

FACTORING

Learning Goals

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

Project!

Exit Tickets

What is QFT and why do we use it?

qft/fourier-transform

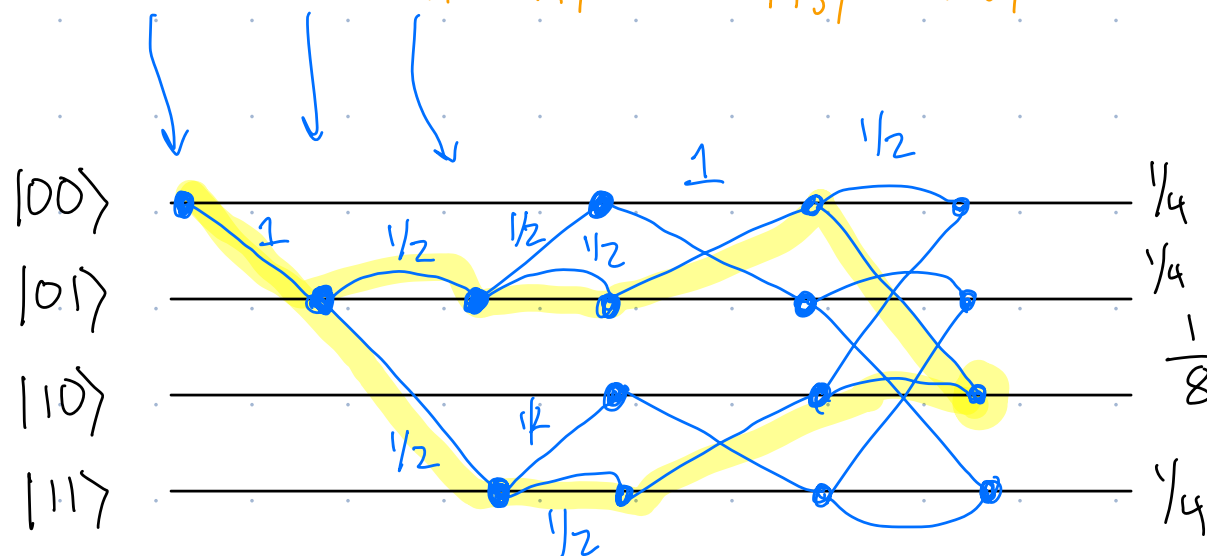
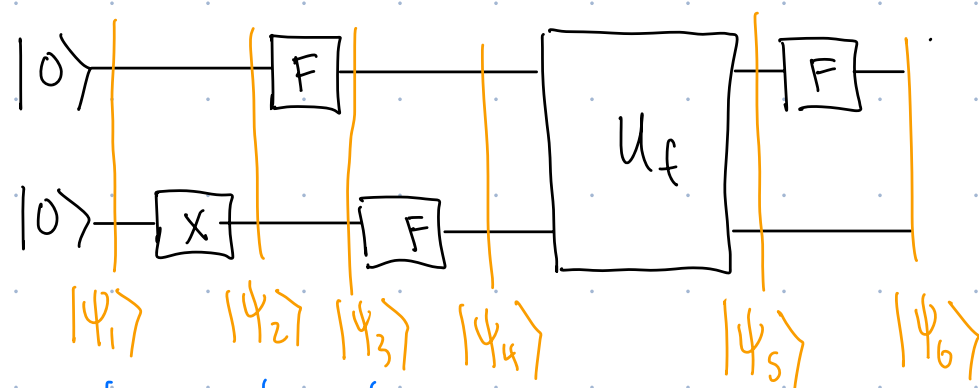
Negative amplitude

Does this probabilistic alg. solve Deutsch's Problem?

A) YES

B) NO

(why?)



