

Quantum Computing

- Week 9 (June 9-10, 2026)
- Topics:
 - Quantum Fourier Transformation
 - Phase Estimation

QFT

- Quantum Fourier Transformation

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

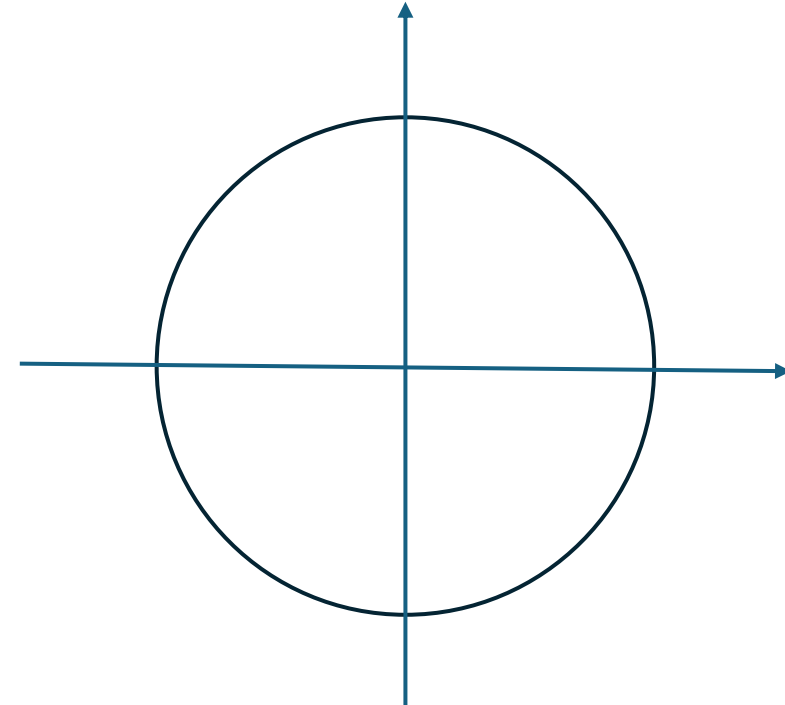
**Quantum Fourier
Transformation**

QFT

- Quantum Fourier Transformation

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

**Quantum Fourier
Transformation**



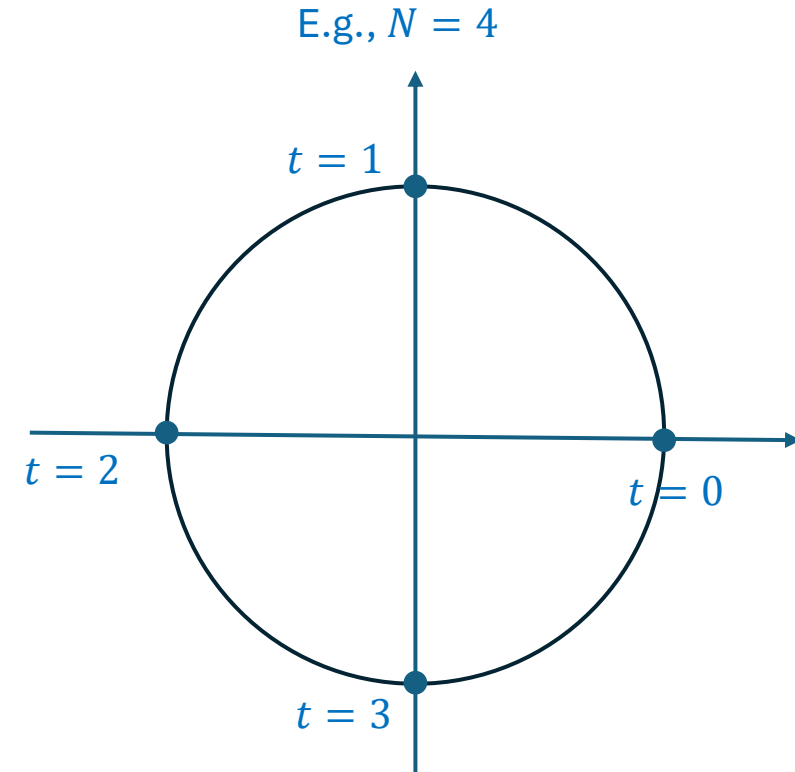
What is $e^{2\pi i(t)/N}$?

