FACTORING

Learning Goals

- Analyze a multi-qubit algorithm [QC5]
- Become familiar with Shor's factoring algorithm (most famous q. alg)

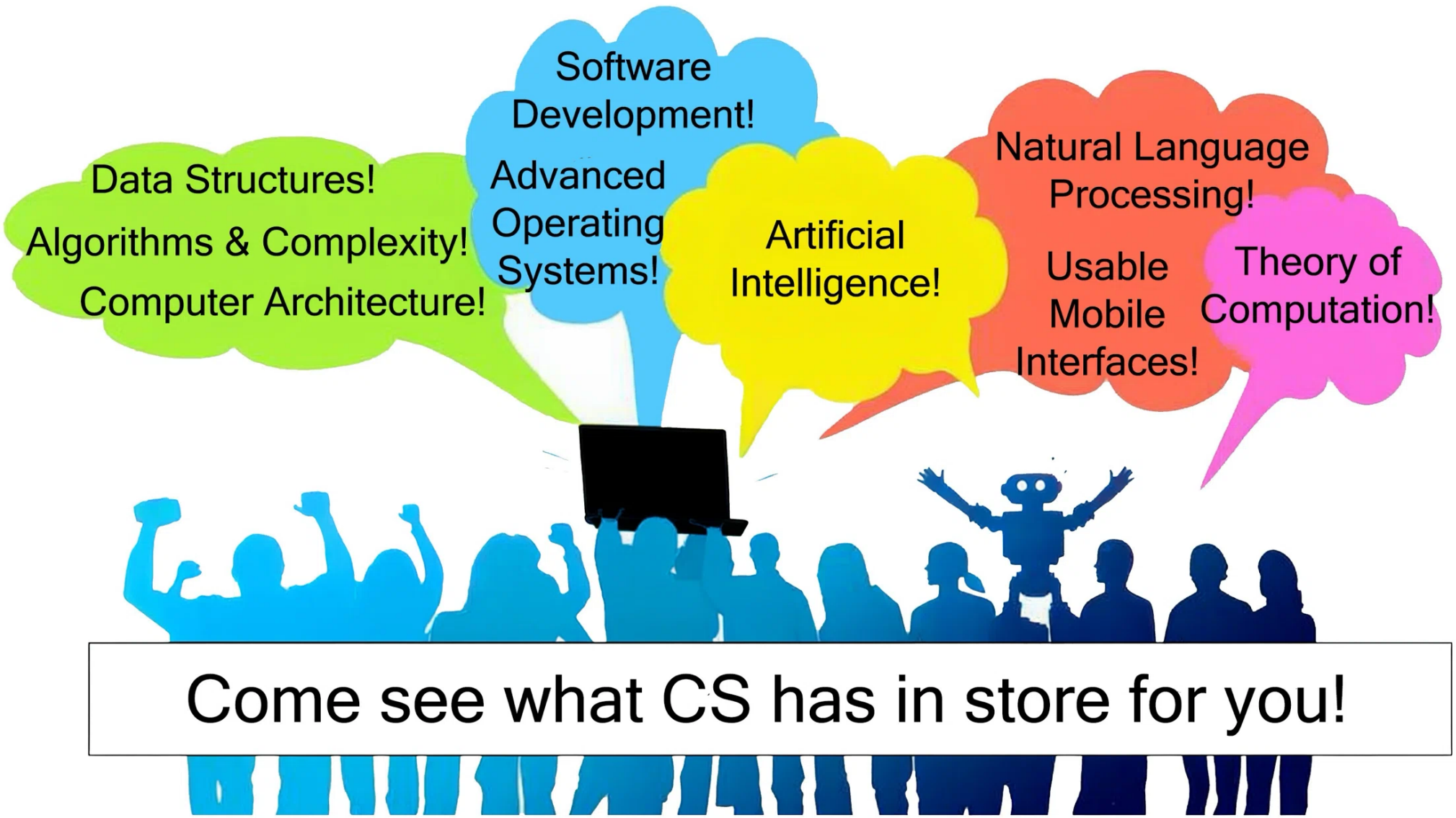
Announcements

- Friday Fall Faculty Forum (2 CS talks 11-12 in Ainn 229)
- Friday W'27, S'27 Course Preview 12:20-1:20 + Pizza
- Exam on Thurs Nov 5. 75 min in class, 2 sides of notecard
  QI3 - QI5, QC1 - QC3, QC5
  last chance until final

Warm-Up

ABCD, partial meas.

