Review

"Quantum bits"

$\mathcal{H}_1$: $|\varphi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$, $\alpha_0, \alpha_1 \in \mathbb{C}$, $|\alpha_0|^2 + |\alpha_1|^2 = 1$.

$\mathcal{H}_n$: $|\varphi\rangle = \sum_{\vec{b}\in\{0,1\}^n} \alpha_{\vec{b}} |\vec{b}\rangle$, $\sum_{\vec{b}\in\{0,1\}^n} |\alpha_{\vec{b}}|^2 = 1$. (ex) $|\varphi\rangle = \frac{1}{\sqrt{2}}|00\rangle - \frac{i}{\sqrt{2}}|11\rangle = \frac{1}{\sqrt{2}}|0\rangle_2 - \frac{i}{\sqrt{2}}|3\rangle_2$.

($\alpha_{\vec{b}}$ 가 observe 될 확률)

"Quantum gate" input → [unitary transformation] → output. (ex) Hadamard gate $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, CNOT gate

Ch 6. Shor's algorithm : integer factorization : running time $O((\log N)^3)$

↑ order finding algorithm.

↑ Quantum phase estimation

↑ Quantum Fourier transform (QFT).

(ex/참고) phase shift gate $R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^k}} \end{pmatrix}$ $k \in \mathbb{N}$.

$|\vec{x}\rangle = |x\rangle_n$, $|00\rangle = |0\rangle_2$, $|111\rangle = |7\rangle_3$.

§6.2 QFT

Def $QFT_n : \mathcal{H}_n \to \mathcal{H}_n$, for $|x\rangle_n$, $x \in \mathbb{Z}_{2^n}$,

$$QFT_n |x\rangle_n = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i \frac{x}{2^n} y} |y\rangle_n \in \mathcal{H}_n \quad \because \sum_{y=0}^{2^n-1} \left(\frac{1}{\sqrt{2^n}}\right)^2 \left|e^{2\pi i \frac{x}{2^n} y}\right|^2 = 1$$

$QFT_n = \left(\frac{e^{2\pi i \frac{x}{2^n} y}}{\sqrt{2^n}}\right)_{x,y \in \mathbb{Z}_{2^n}}$

$$QFT_n^{-1} |x\rangle_n = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{-2\pi i \frac{x}{2^n} y} |y\rangle_n \quad \text{(check)}$$

How to express using circuit?

$$|x\rangle_n \longmapsto \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i \frac{x}{2^n} y} |y\rangle_n \qquad |y\rangle_n = |y_1 y_2 \cdots y_n\rangle, \; y = 2^{n-1} y_1 + \cdots + 2^1 y_{n-1} + y_n$$

$$= \frac{1}{\sqrt{2^n}} \sum_{y_1=0}^{1} \cdots \sum_{y_n=0}^{1} e^{2\pi i x \left(\sum_{\ell=1}^{n} y_\ell 2^{-\ell}\right)} |y_1 \cdots y_n\rangle$$

$$= \frac{1}{\sqrt{2^n}} \sum_{y_1=0}^{1} \cdots \sum_{y_n=0}^{1} e^{2\pi i x y_1 2^{-1}} |y_1\rangle \otimes \cdots \otimes e^{2\pi i x y_n 2^{-n}} |y_n\rangle$$

$$= \frac{1}{\sqrt{2^n}} \left(\sum_{y_1=0}^{1} e^{2\pi i x y_1 2^{-1}} |y_1\rangle\right) \otimes \cdots \otimes \left(\sum_{y_n=0}^{1} e^{2\pi i x y_n 2^{-n}} |y_n\rangle\right)$$

$$= \frac{1}{\sqrt{2^n}} \bigotimes_{\ell=1}^{n} \left(\sum_{y_\ell=0}^{1} e^{2\pi i x y_\ell 2^{-\ell}} |y_\ell\rangle\right) = \frac{1}{\sqrt{2^n}} \bigotimes_{\ell=1}^{n} \left(|0\rangle + e^{2\pi i x 2^{-\ell}} |1\rangle\right)$$

$|x\rangle_n = |x_0 x_1 \cdots x_{n-1}\rangle$.

