FACTORING

Learning Goals

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

Public Key Crypto (RSA)

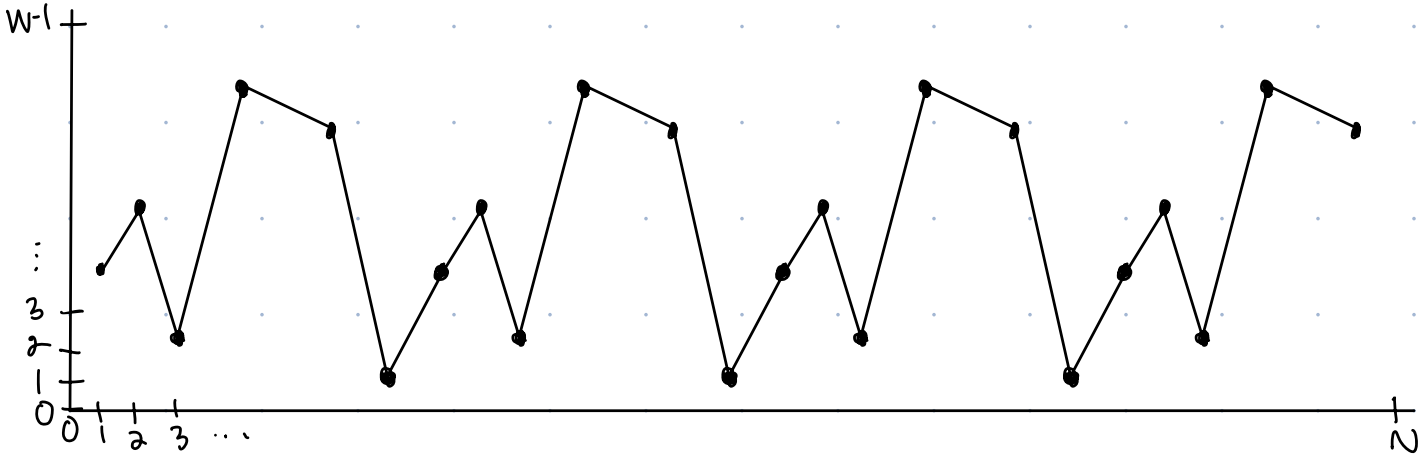
$$\underbrace{6701128736\ldots}_{617\text{ digits}} =$$

Period Finding

Period Finding Problem

Input:

ex:



Output:

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

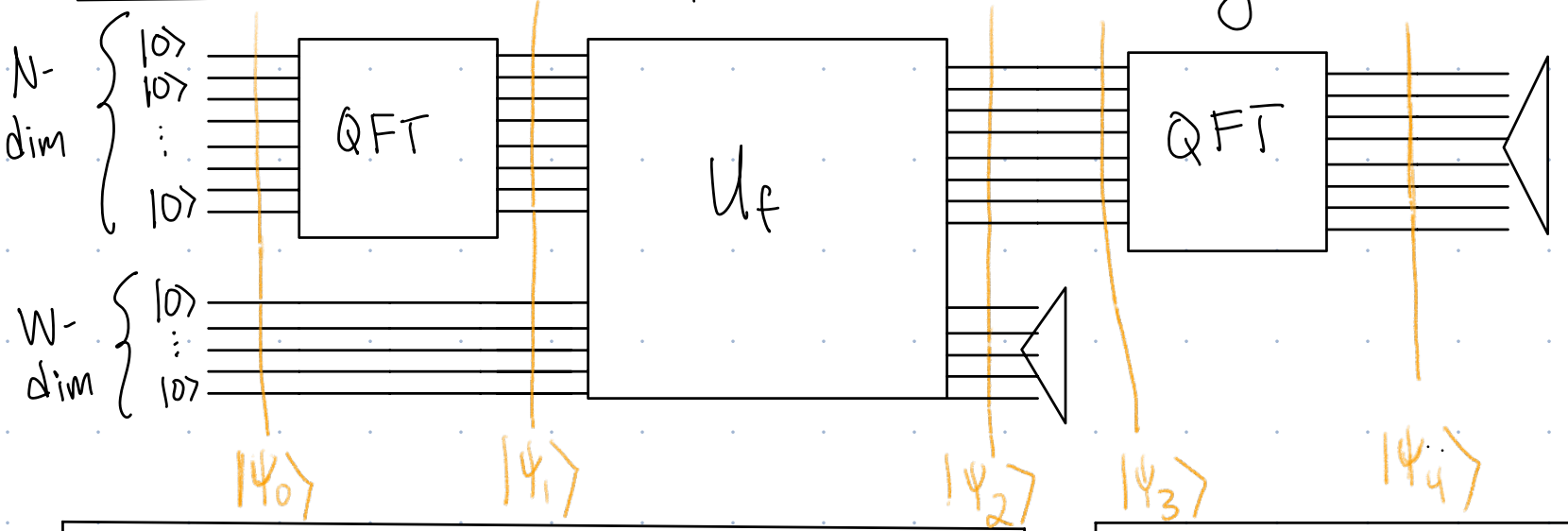
Classically, we code using base 10, not binary. We'll do same:

Ambiguity:

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

A) $O(1)$ B) $O(\log N)$ C) $O(N)$ D) $O(2^N)$

Quantum Circuit for Period Finding

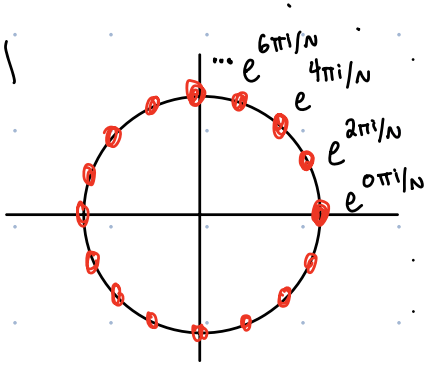


QFT: Quantum Forier Transform

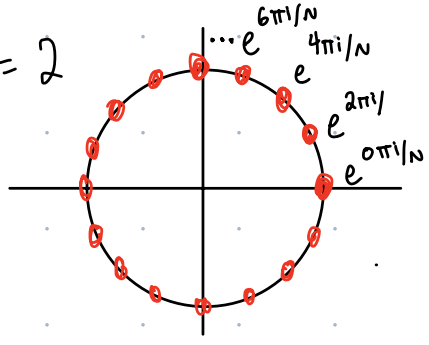
U_f:

Phase of each s.b. state in superposition

X=1



X= 2



$QFT|0\rangle = ?$

go/fourier-transform

Reminder:

 = Standard basis measurement

- Measure entire state:

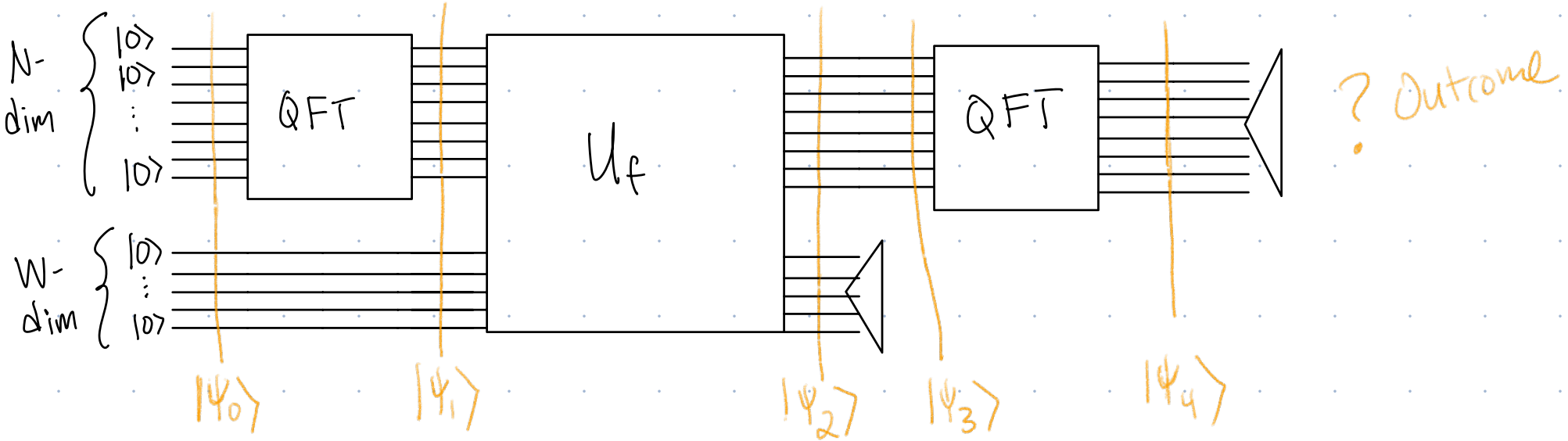
$$|\psi\rangle = \sum_{x=0}^{N-1} a_x |x\rangle \Rightarrow \text{Prob of outcome } |x^*\rangle$$

