EE641000 Quantum Information and Computation

Chung-Chin Lu

Department of Electrical Engineering

National Tsing Hua University

February 21, 2006

Unit Four – Quantum Fourier Transform and Its Applications

Quantum Fourier Transform

Discrete Fourier Transform

- N : a positive integer
- $x_0, x_1, \dots, x_{N-1}$: N complex numbers

$$\boxed{y_k \stackrel{\triangle}{=} \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi ijk/N}}$$

- $y_0, y_1, \dots, y_{N-1}$: the Fourier transform of x_j's
- Discrete Fourier transform : a linear operator on C^N

$$\boldsymbol{e}_j \stackrel{\mathcal{F}}{\mapsto} \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi ijk/N} \boldsymbol{e}_k$$

  – $\{\boldsymbol{e}_0, \boldsymbol{e}_1, \dots, \boldsymbol{e}_{N_1}\}$: standard basis of C^N

Quantum Fourier Transform

- H : the state space of an n-qubit quantum system
- 2^n : the dimension of H
- $\{|j\rangle\}$: an orthonormal basis of H
- Quantum Fourier transform : a linear operator on H

$$|j\rangle \overset{\mathcal{F}}{\longmapsto} \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{2\pi ijk/2^n} |k\rangle$$

  - A unitary operator on H

$$\sum_{k=0}^{2^n-1} \frac{1}{2^{n/2}} e^{2\pi ijk/2^n} \overline{\frac{1}{2^{n/2}} e^{2\pi ij'k/2^n}} = \frac{1}{2^n} \sum_{k=0}^{2^n-1} e^{2\pi i(j-j')k/2^n} = \delta_{jj'}$$

Product Representation

$$|j_1 j_2 \cdots j_n\rangle \stackrel{\mathcal{F}}{\longmapsto} \left(\frac{|0\rangle + e^{2\pi i 0.j_n}|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle + e^{2\pi i 0.j_{n-1}j_n}|1\rangle}{\sqrt{2}}\right)\cdots\left(\frac{|0\rangle + e^{2\pi i 0.j_1 j_2 \cdots j_n}|1\rangle}{\sqrt{2}}\right)$$

- $|j\rangle = |j_1 j_2 \cdots j_n\rangle = |j_1\rangle \otimes |j_2\rangle \otimes \cdots \otimes |j_n\rangle$:
  $j = j_1 2^{n-1} + j_2 2^{n-2} + \cdots + j_n 2^0$ binary representation of j

$$|27\rangle = |11011\rangle$$

- $0.j_l j_{l+1} \cdots j_m = j_l/2 + j_{l+1}/4 + \cdots + j_m/2^{m-l+1}$: binary fraction

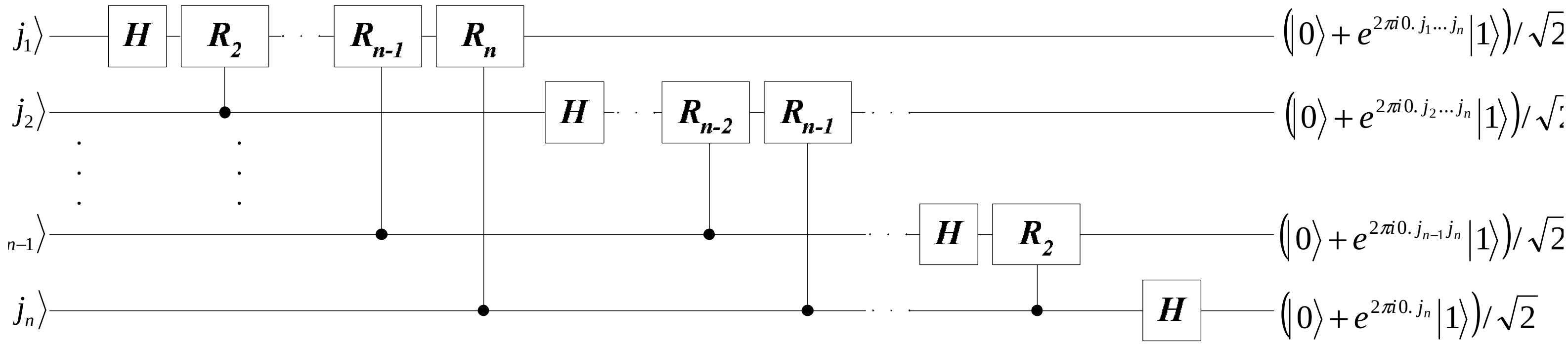
$$0.101 = 1 \cdot 1/2 + 0 \cdot 1/4 + 1 \cdot 1/8 = 5/8 = 20/32$$