QFT

- Quantum Fourier Transformation

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

**Quantum Fourier
Transformation**



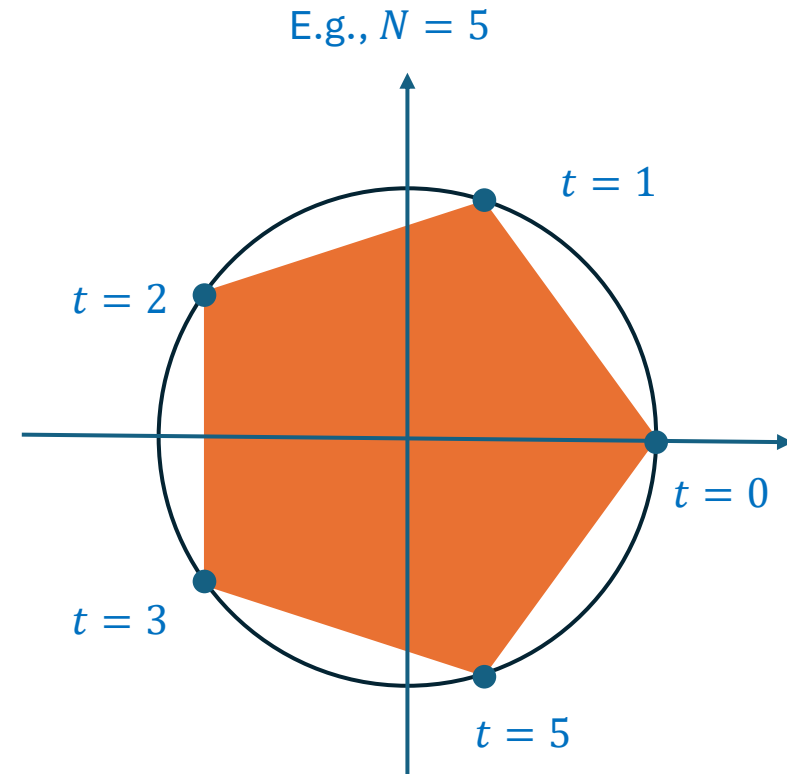
What is $e^{2\pi i(t)/N}$?

QFT

- Quantum Fourier Transformation

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

**Quantum Fourier
Transformation**



What is $e^{2\pi i(t)/N}$?

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

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

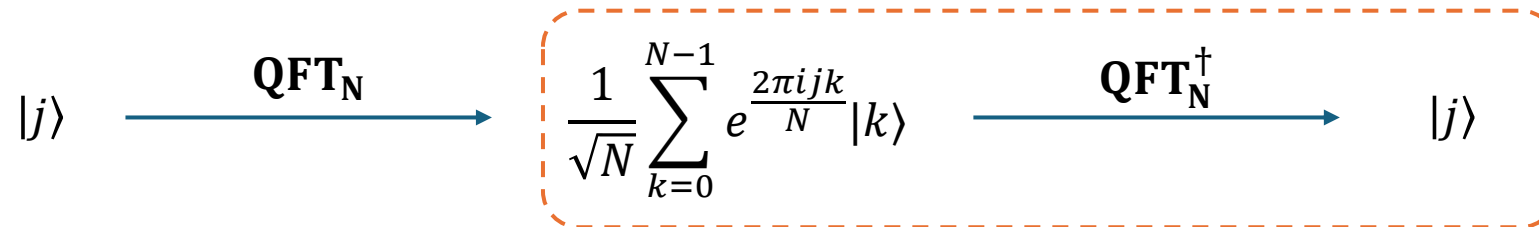
Inverse QFT

- Inverse Quantum Fourier Transformation

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

Inverse QFT

- Another way to understand inverse QFT:



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!

Inverse QFT

- Inverse Quantum Fourier Transformation

$$\text{QFT}_{2^n}^\dagger: \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i k \left(\frac{j}{2^n}\right)} |k\rangle \mapsto |j\rangle$$

Inverse QFT

- Extract j from the phases!
- Let $N = 2^n$, $j \in \{0, 1, 2, \dots, 2^n - 1\}$
- How can we relate $\frac{j}{2^n}$ to $|j\rangle$?

Inverse QFT

- Inverse Quantum Fourier Transformation

$$\text{QFT}_{2^n}^\dagger: \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i k \left(\frac{j}{2^n}\right)} |k\rangle \mapsto |j\rangle$$

Inverse QFT

- Extract j from the phases!
- Let $N = 2^n$, $j \in \{0, 1, 2, \dots, 2^n - 1\}$
- How can we relate $\frac{j}{2^n}$ to $|j\rangle$?
- **Observation:** $j = j_1 \cdot 2^{n-1} + j_2 \cdot 2^{n-2} + \dots + j_{n-1} \cdot 2^1 + j_n \cdot 1$

Inverse QFT

- Inverse Quantum Fourier Transformation

$$\text{QFT}_{2^n}^\dagger: \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i k \left(\frac{j}{2^n}\right)} |k\rangle \mapsto |j\rangle$$