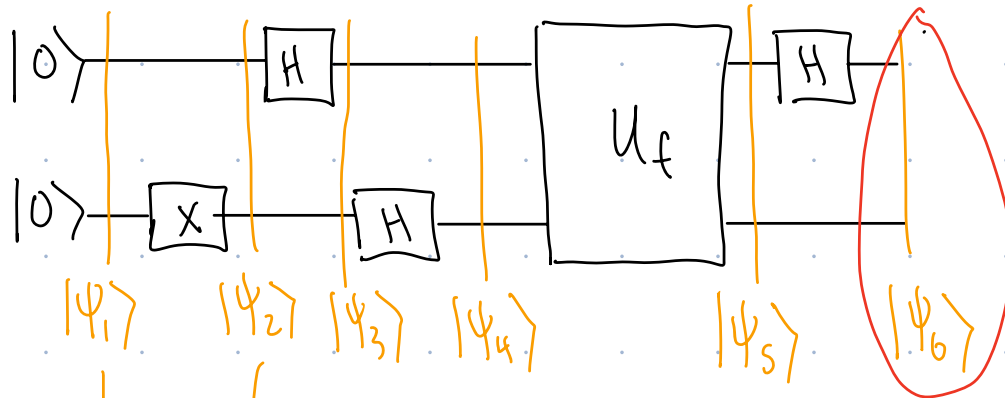
$\frac{1}{8}$ per path $\times 2$ paths: $\frac{1}{4}$

Is this quantum algorithm deterministic?