Exit Tickets

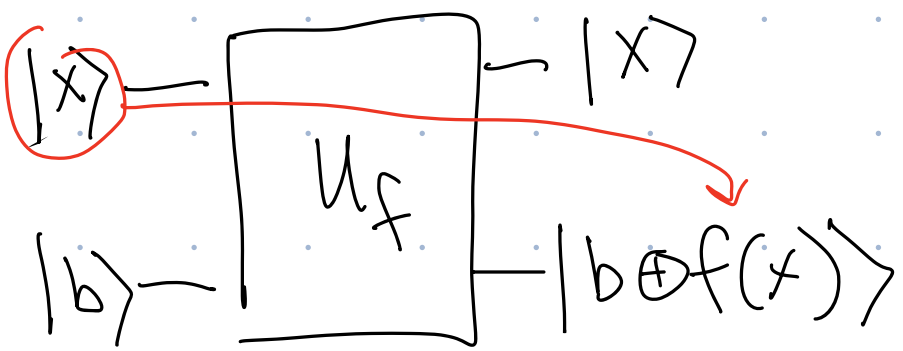


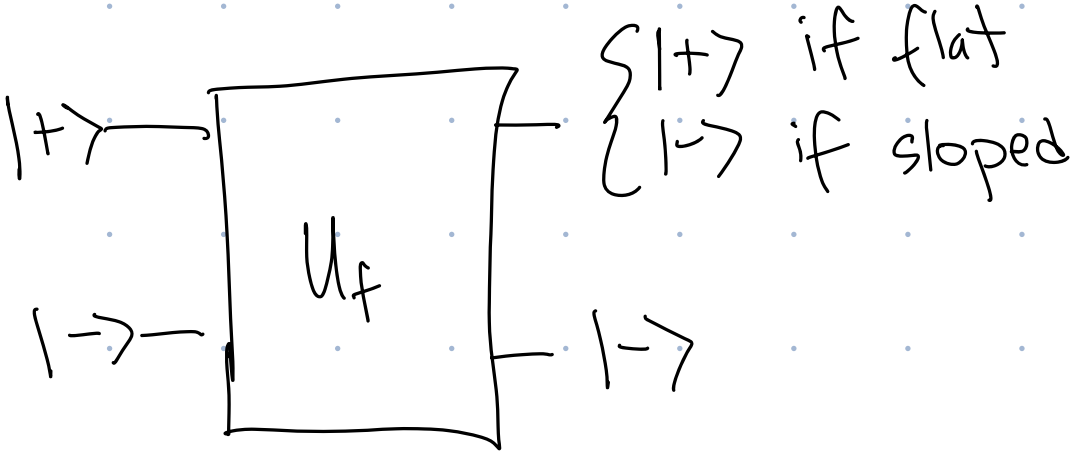
Come see what CS has in store for you!

Computer Science Winter + Spring ‘27 Course Preview

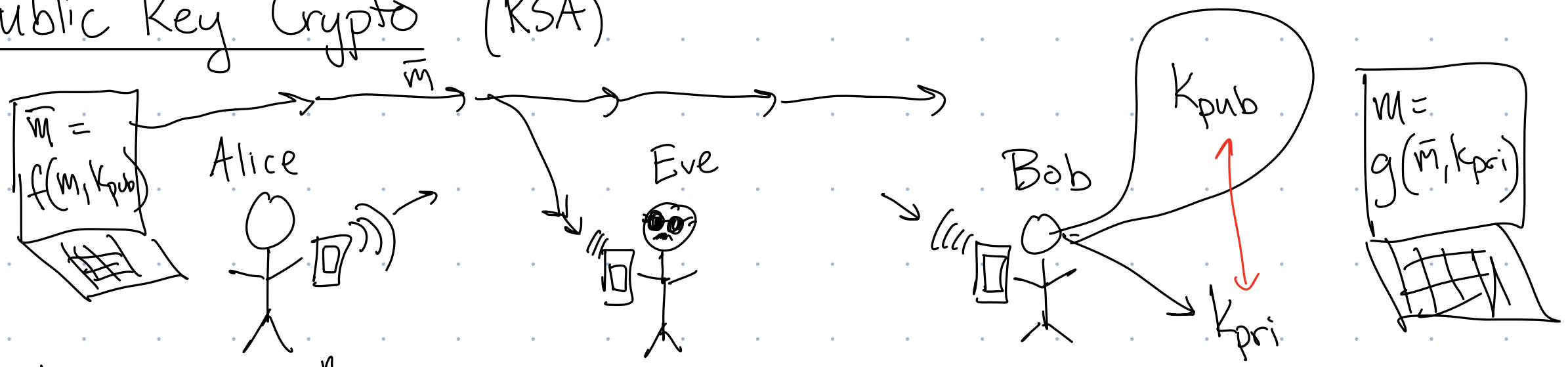
When: 10/30 / 12:20-1:20pm Where: 75 Shannon 102 Why: Pizza + Plotting

Why is kickback significant? DON'T TRUST YOUR INTUITION





Public Key Crypto (RSA)



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

Eve has access to $\bar{m}, k_{pub}, f, g$ — Hard Math Problem → m

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

factoring a large number

$6701128736\ldots = a \times b$

617 digits

?