- Partial measurement (B system)

$$|\psi\rangle_{AB} = \sum_{x=0}^{N-1} \sum_{y=0}^{W-1} a_{xy} |x\rangle|y\rangle \Rightarrow \text{Prob of outcome } |y^*\rangle \text{ is}$$

$\Rightarrow$ Collapse to

Group Excercise: Analyze!



$|\psi_0\rangle =$

$|\psi_1\rangle =$

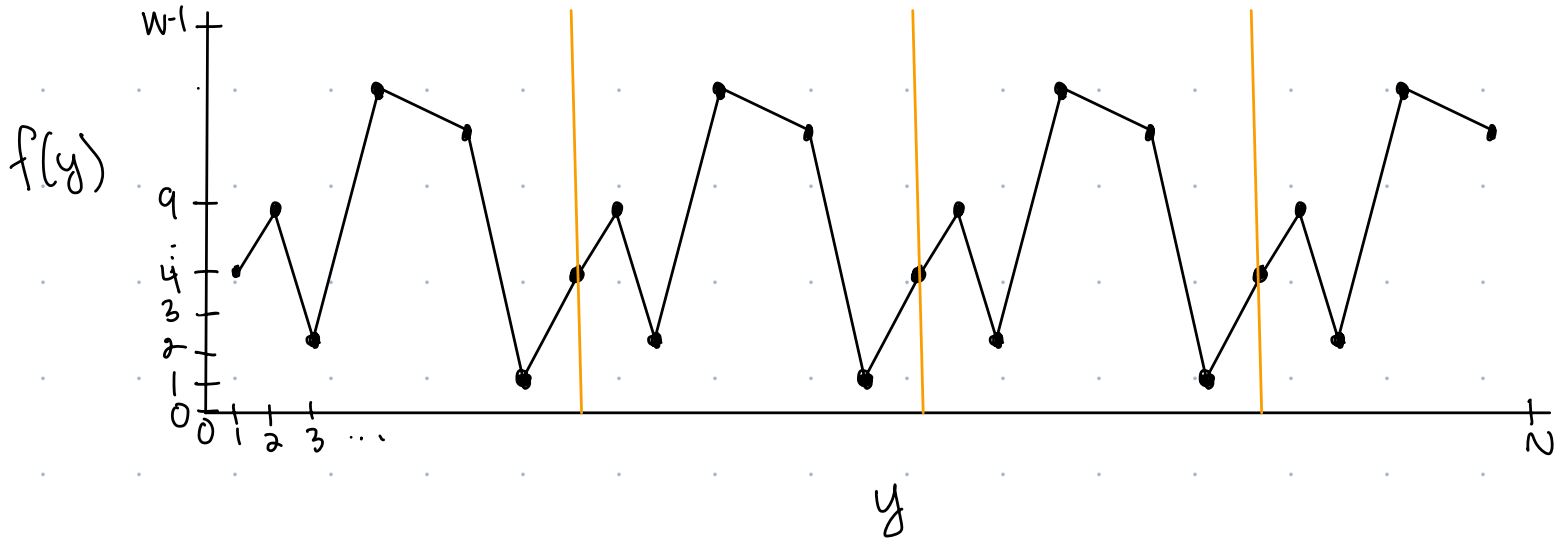
$=$

$|\psi_2\rangle =$

$|\psi_3\rangle \rightarrow$

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 $|f(b^*)\rangle$

$r=5$



outcome $f(b^*)$ $\quad |\psi_3\rangle = \square \sum_{m=0}^{\square} |b^* \square\rangle$