Inverse QFT

- Extract j from the phases!
- Let $N = 2^n$, $j \in \{0, 1, 2, \dots, 2^n - 1\}$
- How can we relate $\frac{j}{2^n}$ to $|j\rangle$?
- **Observation:** $\frac{j}{2^n} = j_1 \cdot 2^{-1} + j_2 \cdot 2^{-2} + \dots + j_{n-1} \cdot 2^{-(n-1)} + j_n \cdot 2^{-n}$

Inverse QFT

- Inverse Quantum Fourier Transformation

$$\text{QFT}_{2^n}^\dagger: \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i k \left(\frac{j}{2^n}\right)} |k\rangle \mapsto |j\rangle$$

Inverse QFT

- $\frac{j}{2^n} = j_1 \cdot 2^{-1} + j_2 \cdot 2^{-2} + \dots + j_{n-1} \cdot 2^{-(n-1)} + j_n \cdot 2^{-n}$
- **Fact:** $e^{2\pi i k \left(a + \frac{j}{2^n}\right)} = e^{2\pi i k \left(\frac{j}{2^n}\right)}$ for any integer $a \geq 1$ (always mod 1 on the exponent)

Inverse QFT

- Inverse Quantum Fourier Transformation

$$\text{QFT}_{2^n}^\dagger: \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i k \left(\frac{j}{2^n}\right)} |k\rangle \mapsto |j\rangle$$

Inverse QFT

- $\frac{j}{2^n} = j_1 \cdot 2^{-1} + j_2 \cdot 2^{-2} + \dots + j_{n-1} \cdot 2^{-(n-1)} + j_n \cdot 2^{-n}$
- Fact: $e^{2\pi i k \left(a + \frac{j}{2^n}\right)} = e^{2\pi i k \left(\frac{j}{2^n}\right)}$ for any integer $a \geq 1$ (always mod 1 on the exponent)
- Let $0.j_1j_2j_3 \dots j_l = j_1 \cdot 2^{-1} + j_2 \cdot 2^{-2} + \dots + j_{l-1} \cdot 2^{-(l-1)} + j_l \cdot 2^{-l}$
- **Fact:** $(0.j_1j_2j_3 \dots j_l) \cdot 2^m = 0.j_{m+1} \dots j_{l-m}$

Inverse QFT

- These notations give us an alternative way to understand (Inverse) QFT...

$$\text{QFT}_n: |j\rangle \mapsto \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i k(0.j_1j_2\dots j_n)} |k\rangle$$

QFT

$$\text{QFT}_n^\dagger: \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i k(0.j_1j_2\dots j_n)} |k\rangle \mapsto |j\rangle$$

Inverse QFT

Inverse QFT

- These notations give us an alternative way to understand (Inverse) QFT...

$$\text{QFT}_n: |j\rangle \mapsto \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i k(0.j_1 j_2 \dots j_n)} |k\rangle$$

QFT

$$\text{QFT}_n^\dagger: \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i k(0.j_1 j_2 \dots j_n)} |k\rangle \mapsto |j\rangle$$

Inverse QFT

- Claim: (Leave as an exercise)

$$\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i k(0.j_1 j_2 \dots j_n)} |k\rangle = \frac{1}{\sqrt{2^n}} \left(\begin{array}{c} (|0\rangle + e^{2\pi i(0.j_n)} |1\rangle) \\ \otimes (|0\rangle + e^{2\pi i(0.j_{n-1}j_n)} |1\rangle) \\ \otimes (|0\rangle + e^{2\pi i(0.j_{n-2}j_{n-1}j_n)} |1\rangle) \\ \vdots \\ \otimes (|0\rangle + e^{2\pi i(0.j_1 j_2 j_3 \dots j_n)} |1\rangle) \end{array} \right)$$

Inverse QFT

- These notations give us an alternative way to understand (Inverse) QFT...

$$\text{QFT}_n: |j\rangle \mapsto \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i k(0.j_1 j_2 \dots j_n)} |k\rangle$$

QFT

$$\text{QFT}_n^\dagger: \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i k(0.j_1 j_2 \dots j_n)} |k\rangle \mapsto |j\rangle$$

Inverse QFT

- Applications: **Phase Estimation**

Phase Estimation

- Let U be a unitary and $|u\rangle$ be an eigenvector of U , i.e., $U|u\rangle = \lambda|u\rangle$, $\lambda \in \mathbb{C}$
- By the normalized condition: $|\lambda| = 1 \Rightarrow \lambda = e^{2\pi i\varphi}$ for some $\varphi \in [0,1)$
- $U|u\rangle = e^{2\pi i\varphi}|u\rangle$
- By the notation introduced before: $U|u\rangle = e^{2\pi i\varphi}|u\rangle = e^{2\pi i(0.\varphi_1\varphi_2\varphi_3\dots)}|u\rangle$