$200,000 prize for factoring 617 digit #
$100,000 " 308 digit
250 digit ✓

Period Finding

Factoring reduces (via number theory) to period finding

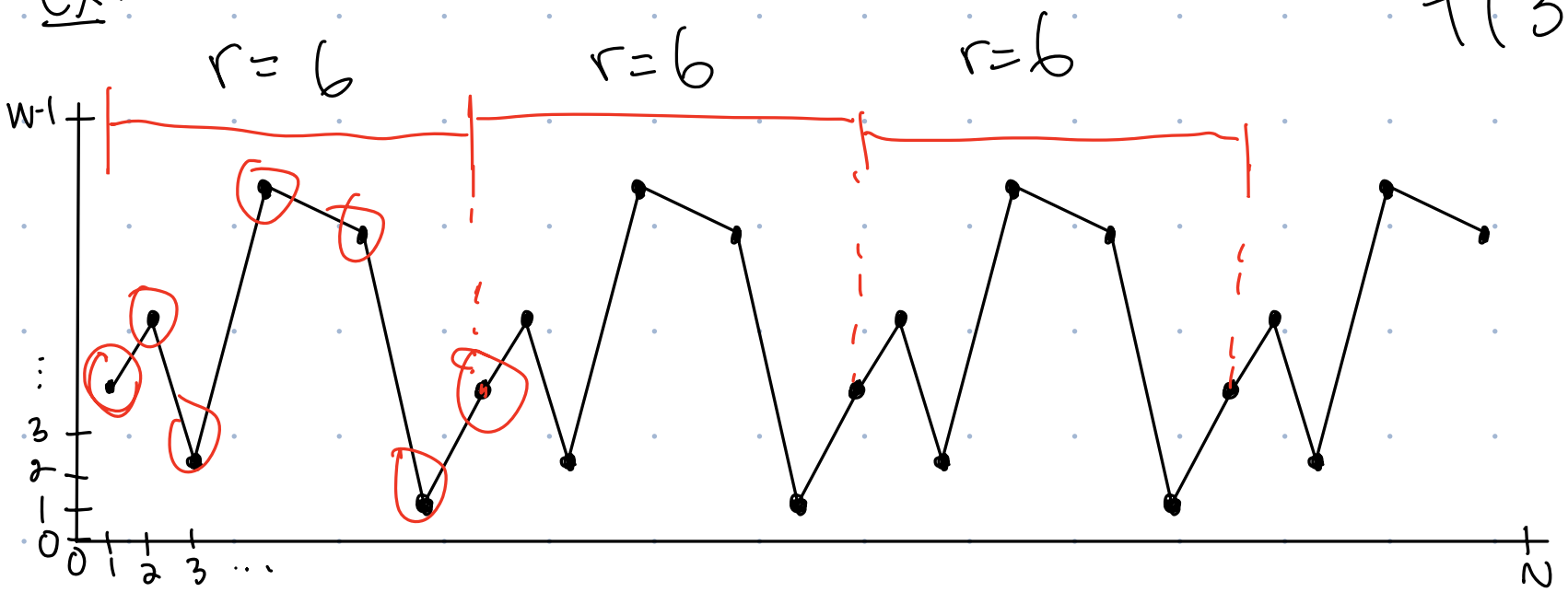
Period Finding Problem

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

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

$f(0) = ?$
$f(10) = ?$
$f(33) = ?$

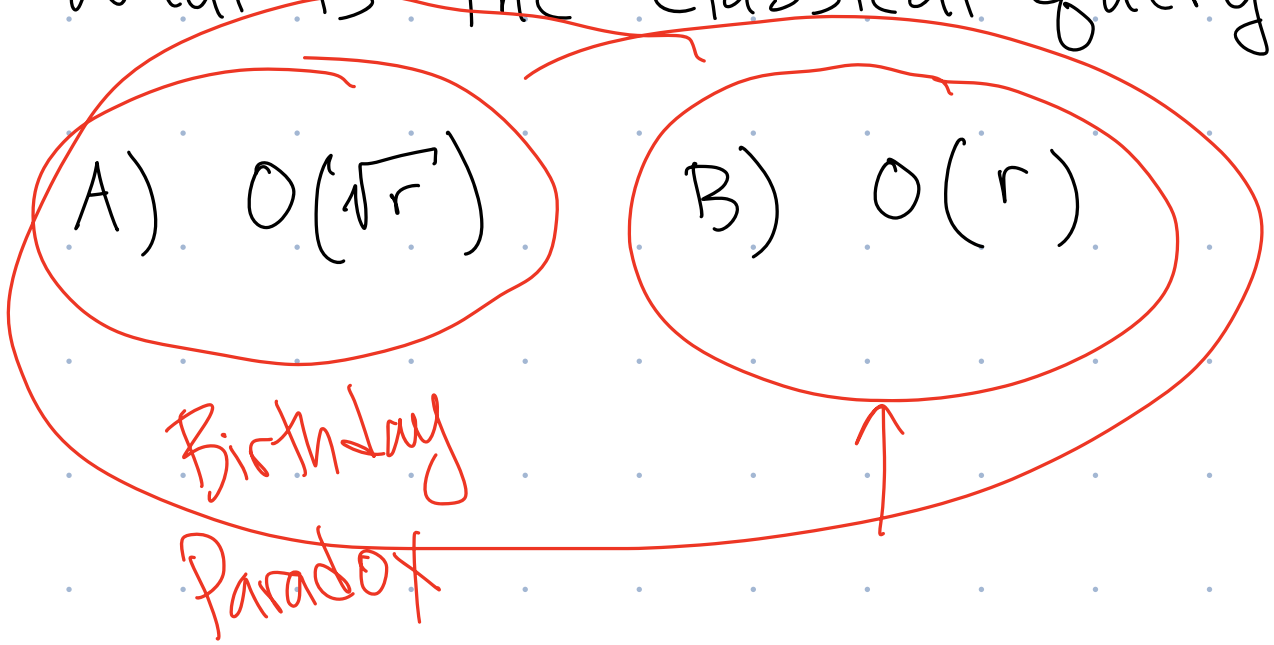
ex:



Output: r

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:

$011 \leftrightarrow 3$

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

$|010\rangle \leftrightarrow |2\rangle$

Standard Basis States

$\underbrace{\{|0\rangle, |1\rangle, |2\rangle, \ldots, |N-1\rangle\}}$

N-dimensional state

Ambiguity: $|3\rangle \Rightarrow |11\rangle$ (2 qubits)

$|3\rangle \Rightarrow |011\rangle$ (3 qubits)

