FACTORING

Learning Goals

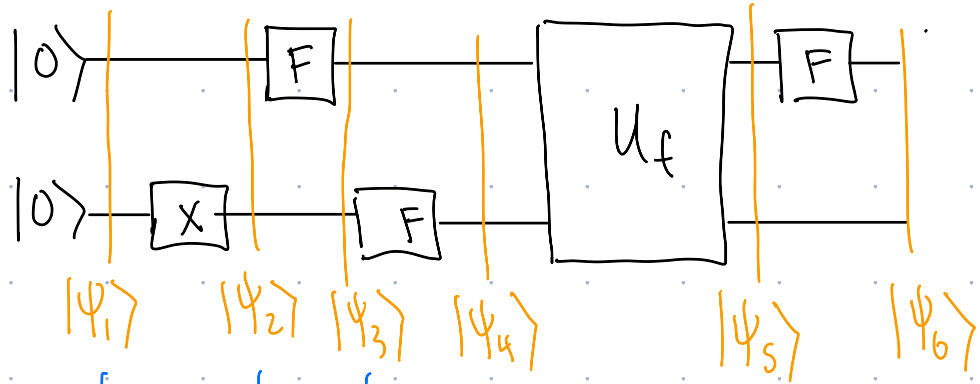
- Analyze a multi-qubit algorithm
- Become familiar with Shor's factoring algorithm (most famous q. alg)

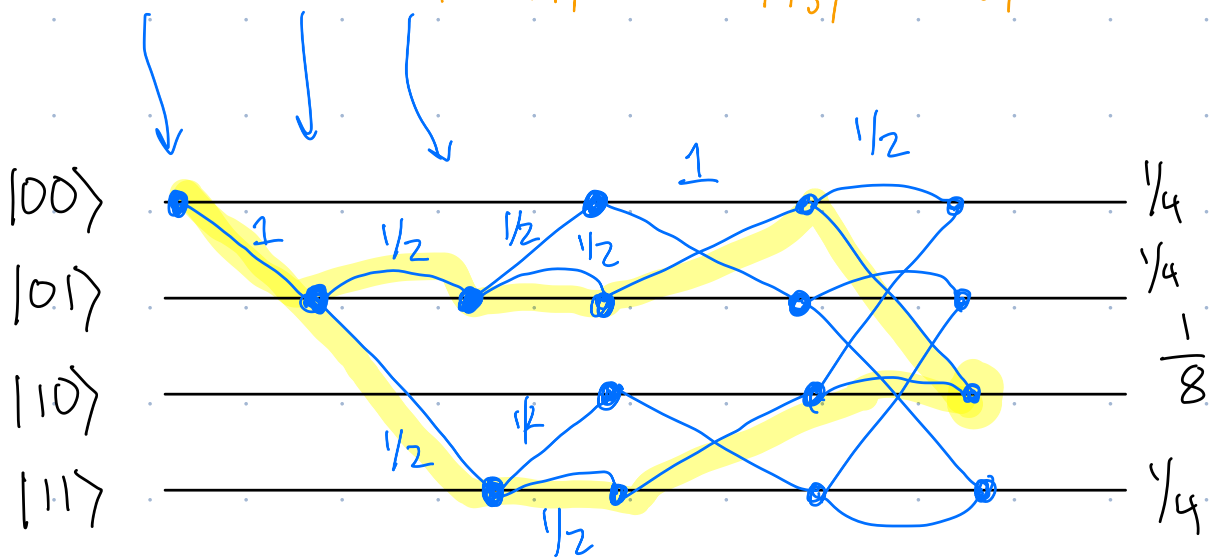
- PS 7 readings

- Go through exit tix

Does this probabilistic alg. solve Deutsch's Problem?

A) YES   B) NO   (why?)

