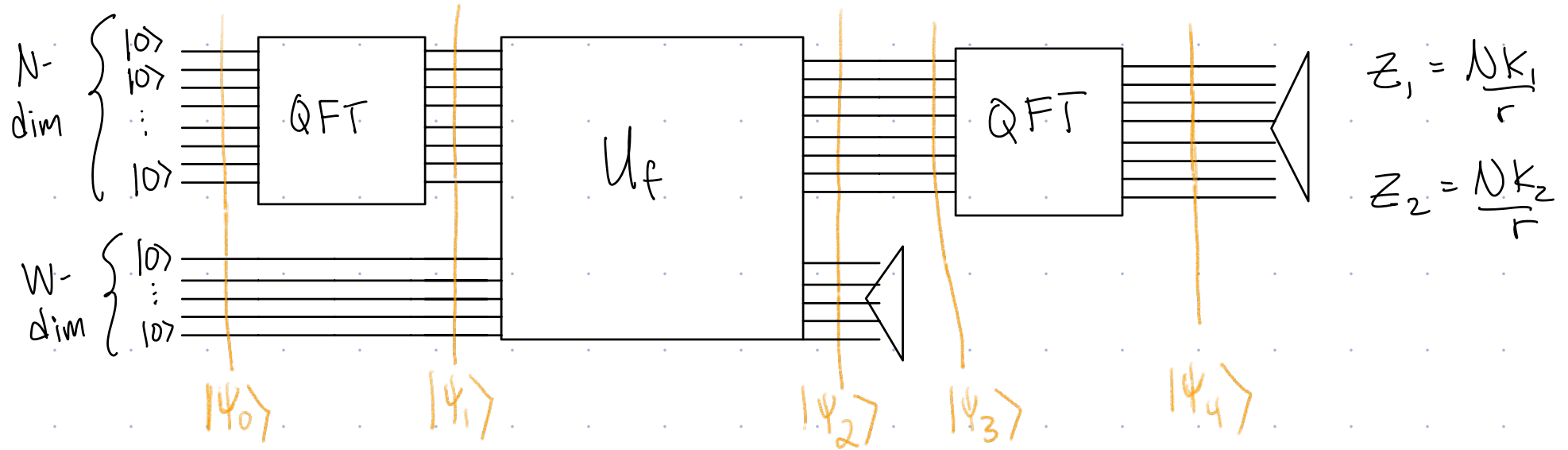
Probability of Outcome $|z\rangle \rightarrow |\text{amplitude of } |z^*\rangle|^2$

Geometric Series Formula:

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

Period Finding Algorithm (Shor's Algorithm)

① Run 2 times:



②

③

Query Complexity of Period Finding

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

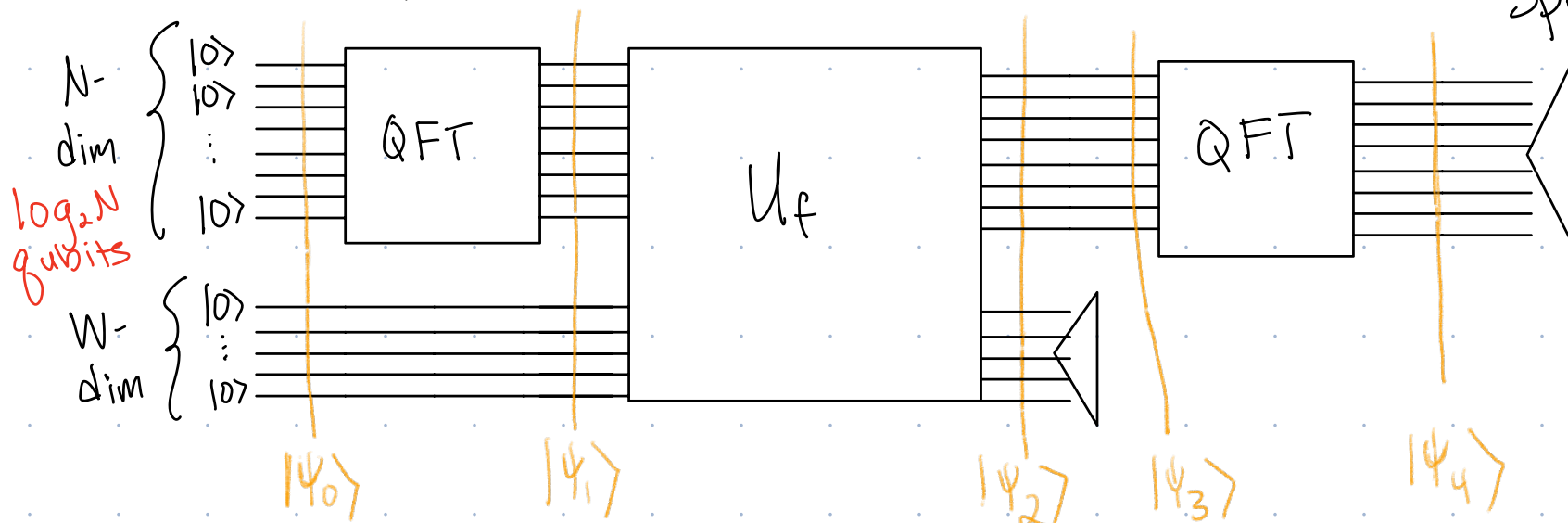
Quantum: $O(1)$

Time Complexity of Factoring

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

Circuit used to factor N .

Nearly Exponential
Speedup!



$O(\log^2 N)$

$O(\log^2 N)$

$O(\log^2 N)$

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

Classical: $e^{O(\log^{1/3} N)}$

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.