Phase Estimation

- Let U be a unitary and $|u\rangle$ be an eigenvector of U , i.e., $U|u\rangle = \lambda|u\rangle$, $\lambda \in \mathbb{C}$
- By the normalized condition: $|\lambda| = 1 \Rightarrow \lambda = e^{2\pi i\varphi}$ for some $\varphi \in [0,1)$
- $U|u\rangle = e^{2\pi i\varphi}|u\rangle$
- By the notation introduced before: $U|u\rangle = e^{2\pi i\varphi}|u\rangle = e^{2\pi i(0.\varphi_1\varphi_2\varphi_3\dots)}|u\rangle$
- **Goal of Phase Estimation: Compute or Estimate $\varphi = 0.\varphi_1\varphi_2\varphi_3 \dots$**
- What does **estimation** mean? Compute $\varphi' = 0.\varphi_1\varphi_2\varphi_3 \dots \varphi_n$ so that $|\varphi - \varphi'|$ is small

Phase Estimation

- Phase estimation via inverse QFT

$$\mathbf{QFT}_{2^n}^\dagger: \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i k(0.j_1 j_2 \dots j_n)} |k\rangle \mapsto |j\rangle$$

Inverse QFT

- For $U|u\rangle = e^{2\pi i \varphi} |u\rangle = e^{2\pi i(0.\varphi_1 \varphi_2 \varphi_3 \dots)} |u\rangle$, if we have: $\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i k(0.\varphi_1 \varphi_2 \varphi_3 \dots)} |k\rangle$
- Then what is $\mathbf{QFT}_{2^n}^\dagger \left(\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i k(0.\varphi_1 \varphi_2 \varphi_3 \dots)} |k\rangle \right)$?

Phase Estimation

- Phase estimation via inverse QFT
- For $U|u\rangle = e^{2\pi i\varphi}|u\rangle = e^{2\pi i(0.\varphi_1\varphi_2\varphi_3\dots)}|u\rangle$, suppose that we have: $\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi ik(0.\varphi_1\varphi_2\varphi_3\dots)}|k\rangle$
- Then what is $\text{QFT}_{2^n}^\dagger \left(\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi ik(0.\varphi_1\varphi_2\varphi_3\dots)}|k\rangle \right)$?
- **Case 1:** $\varphi = 0.\varphi_1\varphi_2 \dots \varphi_t$ where $t \leq n$

$$\text{QFT}_{2^n}^\dagger \left(\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi ik(0.\varphi_1\varphi_2\dots\varphi_t)}|k\rangle \right) \mapsto |\varphi_1\varphi_2 \dots \varphi_t\varphi_{t+1} \dots \varphi_n\rangle$$

By Inverse QFT ($\varphi_{t+1} \dots \varphi_n = 0 \dots 0$)

Phase Estimation

- Phase estimation via inverse QFT
- For $U|u\rangle = e^{2\pi i\varphi}|u\rangle = e^{2\pi i(0.\varphi_1\varphi_2\varphi_3\dots)}|u\rangle$, suppose that we have: $\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi ik(0.\varphi_1\varphi_2\varphi_3\dots)}|k\rangle$
- Then what is $\text{QFT}_{2^n}^\dagger \left(\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi ik(0.\varphi_1\varphi_2\varphi_3\dots)}|k\rangle \right)$?
- **Case 2:** $\varphi = 0.\varphi_1\varphi_2 \dots \varphi_t$ where $t > n$ or $t \rightarrow \infty$

$$\text{QFT}_{2^n}^\dagger \left(\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi ik(0.\varphi_1\varphi_2\dots\varphi_t)}|k\rangle \right) \mapsto |\varphi'\rangle \mapsto_{\text{measure}} \varphi'_1 \dots \varphi'_n$$

By Inverse QFT

Phase Estimation

- Phase estimation via inverse QFT

- For $U|u\rangle = e^{2\pi i\varphi}|u\rangle = e^{2\pi i(0.\varphi_1\varphi_2\varphi_3\dots)}|u\rangle$, suppose that we have: $\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi ik(0.\varphi_1\varphi_2\varphi_3\dots)}|k\rangle$

- Then what is $\text{QFT}_{2^n}^\dagger \left(\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi ik(0.\varphi_1\varphi_2\varphi_3\dots)}|k\rangle \right)$?

- **Case 2:** $\varphi = 0.\varphi_1\varphi_2 \dots \varphi_t$ where $t > n$ or $t \rightarrow \infty$

$$\text{QFT}_{2^n}^\dagger \left(\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi ik(0.\varphi_1\varphi_2\dots\varphi_t)}|k\rangle \right) \mapsto |\varphi'\rangle \mapsto_{\text{measure}} \varphi'_1 \dots \varphi'_n$$

By Inverse QFT

Theorem (informal):

$$\Pr[|\varphi - \varphi'| \leq 2^{-n+2}] \geq \frac{1}{2},$$

which means that φ' gives a good estimation of φ .