Proof

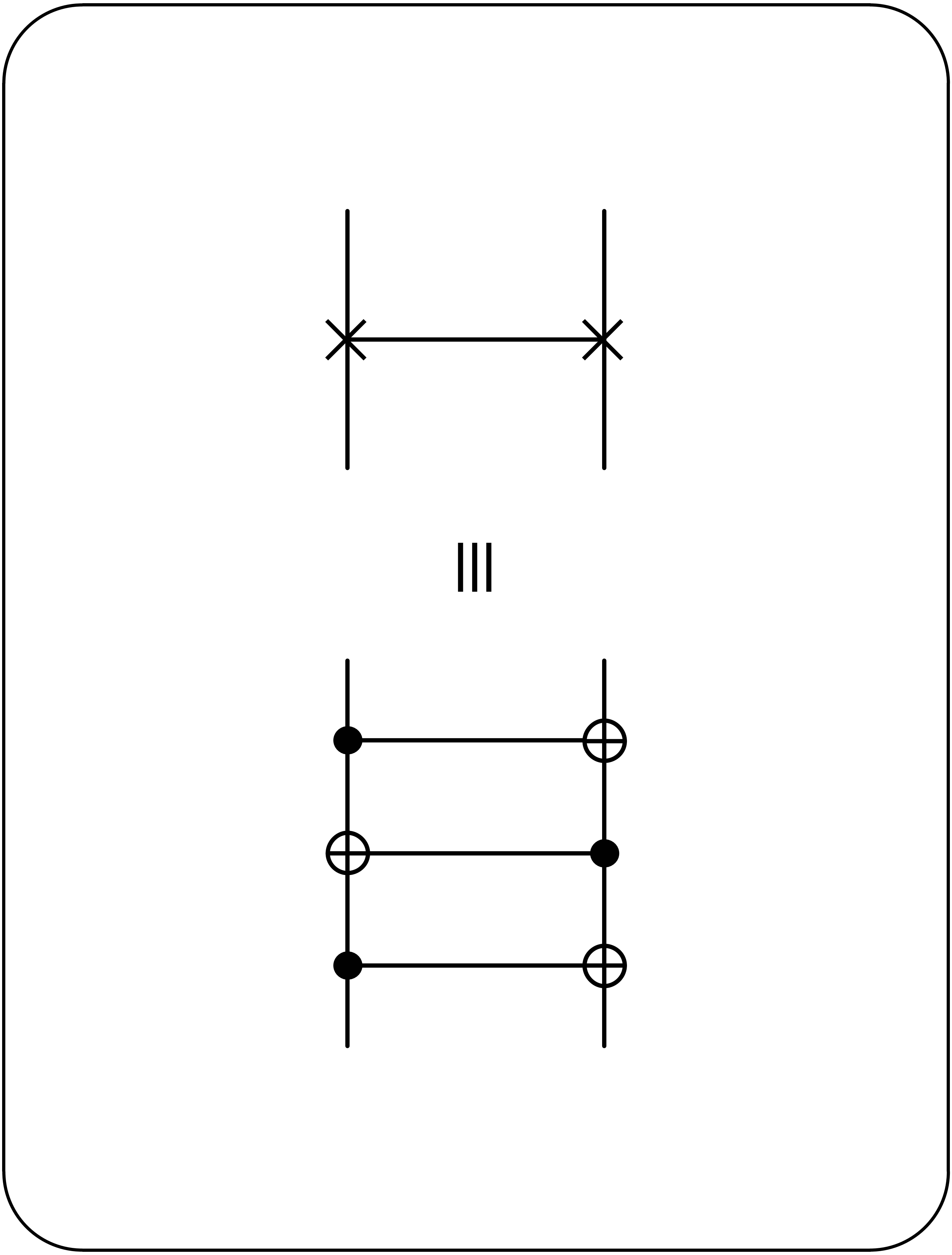
$$
\begin{aligned}
& |j\rangle = |j_1 j_2 \cdot j_n\rangle \\
\overset{\mathcal{F}}{\longmapsto} \quad & \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{2\pi i j k/2^n} |k\rangle \\
= \quad & \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} e^{2\pi i j (\sum_{l=1}^{n} k_l 2^{-l})} |k_1 \cdots k_n\rangle \\
= \quad & \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} \bigotimes_{l=1}^{n} e^{2\pi i j k_l 2^{-l}} |k_l\rangle \\
= \quad & \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \left(\sum_{k_l=0}^{1} e^{2\pi i j k_l 2^{-l}} |k_l\rangle \right) = \bigotimes_{l=1}^{n} \frac{|0\rangle + e^{2\pi i j 2^{-l}} |1\rangle}{\sqrt{2}}
\end{aligned}
$$

$$= \quad \frac{|0\rangle + e^{2\pi i 0.j_n}|1\rangle}{\sqrt{2}} \frac{|0\rangle + e^{2\pi i 0.j_{n-1}j_n}|1\rangle}{\sqrt{2}} \cdots \frac{|0\rangle + e^{2\pi i 0.j_1 j_2 \cdots j_n}|1\rangle}{\sqrt{2}}$$

An Efficient Circuit Implementation



- A swap circuit network is necesarry



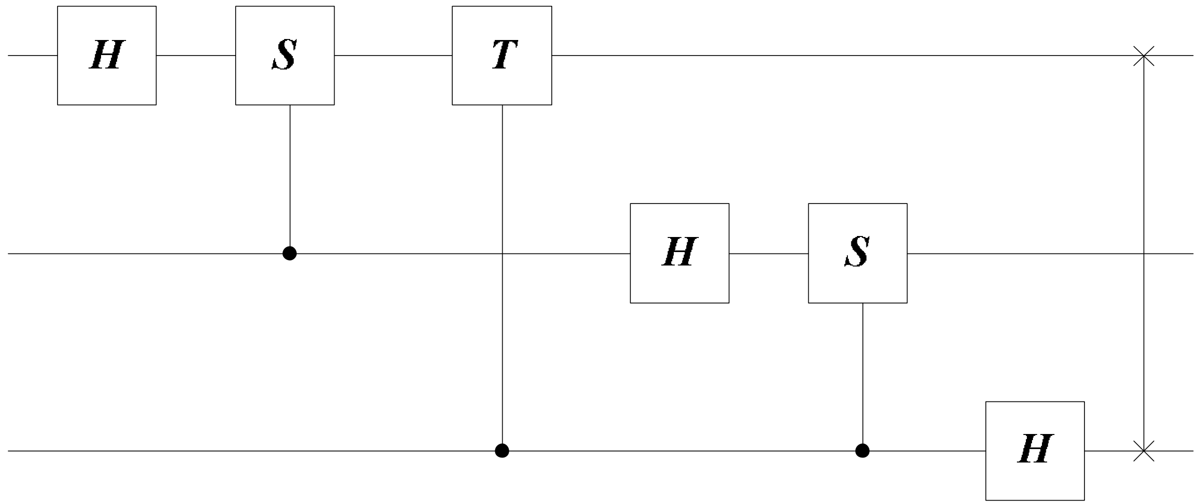
- $|0\rangle \overset{H}{\mapsto} (|0\rangle + |1\rangle)/\sqrt{2}$ and $|1\rangle \overset{H}{\mapsto} (|0\rangle - |1\rangle)/\sqrt{2}$:

$$\boxed{|j_l\rangle \overset{H}{\mapsto} (|0\rangle + e^{2\pi i 0.j_l}|1\rangle)/\sqrt{2}}$$