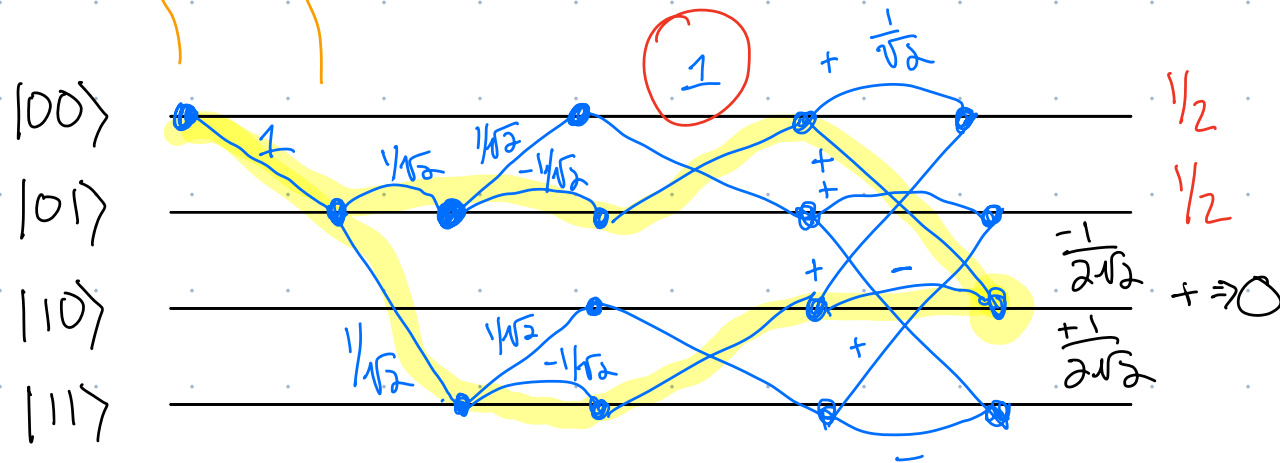
A) YES

B) NO

C) Sort of



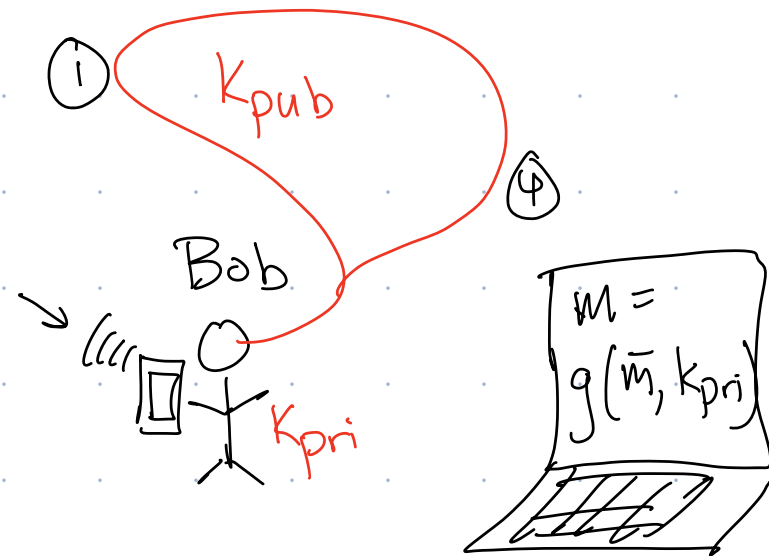
$$f(0) = f(1) = 1$$



$$f(0) = 1$$

$$f(1) = 0$$

Public Key Crypto (RSA)



③ Secret message
 $m \in \{0,1\}^n$

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

If could solve hard math problem $\rightarrow$ could learn m
factoring a large number

6701128736....

= a x b

617 digits

\$200,000

\$100K

308 digits

250 digit

X

Period Finding

Factoring reduces to period finding (number theory)

Period Finding Problem

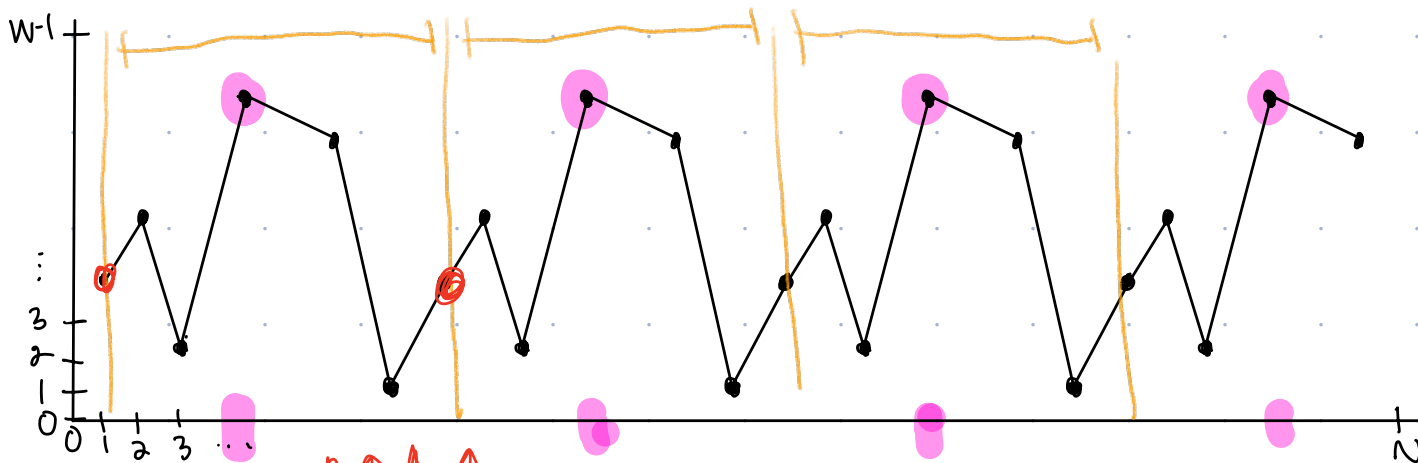
Input: Query access to $f: \{0, 1, 2, \dots, N-1\} \rightarrow \{0, 1, 2, \dots, W-1\}$

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

ex: f

$r=6$

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



Output: r

What is the classical query complexity of period finding?

