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 $\overline{m}$, K_{pub}, f

If she could solve a hard math problem, she could learn m.

$6701128736\ldots$ =

Period Finding

Period Finding Problem

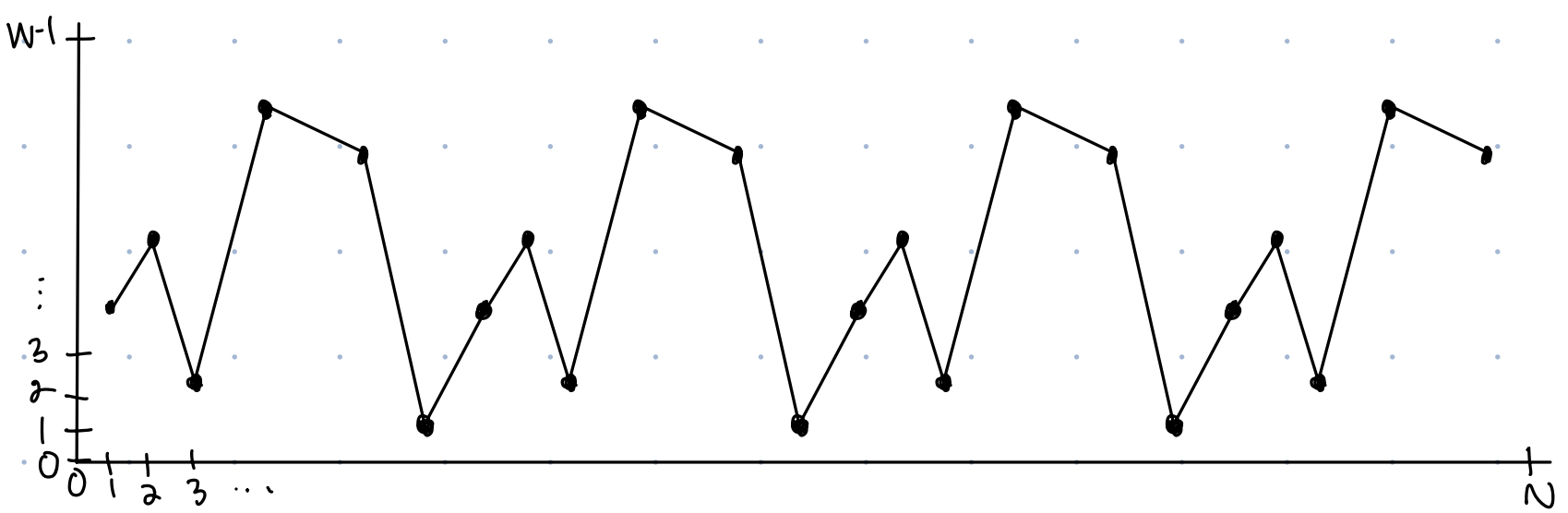
Input: Query access to f

-

-

-

ex:



Output:

What is the classical query complexity of period finding

A) $O(\sqrt{r})$ B) $O(r)$ C) $O(r^2)$ D) $O(N)$

Bits to Digits

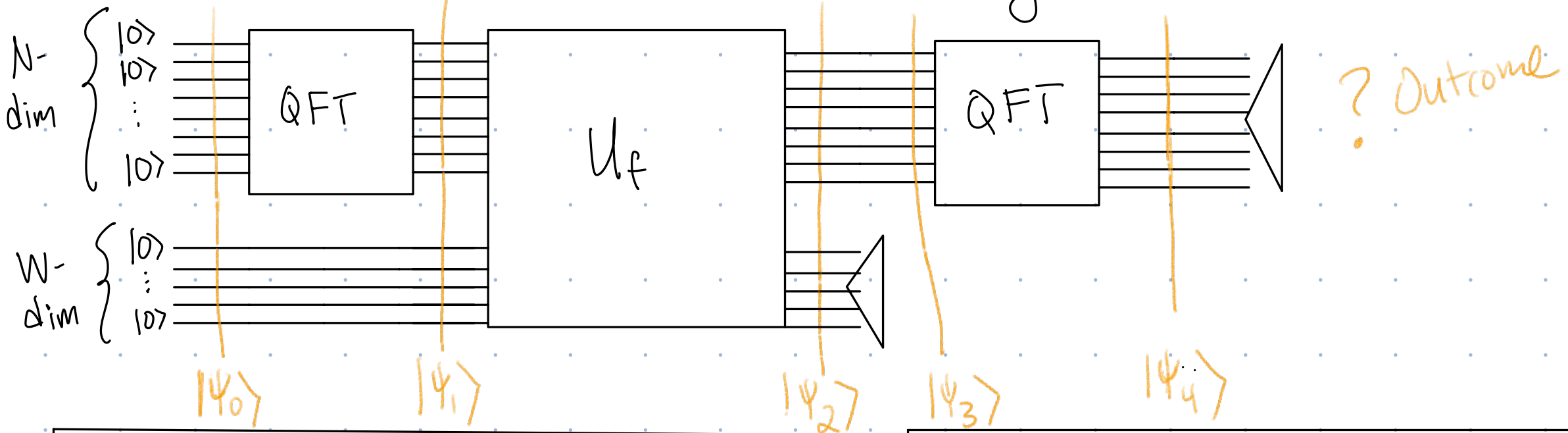
Classically, we code using base 10, not binary. We'll do same:

