Quantum Computing

- Lectures 15 and 16 (July 2-3, 2025)

- Topics:
  - Factoring
  - Order Finding
  - Order Finding via Phase Estimation
  - Order Finding via Shor’s algorithm

QFT and inverse QFT

- Quantum Fourier Transformation

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

QFT

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

Inverse QFT

$$\mathbf{QFT_N^\dagger QFT_N} = \boldsymbol{I}$$

QFT and inverse QFT

- Inverse Quantum Fourier Transformation

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

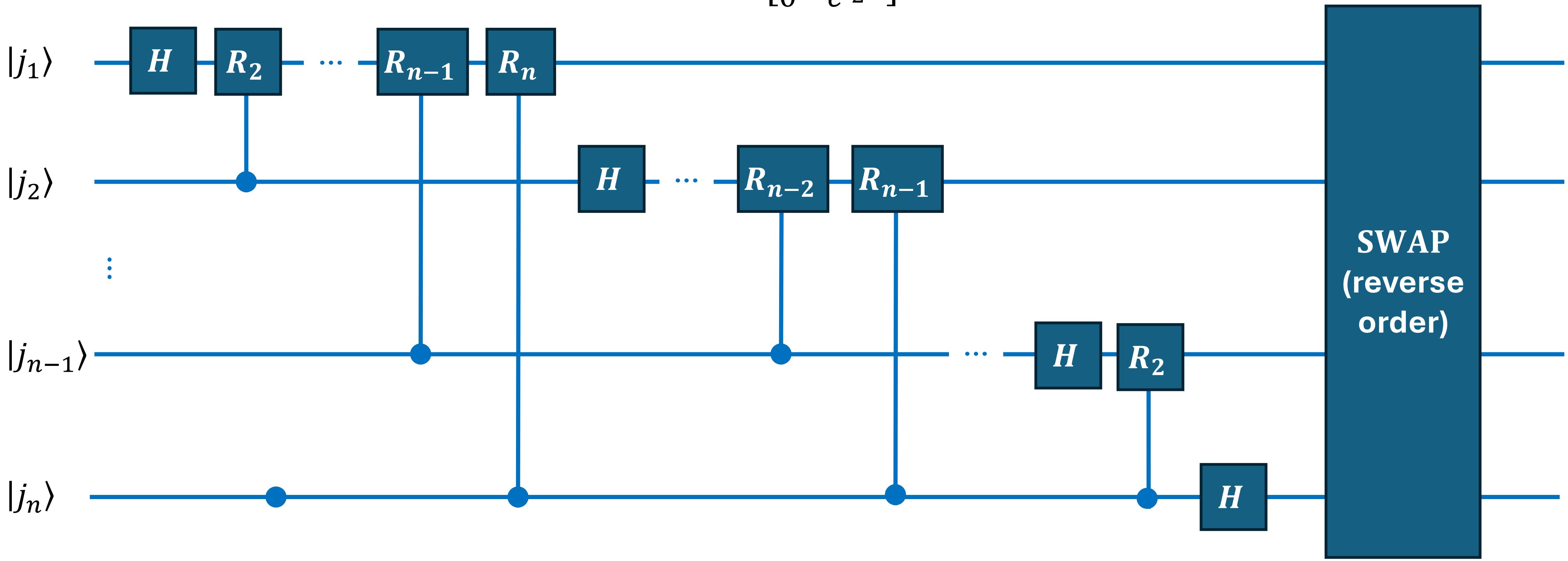
Inverse QFT

- Extract j from the phases!

QFT and inverse QFT

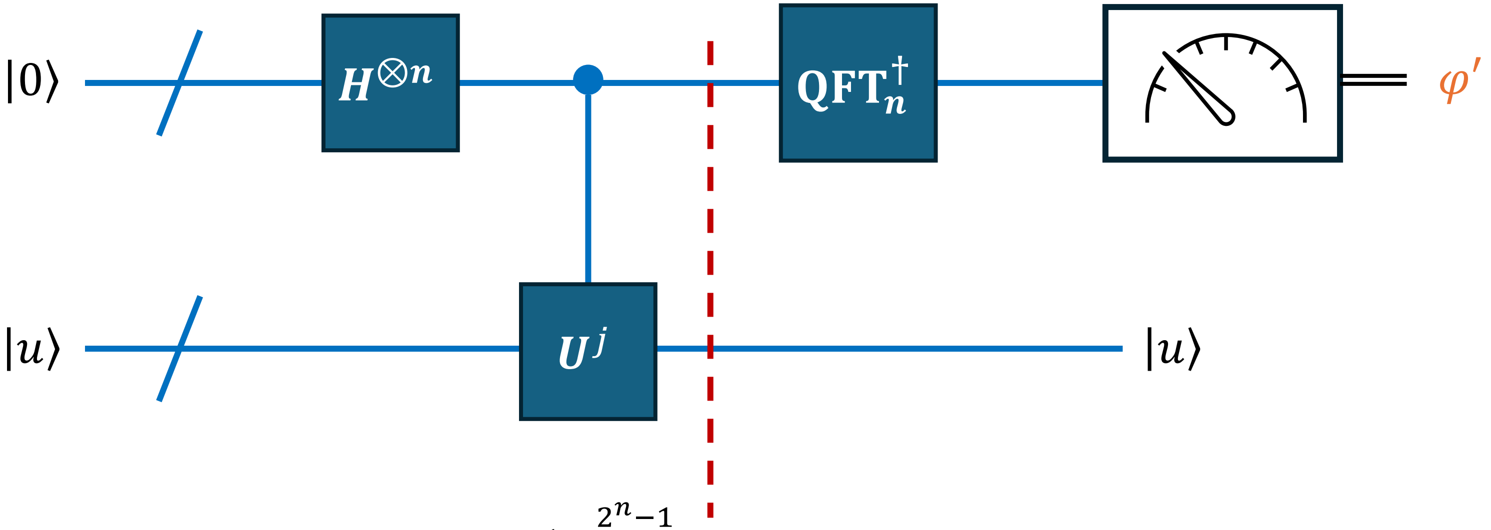
- Circuit for QFT (and similarly, inverse QFT)

