

Quantum Computing

- Week 10 (June 16-17)
- Topics:
 - Factoring
 - Order Finding
 - Order Finding via Phase Estimation
 - Order Finding via Shor's algorithm

QFT and inverse QFT

- Quantum Fourier Transformation

$$\text{QFT}_N: |j\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{\frac{2\pi ijk}{N}} |k\rangle$$

QFT

$$\text{QFT}_N^\dagger: |j\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{-\frac{2\pi ijk}{N}} |k\rangle$$

Inverse QFT

$$\text{QFT}_N^\dagger \text{QFT}_N = I$$

QFT and inverse QFT

- Inverse Quantum Fourier Transformation

$$\text{QFT}_N^\dagger: \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{\frac{2\pi i j k}{N}} |k\rangle \mapsto |j\rangle$$

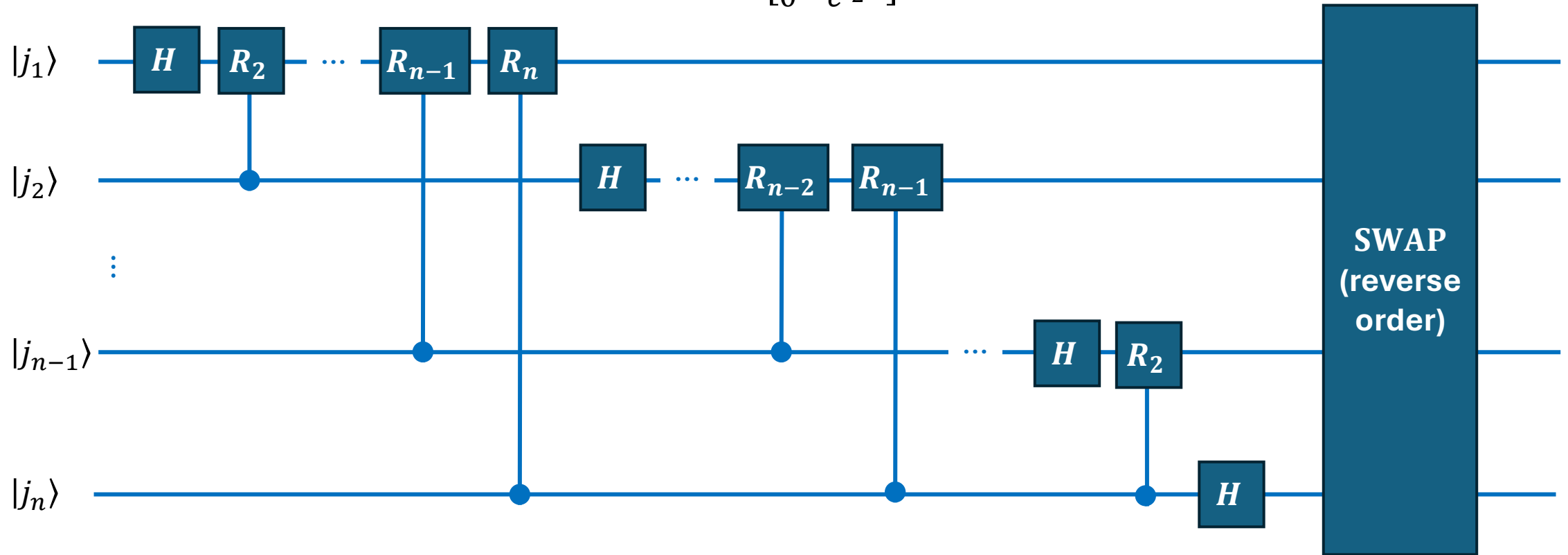
Inverse QFT

- Extract j from the phases

QFT and inverse QFT

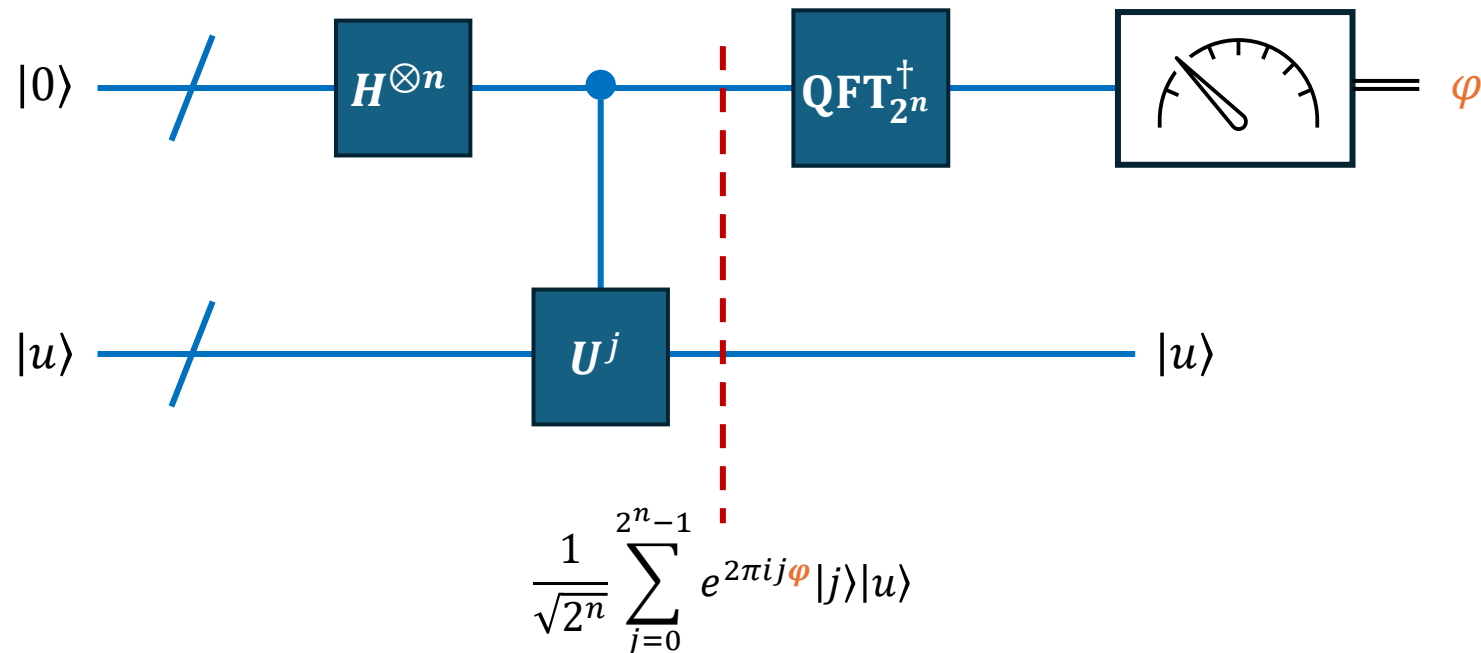
- Circuit for QFT (and similarly, inverse QFT)

$$R_k := \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^k}} \end{bmatrix}$$