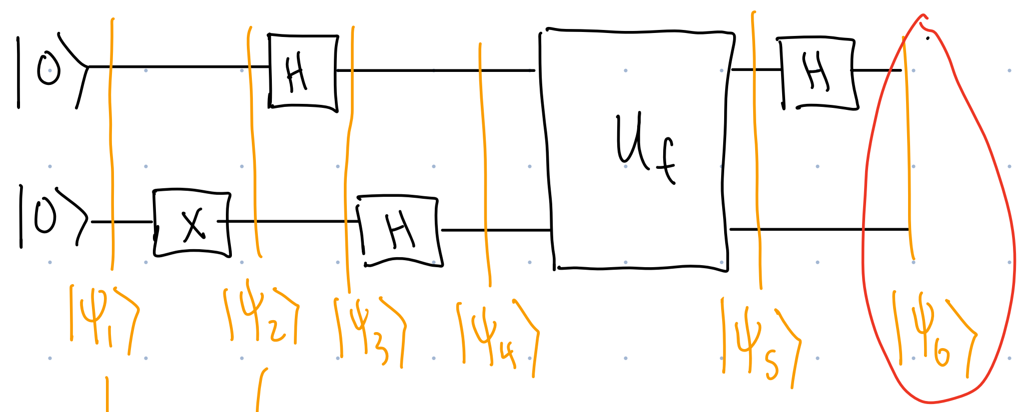




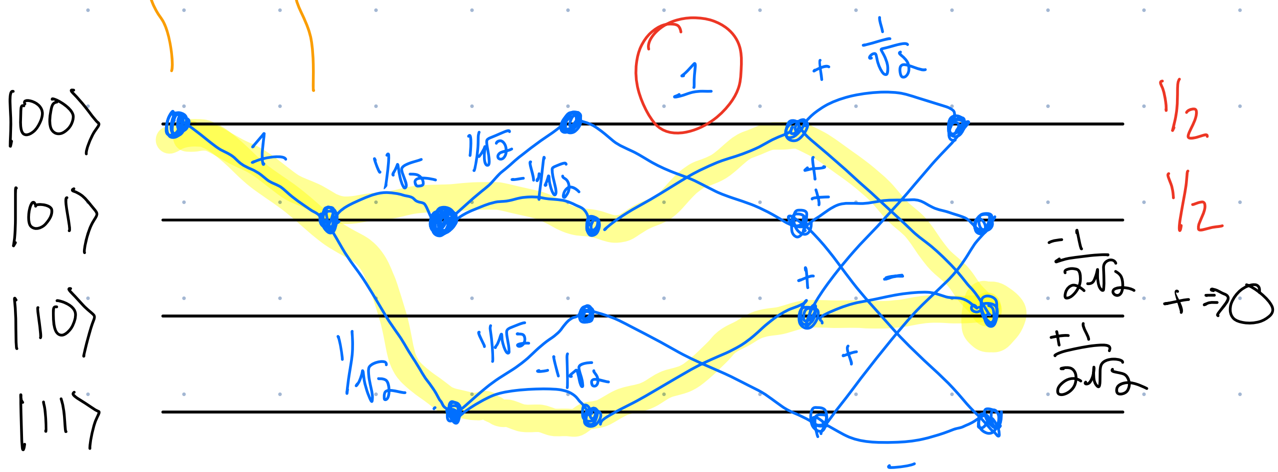
$\frac{1}{8}$ per path × 2 path : 1/4

Is this quantum algorithm deterministic?