$|0\rangle$

$|3\rangle \Rightarrow |0000\ldots00\,11\rangle$ (lots of qubits)

$$|\psi\rangle = \sum_{k=0}^{N-1} a_k |k\rangle$$

$$\sum |a_k|^2 = 1$$

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

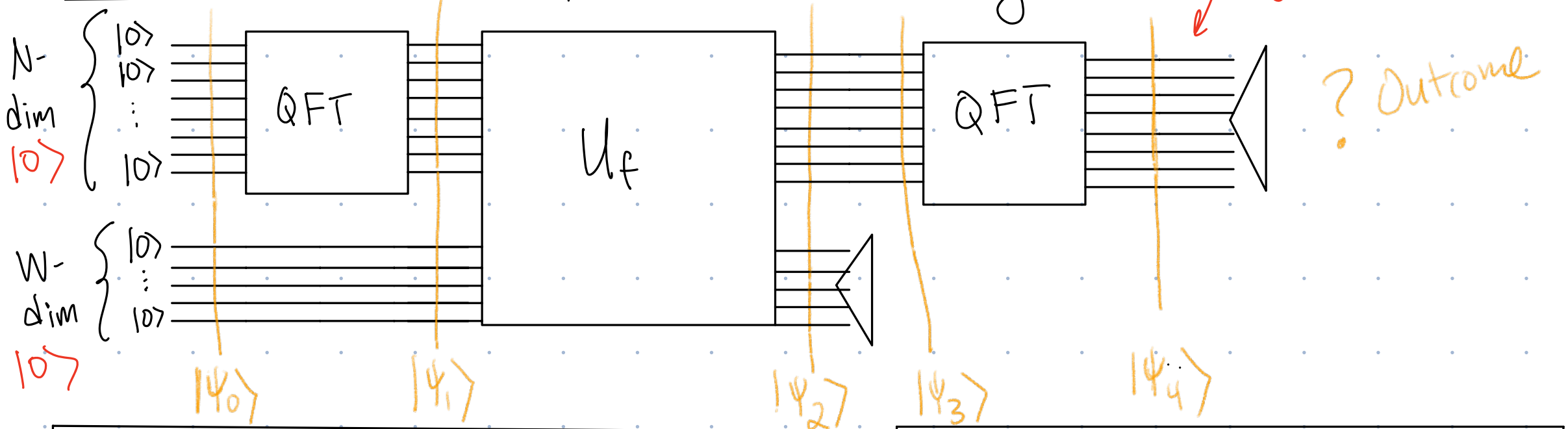
A) $\lceil \log_2 3 \rceil$ B) 3 C) $\log_2 N$ D) N

2 qubits → $|11\rangle$ → $|3\rangle$

3 qubits → $|111\rangle$ → $|7\rangle$

4 qubits → $|1111\rangle$ → $|15\rangle$

Quantum Circuit for Period Finding



QFT: Quantum Forier Transform

N-dim standard basis state

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

U_f:

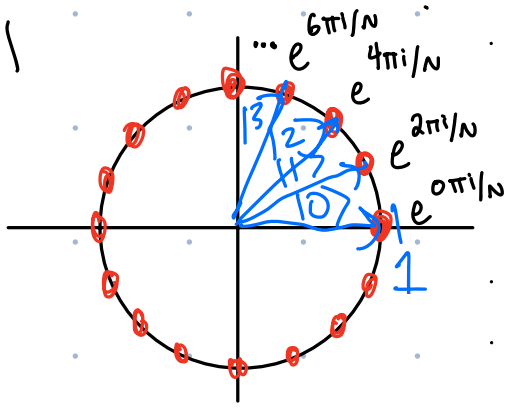
$$U_f |y\rangle|b\rangle \xrightarrow{\text{(x)}} |y\rangle|b + f(y) \bmod W\rangle$$