Birthday

Brute Force

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

B) $O(r)$

C) $O(r^2)$

D) $O(n)$

Paradox

Bits to Digits

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

$$011 \leftrightarrow 3$$

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

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

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

$$|3\rangle \leftrightarrow |000000000011\rangle$$

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

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

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

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

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

If there N possible
Standard Basis States

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

$|N-1\rangle\}$

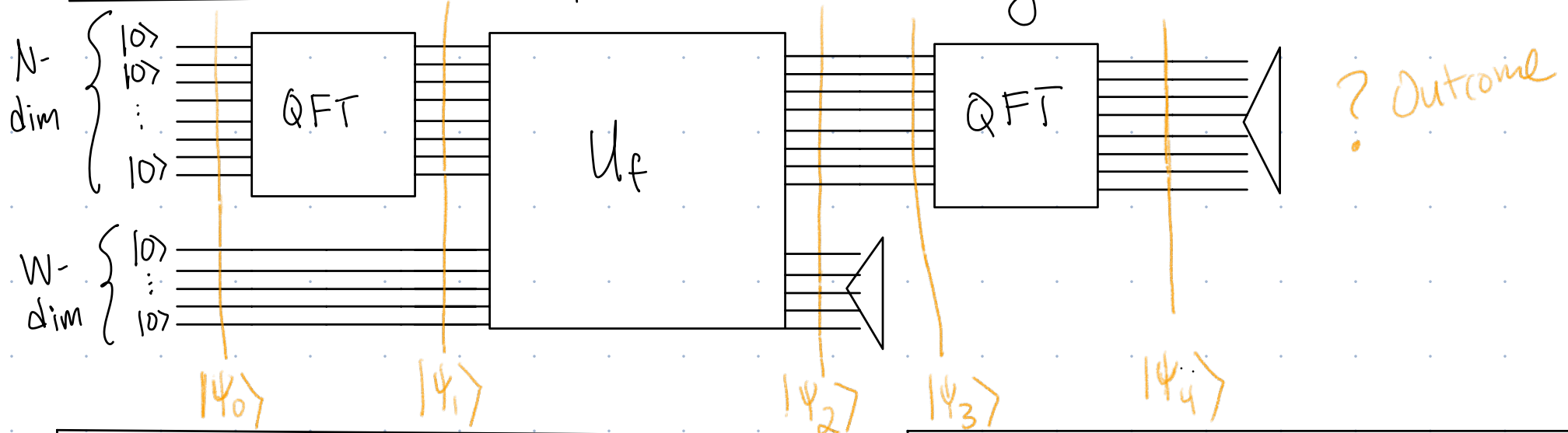
" N -dimensional state"

$|1111\rangle$

$|7\rangle$

Quantum Circuit for Period Finding

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



QFT: Quantum Fourier Transform

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

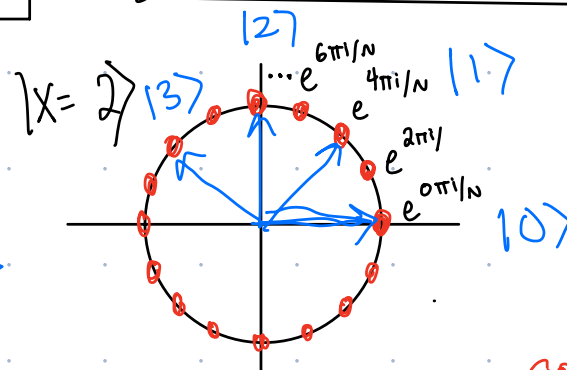
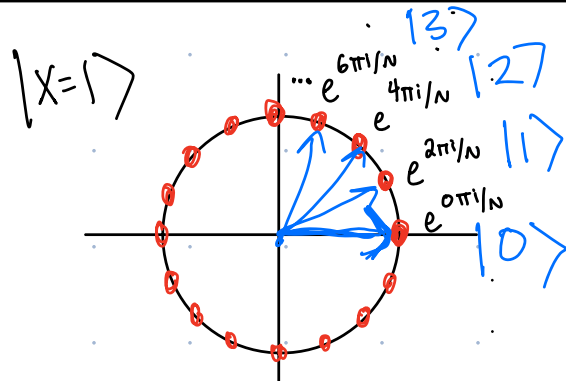
$\uparrow$
N-dim standard basis state

U_f :

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

$\uparrow \quad \uparrow$
N-dim W-dim
S.b. states

Phase of each s.b. state in superposition



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

go/fourier-transform

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

$\triangleleft$ = Standard
basis
measurement

- Measure entire state:

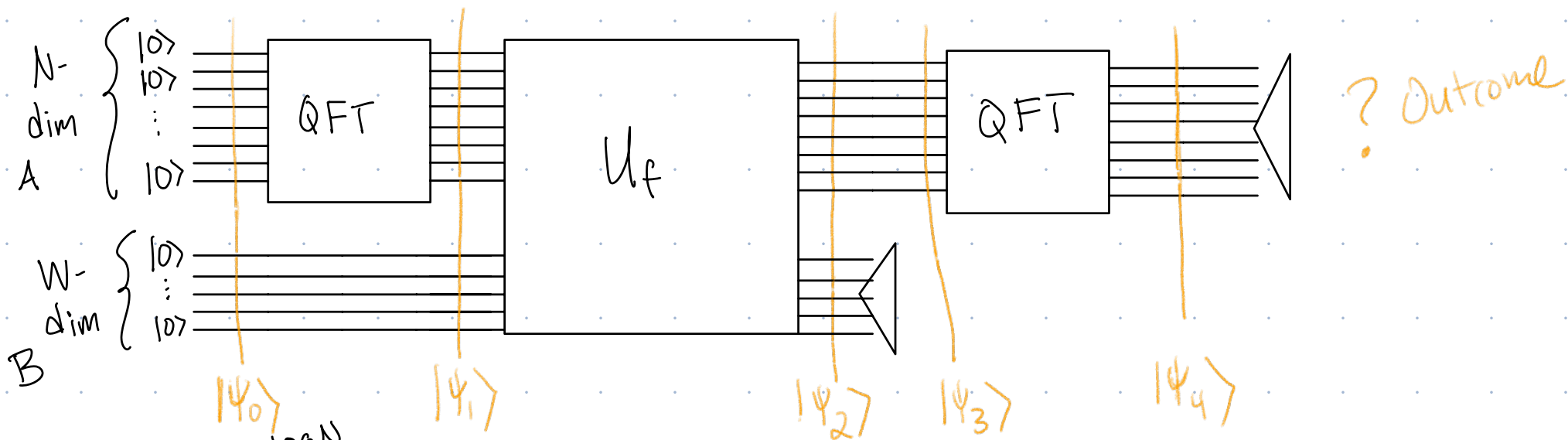
$$|\psi\rangle = \sum_{x=0}^{N-1} a_x |x\rangle \Rightarrow \text{Prob of outcome } |x^*\rangle \text{ is } |a_{x^*}|^2$$

- Partial measurement (B system)

$$|\psi\rangle_{AB} = \sum_{x=0}^{N-1} \sum_{y=0}^{W-1} a_{xy} |x\rangle_A |y\rangle_B \Rightarrow \text{Prob of outcome } |y^*\rangle \text{ is } \sum_{x=0}^{N-1} |a_{xy^*}|^2$$

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

Group Exercise: Analyze!



$$|\psi_0\rangle = \underbrace{|000\dots 0\rangle_A}_{\log N} |000\dots 0\rangle_B = |10\rangle_A |0\rangle_B$$

$$|\psi_1\rangle = (\text{QFT}_A \otimes I_B) |10\rangle_A |0\rangle_B = (\text{QFT}_A |0\rangle_A) \otimes I_B |0\rangle_B$$

$$= \left(\frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi i \cdot 0 \cdot y/N} |y\rangle \right)_A \otimes |0\rangle_B = \left(\sum_{y=0}^{N-1} \frac{1}{\sqrt{N}} |y\rangle \right)_A \otimes |0\rangle_B$$

$$|\psi_2\rangle = U_f \left(\frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} |y\rangle |0\rangle \right) = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} U_f |y\rangle |0\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} |y\rangle |f(y) + 0 \pmod{w}\rangle$$

$$= \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} |y\rangle_A |f(y)\rangle_B$$

$\begin{matrix} \uparrow & \uparrow \\ x \rightarrow y & y \rightarrow 0 \end{matrix}$

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

$r=5$