A) YES B) NO C) sort of



$f(0) = f(1) = 1$



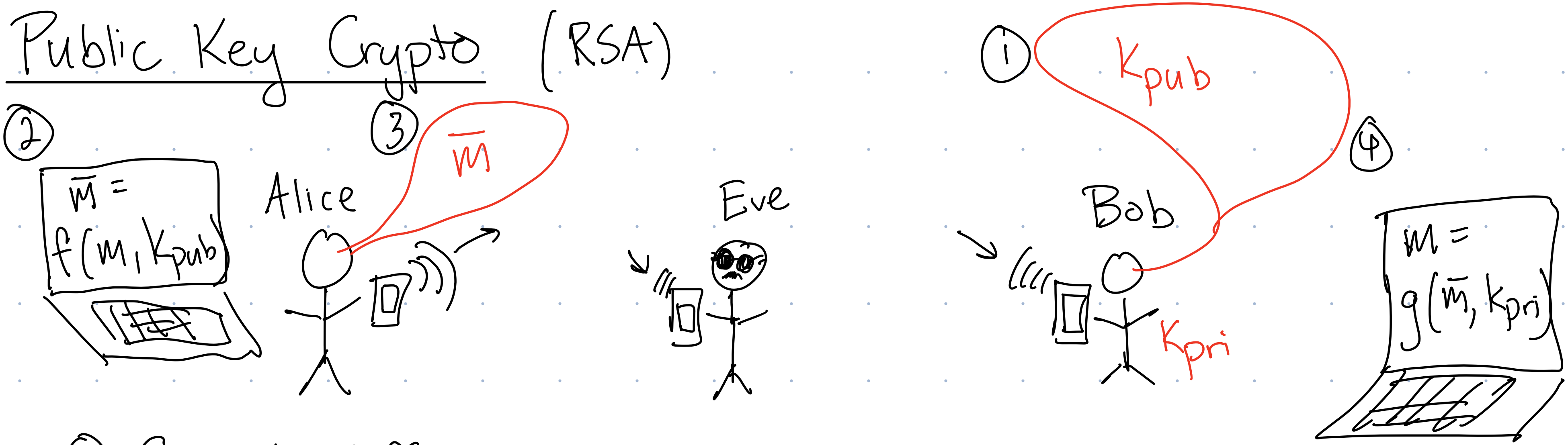
$1/2$

$1/2$

$f(0)=1$

$f(1)=0$

Public Key Crypto (RSA)



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

Eve has K_{pub}, $f(m, K_{pub}) = \bar{m}$

If could solve $\underbrace{\text{hard math problem}}_{\text{factoring a large number}}$ → could learn m

$\underbrace{670112873\,6\ldots}_{617 \text{ digits}} = a \times b$

\$200,000

\$100K 308 digits

X 250 digit

Period Finding

Factoring reduces to period finding (number theory)

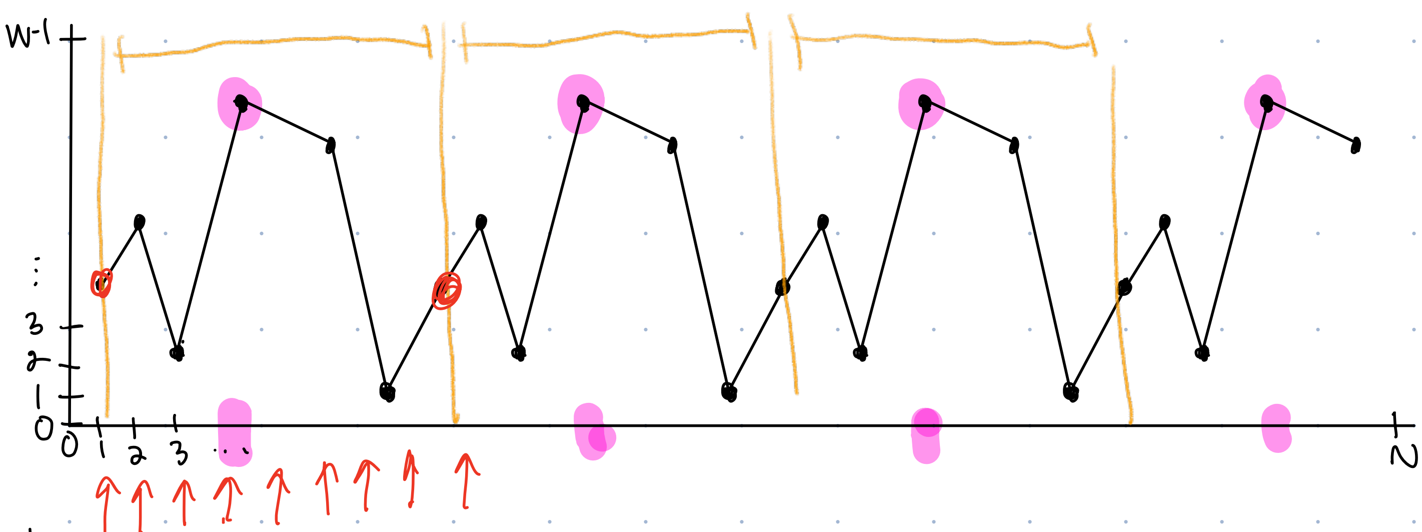
Period Finding Problem

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

- f has unknown period r
- no repeated values within a period
- $N > r^2$ (many repeats)

$f(x) = f(x+r)$

ex: f $r=6$



Output: r

What is the classical query complexity of period finding?