$x = 2^{n-1} x_0 + \cdots + 2^0 x_{n-1}$

$$= \frac{1}{\sqrt{2^n}} \left(|0\rangle + e^{2\pi i \cdot 0.x_{n-1}} |1\rangle\right) \left(|0\rangle + e^{2\pi i \cdot 0.x_{n-2} x_{n-1}} |1\rangle\right) \cdots \left(|0\rangle + e^{2\pi i \cdot 0.x_0 \cdots x_{n-1}} |1\rangle\right)$$

$2\pi i x 2^{-\ell}$

slide

$|x_j\rangle$ — H — $\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i 0.x_j}|1\rangle\right)$ $\left(\because \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right)$

$\frac{1}{\sqrt{2}}|0\rangle + e^{2\pi i \cdot 0.x_j \cdots x_{k-1}}|1\rangle$ — R_{k+1} — $\frac{1}{\sqrt{2}}|0\rangle + e^{2\pi i \cdot 0.x_j \cdots x_k}|1\rangle$

$|x_k\rangle$ — $|x_k\rangle$

$|x_0\rangle$ — H — $\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i 0.x_0}|1\rangle\right)$

$\frac{1}{\sqrt{2}}|0\rangle + e^{2\pi i \cdot 0.x_j}|1\rangle$ — R_{j+1} — $\frac{1}{\sqrt{2}}|0\rangle + e^{2\pi i \cdot 0.x_j x_{j+1}}$

$|x_{j+1}\rangle$ — $|x_{j+1}\rangle$

$\frac{1}{\sqrt{2}}|0\rangle + e^{2\pi i \cdot 0.x_0}|1\rangle$ — R_2 — $\frac{1}{\sqrt{2}}|0\rangle + e^{2\pi i \cdot 0.x_0 x_1}|1\rangle$

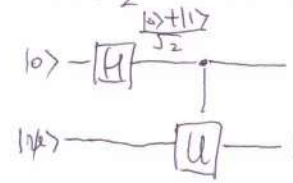
$|x_1\rangle$ — $|x_1\rangle$

§6.3 Quantum phase estimation.

operator U has an eigenvector $|\psi\rangle$ with eigenvalue λ, $|\lambda|=1 \Rightarrow \lambda = e^{2\pi i\omega}$.

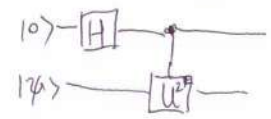
Goal: approximate $\omega \approx \frac{x}{2^n}$, $x \in \mathbb{Z}_{2^n}$. n: precision parameter.

$\omega \in \mathbb{R}$, $\frac{x}{2^n} \in [0,1)$ $\Rightarrow \Delta(\omega, n, x) := \omega - \frac{x}{2^n} - \left[\omega - \frac{x}{2^n}\right]$ (가장 가까운 정수) (*)



$\frac{|0\rangle}{\sqrt{2}} \otimes |\psi\rangle \Rightarrow \frac{|0\rangle}{\sqrt{2}} \otimes |\psi\rangle$

$\frac{|1\rangle}{\sqrt{2}} \otimes |\psi\rangle \Rightarrow \frac{|1\rangle}{\sqrt{2}} \otimes e^{2\pi i\omega}|\psi\rangle = \frac{1}{\sqrt{2}} e^{2\pi i\omega} |1\rangle \otimes |\psi\rangle$ $\Big\} \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\omega}|1\rangle\right) \otimes |\psi\rangle$



$\frac{|0\rangle}{\sqrt{2}} \otimes |\psi\rangle \Rightarrow \frac{|0\rangle}{\sqrt{2}} \otimes |\psi\rangle$

$\frac{|1\rangle}{\sqrt{2}} \otimes |\psi\rangle \Rightarrow \frac{|1\rangle}{\sqrt{2}} \otimes \left(e^{2\pi i\omega}\right)^{2^k} |\psi\rangle = \frac{1}{\sqrt{2}} e^{2\pi i(2^k\omega)} |1\rangle \otimes |\psi\rangle$ $\Big\} \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i(2^k\omega)}|1\rangle\right) \otimes |\psi\rangle$