- $R_l = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i 2^{-l}} \end{bmatrix} = e^{2\pi i 2^{-(l+1)}} R_z(2\pi 2^{-l}) \, : \, 2\pi 2^{-l}$ rotation about z-axis in the Bloch sphere

$$\big|j_1 j_2 \cdots j_n\big\rangle \overset{H}{\mapsto} \frac{|0\rangle + e^{2\pi i 0.j_1}|1\rangle}{\sqrt{2}}\big|j_2 \cdots j_n\big\rangle \overset{C(R_2)}{\mapsto} \frac{|0\rangle + e^{2\pi i 0.j_1 j_2}|1\rangle}{\sqrt{2}}\big|j_2 \cdots j_n\big\rangle$$
$$\overset{C(R_3)}{\mapsto} \cdots \overset{C(R_n)}{\mapsto} \frac{|0\rangle + e^{2\pi i 0.j_1 j_2 \cdots j_n}|1\rangle}{\sqrt{2}}\big|j_2 \cdots j_n\big\rangle$$

A Concrete Example - Three-Qubit



- $S = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i 2^{-2}} \end{bmatrix}$ and $T = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i 2^{-3}} \end{bmatrix}$

Complexity

- n Hadamard gates
- $(n-1)+(n-2)+\cdots+1 = n(n-1)/2$ controlled rotation gates
- $n/2$ swap gates $= 3n/2$ C-NOT gates
- Total complexity of quantum Fourier transform $= O(n^2)$ gates
  - The complexity of classical fast Fourier transform (FFT) $= O(n2^n)$

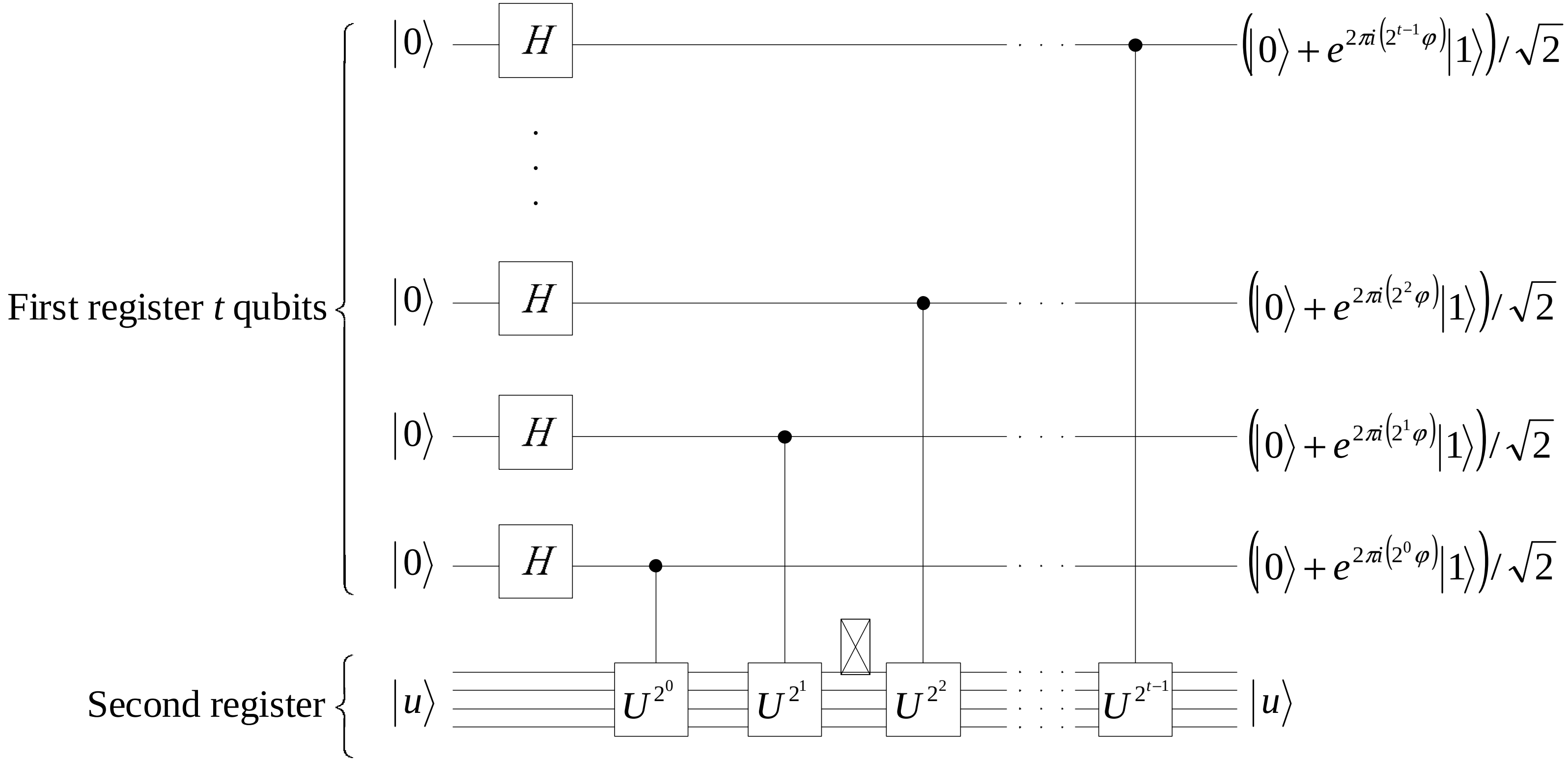
Obstacles in Using Quantum Fourier Transform

- The complex amplitudes cannot be directly accessed by measurement
- No efficient ways to prepare the original state to be Fourier transformed

Quantum Phase Estimation

Phase Estimation - First Stage

- $|u\rangle$ and $e^{2\pi i\varphi}$: an eigenvector and the associated eigenvalue of a unitary operator U on an m-qubit system
  - φ : a quantity in $[0, 1)$ to be estimated
  - $|u\rangle$: assumed be prepared by some black box
- Two registers are used
  - The 1st register : t qubits initially in the state $|0\rangle$ and the number t is dependent on
    - The number of digits of accuracy we want in the estimate for φ
    - The probability with which we want the phase estimation procedure to be successful
  - The 2nd register : m qubits initially prepared in the state $|u\rangle$