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

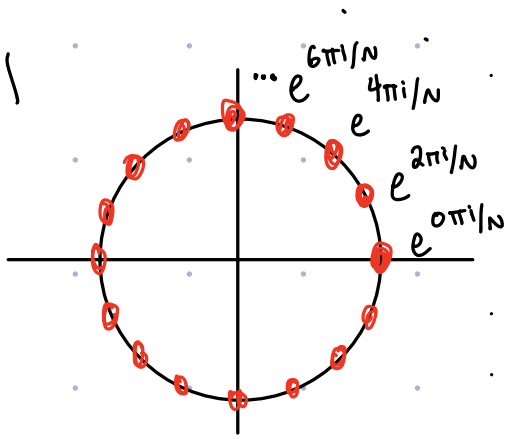


QFT: Quantum Forier Transform

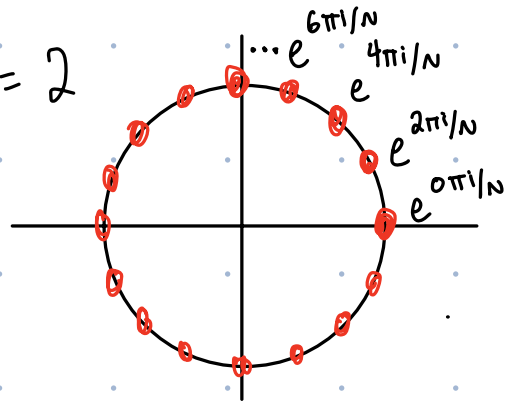
U_f:

Phase of each standard basis 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:

$|\psi\rangle = \sum_{x=0}^{N-1} a_x |x\rangle$ ⟹ Prob of outcome $|y\rangle$

($|x\rangle$: standard basis state)

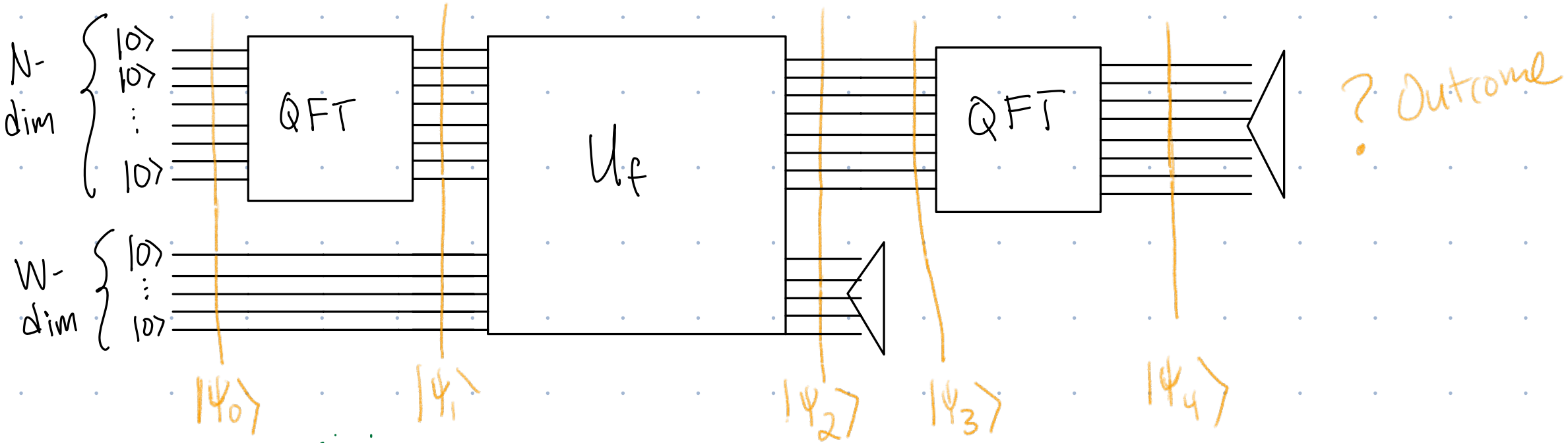
- Partial measurement (B system)