Do this simultaneously for $k = 0, \cdots, n-1$ & trace out $|\psi\rangle$. $\omega \approx \frac{x}{2^n} = 0.x_0x_1\cdots x_{n-1}$

$$\Rightarrow \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i(2^{n-1}\omega)}|1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i(2^{n-2}\omega)}|1\rangle\right) \otimes \cdots \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i(2^1\omega)}|1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i(2^0\omega)}|1\rangle\right)$$

$$= \frac{1}{\sqrt{2^n}}\left(|0\rangle + e^{2\pi i 0.x_{n-1}}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.x_{n-2}x_{n-1}}|1\rangle\right) \cdots \left(|0\rangle + e^{2\pi i 0.x_0x_1\cdots x_{n-1}}|1\rangle\right)$$

$\xrightarrow{QFT_n^{-1}} |x_0x_1\cdots x_{n-1}\rangle_R = |x\rangle_n$ $\quad \therefore \omega = \frac{x}{2^n}$, $\lambda = e^{2\pi i\omega}$: eigenvalue

(*), $e^{2\pi i(\omega - \frac{x}{2^n})} = e^{2\pi i \Delta(\omega, n, x)}$

Algorithm : $U, |\psi\rangle \Rightarrow QFT_n^{-1}\left(\frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i y\omega}|y\rangle_n\right) = QFT_n^{-1}|\psi_n(\omega)\rangle$

$=: |\psi_n(\omega)\rangle$

$2^n = N$

$$= \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi i\omega y}\, QFT_n^{-1}|y\rangle_n$$

$\Delta := \Delta(\omega, n, x)$

$$= \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi i\omega y} \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} e^{-2\pi i \frac{y}{N}x}|x\rangle_n = \sum_{x=0}^{N-1} \frac{1}{N}\left(\sum_{y=0}^{N-1} e^{2\pi i\Delta y}\right)|x\rangle_n$$

$\Delta = 0 \Rightarrow x = 2^n\omega$, $p(x) = 1$ $\quad |1 - e^{2\pi i\theta}| = |e^{-\pi i\theta} - e^{\pi i\theta}|$

$\Downarrow$ $p(x) = \left|\frac{1}{N}\sum_{y=0}^{N-1} e^{2\pi i\Delta y}\right|^2$

$\Delta \neq 0 \Rightarrow p(x) = \frac{1}{N^2}\left|\frac{1 - e^{2\pi i N\Delta}}{1 - e^{2\pi i\Delta}}\right|^2 = \frac{1}{N^2}\frac{\sin^2(N\pi\Delta)}{\sin^2\pi\Delta}$ $\quad = 2|\sin\pi\theta|$

$= \frac{1}{N^2}\left|\sum_{y=0}^{N-1} e^{2\pi i\Delta y}\right|^2$

Thm 6.3.7

(1) $2^n\omega \in \mathbb{Z} \Rightarrow x = 2^n\omega$ with prob 1.

(2) $|\Delta(\omega, n, x)| \le \frac{1}{2^{n+1}}$ with prob at least $\frac{4}{\pi^2}$

(3) $|\Delta(\omega, n, x)| < \frac{1}{2^n}$ " " $\frac{8}{\pi^2}$.

§6.4 Order finding

Input : $N \in \mathbb{N}$, $a \in \mathbb{Z}_N$, $\gcd(a, N) = 1$ Output : order r of a mod N, $a^r \equiv 1 \bmod N$

Def $c \in \mathbb{Z}$, $\gcd(c, N) = 1$. $U_c : \mathcal{H}_n \to \mathcal{H}_n$ $\quad |x\rangle_n \longmapsto \begin{cases} |cx \bmod N\rangle_n & \text{if } 0 \le x < N \\ |x\rangle_n & \text{if } N \le x < 2^n \end{cases}$

$\Rightarrow$ unitary $\because$ permutation.