Phase Estimation

- Phase estimation via inverse QFT
- For $U|u\rangle = e^{2\pi i\varphi}|u\rangle = e^{2\pi i(0.\varphi_1\varphi_2\varphi_3\dots)}|u\rangle$.
- Suppose that we have: $\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi ik(0.\varphi_1\varphi_2\varphi_3\dots)}|k\rangle$
- Then what is $\text{QFT}_{2^n}^\dagger \left(\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi ik(0.\varphi_1\varphi_2\varphi_3\dots)}|k\rangle \right)$?

$\text{QFT}_{2^n}^\dagger \left(\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi ik(0.\varphi_1\varphi_2\varphi_3\dots)}|k\rangle \right) \mapsto |\varphi'\rangle,$
where the measurement on $|\varphi'\rangle$ gives a good estimation of φ

Phase Estimation

- inverse QFT for phase estimation



Phase Estimation

- inverse QFT for phase estimation



- How can we generate this state if we have the unitary and the eigenvector:

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

- (Leave as an exercise)

Exercise

- (1) Prove this equality:

$$\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i k (0.j_1 j_2 \dots j_n)} |k\rangle = \frac{1}{\sqrt{2^n}} \left(\begin{array}{c} (|0\rangle + e^{2\pi i (0.j_n)} |1\rangle) \\ \otimes (|0\rangle + e^{2\pi i (0.j_{n-1} j_n)} |1\rangle) \\ \otimes (|0\rangle + e^{2\pi i (0.j_{n-2} j_{n-1} j_n)} |1\rangle) \\ \vdots \\ \otimes (|0\rangle + e^{2\pi i (0.j_1 j_2 j_3 \dots j_n)} |1\rangle) \end{array} \right) = \frac{1}{\sqrt{2^n}} \left(\otimes_{i=1}^n \left(\sum_{k_i=0}^1 e^{2\pi i k_i (0.j_{n-i+1} \dots j_n)} |k_i\rangle \right) \right)$$

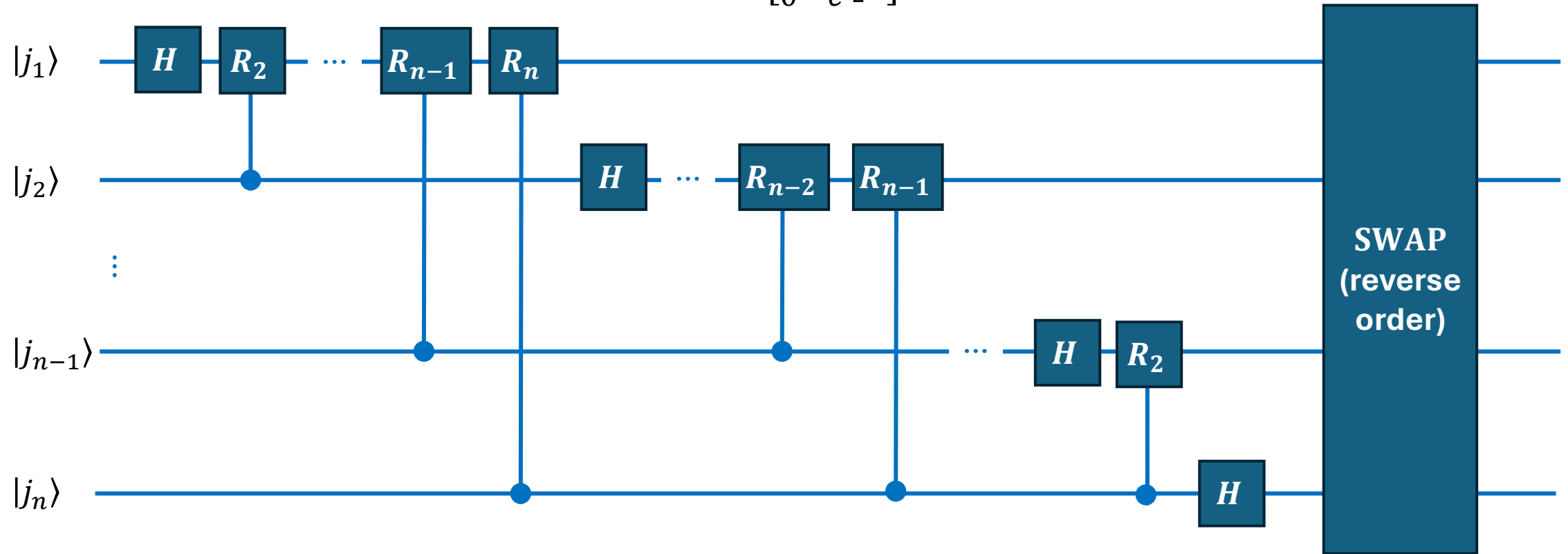
Hint:

- (2) Given U and $|u\rangle$ where $U|u\rangle = e^{2\pi i k \varphi} |u\rangle$. Suppose that $\varphi = 0.\varphi_1 \varphi_2 \dots \varphi_n$. Generate

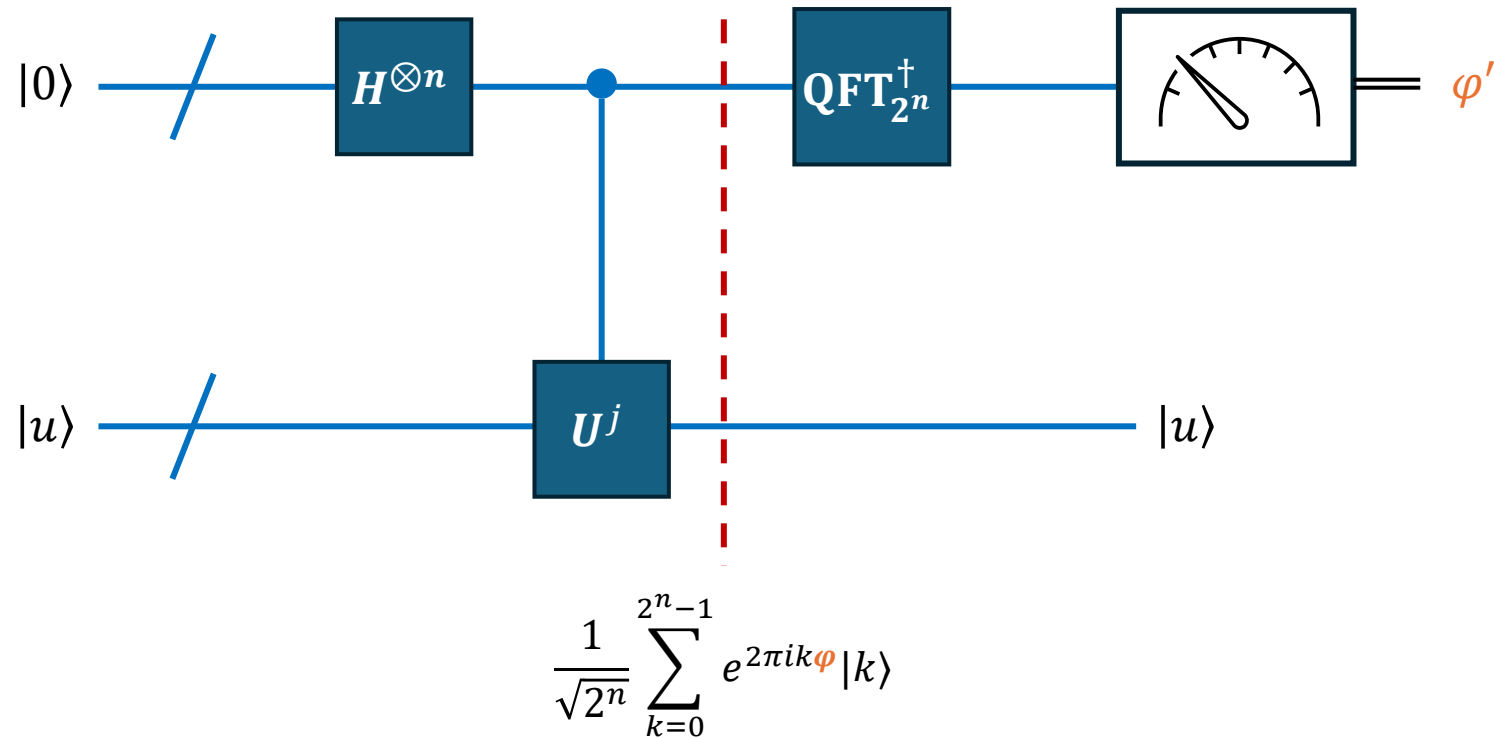
$$\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i k \varphi} |k\rangle \quad (\text{Hint: Use control-}U^j)$$

Summary of QFT and inverse QFT

- Circuit for QFT (and similarly, inverse QFT) $R_k := \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^k}} \end{bmatrix}$



Summary of Phase estimation



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

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
-
- Suppose we have the following state: (Let n be a large enough integer, e.g., $n \approx L + 2$)

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle |f(x)\rangle$$

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
- Suppose we have the following state: (Let n be a large enough integer, e.g., $n \approx L + 2$)

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle |f(x)\rangle$$

- We should have $\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle |f(x)\rangle = \frac{1}{\sqrt{r}} \sum_{l=0}^{r-1} (\dots)$

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
- Suppose we have the following state: (Let n be a large enough integer)

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle |f(x)\rangle$$

- We should have $\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle |f(x)\rangle = \frac{1}{\sqrt{r}} \sum_{l=0}^{r-1} (\dots)$

We need a good basis to express this “periodic state”...