First register t qubits
Second register
$|0\rangle$
$|u\rangle$
H
U^{2^0}
U^{2^1}
U^{2^2}
$U^{2^{t-1}}$
$\left(|0\rangle + e^{2\pi i\left(2^{t-1}\varphi\right)}|1\rangle\right)/\sqrt{2}$
$\left(|0\rangle + e^{2\pi i\left(2^{2}\varphi\right)}|1\rangle\right)/\sqrt{2}$
$\left(|0\rangle + e^{2\pi i\left(2^{1}\varphi\right)}|1\rangle\right)/\sqrt{2}$
$\left(|0\rangle + e^{2\pi i\left(2^{0}\varphi\right)}|1\rangle\right)/\sqrt{2}$
$|u\rangle$

- Output state of the 1st register :

$$\frac{|0\rangle + e^{2\pi i 2^{t-1}\varphi}|1\rangle}{\sqrt{2}} \frac{|0\rangle + e^{2\pi i 2^{t-2}\varphi}|1\rangle}{\sqrt{2}} \cdots \frac{|0\rangle + e^{2\pi i 2^{0}\varphi}|1\rangle}{\sqrt{2}}$$

$$= \quad \frac{1}{2^{t/2}} \sum_{k=0}^{2^t-1} e^{2\pi i k\varphi}|k\rangle$$

  – When $\varphi = 0.b_1 b_2 \cdots b_t$, we have the output state

$$\frac{|0\rangle + e^{2\pi i 0.b_t}|1\rangle}{\sqrt{2}} \frac{|0\rangle + e^{2\pi i 0.b_{t-1}b_t}|1\rangle}{\sqrt{2}} \cdots \frac{|0\rangle + e^{2\pi i 0.b_1 b_2 \cdots b_t}|1\rangle}{\sqrt{2}}$$

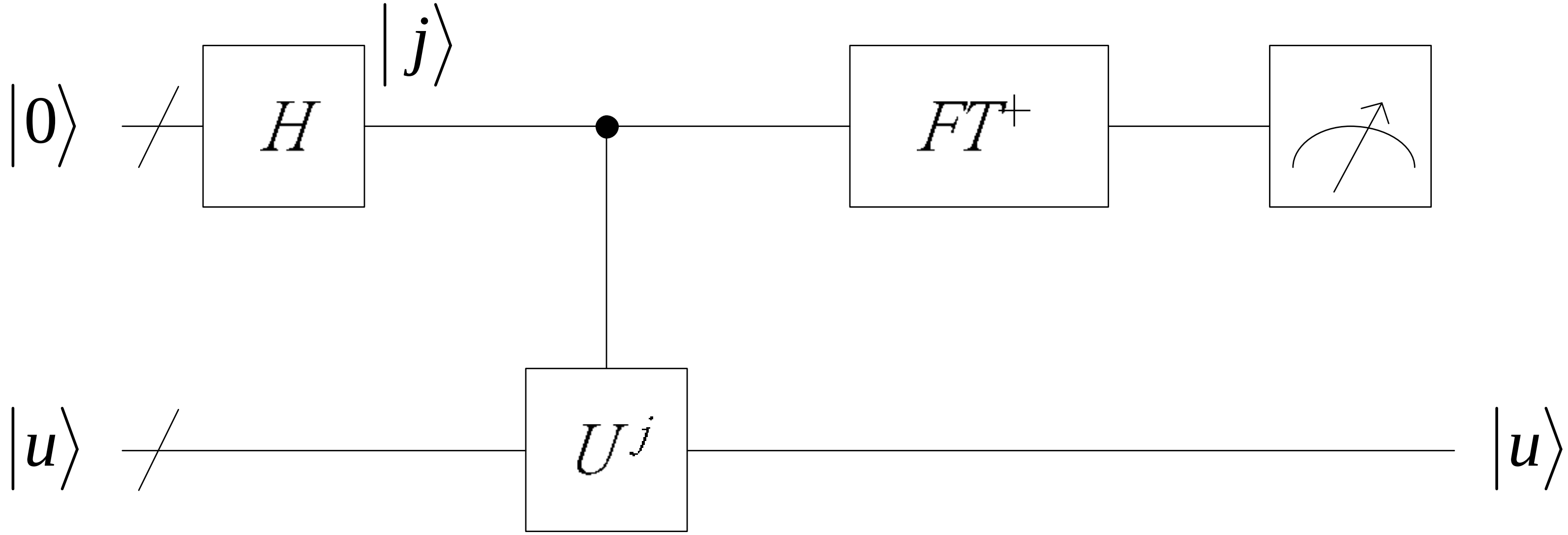
  which is the Fourier transform of the state $|b_1 b_2 \cdots b_t\rangle$

Proof

$$
\begin{array}{ll}
 & |0\rangle \otimes \cdots \otimes |0\rangle \otimes |0\rangle \otimes |u\rangle \\
\xrightarrow{\otimes^t H} & H|0\rangle \otimes \cdots \otimes H|0\rangle \otimes \dfrac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |u\rangle \\
\xrightarrow{C_t(U^{2^0})} & H|0\rangle \otimes \cdots \otimes \dfrac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \dfrac{|0\rangle + e^{2\pi i 2^0 \varphi}|1\rangle}{\sqrt{2}} \otimes |u\rangle \\
\xrightarrow{C_{t-1}(U^{2^1})} & H|0\rangle \otimes \cdots \otimes \dfrac{|0\rangle + e^{2\pi i 2^1 \varphi}|1\rangle}{\sqrt{2}} \otimes \dfrac{|0\rangle + e^{2\pi i 2^0 \varphi}|1\rangle}{\sqrt{2}} \otimes |u\rangle \\
\vdots & \\
\xrightarrow{C_1(U^{2^{(t-1)}})} & \dfrac{|0\rangle + e^{2\pi i 2^{t-1} \varphi}|1\rangle}{\sqrt{2}} \otimes \cdots \otimes \dfrac{|0\rangle + e^{2\pi i 2^1 \varphi}|1\rangle}{\sqrt{2}} \otimes
\end{array}
$$

$$\frac{|0\rangle + e^{2\pi i 2^0 \varphi}|1\rangle}{\sqrt{2}} \otimes |u\rangle$$