Prop 6.4.K

① $\forall k \in \mathbb{Z}, \forall t \in \mathbb{N}$, U_{at} has eigenstate $|u_k\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{-2\pi i \frac{k}{r} s} |a^s \bmod N\rangle_n$

with eigenvalue $e^{2\pi i \frac{tk}{r}}$.

pf) $\mathbb{Z}_r \to \mathbb{Z}_r$, $s \mapsto (s+t) \bmod r$: bijection.

$$U_{at}|u_k\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{-2\pi i \frac{ks}{r}} U_{at} |a^s \bmod N\rangle_n = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{-2\pi i \frac{k}{r} s} |a^{s+t} \bmod N\rangle$$

$$= e^{2\pi i \frac{kt}{r}} \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{-2\pi i \frac{k}{r}(s+t) \bmod r} |a^{(s+t) \bmod r} \bmod N\rangle_n$$

$$= e^{2\pi i \frac{kt}{r}} \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{-2\pi i \frac{k}{r} s} |a^s \bmod N\rangle_n = e^{2\pi i \frac{kt}{r}} |u_k\rangle.$$

② $(|u_0\rangle, \cdots, |u_{r-1}\rangle)$: orthonormal (check)

③ $\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |u_k\rangle = |1\rangle_n$

$$\therefore = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{-2\pi i \frac{ks}{r}} |a^s \bmod N\rangle_n = \frac{1}{r} \sum_s \left(\sum_k e^{-2\pi i \frac{k}{r} s} \right) |a^s \bmod N\rangle_n$$

$s=0 \Rightarrow \frac{1}{r} \sum_{k=0}^{r-1} 1 = 1$, $|a^s \bmod N\rangle_n = |1\rangle_n$ $\quad \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |u_k\rangle$: quantum state

$\therefore$ holds

contains $|u_0\rangle \sim |u_{r-1}\rangle$ ↓ with prob $\frac{1}{r}$

Use order finding using U_a. (Instead eigenvector $|\varphi\rangle$, prepare $|1\rangle_n$)

Thm 6.4.8 Algorithm computes the order r of $a \bmod N$ with prob at least 0.399

running time $O((\log N)^3)$ $\quad \frac{k}{r} \approx \frac{x}{2^n}$

Algorithm $\left| \frac{x_1}{2^n} - \frac{p_1}{q_1} \right| \le \frac{1}{2^n}$ $\quad \frac{p}{q}$: continued fraction —— (**) (pg. 236)

Apply continued fraction on $\frac{x_1}{2^n}$ ⇒ ~~$m_1 = p_1, r_1 = q_1$~~

repeat : $\left| \frac{x_2}{2^n} - \frac{p_2}{q_2} \right| \le \frac{1}{2^n}$ ⇒ ~~$m_2 = p_2, r_2 = q_2$~~

return : $r = \mathrm{lcm}(q_1, q_2)$ — ①

$\frac{k_1}{r} \approx \frac{x_1}{2^n}$, $\frac{k_2}{r} \approx \frac{x_2}{2^n}$

How do we get r?

(**) : $\frac{7}{16} = 0 + \frac{1}{\frac{16}{7}} = 0 + \frac{1}{2 + \frac{2}{7}} = 0 + \frac{1}{2 + \frac{1}{\frac{7}{2}}} = 0 + \frac{1}{2 + \frac{1}{3 + \frac{1}{2}}} \Rightarrow \frac{7}{16} = [0, 2, 3, 2]$

convergent : $0, 0 + \frac{1}{2} = \frac{1}{2}, 0 + \frac{1}{2 + \frac{1}{3}} = \frac{3}{7}$. $\frac{7}{16}$

② Lem 6.4.11 $\frac{k_j}{r} = \frac{m_j}{r_j}$, $j = 1, 2$. $\quad \gcd(k_1, k_2, r) = 1 \Rightarrow r = \mathrm{lcm}(r_1, r_2)$