Period Finding

- Suppose that we have a function f with a period r
 - ...and $f(x_1) \neq f(x_2)$ for any distinct $x_1, x_2 \in \{0, \dots, r - 1\}$.
- We define the following Fourier basis $\{|\hat{f}(0)\rangle, |\hat{f}(1)\rangle, \dots, |\hat{f}(r - 1)\rangle\}$, where:

$$|\hat{f}(l)\rangle = \frac{1}{\sqrt{r}} \sum_{x=0}^{r-1} e^{-2\pi i \cdot l \cdot \left(\frac{x}{r}\right)} |f(x)\rangle$$

Period Finding

- Suppose that we have a function f with a period r
 - ...and $f(x_1) \neq f(x_2)$ for any distinct $x_1, x_2 \in \{0, \dots, r-1\}$.
- We define the following Fourier basis $\{|\hat{f}(0)\rangle, |\hat{f}(1)\rangle, \dots, |\hat{f}(r-1)\rangle\}$, where:

$$|\hat{f}(l)\rangle = \frac{1}{\sqrt{r}} \sum_{x=0}^{r-1} e^{-2\pi i \cdot l \cdot \left(\frac{x}{r}\right)} |f(x)\rangle$$

$|\hat{f}(l_1)\rangle$ is always orthogonal to $|\hat{f}(l_2)\rangle$ if $l_1 \neq l_2$

Period Finding

- Suppose that we have a function f with a period r
 - ...and $f(x_1) \neq f(x_2)$ for any distinct $x_1, x_2 \in \{0, \dots, r-1\}$.
- We define the following Fourier basis $\{|\hat{f}(0)\rangle, |\hat{f}(1)\rangle, \dots, |\hat{f}(r-1)\rangle\}$, where:

$$|\hat{f}(l)\rangle = \frac{1}{\sqrt{r}} \sum_{x=0}^{r-1} e^{-2\pi i \cdot l \cdot (\frac{x}{r})} |f(x)\rangle$$

- Then we also have:

$$|f(x)\rangle = \frac{1}{\sqrt{r}} \sum_{l=0}^{r-1} e^{2\pi i \cdot x \cdot (\frac{l}{r})} |\hat{f}(l)\rangle$$

Period Finding

- Suppose that we have a function f with a period r
 - ...and $f(x_1) \neq f(x_2)$ for any distinct $x_1, x_2 \in \{0, \dots, r-1\}$.
- We define the following Fourier basis $\{|\hat{f}(0)\rangle, |\hat{f}(1)\rangle, \dots, |\hat{f}(r-1)\rangle\}$, where: $|\hat{f}(l)\rangle = \frac{1}{\sqrt{r}} \sum_{x=0}^{r-1} e^{-2\pi i \cdot l \cdot (\frac{x}{r})} |f(x)\rangle$
- And we also have: $|f(x)\rangle = \frac{1}{\sqrt{r}} \sum_{l=0}^{r-1} e^{2\pi i \cdot x \cdot (\frac{l}{r})} |\hat{f}(l)\rangle$
- Continue the calculation and apply inverse QFT: $\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle |f(x)\rangle = \dots = \frac{1}{\sqrt{r}} \sum_{l=0}^{r-1} \left| \left(\frac{l}{r} \right)' \right\rangle |\hat{f}(l)\rangle$