Phase Estimation - Second Stage



- Apply inverse Fourier transform $\mathcal{F}^{-1}$ on the t qubits in the 1st register

- Output state of the 1st register at the 2nd stage after $\mathcal{F}^{-1}$:
  - When $\varphi = 0.b_1 b_2 \cdots b_t$, we let $b = \varphi 2^t = b_1 2^{t-1} + b_2 2^{t-2} + \cdots + b_t 2^0$ and the output state is

$$\begin{aligned}
&\mathcal{F}^{-1}\left(\frac{1}{2^{t/2}}\sum_{k=0}^{2^t-1} e^{2\pi i k\varphi}|k\rangle\right) \\
&= \frac{1}{2^{t/2}}\sum_{k=0}^{2^t-1} e^{\frac{2\pi i k b}{2^t}} \frac{1}{2^{t/2}}\sum_{j=0}^{2^t-1} e^{\frac{-2\pi i j k}{2^t}} |j\rangle \\
&= \frac{1}{2^t}\sum_{j=0}^{2^t-1}\sum_{k=0}^{2^t-1} e^{\frac{2\pi i k(b-j)}{2^t}} |j\rangle = |b\rangle = |b_1 b_2 \cdots b_t\rangle
\end{aligned}$$

  - When $\varphi = b2^{-t} + \delta$ with integer b, $0 \le b \le 2^t - 1$, and $0 < \delta < 2^{-t}$, the output state $|\tilde{\varphi}\rangle$ is

$$|\tilde{\varphi}\rangle = \mathcal{F}^{-1}\left(\frac{1}{2^{t/2}}\sum_{k=0}^{2^t-1} e^{2\pi i k\varphi}|k\rangle\right)$$

$$= \quad \frac{1}{2^{t/2}}\sum_{k=0}^{2^t-1} e^{2\pi i k\varphi}\frac{1}{2^{t/2}}\sum_{j=0}^{2^t-1} e^{\frac{-2\pi i jk}{2^t}}|j\rangle = \frac{1}{2^t}\sum_{j=0}^{2^t-1}\sum_{k=0}^{2^t-1} e^{2\pi i k(\varphi-\frac{j}{2^t})}|j\rangle$$

$$= \quad \sum_{j=0}^{2^t-1}\frac{1}{2^t}\frac{1-e^{2\pi i(\varphi 2^t-j)}}{1-e^{2\pi i(\varphi-j2^{-t})}}|j\rangle = \sum_{j=0}^{2^t-1}\frac{1}{2^t}\frac{1-e^{2\pi i(\varphi 2^t-(b+j))}}{1-e^{2\pi i(\varphi-(b+j)2^{-t})}}|b+j\rangle$$

$$= \quad \sum_{j=0}^{2^t-1}\frac{1}{2^t}\frac{1-e^{2\pi i(\delta 2^t-j)}}{1-e^{2\pi i(\delta-j2^{-t})}}|b+j\rangle = \sum_{j=-2^{t-1}+1}^{2^{t-1}}\frac{1}{2^t}\frac{1-e^{2\pi i(\delta 2^t-j)}}{1-e^{2\pi i(\delta-j2^{-t})}}|b+j\rangle$$

where $|b+j\rangle = |b+j(\mathrm{mod}\ 2^t)\rangle$

- Apply projective measurement in the computational basis
  - When $\varphi = 0.b_1 b_2 \cdots b_t$, the result m of the measurement is $b = b_1 2^{t-1} + b_2 2^{t-2} + \cdots + b_t 2^0$ with probability one
  - When $\varphi = b2^{-t} + \delta$ with integer b, $0 \le b \le 2^t - 1$, and $0 < \delta < 2^{-t}$, the probability that the result m of the measurement is $(b + j)(\bmod 2^t)$, $-(2^{t-1} - 1) \le j \le 2^{t-1}$ is

$$|\langle b{+}j(\bmod 2^t)|\tilde{\varphi}\rangle|^2 = \frac{1}{2^{2t}} \frac{|1 - e^{2\pi i(\delta 2^t - j)}|^2}{|1 - e^{2\pi i(\delta - \frac{j}{2^t})}|^2} \le \frac{1}{2^{2(t+1)}(\delta - \frac{j}{2^t})^2}$$

    - $|1 - e^{i\theta}| \le 2$
    - $|1 - e^{i\theta}| = 2|\sin\theta/2| \ge 2|\theta|/\pi$ for all $-\pi \le \theta \le \pi$
    - $-\pi \le 2\pi(\delta - j2^{-t}) \le \pi$ when $-(2^{t-1} - 1) \le j \le 2^{t-1}$

Thus the probability that the measurement result m is $|m-b|>e$ for some positive integer e as the desired tolerance to error is

$$
\begin{aligned}
& \mathcal{P}(|m-b|>e) \\
= \quad & \frac{1}{4}\left(\sum_{j=-2^{t-1}+1}^{-(e+1)} \frac{1}{(j-\delta 2^t)^2} + \sum_{j=e+1}^{2^{t-1}} \frac{1}{(j-\delta 2^t)^2}\right) \\
\leq \quad & \frac{1}{4}\left(\sum_{j=-2^{t-1}+1}^{-(e+1)} \frac{1}{j^2} + \sum_{j=e+1}^{2^{t-1}} \frac{1}{(j-1)^2}\right) \leq \frac{1}{2}\sum_{j=e}^{2^{t-1}-1} \frac{1}{j^2} \\
\leq \quad & \frac{1}{2}\int_{e-1}^{2^{t-1}-1} \frac{1}{x^2}dx \leq \frac{1}{2}\int_{e-1}^{\infty} \frac{1}{x^2}dx \\
= \quad & \frac{1}{2(e-1)}
\end{aligned}
$$