Birthday Paradox

$\boxed{A)\ O(\sqrt{r})}$

Brute Force

$\boxed{B)\ O(r)}$

C) $O(r^2)$

D) $O(N)$

Bits to Digits

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

$011 \leftrightarrow 3$

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

If there N possible Standard Basis States

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

"N-dimensional state"

Ambiguity: $|3\rangle \leftrightarrow |11\rangle$

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

$|3\rangle \leftrightarrow |0000000011\rangle$

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

$2^{\#\text{qubits}} = \#$ standard b.s.

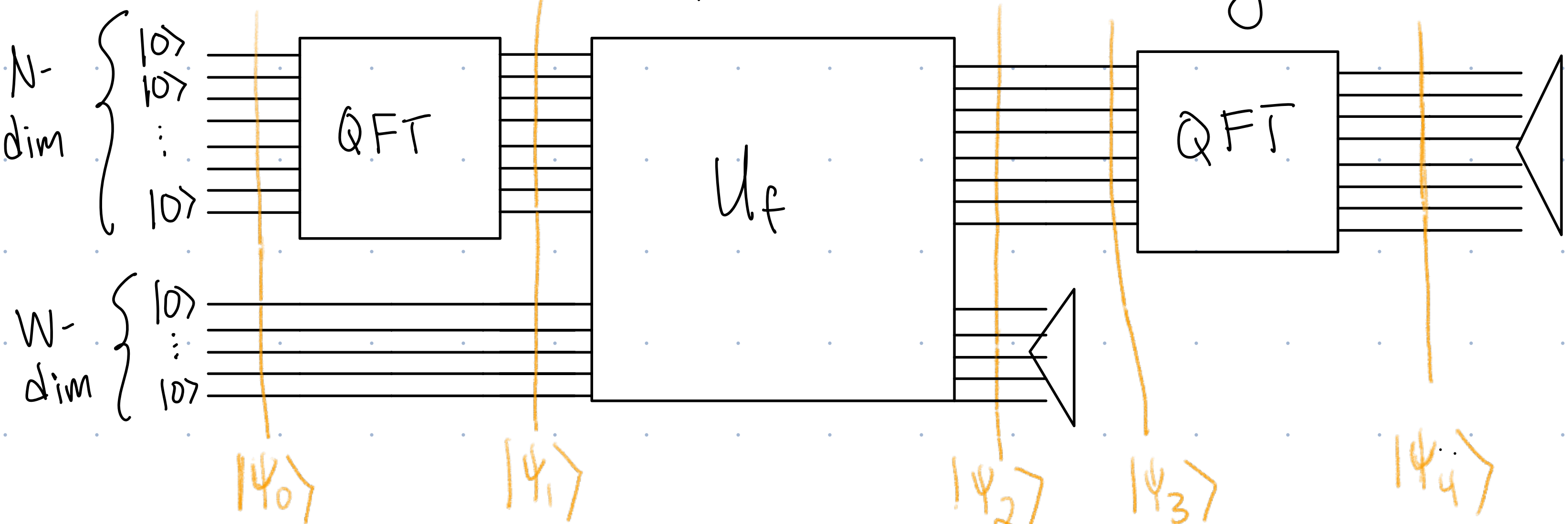
A) $O(1)$ $\boxed{\text{B) } O(\log N)}$ C) $O(N)$ D) $O(2^N)$