$|\psi\rangle = \sum_x \sum_z a_{xy} |x\rangle_A |z\rangle_B$ ⇒ Prob of outcome

($|x\rangle$, $|z\rangle$: standard basis states)

⇒ Collapses

Group Excercise: Analyze!



$|\psi_0\rangle =$

$|\psi_1\rangle =$

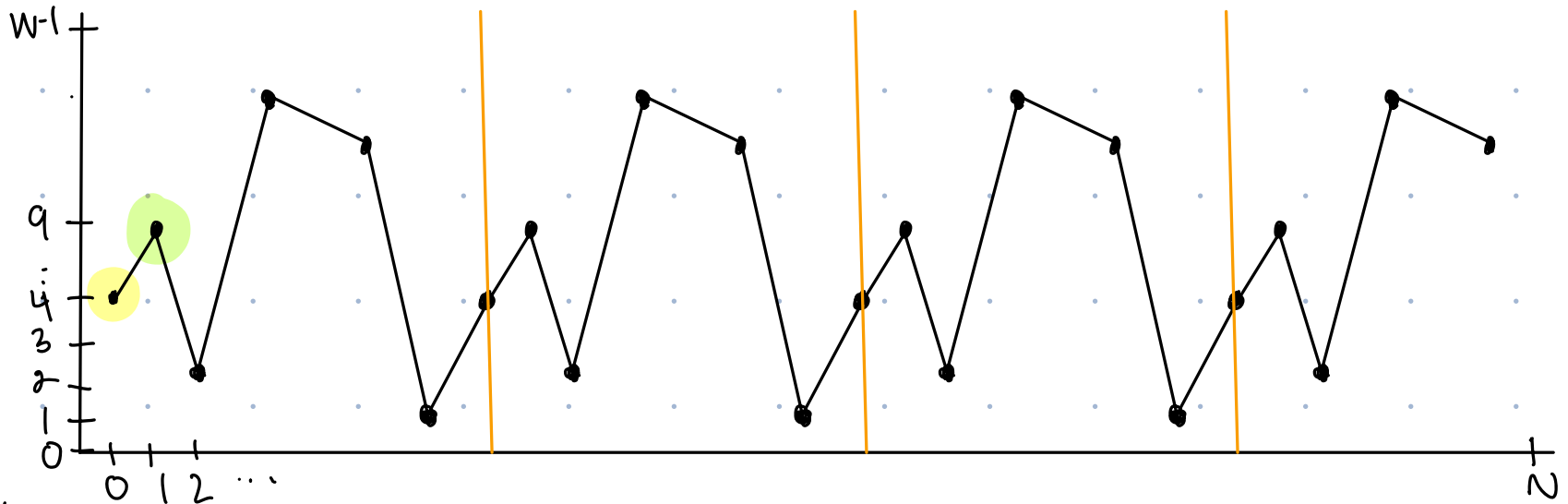
$=$

$|\psi_2\rangle =$

$=$

ex:

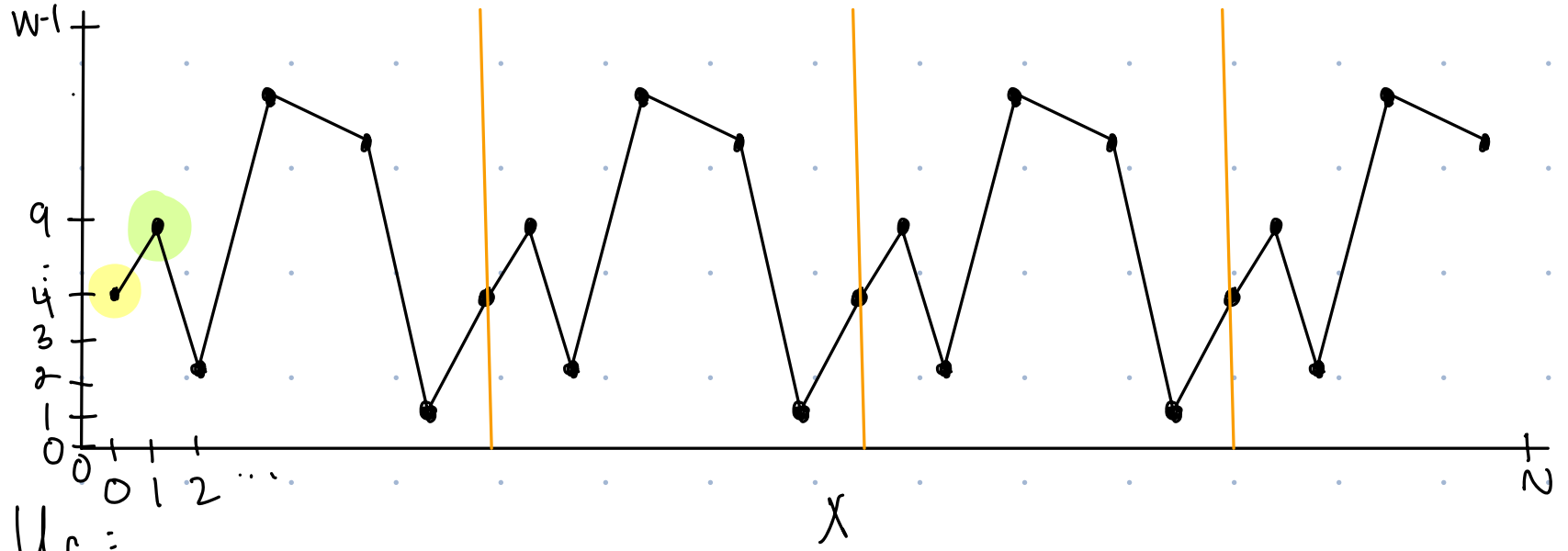
$r = 6$



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

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

$r = 6$



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.

} b^* is smallest pre-image of y in f.

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

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

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

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

measure $|9\rangle$

collapse

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

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

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

Measure $|9\rangle$ → Collapse

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

Plugging In:

$|\psi_4\rangle =$

$|\psi_5\rangle =$

$=$

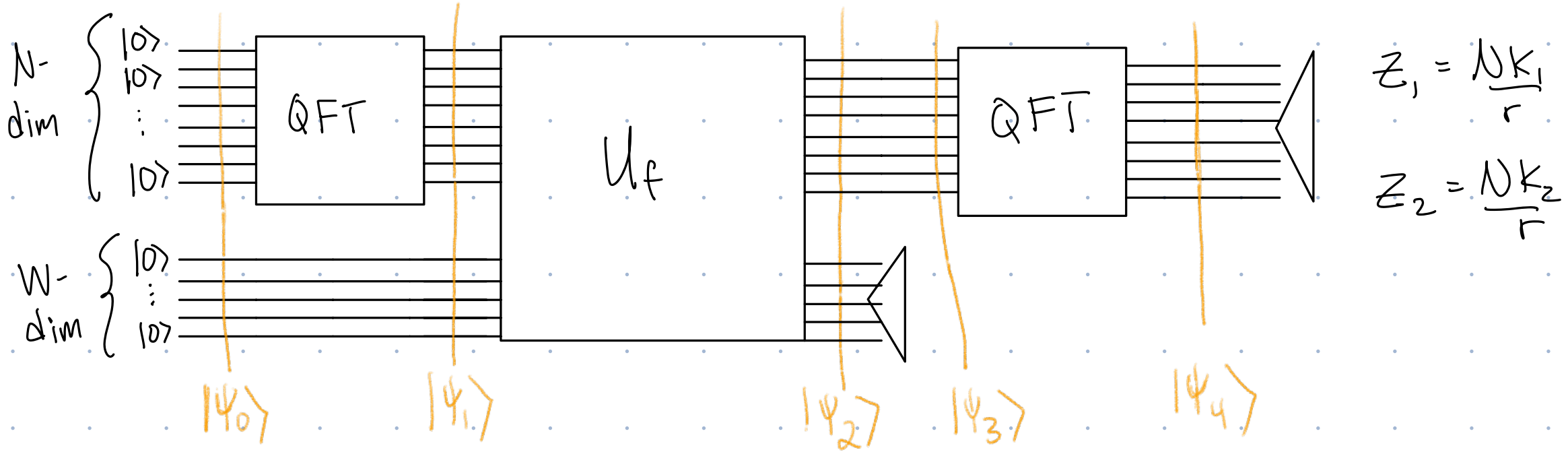
Probability of Outcome $|z\rangle$

Geomtric Series Formula:

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

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:

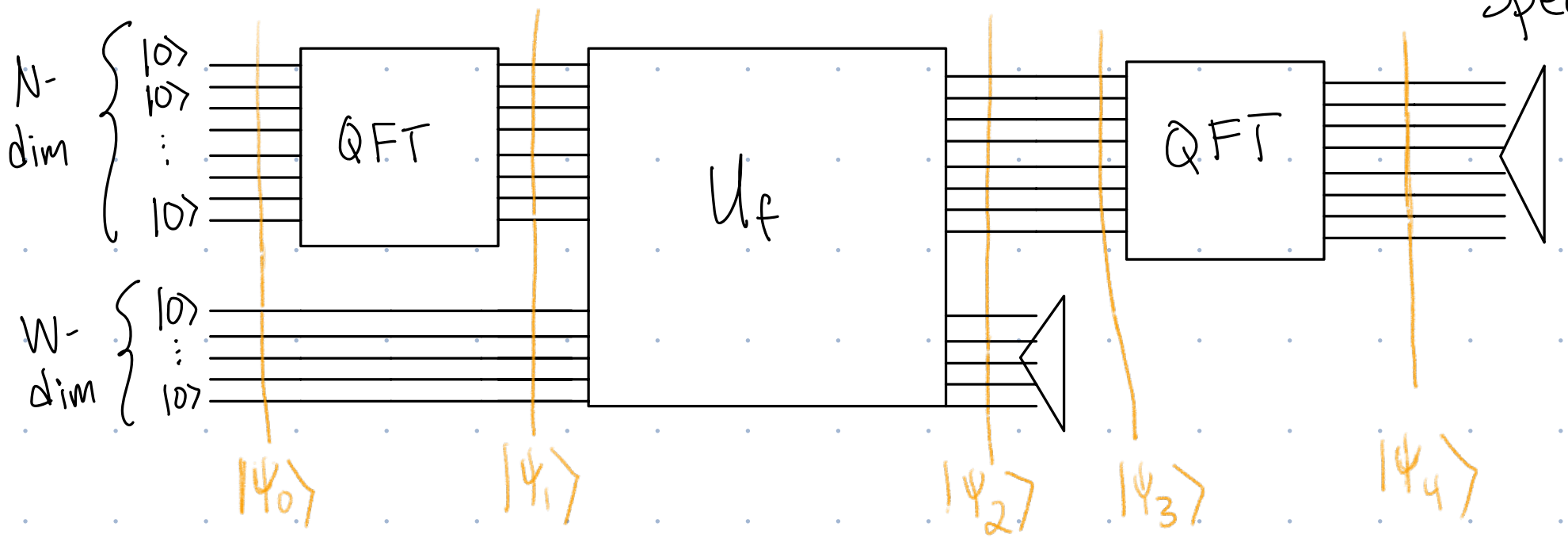
Quantum:

Time Complexity of Factoring

Quantum: $O(\log_2 N)$

Nearly Exponential Speedup!

Circuit used to factor N.



Classical:

- Largest number factored using Shor's alg*

A) 21 3×7

B) 35 5×7

C) 91 9×13

D) 221 13×17

* without shortcuts that are not scalable [Martin-López et al]

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.