FACTORING

Learning Goals

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

Public Key Crypto (RSA)

Eve has access to:

If she could:

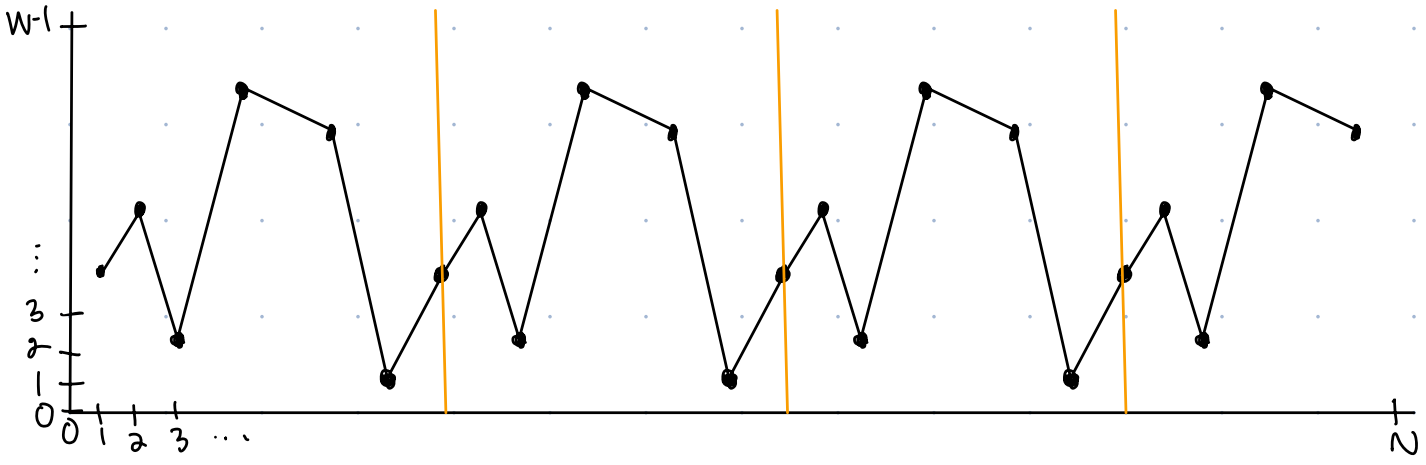
6701128736....

Factoring reduces (via number theory) to period finding:

Period Finding Problem

Input:

ex:



Output: r

What is the classical query complexity of factoring?

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:

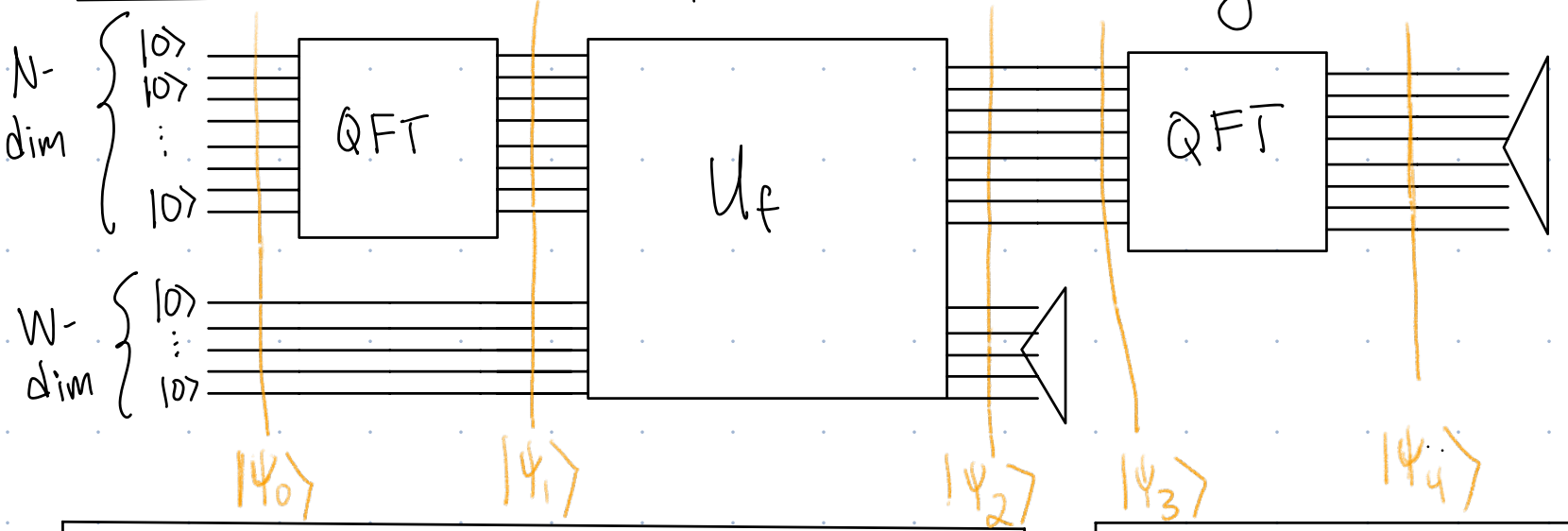
Standard Basis States:

Ambiguity:

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

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

Quantum Circuit for Period Finding

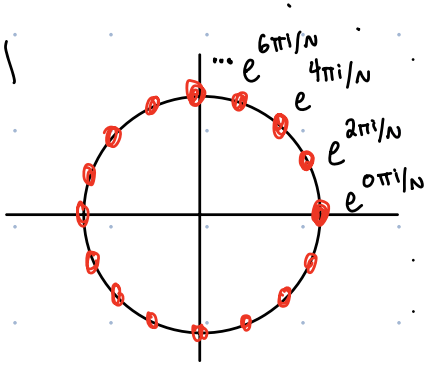


QFT: Quantum Forier Transform

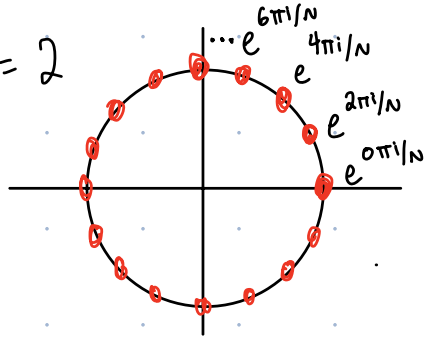
U_f:

Phase of each s.b. state in superposition

X=1



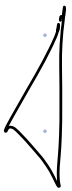
X= 2



$QFT|0\rangle = ?$

go/fourier-transform

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

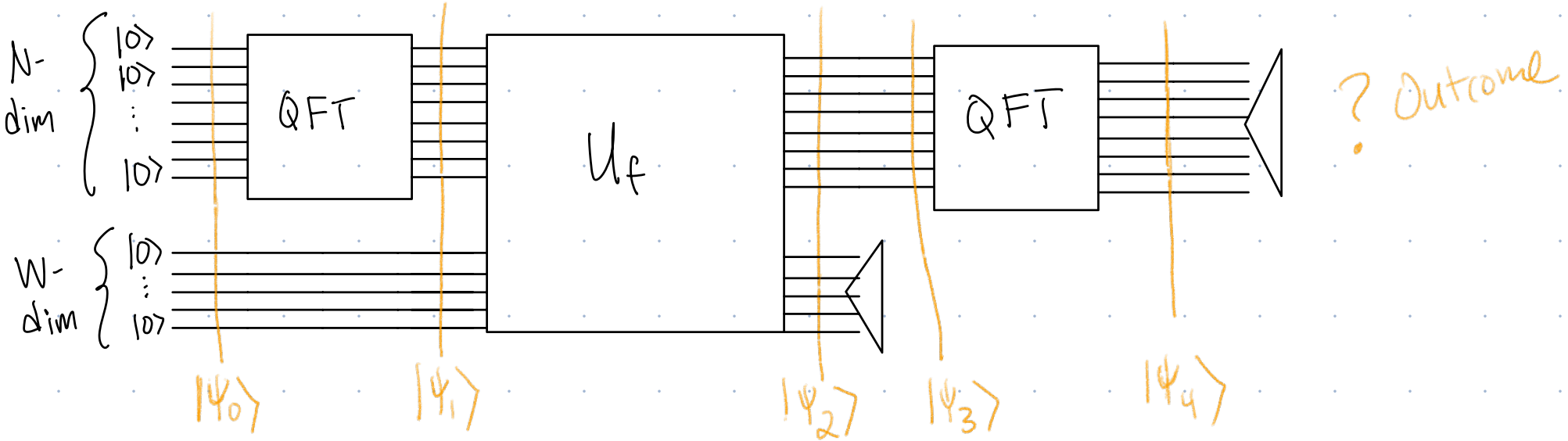
 = Standard basis measurement

- Measure entire state:

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

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

Group Excercise: Analyze!