25

The Selection of the Value of t

- Approximating φ to an accuracy $2^{-n} \Rightarrow e = 2^{t-n} - 1$

$$
\begin{aligned}
& |m - b| \le e = 2^{t-n} - 1 \\
\Rightarrow \quad & |\varphi - m2^{-t}| = |\delta + (b-m)2^{-t}| \le \delta + (2^{t-n} - 1)2^{-t} \le 2^{-n}
\end{aligned}
$$

- $p = t - n$: determining the probability that the measurement result assures this accuracy, which is lower-bounded by

$$1 - \frac{1}{2(2^p - 2)} \stackrel{\triangle}{=} 1 - \epsilon$$

$$\boxed{t = n + p = n + \lceil \log_2 \left(2 + \tfrac{1}{2\epsilon}\right) \rceil}$$

- $\epsilon = 10^{-2} \Rightarrow p = 6$; $\epsilon = 10^{-3} \Rightarrow p = 9$; $\epsilon = 10^{-4} \Rightarrow p = 13$

What If An Eigenstate Cannot Be Prepared for U ?

- $|\psi\rangle = \sum_u c_u |u\rangle$: a generic state expanded by an eigenbasis $\{|u\rangle\}$ of the unitary operator U
- $e^{2\pi i \varphi_u}$: eigenvalue associated with eigenstate $|u\rangle$
- $|\eta\rangle = \sum_u c_u |\tilde{\varphi}_u\rangle |u\rangle$: output state of the composite quantum system after running the phase estimation algorithm
- $\rho^{12} = |\eta\rangle\langle\eta|$: density operator of the composite system
- $\rho^1 = \mathrm{tr}_2(\rho^{12})$: density operator of the 1st register

$$\rho^1 = \sum_u \sum_{u'} c_u \overline{c_{u'}} |\tilde{\varphi}_u\rangle\langle\tilde{\varphi}_{u'}| \; \mathrm{tr}(|u\rangle\langle u'|) = \sum_u |c_u|^2 |\tilde{\varphi}_u\rangle\langle\tilde{\varphi}_u|$$

- $\{|m\rangle\langle m|\}$: projective measurement with computational basis $\{|m\rangle\}$
- $\mathcal{P}(m,u)$: the probability that the state of the 1st register is $|\tilde{\varphi}_u\rangle$ and the result m occurs

$$\mathcal{P}(m,u) = \mathcal{P}(u)\mathcal{P}(m|u) = |c_u|^2 \,\mathrm{tr}(|m\rangle\langle m|\tilde{\varphi}_u\rangle\langle\tilde{\varphi}_u|) = |c_u|^2|\langle m|\tilde{\varphi}_u\rangle|^2$$

- If $t = n + \lceil \log_2 \left(2 + \frac{1}{2\epsilon}\right) \rceil$ is selected, the probability for measuring φ_u accurate to n bits by the phase estimation algorithm is at least $|c_u|^2(1-\epsilon)$

Modular Arithmetic

The Ring of Integers Modulo N

- N : a positive integer
- $Z_N = \{0, 1, \ldots, N-1\}$: the ring of integers modulo N
  - Modular addition : $x, y \in Z_N$, $x + y \stackrel{\triangle}{=} (x + y) \pmod{N}$
    - * Associative : $(x + y) + z = x + (y + z)$
    - * Additive identity : $0 + x = x + 0 = x$
    - * Additive inverse : $x + (N - x) = 0$
    - * Commutative : $x + y = y + x$
  - Modular multiplication : $x, y \in Z_N$, $xy \stackrel{\triangle}{=} (xy) \pmod{N}$
    - * Associative : $(xy)z = x(yz)$
    - * Distributive : $(x + y)z = (xz) + (yz)$ and $x(y + z) = (xy) + (xz)$
    - * Multiplicative identity : $1x = x1 = x$
    - * Commutative : $xy = yx$

- Multiplicative inverse : $x \in Z_N$ is said to have a (multiplicative) inverse if there exists a $y \in Z_N$ such that $xy = 1$, i.e., $xy \equiv 1 \pmod{N}$
  - Example : 5 has an inverse in Z_6 but 3 does not
  - $x \in Z_N$ has an inverse x^{-1} if and only if $(x, N) = 1$
- $Z_N^* = \{x \in Z_N | x^{-1} \text{ exists}\}$: the group of invertible elements in Z_N
  - Closure : if $x, y \in Z_N^*$, then $xy \in Z_N^*$
  - Associative : $(xy)z = x(yz)$
  - Multiplicative identity : $1 \in Z_N^*$ and $1x = x1 = x$
  - Multiplicative inverse : $xx^{-1} = 1$
  - Commutative : $xy = yx$
- p : a prime number
  - $Z_p^* = Z_p \backslash \{0\}$ and then Z_p is a field

The Euler φ Function

- $\varphi(N) = |Z_N^*|$: the Euler φ function
- Properties :
  - If $N = p^k$ then $\varphi(p_k) = p^k - p^{k-1} = p^{k-1}(p-1)$
  - If $(M, N) = 1$, then $\varphi(MN) = \varphi(M)\varphi(N)$
    * Each element in Z_{MN} can be uniquely represented as $i + jM$ with $0 \leq i \leq M-1$ and $0 \leq j \leq N-1$
    * If $(i, M) > 1$ then $(i + jM, M) > 1$ and then $(i + jM, MN) > 1$ for all j
    * For a fixed i, $(i, M) = 1$, if $i + jM = i + j'M \pmod{N}$, then $(j - j')M = 0 \pmod{N}$ and then $j = j'$. Thus $Z_N = \{i + jM \pmod{N}, 0 \leq j \leq N-1\}$ and there are exactly $\varphi(N)$ of $i + jM$, $0 \leq j \leq N-1$, which are co-prime with N and with M respectively

- If $N = \Pi_i p_i^{k_i}$ is the prime factorization of N, then $\varphi(N) = \Pi_i p_i^{k_i-1}(p_i - 1)$
- Examples :

$$\begin{aligned}
\varphi(7) &= 6, \\
\varphi(27) &= 9(3-1) = 18 \\
\varphi(21) &= \varphi(3)\varphi(7) = 2 \cdot 6 = 12 \\
\varphi(1800) &= \varphi(2^3)\varphi(3^2)\varphi(5^2) = 2^2(2-1)3(3-1)5(5-1) = 480
\end{aligned}$$