$(\gcd(r_j, m_j) = 1)$

The Algorithm of Shor

Wook Yoon

Seoul National University
ynwk178@snu.ac.kr

September 16, 2025

Quantum Fourier Transform

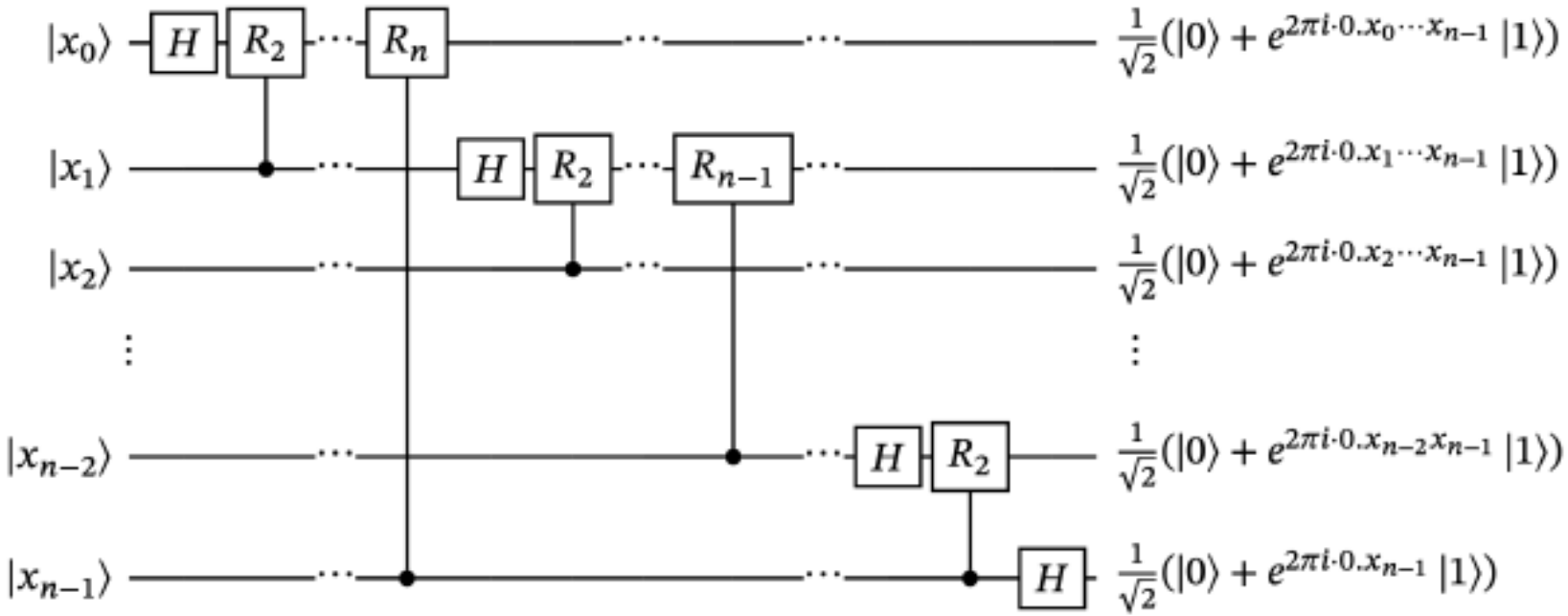


Figure 6.2.1. A quantum circuit that computes QFT_n up to a permutation that reverses the order of the output qubits.