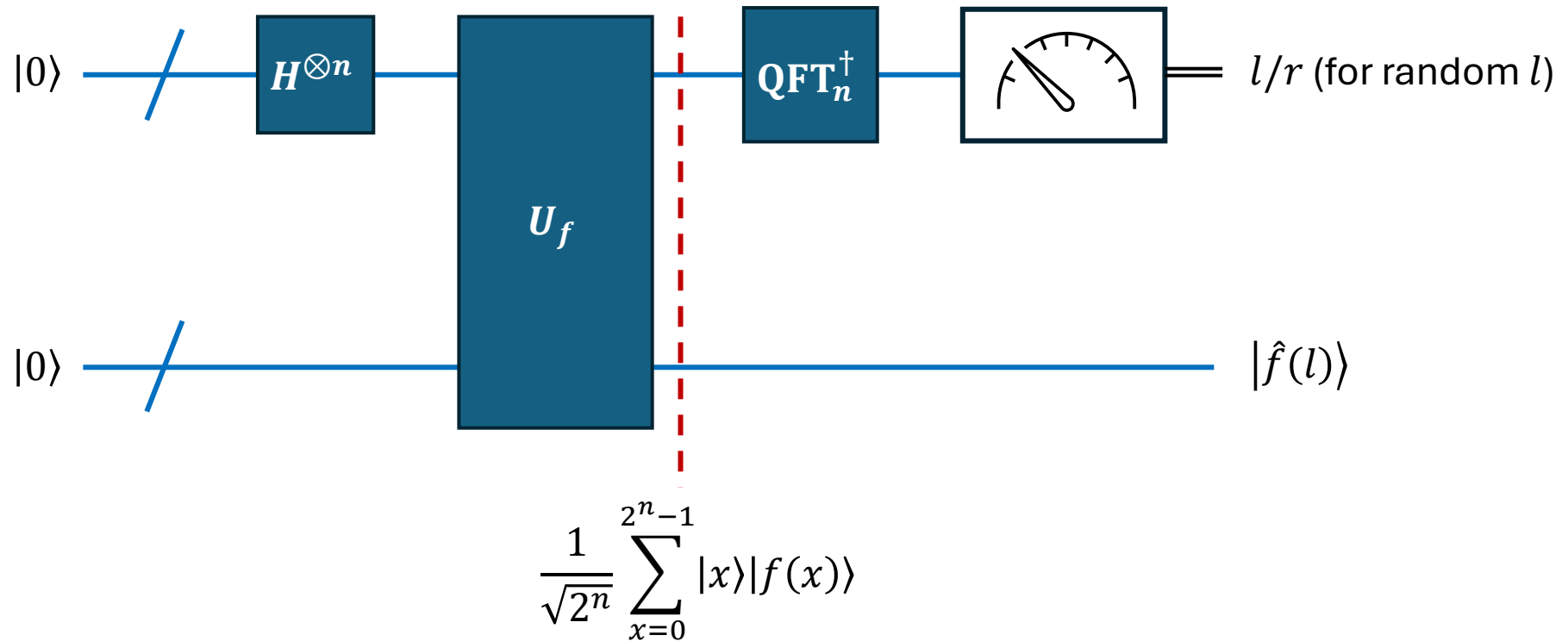
Period Finding

- Suppose that we have a function f with a period r
 - ...and $f(x_1) \neq f(x_2)$ for any distinct $x_1, x_2 \in \{0, \dots, r-1\}$.
- We define the following Fourier basis $\{|\hat{f}(0)\rangle, |\hat{f}(1)\rangle, \dots, |\hat{f}(r-1)\rangle\}$, where: $|\hat{f}(l)\rangle = \frac{1}{\sqrt{r}} \sum_{x=0}^{r-1} e^{-2\pi i \cdot l \cdot \left(\frac{x}{r}\right)} |f(x)\rangle$
- And we also have: $|f(x)\rangle = \frac{1}{\sqrt{r}} \sum_{l=0}^{r-1} e^{2\pi i \cdot x \cdot \left(\frac{l}{r}\right)} |\hat{f}(l)\rangle$
- Continue the calculation and apply inverse QFT: $\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle |f(x)\rangle = \dots = \frac{1}{\sqrt{r}} \sum_{l=0}^{r-1} \left| \left(\frac{l}{r}\right)' \right\rangle |\hat{f}(l)\rangle$
- Measure the first n -qubit system gives us a good estimation of $\left(\frac{l}{r}\right)$
- Apply many times, we get $\left\{ \left(\frac{l_1}{r}\right)', \left(\frac{l_2}{r}\right)', \dots \right\}$ (with different l), which allows us to recover r

Exercise

- Prove $|\hat{f}(l)\rangle = \frac{1}{\sqrt{r}} \sum_{x=0}^{r-1} e^{-2\pi i \cdot l \cdot (\frac{x}{r})} |f(x)\rangle$ forms a basis, and $|f(x)\rangle = \frac{1}{\sqrt{r}} \sum_{l=0}^{r-1} e^{2\pi i \cdot x \cdot (\frac{l}{r})} |\hat{f}(l)\rangle$
 - r is the period of f (Hint: $\sum_{l=0}^{r-1} e^{2\pi i \cdot l \cdot (\frac{a-b}{r})} = r$ if $a = b \pmod{r}$; Otherwise, $= 0$)
 - $f(x_1) \neq f(x_2)$ for distinct $x_1, x_2 \in \{0, \dots, r-1\}$
- How can we create the state $\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle |f(x)\rangle$ if we have U_f ?

Summary of Period Finding

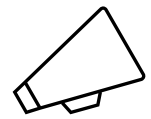


Next Week

- **Factoring**

Reference

- **[NC00]**: Chapter 5
- **[KLM07]**: Chapter 7



No lectures in Week 11 (June 23-24)