Fermat's Little Theorem

- $x \in Z_N^*$

$$\boxed{x^{\varphi(N)} \equiv 1 \pmod{N}}$$

- Since $x \in Z_N^*$, the mapping $y \mapsto xy \pmod{N}$ is a permutation on Z_N^*, Thus we have $\{xy \pmod{N} | y \in Z_N^*\} = Z_N^*$ and then

$$\begin{aligned} & \Pi_{y \in Z_N^*} xy \equiv \Pi_{y \in Z_N^*} y \pmod{N} \\ \Rightarrow \quad & x^{\varphi(N)} \Pi_{y \in Z_N^*} y \equiv \Pi_{y \in Z_N^*} y \pmod{N} \\ \Rightarrow \quad & x^{\varphi(N)} \equiv 1 \pmod{N} \end{aligned}$$

The order of x modulo N

- x, N : relatively prime positive integers with $x < N$
- $o_N(x)$: the order of x modulo N, which is the least positive integer r such that

$$x^r \equiv 1 \pmod{N}$$

- Example : $o_{21}(5) = 6$

$$5^1 \equiv 5 \pmod{21},\ 5^2 \equiv 4 \pmod{21},\ 5^3 \equiv 20 \pmod{21},$$
$$5^4 \equiv 16 \pmod{21},\ 5^5 \equiv 17 \pmod{21},\ 5^6 \equiv 1 \pmod{21}$$

- $o_N(x) | \varphi(N)$

Quantum Order-Finding Algorithm

A Unitary Operator for Finding $o_N(x)$

- x, N : relatively prime positive integers with $x < N$
- $L = \lceil \log_2 N \rceil$: the minimum number of bits to represent N
- H : the state space of an L-qubit quantum system
- $\{|y\rangle, 0 \le y \le 2^L - 1\}$: a computational basis of H
- $U_{x,N}$: a unitary operator on H such that

$$U_{x,N}|y\rangle \triangleq \begin{cases} |xy \pmod N\rangle, & \text{if } 0 \le y \le N-1, \\ |y\rangle, & \text{if } N \le y \le 2^L - 1. \end{cases}$$

  – Since $x \in Z_N^*$, the mapping $\pi : y \mapsto xy \pmod N$ is a permutation on Z_N.

Special Eigenvalues and Eigenstates of $U_{x,N}$

- $r = o_N(x)$: the order of x modulo N
- $e^{(2\pi is)/r}$, $0 \leq s \leq r-1$: eigenvalues of $U_{x,N}$ associated with eigenstates $|u_s\rangle$

$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{\frac{-2\pi isk}{r}} |x^k \pmod N\rangle$$

$$U_{x,N}|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{\frac{-2\pi isk}{r}} |x^{k+1} \pmod N\rangle = e^{\frac{2\pi is}{r}} |u_s\rangle$$

- $|u_s\rangle$, $0 \leq s \leq r-1$: inverse Fourier transform of $|x^k (\mathrm{mod}\ N)\rangle$, $0 \leq k \leq r-1$, and then

$$|x^k \pmod N\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{\frac{2\pi isk}{r}} |u_s\rangle$$

- To find the order $r = o_N(x)$ of x modulo N, we estimate the phase s/r of the corresponding eigenvalue $e^{\frac{2\pi i s}{r}}$ of eigenstate $|u_s\rangle$ of $U_{x,N}$

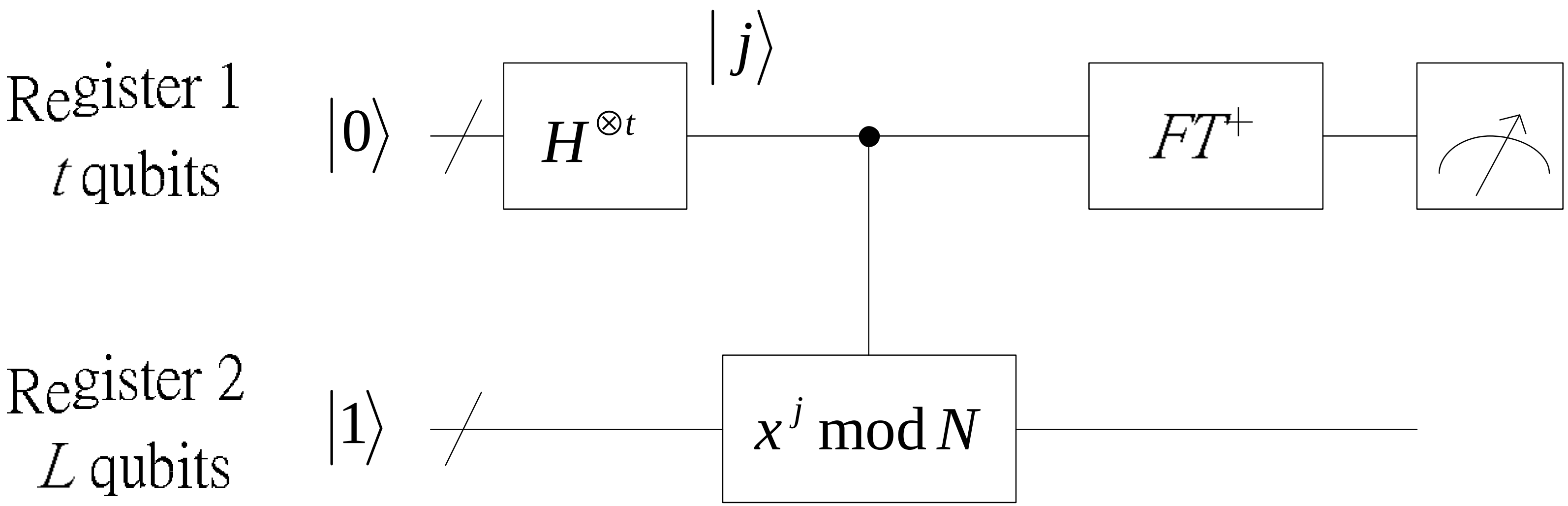
Preparing the initial state of the 2st Register