$|\psi_0\rangle =$

$|\psi_1\rangle =$

$=$

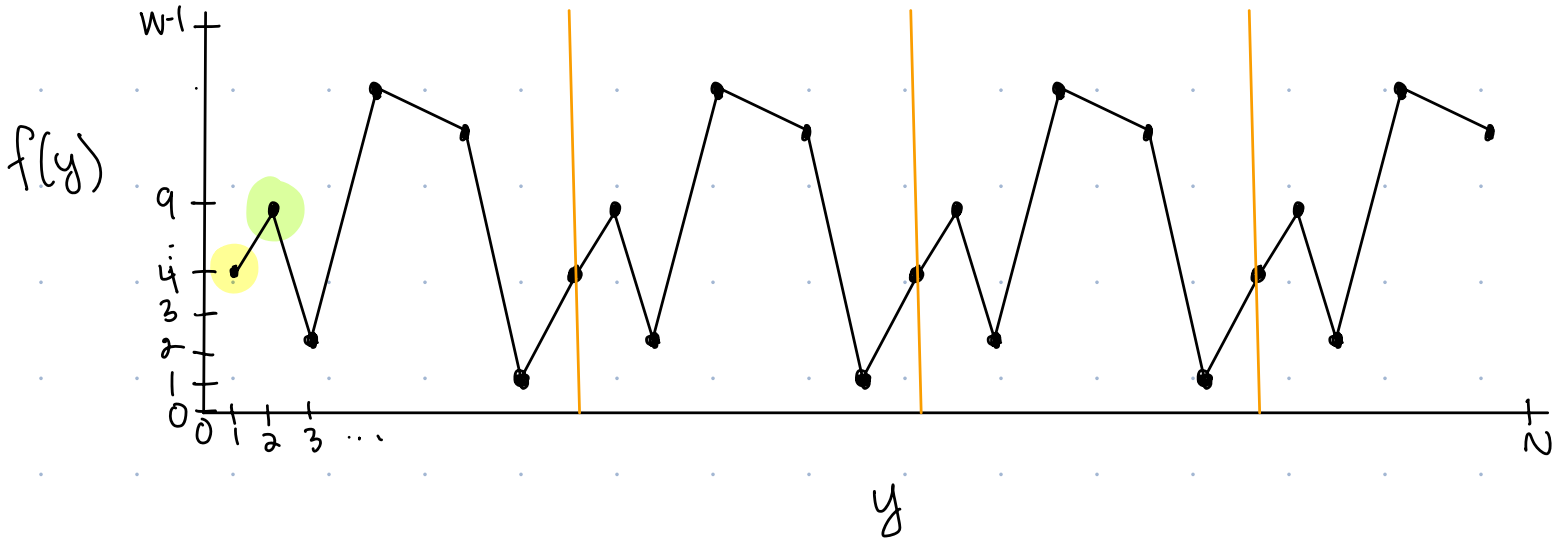
$|\psi_2\rangle =$

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

(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:

$|\psi_4\rangle =$

$|\psi_5\rangle =$

$=$

$=$

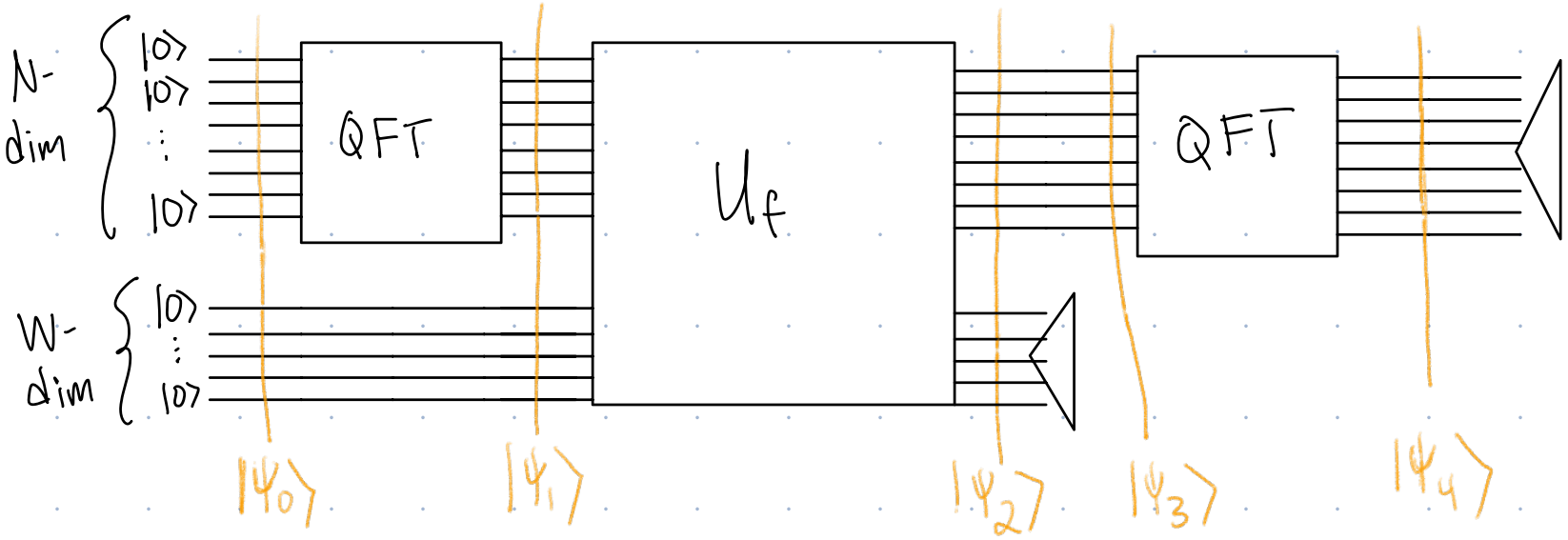
Probability of Outcome $|z^*\rangle \rightarrow |\text{amplitude of } |z^*\rangle|^2$

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:



$z_1 = \frac{Nk_1}{r}$

$z_2 = \frac{Nk_2}{r}$

②

③

Query Compexity of Period Finding

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

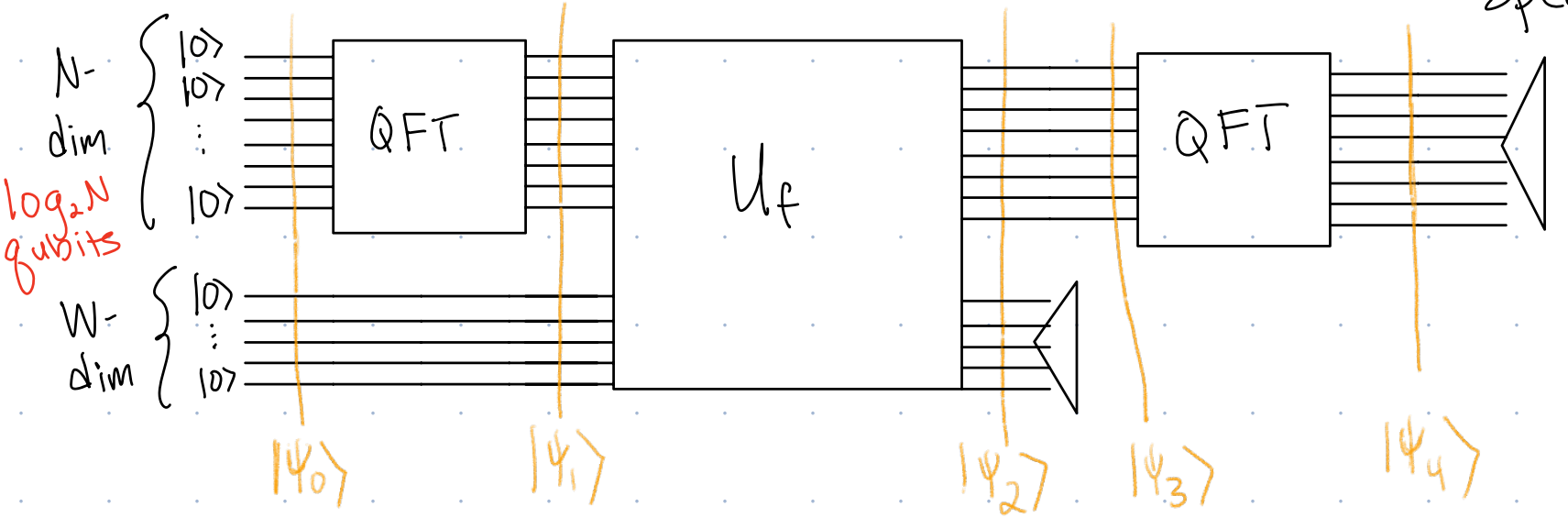
Quantum: $O(1)$

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.