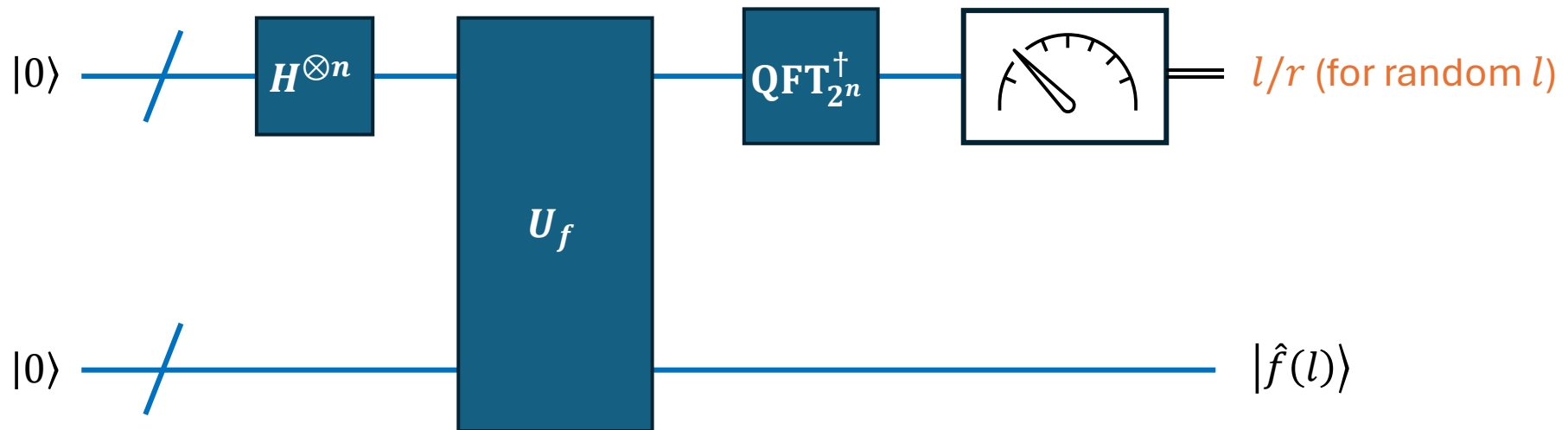
Phase Estimation

- Given U and $|u\rangle$ s.t. $U|u\rangle = e^{2\pi i\varphi}|u\rangle = e^{2\pi i(0.\varphi_1\varphi_2\varphi_3\dots)}|u\rangle$
- Compute or estimate $(0.\varphi_1\varphi_2\varphi_3\dots)$



Period Finding

- Suppose that we have a function f with a period $r < 2^L$.
- Namely, there exists a minimal $r > 0$ such that $f(x + r) = f(x)$
- Goal: Find r



Factoring

- Let $N = pq$, where p and q are large primes
- **Factoring:** Given N , find p and q
- Easy case 1: $|p - q|$ is too small (e.g., $p = q$ or $p \approx q \approx \sqrt{N}$)
- Easy case 2: $|p - q|$ is too large
- Worst case: No known efficient classical algorithm

- Applications:
 - **RSA cryptosystems**

RSA896	270	896	US\$75,000 ^[d]	
RSA280	280	928		
RSA290	290	962		
RSA300	300	995		
RSA309	309	1024		
RSA1024	309	1024	US\$100,000 ^[d]	

Source: RSA_Factoring_Challenge, Wikipedia

Order Finding

- Let N and x be two positive integers
- Algebra fact: Multiplication mod N forms a **group** \mathbb{Z}_N^*
- Quick question: If $x \in \mathbb{Z}_N^*$, then _____

Order Finding

- Let N and x be two positive integers
- Algebra fact: Multiplication mod N forms a **group** \mathbb{Z}_N^*
- Quick question: If $x \in \mathbb{Z}_N^*$, then $\gcd(x, N) = 1$

Order Finding

- Let N and x be two positive integers
- Algebra fact: Multiplication mod N forms a **group** \mathbb{Z}_N^*
- Quick question: If $x \in \mathbb{Z}_N^*$, then $\gcd(x, N) = 1$

- **Order (mod N):** The minimal integer r such that $x^r = 1 \pmod{N}$
- **Order Finding:** Find r

Order Finding

- Let N and x be two positive integers
- Algebra fact: Multiplication mod N forms a **group** \mathbb{Z}_N^*
- Quick question: If $x \in \mathbb{Z}_N^*$, then $\gcd(x, N) = 1$

- **Order (mod N):** The minimal integer r such that $x^r = 1 \pmod{N}$
- **Order Finding:** Find r

- **Two approaches:**
 - (1) Phase estimation
 - (2) Shor's approach (Homework)

Order Finding

- **Order (mod N):** The minimal integer r such that $x^r = 1 \pmod{N}$
- **Order Finding:** Let N and $x \in \mathbb{Z}_N^*$ be two positive integers. Find the order r of x .
- **Phase estimation approach:**
 - Use qubits to express modulo N
 - Let $U_x: |v\rangle \mapsto |v \cdot x \pmod{N}\rangle$
 1. Is U_x a unitary? What if $x \notin \mathbb{Z}_N^*$
 2. What are the eigenvalues of U_x^r and U_x ?
 3. Let $|u_k\rangle$ be the eigenvector of U_x with k -th root of unity. How can we generate $|u_k\rangle$?
 4. Given $(\frac{k_1}{r}, \frac{k_2}{r}, \dots)$, where all k values are random, how can we recover r ?
 5. Given r , how can we decompose N ?

Order Finding

- $U_x: |v\rangle \mapsto |v \cdot x \bmod N\rangle$
- Let $|u\rangle$ be an eigenvector of U_x (with eigenvalue λ)

$$U_x|u\rangle = \lambda|u\rangle$$

Order Finding

- $U_x: |v\rangle \mapsto |v \cdot x \bmod N\rangle$
- Let $|u\rangle$ be an eigenvector of U_x (with eigenvalue λ)

$$U_x^k |u\rangle = \lambda^k |u\rangle$$

Order Finding

- $U_x: |v\rangle \mapsto |v \cdot x \bmod N\rangle$
- Let $|u\rangle$ be an eigenvector of U_x (with eigenvalue λ). Let r be the order of x