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



Phase Estimation

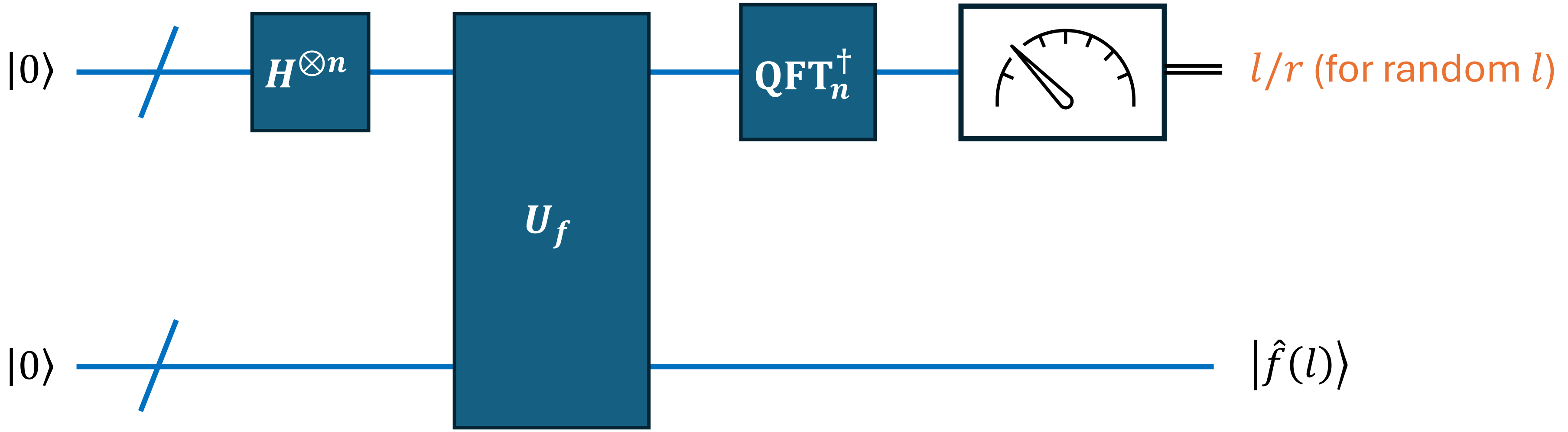
- Given $\boldsymbol{U}$ and $|u\rangle$ s.t. $\boldsymbol{U}|u\rangle = e^{2\pi i\varphi}|u\rangle = e^{2\pi i(0.\varphi_1\varphi_2\varphi_3\ldots)}|u\rangle$
- Compute or estimate $(0.\varphi_1\varphi_2\varphi_3\ldots)$



$$\frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1} e^{2\pi i k\varphi}|k\rangle|u\rangle$$

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., $p = q$)
- 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 (Exercise tomorrow)

Order Finding

- **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.