↑ N-dim stand. basis

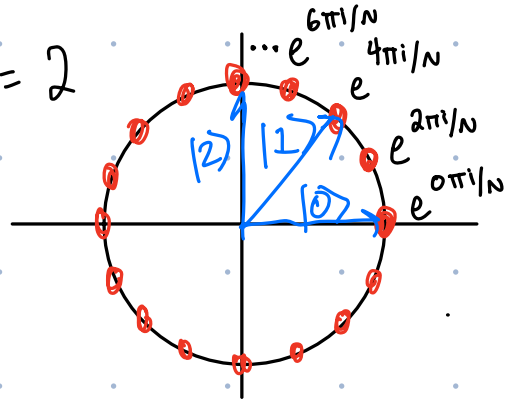
↑ W-dim stand. basis

Phase of each standard basis state in superposition

X=1



X= 2



$QFT|0\rangle = ?$

go/fourier-transform

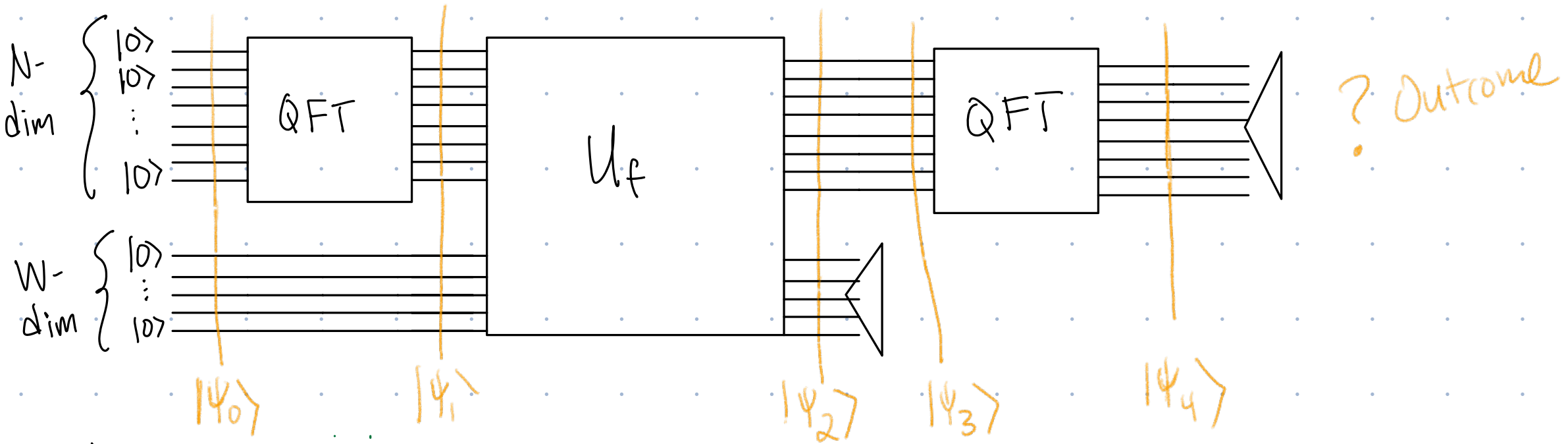
$$QFT|0\rangle = \frac{1}{\sqrt{N}} \sum_{g=0}^{N-1} e^{2\pi i \cdot 0 \cdot g/N} |g\rangle$$

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

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

Equal superposition state

Group Excercise: Analyze!



$$|\psi_0\rangle = |0\rangle|0\rangle$$

$$|\psi_1\rangle = (QFT|0\rangle)|0\rangle = \left(\frac{1}{\sqrt{N}}\sum_{g=0}^{N-1} e^{2\pi i \cdot 0 \cdot g/N}|g\rangle\right)|0\rangle = \frac{1}{\sqrt{N}}\sum_{g=0}^{N-1}|g\rangle|0\rangle$$

$$|\psi_2\rangle = U_f\left(\frac{1}{\sqrt{N}}\sum_{g=0}^{N-1}|g\rangle|0\rangle\right) = \frac{1}{\sqrt{N}}\sum_{g=0}^{N-1} U_f(|g\rangle|0\rangle)$$

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

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

$\log_2 N$ $\log_2 W$

Qubits: $\log_2 N + \log_2 W \rightarrow 2^{\log_2 N + \log_2 W} = N \cdot W$

Dimension: $\log_2 N + \log_2 W$

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

$\triangleleft$ = Standard basis measurement

$$\left|\sum_{x=0}^{N-1} a_x \langle y|x\rangle\right|^2$$

↑

- Measure entire state:

$|\psi\rangle = \sum_{x=0}^{N-1} a_x |x\rangle$ ⟹ Prob of outcome $|y\rangle$ is $|\langle y|\psi\rangle|^2 = |a_y|^2$

↑ standard basis state

- Partial measurement (B system)

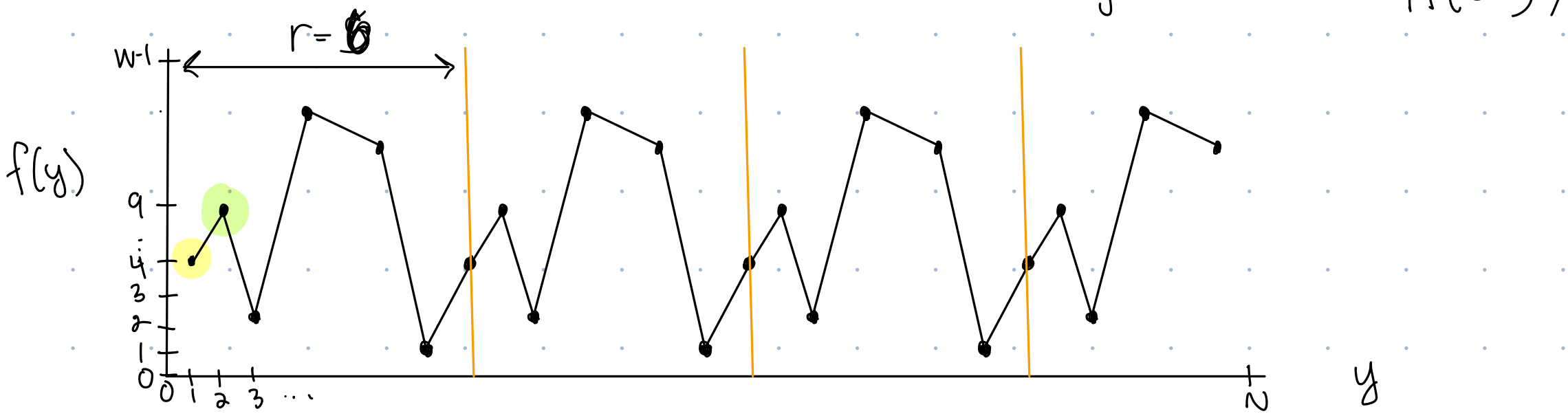
$|\psi\rangle = \sum_x \sum_z a_{xz} |x\rangle_A |z\rangle_B$ ⟹ Prob of outcome $|y\rangle_B$