$|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, \dots |111\rangle$

$|0\rangle$ $|1\rangle$ $|2\rangle$ $|3\rangle$ $|4\rangle, \dots$ $|7\rangle$

Quantum Circuit for Period Finding

$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$



? Outcome

QFT: Quantum Fourier Transform

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

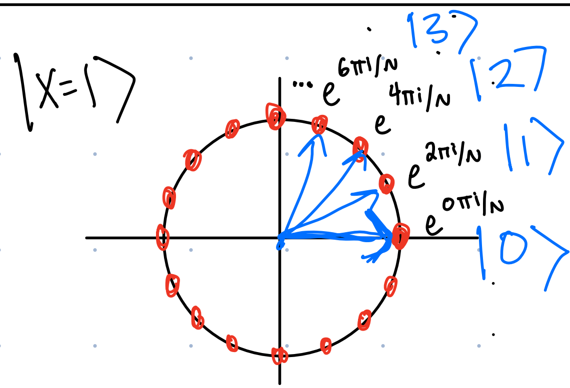
N-dim standard basis state

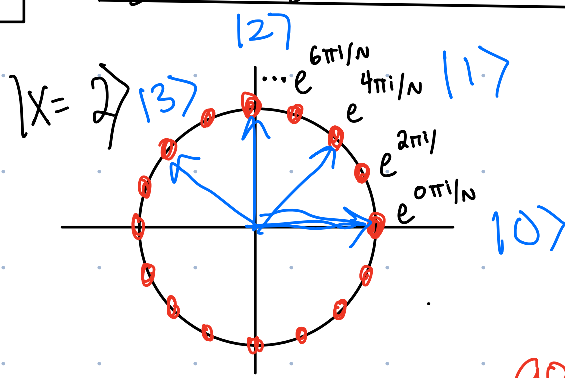
U_f:

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

N-dim W-dim
s.b. states

Phase of each s.b. state in superposition

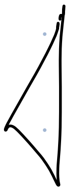




$QFT|0\rangle = ?$

go/fourier-transform

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

 = 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)

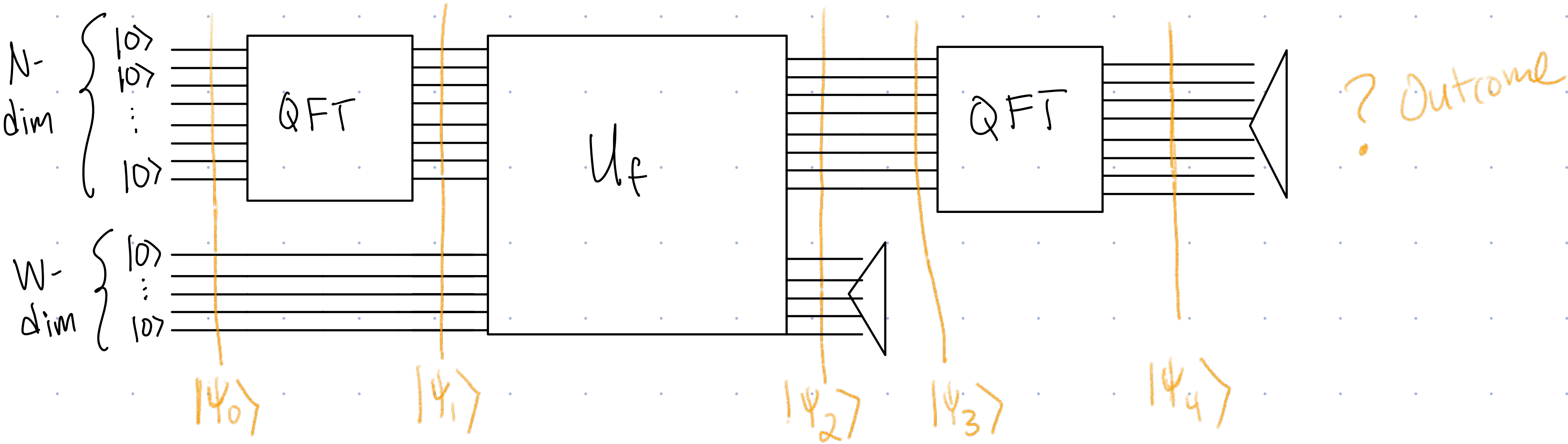
10

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

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

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

Group Excercise: Analyze!



$|\psi_0\rangle =$

$|\psi_1\rangle =$

$=$

$|\psi_2\rangle =$

$|\psi_3\rangle \longrightarrow$