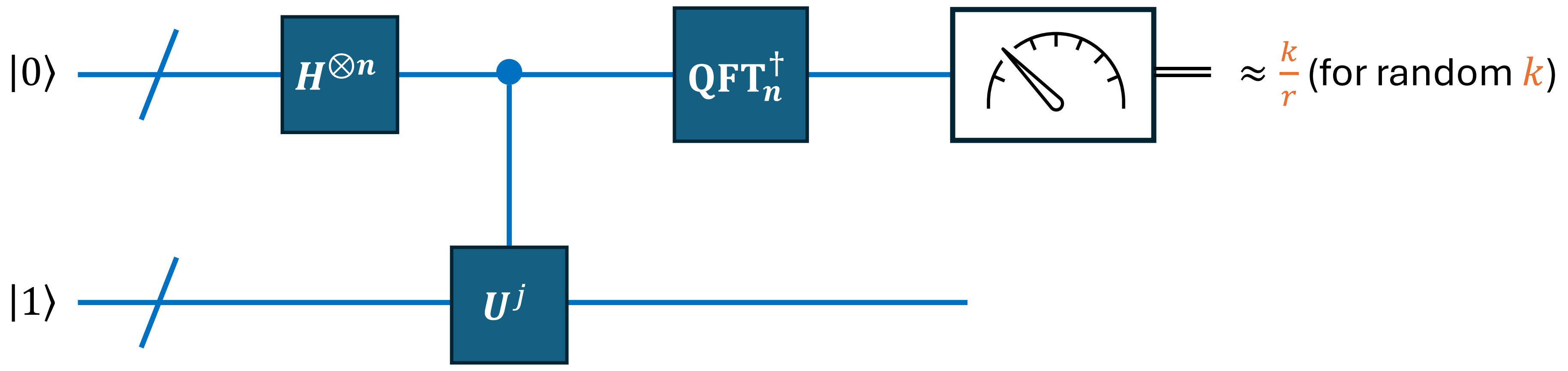
- **Phase estimation approach:**
  - Use qubits to express modulo N
  - Let $U_x\colon |v\rangle \mapsto |v \cdot x \mod N\rangle$

1. What are the eigenvalues of U_x^r and U_x
2. Let $|u_k\rangle$ be the eigenvalue of U_x with k-th root of unity. How can we generate $|u_k\rangle$?
3. Given $(\frac{k_1}{r}, \frac{k_2}{r}, \ldots)$, where all k values are random, how can we recover r?
4. Given r, how can we decompose N?

Order Finding

- **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.

- **Phase estimation approach:**
  - Let $U_x\colon |v\rangle \mapsto |v \cdot x \mod N\rangle$



Reduction: Factoring to Order Finding

- **Reduction (Informal):** We say $\boldsymbol{P_2}$ **is reducible to** $\boldsymbol{P_1}$ if solving $\boldsymbol{P_1}$ ⇒ solving $\boldsymbol{P_2}$
  - We usually require the "⇒" here is some efficient algorithm

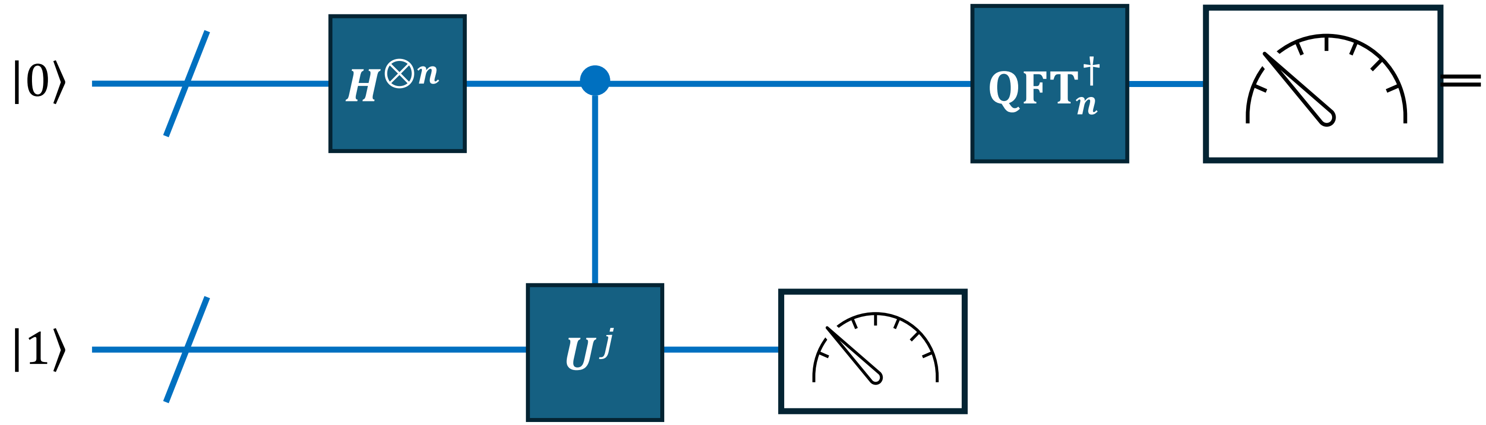
- P_1 **(Order finding) = "**Given N and x, find r (i.e., the minimal r s.t. $x^r = 1\ (mod\ N)$)"
- P_2 **(Factoring) = "**Given $N = pq$, find the two primes p and q"

- 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 $x\ (mod\ N)$, …
  - …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 $U_x\colon |v\rangle \mapsto |v \cdot x \mod N\rangle$



$\approx m \cdot j$

where j is random

and $\frac{m \cdot j}{N} \approx \frac{j}{r}$

Reference

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