↑ ↑ standard basis states

$p = \sum_x |a_{xy}|^2$

⟹ Collapses $\frac{1}{\sqrt{p}} \sum_x a_{xy} |x\rangle|y\rangle$

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 $|f(b^*)\rangle$



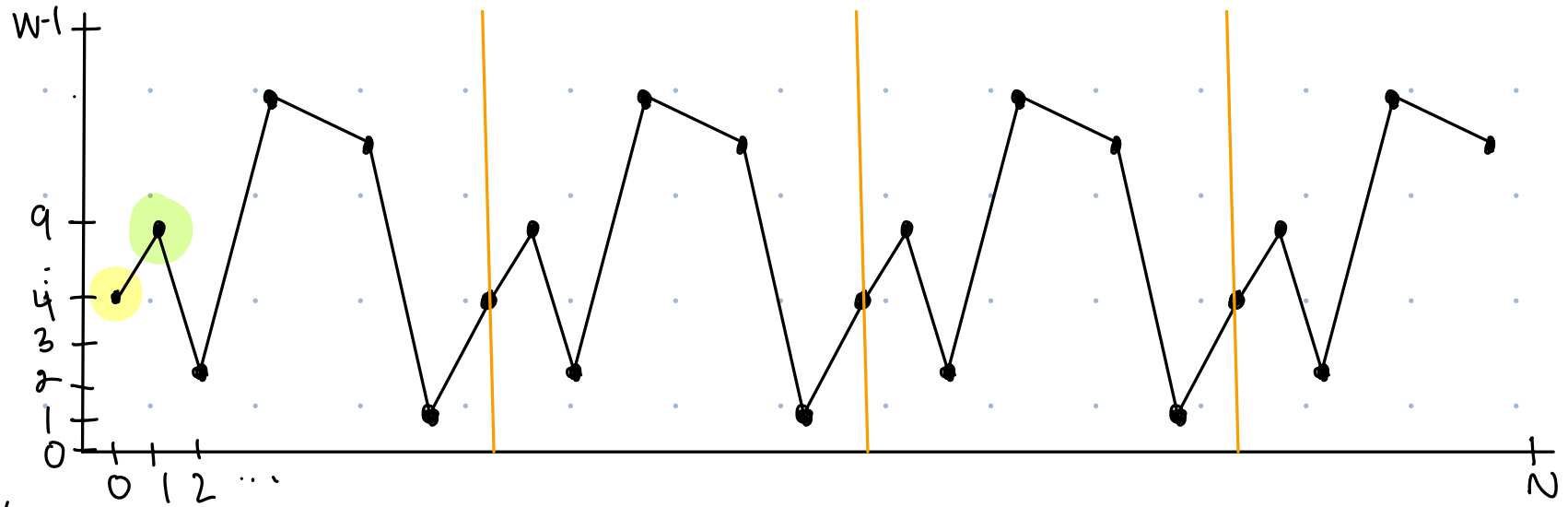
(outcome $f(b^*)$) $|\psi_3\rangle = \square \sum_{m=0}^{\square} |b^* + \square\rangle$

Geomtric Series Formula:

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

ex:

$r = 6$



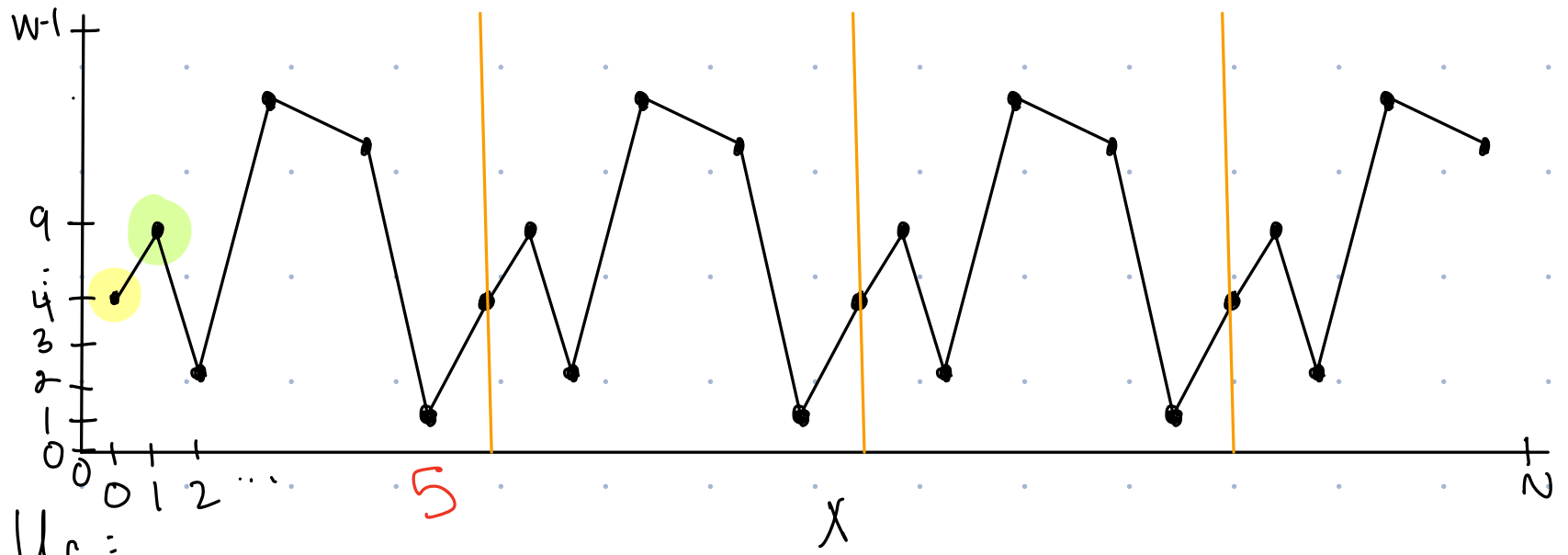
$$\frac{1}{\sqrt{N}} \sum_{g=0}^{N-1} |g\rangle |f(g)\rangle =$$