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

Plugging In:

$|\psi_4\rangle$

$|\psi_5\rangle =$

$=$

$=$

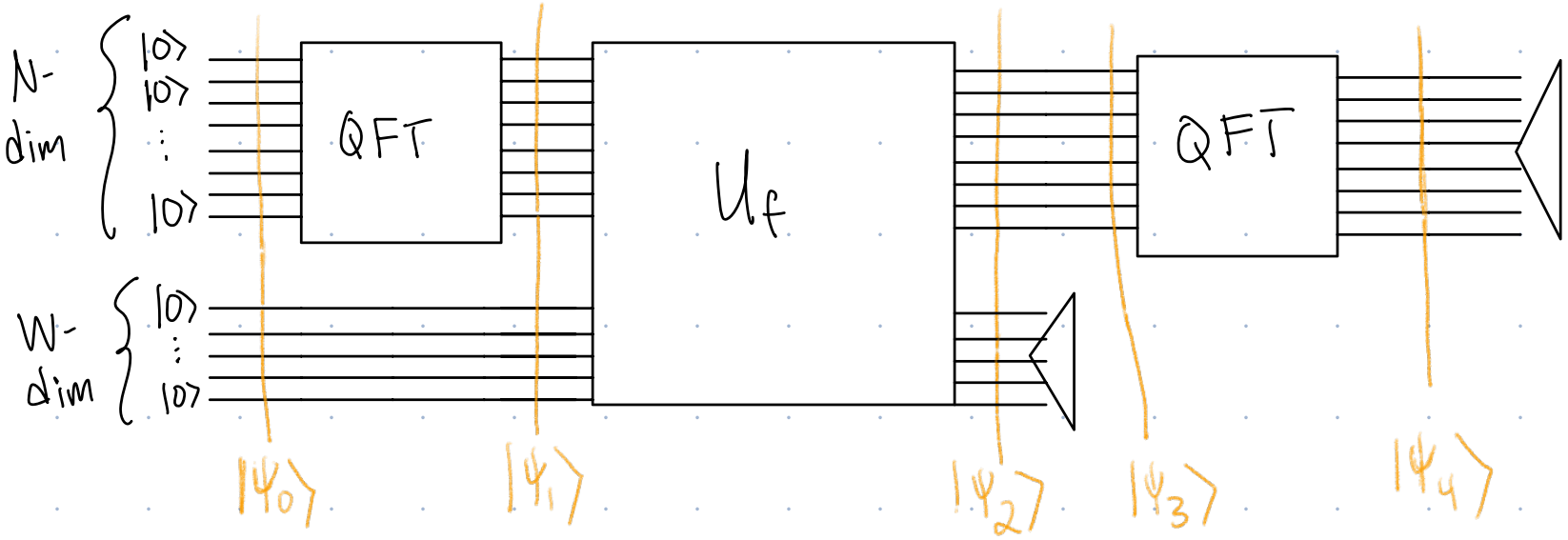
Probability of Outcome $|z\rangle$

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