$$U_x^r |u\rangle = \lambda^r |u\rangle = |u\rangle \Rightarrow \lambda^r = 1$$

Order Finding

- $U_x: |v\rangle \mapsto |v \cdot x \bmod N\rangle$
- Let $|u\rangle$ be an eigenvector of U_x (with eigenvalue λ). Let r be the order of x

$$U_x^r |u\rangle = \lambda^r |u\rangle = |u\rangle \Rightarrow \lambda^r = 1$$

- **The eigenvalues of U_x are r -th roots of unity**

$$\lambda_0 = 1, \lambda_1 = e^{\frac{2\pi i}{r}}, \dots, \lambda_s = e^{\frac{2\pi i}{r} \cdot s}, \dots, \lambda_{r-1} = e^{\frac{2\pi i}{r} \cdot (r-1)}$$

Order Finding

- $U_x: |v\rangle \mapsto |v \cdot x \bmod N\rangle$
- $\lambda_s = e^{\frac{2\pi i}{r} \cdot s}$ ($s \in \{0, \dots, r - 1\}$) are eigenvalues of U_x

Order Finding

- $U_x: |v\rangle \mapsto |v \cdot x \bmod N\rangle$
- $\lambda_s = e^{\frac{2\pi i}{r} \cdot s}$ ($s \in \{0, \dots, r - 1\}$) are eigenvalues of U_x

$$U_x |x^k \bmod N\rangle = |x^{k+1} \bmod N\rangle$$

Order Finding

- $U_x: |v\rangle \mapsto |v \cdot x \bmod N\rangle$
- $\lambda_s = e^{\frac{2\pi i}{r} \cdot s}$ ($s \in \{0, \dots, r-1\}$) are eigenvalues of U_x

$$U_x \left(\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |x^k \bmod N\rangle \right) = U_x \left(\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |x^{k+1} \bmod N\rangle \right)$$

Order Finding

- $U_x: |v\rangle \mapsto |v \cdot x \bmod N\rangle$
- $\lambda_s = e^{\frac{2\pi i}{r} \cdot s}$ ($s \in \{0, \dots, r-1\}$) are eigenvalues of U_x

$$U_x \left(\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |x^k \bmod N\rangle \right) = \left(\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |x^{k+1} \bmod N\rangle \right)$$
$$= \left(\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |x^k \bmod N\rangle \right)$$

Order Finding

- $U_x: |v\rangle \mapsto |v \cdot x \bmod N\rangle$
- $\lambda_s = e^{\frac{2\pi i}{r} \cdot s}$ ($s \in \{0, \dots, r-1\}$) are eigenvalues of U_x
- $\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |x^k \bmod N\rangle$ is an eigenvector (with eigenvalue $\lambda_0 = 1$) of U_x
- U_x appears to be a **cyclic shift operator**

Order Finding

- $U_x: |v\rangle \mapsto |v \cdot x \bmod N\rangle$
- $\lambda_s = e^{\frac{2\pi i}{r} \cdot s}$ ($s \in \{0, \dots, r-1\}$) are eigenvalues of U_x
- $\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |x^k \bmod N\rangle$ is an eigenvector (with eigenvalue $\lambda_0 = 1$) of U_x
- U_x appears to be a **cyclic shift operator**

$$U_x \left(\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |x^k \bmod N\rangle \right) = \left(\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |x^{k+1} \bmod N\rangle \right)$$

Order Finding

- $U_x: |v\rangle \mapsto |v \cdot x \bmod N\rangle$
- $\lambda_s = e^{\frac{2\pi i}{r} \cdot s}$ ($s \in \{0, \dots, r-1\}$) are eigenvalues of U_x
- $\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |x^k \bmod N\rangle$ is an eigenvector (with eigenvalue $\lambda_0 = 1$) of U_x
- U_x appears to be a **cyclic shift operator**

$$U_x \left(\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} c_k |x^k \bmod N\rangle \right) = \left(\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} c_k |x^{k+1} \bmod N\rangle \right)$$

Order Finding

- $U_x: |v\rangle \mapsto |v \cdot x \bmod N\rangle$
- $\lambda_s = e^{\frac{2\pi i}{r} \cdot s}$ ($s \in \{0, \dots, r-1\}$) are eigenvalues of U_x
- $\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |x^k \bmod N\rangle$ is an eigenvector (with eigenvalue $\lambda_0 = 1$) of U_x
- U_x appears to be a **cyclic shift operator**

$$\begin{aligned} U_x \left(\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} c_k |x^k \bmod N\rangle \right) &= \left(\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} c_k |x^{k+1} \bmod N\rangle \right) \\ &= \left(\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} c_{k-1} |x^k \bmod N\rangle \right) \end{aligned}$$