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

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

measure $|13\rangle$ → $\frac{1}{\sqrt{N}} \frac{1}{\sqrt{P}} \Big(|3\rangle + |9\rangle + |15\rangle + \cdots \Big)$

$r = 6$



After U_f:

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

We only learn $f(b^*)$, not b^*

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

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

$$|\psi_3\rangle = \Big(\frac{1}{\sqrt{\frac{1}{r}}} \frac{1}{\sqrt{N}} \sum_{m=0}^{\frac{N}{r}-1} |b^* + mr\rangle \Big) |f(b^*)\rangle$$

$$p = \frac{N}{r} \left| \frac{1}{\sqrt{N}} \right|^2 = \frac{N}{r} \cdot \frac{1}{N} = \frac{1}{r}$$

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

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

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

$$P(|9\rangle) = \left|\frac{1}{\sqrt{N}}\right|^2 + \left|\frac{1}{\sqrt{N}}\right|^2 + \left|\frac{1}{\sqrt{N}}\right|^2 + \cdots$$

$$= \underbrace{\frac{1}{N} + \frac{1}{N} + \frac{1}{N} + \cdots + \frac{1}{N}}_{\frac{N}{r} \text{ term}}$$

$$= \frac{1}{r}$$

$$\Rightarrow \text{collapse} \quad \frac{1}{\sqrt{\frac{1}{r}}} \Big(\frac{1}{\sqrt{N}} |1\rangle + \frac{1}{\sqrt{N}} |7\rangle + \frac{1}{\sqrt{N}} |13\rangle + \cdots \Big) |9\rangle$$

$$|\psi_4\rangle = QFT\left(\sqrt{\frac{r}{N}}\sum_{m=0}^{\frac{N}{r}-1}|b^*+mr\rangle\right) = \sqrt{\frac{r}{N}}\sum_{m=0}^{\frac{N}{r}-1} QFT\,|b^*+mr\rangle$$

$$= \sqrt{\frac{r}{N}}\sum_{m=0}^{\frac{N}{r}-1}\frac{1}{\sqrt{N}}\sum_{z=0}^{N-1} e^{2\pi i\,(b^*+mr)\,z/N}\,|z\rangle$$

$$P_r(|y\rangle) = \left|\langle y|\sqrt{\frac{r}{N}}\sum_{m=0}^{\frac{N}{r}-1}\frac{1}{\sqrt{N}}\sum_{z=0}^{N-1} e^{2\pi i\,(b^*+mr)\,z/N}\,|z\rangle\right|^2$$

$$= \left|\sqrt{\frac{r}{N}}\sum_{m=0}^{\frac{N}{r}-1}\frac{1}{\sqrt{N}}\sum_{z=0}^{N-1} e^{2\pi i\,(b^*+mr)\,z/N}\,\langle y|z\rangle\right|^2$$

$$= \left|\sqrt{\frac{r}{N}}\sum_{m=0}^{\frac{N}{r}-1}\frac{1}{\sqrt{N}}\, e^{2\pi i\,(b^*+mr)\,y/N}\right|^2$$

$$|a\cdot b|^2 = |a|^2\cdot|b|^2$$

$$e^{2\pi i\,(b^*+mr)\,y/N} \to e^{2\pi i b^* y/N}\, e^{2\pi i mry/N}$$

$$= \left|\frac{\sqrt{r}}{N}\, e^{2\pi i b^* y/N}\sum_{m=0}^{\frac{N}{r}-1}\left(e^{2\pi i ry/N}\right)^m\right|^2$$

$$= \frac{r}{N^2}\left|\sum_{m=0}^{\frac{N}{r}-1}\left(e^{2\pi i ry/N}\right)^m\right|^2$$

$$= \sqrt{\frac{r}{N}} \sum_{m=0}^{\frac{N}{r}-1} \frac{1}{\sqrt{N}} \sum_{z=0}^{N-1} e^{2\pi i (b + mr) z / N} |z\rangle$$

$$\frac{r}{N^2} \left| \sum_{m=0}^{\frac{N}{r}-1} \left(e^{2\pi i r y / N} \right)^m \right|^2$$

$a = e^{2\pi i r y/N}$

Geomtric Series Formula:

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

$a=1$ ↙ $\qquad$ $a\neq 1$ ↘

$$\frac{r}{N^2}\left|\frac{N}{r}\right|^2 = \frac{1}{r}$$

When does $e^{2\pi i r y/N} = 1$?