Quantum Fourier Transform

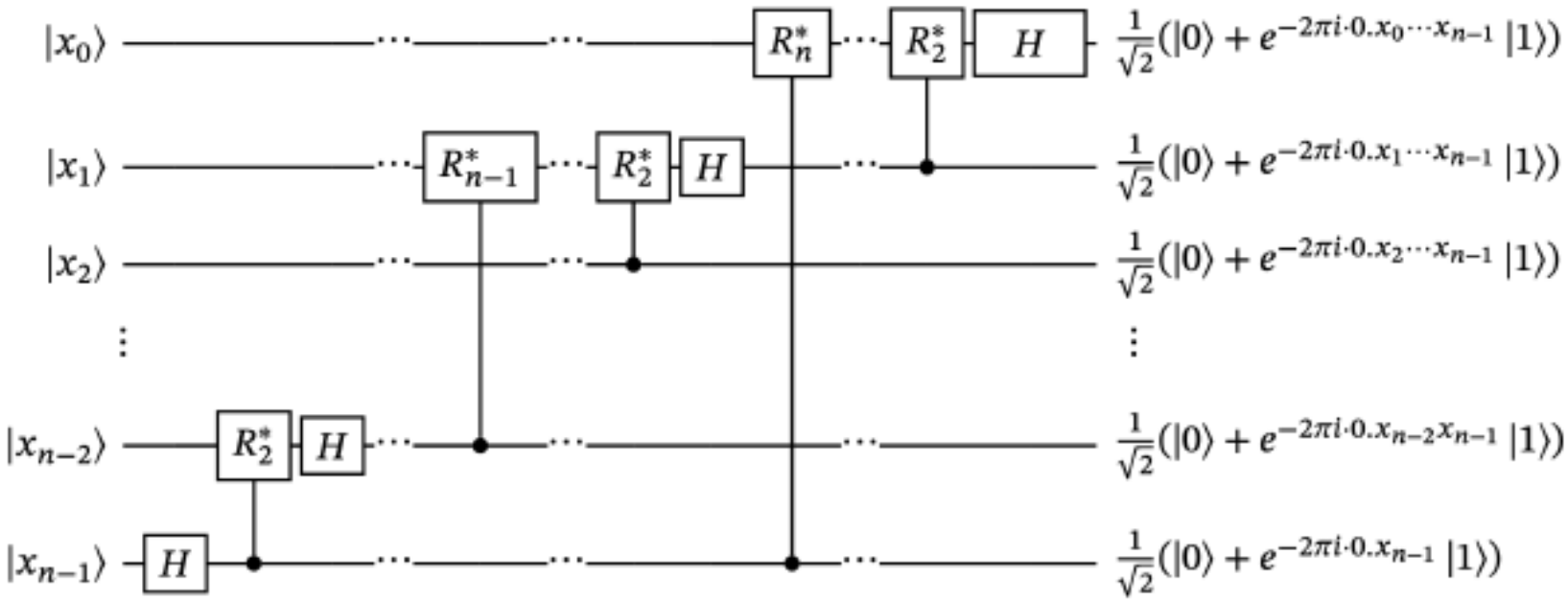


Figure 6.2.4. Quantum circuit that computes QFT_n^{-1} up to a permutation that reverses the order of the output bits.