Order Finding

- $U_x: |v\rangle \mapsto |v \cdot x \bmod N\rangle$
- $\lambda_s = e^{\frac{2\pi i}{r} \cdot s}$ ($s \in \{0, \dots, r-1\}$) are eigenvalues of U_x
- $\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |x^k \bmod N\rangle$ is an eigenvector (with eigenvalue $\lambda_0 = 1$) of U_x
- U_x appears to be a **cyclic shift operator**

$$U_x \left(\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} c_k |x^k \bmod N\rangle \right) = \left(\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} c_{k-1} |x^k \bmod N\rangle \right) = \lambda_s \left(\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} c_k |x^k \bmod N\rangle \right)$$

Order Finding

- $U_x: |v\rangle \mapsto |v \cdot x \bmod N\rangle$
- $\lambda_s = e^{\frac{2\pi i}{r} \cdot s}$ ($s \in \{0, \dots, r-1\}$) are eigenvalues of U_x
- $\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |x^k \bmod N\rangle$ is an eigenvector (with eigenvalue $\lambda_0 = 1$) of U_x
- U_x appears to be a **cyclic shift operator**

$$U_x \left(\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} c_k |x^k \bmod N\rangle \right) = \left(\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} c_{k-1} |x^k \bmod N\rangle \right) = \lambda_s \left(\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} c_k |x^k \bmod N\rangle \right)$$

$$\Rightarrow c_k = \lambda_s^{-1} c_{k-1} (c_{-1} = c_{r-1})$$

Order Finding

- $U_x: |v\rangle \mapsto |v \cdot x \bmod N\rangle$
- $\lambda_s = e^{\frac{2\pi i}{r} \cdot s}$ ($s \in \{0, \dots, r-1\}$) are eigenvalues of U_x
- $\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |x^k \bmod N\rangle$ is an eigenvector (with eigenvalue $\lambda_0 = 1$) of U_x
- U_x appears to be a **cyclic shift operator**

$$c_k = \lambda_s^{-1} c_{k-1} (c_{-1} = c_{r-1})$$

- Let $c_0 = 1$, $c_k = e^{-\frac{2\pi i}{r} \cdot s \cdot k}$

Order Finding

- $U_x: |v\rangle \mapsto |v \cdot x \bmod N\rangle$
- $\lambda_s = e^{\frac{2\pi i}{r} \cdot s}$ ($s \in \{0, \dots, r-1\}$) are eigenvalues of U_x
- $\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |x^k \bmod N\rangle$ is an eigenvector (with eigenvalue $\lambda_0 = 1$) of U_x
- U_x appears to be a **cyclic shift operator**

$$c_k = \lambda_s^{-1} c_{k-1} \quad (c_{-1} = c_{r-1})$$

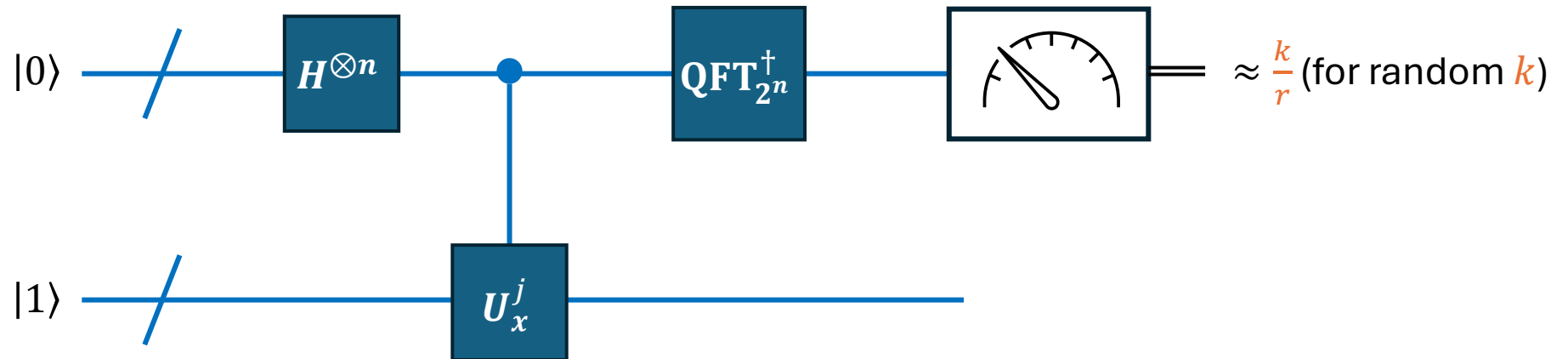
- Let $c_0 = 1$, $c_k = e^{-\frac{2\pi i}{r} \cdot s \cdot k}$, then