$$\frac{2\pi i r y}{N} = 2\pi i \cdot k \quad k \in \mathbb{Z}$$

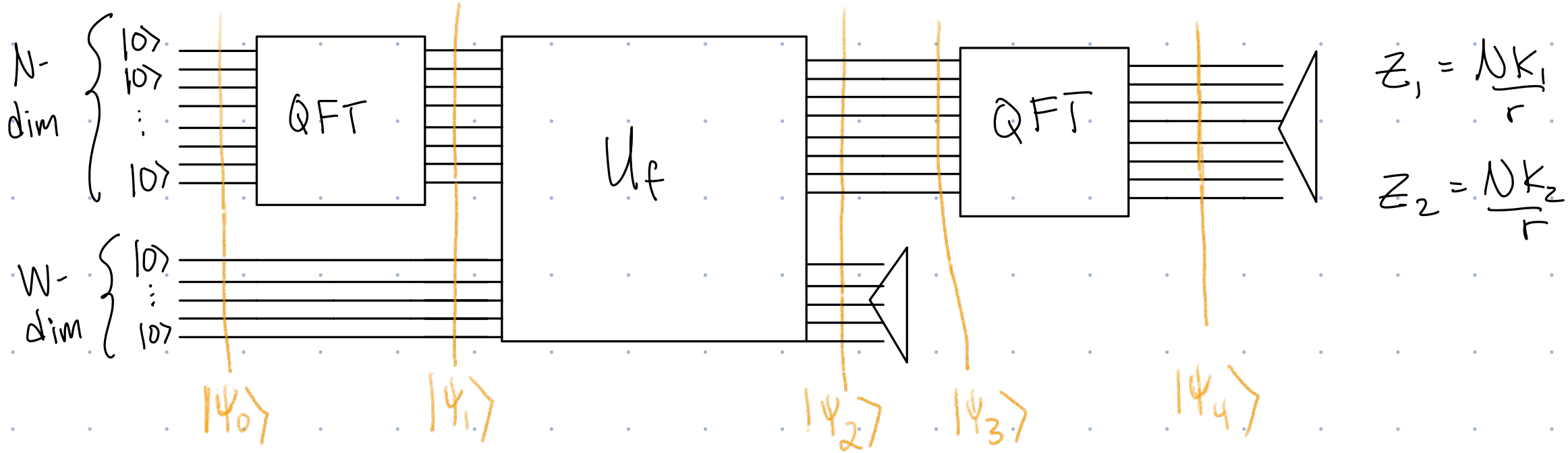
$$y = \frac{k \cdot N}{r}$$

$$= \frac{1-\left(e^{2\pi i r y/N}\right)^{\frac{N}{r}}}{1-e^{2\pi i r y/N}}$$

$$= \frac{1-e^{2\pi i y}}{1-e^{2\pi i r y/N}} = 0$$

Period Finding Algorithm (Shor's Algorithm)

① Run 2 times:



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

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

② Classical Post-processing:

$\frac{z_1}{N}$, $\frac{z_2}{N}$

$\frac{k_1}{r}$, $\frac{k_2}{r}$

↓ Continued Fraction

$\frac{s_1}{t_1}$, $\frac{s_2}{t_2}$, ...

$s_1 \; s_2 \; s_3 \; s_4$

$t_1 \; t_2 \; t_3 \; t_4$

Guess for r

③ Plug back in to $f(0)$, $f(r)$

Query Compexity of Period Finding

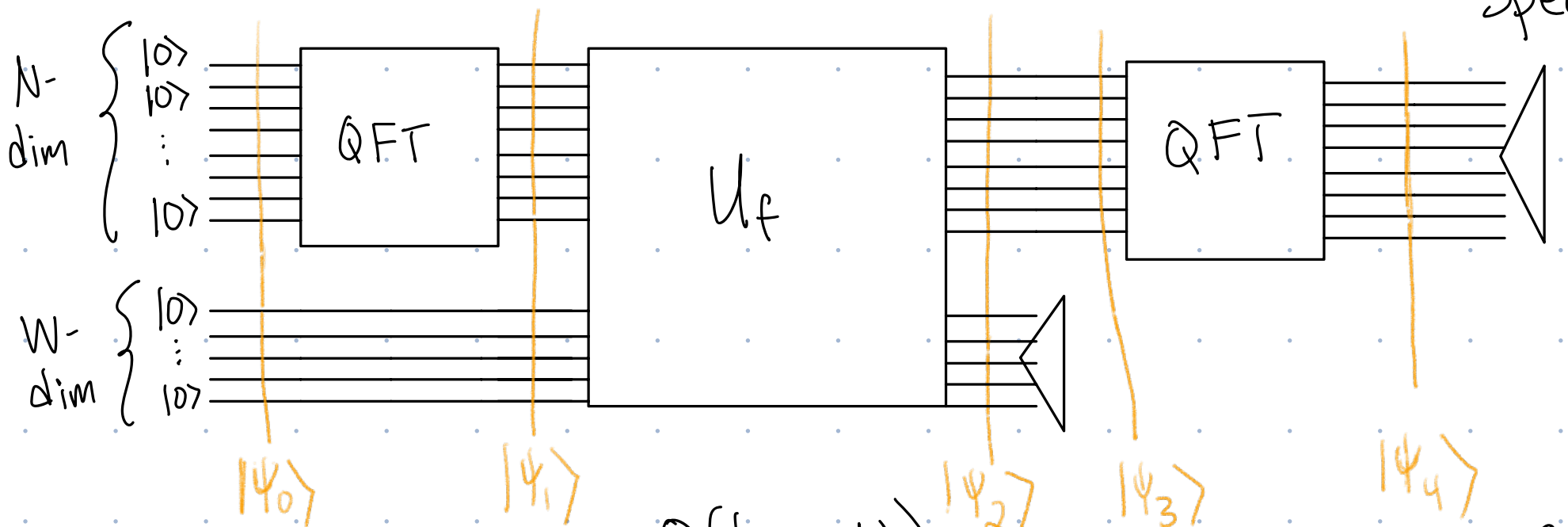
Classical: $\Omega(\sqrt{r})$

Quantum: $O(1)$

Time Complexity of Factoring

Quantum:

Circuit used to factor N.



Nearly Exponential Speedup!

$O(\log_2^2 N)$ $O(\log_2 N)$ $O(\log_2^{2} N) = O(\log_2^2 N)$

$O(\log_2^{1/3} N)$

Classical: e

Number Field Sieve

- 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]

10^{600}

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.