2

3

Query Compexity of Period Finding

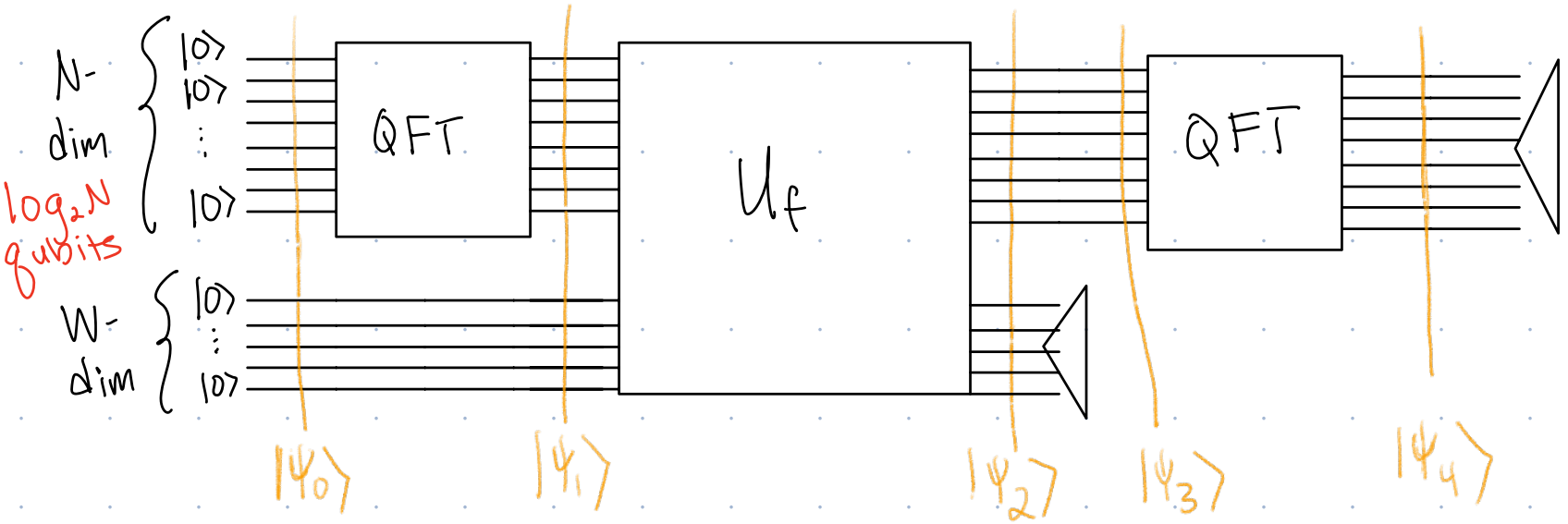
Classical:

Quantum:

Time Complexity of Factoring

Quantum:

Circuit used to factor N.

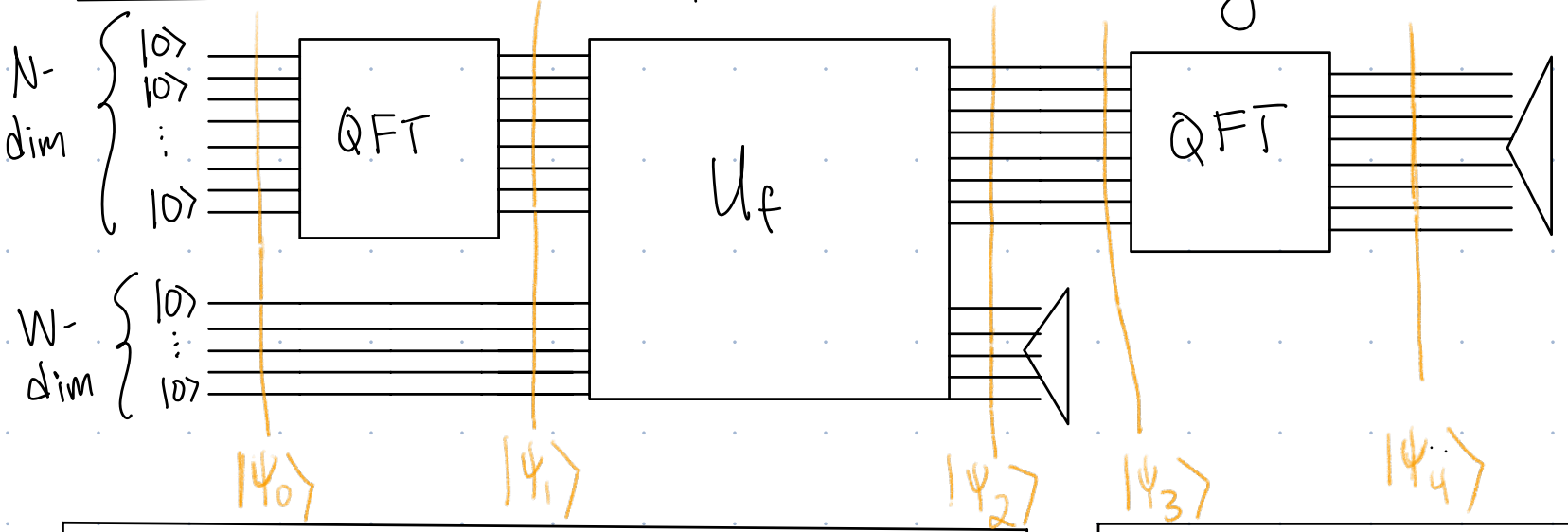


Classical:

Pesky Detail:

Quantum Circuit for Period Finding

GROUP WORK Version



QFT: Quantum Forier Transform

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

↑ N-dim standard basis state

U_f:

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

↑ N-dim standard basis state

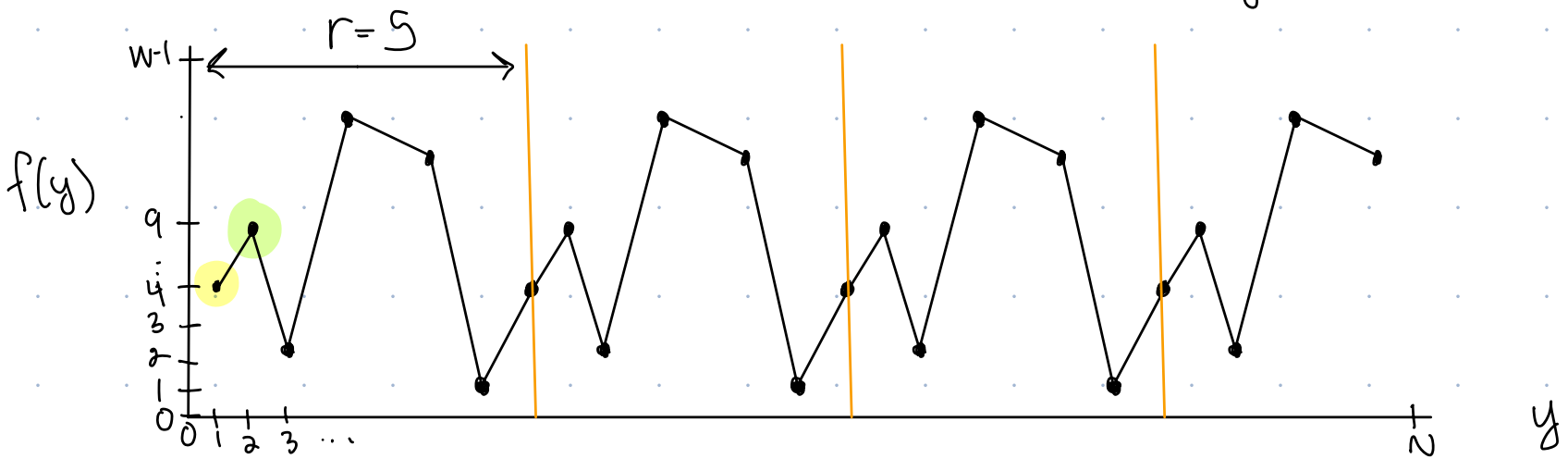
↑ W-dim standard basis state

$|\psi_0\rangle =$

$|\psi_1\rangle =$

$|\psi_2\rangle =$

For the following example, what does state $|\psi_3\rangle$ collapse to if outcome is $|4\rangle$? If outcome is $|9\rangle$? What is pattern if get outcome $|f(b^*)\rangle$

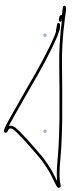


(outcome $f(b^*)$) $|\psi_3\rangle = \square \sum_{m=0}^{\square} |b^* \square\rangle$

Geometric Series Formula:

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

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)

$$|\psi\rangle_{AB} = \sum_{x=0}^{N-1}\sum_{y=0}^{W-1} a_{xy}|x\rangle|y\rangle \Rightarrow \text{Prob of outcome } |y\rangle \text{ is}$$

$$P(|y\rangle) = \sum_{x=0}^{N-1} |a_{xy}|^2$$

$$\Rightarrow \text{Collapse to } \frac{1}{\sqrt{P(|y\rangle)}} \sum_{x=0}^{N-1} a_{xy}|x\rangle|\cancel{y}\rangle$$

Destroyed

only terms with that specific $|y\rangle$