$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-\frac{2\pi i}{r} \cdot s \cdot k} |x^k \bmod N\rangle,$$

- where $U_x |u_s\rangle = \lambda_s |u_s\rangle$

Order Finding

- **Order (mod N):** The minimal integer r such that $x^r = 1 \pmod{N}$
- **Order Finding:** Let N and $x \in \mathbb{Z}_N^*$ be two positive integers. Find the order r of x .
- **Phase estimation approach:**
 - Let $U_x: |v\rangle \mapsto |v \cdot x \pmod{N}\rangle$

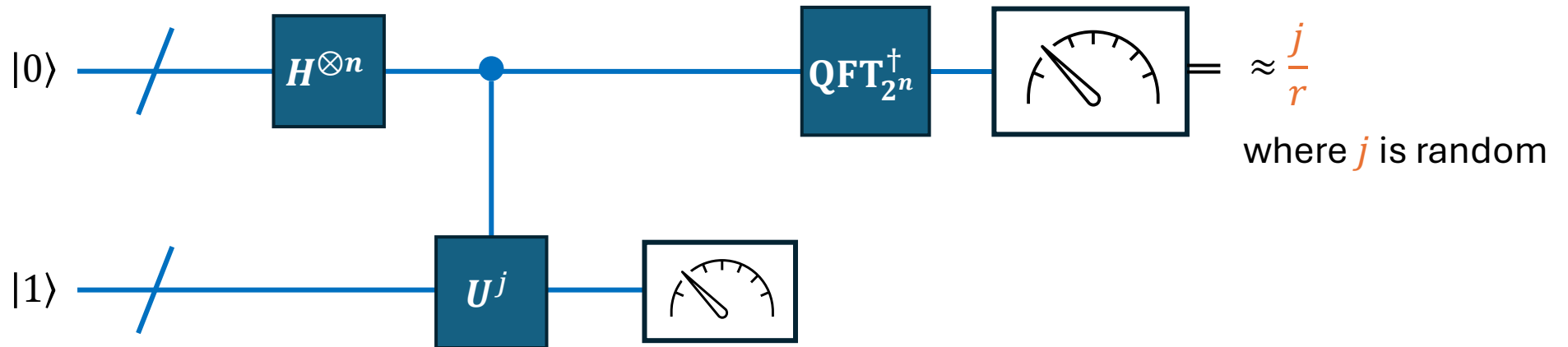


Reduction: Factoring to Order Finding

- **Reduction (Informal):** We say P_2 is reducible to P_1 if solving $P_1 \Rightarrow$ solving P_2
 - We usually require the “ \Rightarrow ” here is some efficient algorithm
- P_1 (**Order finding**) = “Given N and x , find r (i.e., the minimal r s.t. $x^r = 1 \pmod{N}$)”
- P_2 (**Factoring**) = “Given $N = pq$, find the two primes p and q ”
- Question: If we can solve P_1 , then how can we solve P_2 ?
 - Namely, if we can always compute the order r of arbitrary $x \pmod{N}$, ...
 - ...then how to decompose N ?

Order Finding via Shor's algorithm

- **Order (mod N):** The minimal integer r such that $x^r = 1 \pmod{N}$
- **Order Finding:** Let N and x be two positive integers. Find the order r of x .
- **Shor's algorithm:** (Same circuit but different analysis)
 - Let $U_x: |v\rangle \mapsto |v \cdot x \pmod{N}\rangle$

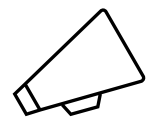


Reference

- **[NC00]:** Chapter 5
- **[KLM07]:** Chapter 7 (Tip: Check out Fig 7.16)

Third Homework Set

- Factoring via Shor's algorithm
- Will be announced in Moodle
- **Deadline: July 15th, 2026 at 23:59**



No lectures in Week 11 (June 23-24)