Quantum Phase Estimation

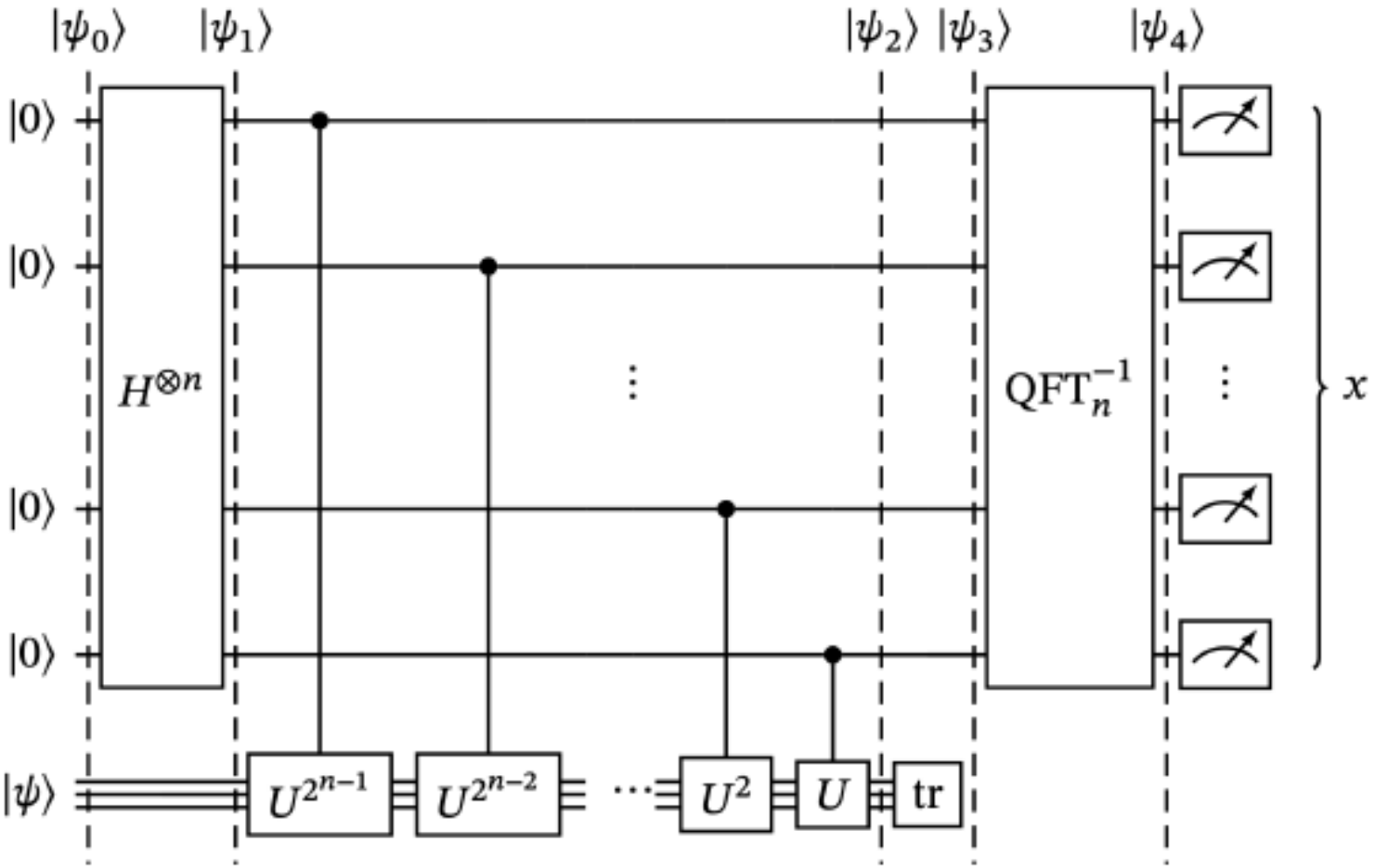


Figure 6.3.1. Quantum circuit for phase estimation.

Order Finding

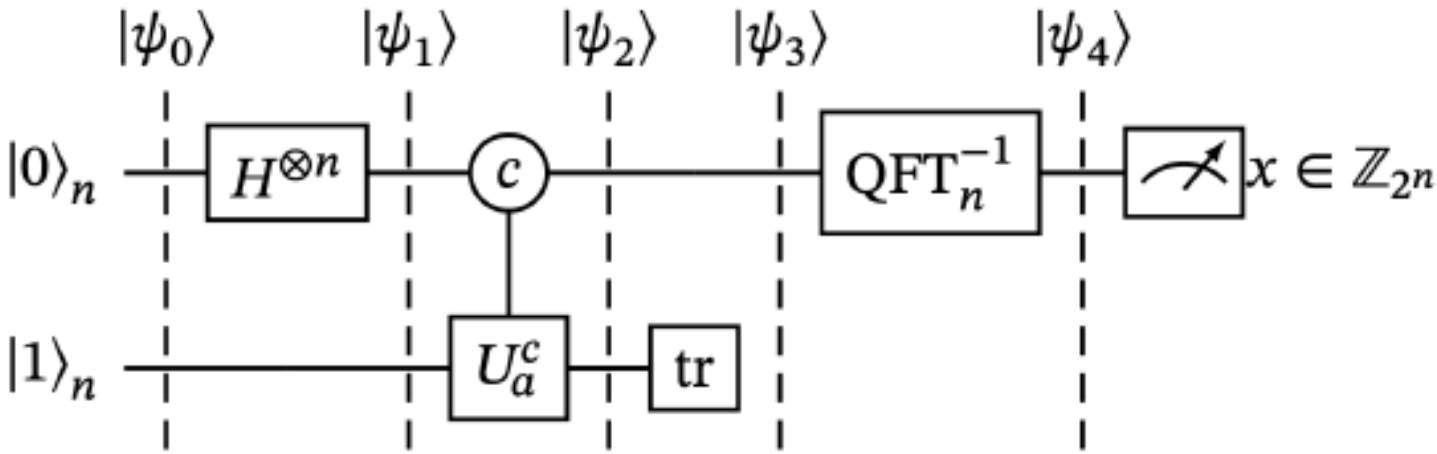


Figure 6.4.1. The modified phase estimation circuit Q_a used in the order finding algorithm.

Thank you for your attention!