- Unable to prepare any of eigenstates $|u_s\rangle$
- An observation:

$$\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}|u_s\rangle = |1\rangle$$

  - $|1\rangle$: the initial state of 2nd register to be prepared

Implementing Quantum Order-Finding Algorithm



$$|0\rangle|1\rangle \quad \xrightarrow{H^{\otimes t}\otimes I} \quad \frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}|j\rangle|1\rangle \xrightarrow{\hat{U}_{x,N}} \frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}|j\rangle|x^j \pmod{N}\rangle$$

$$= \quad \frac{1}{\sqrt{r2^t}}\sum_{s=0}^{r-1}\sum_{j=0}^{2^t-1} e^{2\pi i sj/r}|j\rangle|u_s\rangle \xrightarrow{\mathcal{F}^{-1}\otimes I} \frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}|\frac{\tilde{s}}{r}\rangle|u_s\rangle$$

- $\hat{U}_{x,N}$: the controlled-$U_{x,N}^j$ unitary operator on the $(t+L)$-qubit composite system
- $|\frac{\tilde{s}}{r}\rangle = \sum_{x=-2^{t-1}+1}^{2^{t-1}} \frac{1}{2^t}\frac{1-e^{2\pi i(\delta_s 2^t - x)}}{1-e^{2\pi i(\delta_s - x2^{-t})}}|b_s + x\rangle$ with $s/r = b_s 2^{-t} + \delta_s$ such that $0 \le b_s \le 2^t - 1$ and $0 < \delta_s < 2^{-t}$

- $L = \lceil \log_2 N \rceil$: minimum number of bits to represent N
- $t = 2L + 1 + \lceil \log_2 \left(2 + \frac{1}{2\epsilon}\right) \rceil$
  - $2L + 1$: accuracy of phase estimation to $2^{-(2L+1)}$
  - $(1 - \epsilon)/r$: the least probability that an estimate of the phase $\varphi \approx s/r$ accurate to $(2L + 1)$ bits
- How to deduce r from the phase estimate φ ?

Continued Fraction Expansion

- Continued fractions : representing real numbers
  - Finite continued fractions :

$$[a_0, a_1, \cdots, a_M] \stackrel{\triangle}{=} a_0 + \frac{1}{a_1 + \frac{1}{\cdots + \frac{1}{a_M}}},$$

    where a_0 a real number, $a_1, \ldots, a_M$ positive real numbers
  - Finite simple continued fractions : finite continued fractions with a_i's all integers
  - Infinite simple continued fractions :

$$[a_0, a_1, a_2, \cdots] \stackrel{\triangle}{=} a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\cdots}}},$$

    where a_0 an integer and $a_i, i \geq 1$ positive integers

- Example : $30/17 = [1, 1, 3, 4]$

$$\frac{30}{17} \to 1+\frac{13}{17} \to 1+\frac{1}{\frac{17}{13}} \to 1+\frac{1}{1+\frac{4}{13}} \to 1+\frac{1}{1+\frac{1}{\frac{13}{4}}} \to 1+\frac{1}{1+\frac{1}{3+\frac{1}{4}}}$$

- α is a rational number if and only if α is uniquely expressible as a finite simple continued fraction $[a_0, a_1, \cdots, a_M]$ with $a_M \geq 2$ if $M \geq 1$

- α is an irrational number if and only if α is uniquely expressible as an infinite simple continued fraction

- $\gamma_m = [a_0, a_1, \ldots, a_m]$ is called the mth convergent of a finite continued fraction $\alpha = [a_0, a_1, \cdots, a_M]$

- Example : $\alpha = 30/17 = [1, 1, 3, 4]$

$$\gamma_0 = [1] = 1,\ \gamma_1 = [1, 1] = 2,\ \gamma_2 = [1, 1, 3] = \frac{7}{4},\ \gamma_3 = \alpha = \frac{30}{17}$$

A Theorem

- α : a real number
- p/q : a rational number with $q > 0$ and $(p,q) = 1$

If

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{2q^2},$$

then p/q is a convergent of the simple continued fraction expansion of α

- With $\alpha = 30/17 = [1,1,3,4]$, we have $7/4 = [1,1,3]$ is a convergent of the simple continued fraction expansion of α since

$$|7/4 - \alpha| = 1/(4 \cdot 17) \leq 1/(2 \cdot 4^2)$$

- Not every convergent of α satisfies the above inequality

$$|1-\alpha| = 13/17 > 1/(2\cdot 1^2)$$

where 1 is a convergent of the simple continued fraction expansion of α

The Implication

- With probability $\geq (1-\epsilon)/r$, the estimated phase φ approximates s/r accurate to $(2L+1)$ bits, i.e.,

$$\left|\varphi - \frac{s}{r}\right| \leq \frac{1}{2^{(2L+1)}} = \frac{1}{2(2^L)^2} \leq \frac{1}{2N^2} \leq \frac{1}{2r^2}$$

- Continued fraction algorithm efficiently produces numbers s' and r', with no common divisor, such that $s'/r' = s/r$ once a convergent s'/r' of the estimated phase φ satisfies

$$\left|\varphi - \frac{s'}{r'}\right| \leq \frac{1}{2^{(2L+1)}}$$

- r' : candidate of r
- Verification : Is $x^{r'} \equiv 1 \pmod{N}$?

Failure of the Order-Finding Algorithm

- Case I : with probability at most ϵ, the phase estimation procedure produces a bad estimate φ with an error greater than $2^{-(2L+1)}$ to each s/r
- Case II : the continued fraction algorithm returns an r' which is a proper divisor of r in case that s and r has a common divisor

Quantum Factoring Algorithm

A Theorem

- N : a positive integer with $N \geq 4$
- $2 \leq x \leq N - 2$
- $x^2 \equiv 1 \pmod{N}$

Then at least one of $\gcd(x-1, N)$ and $\gcd(x+1, N)$ is a proper factor of N

A Theorem

- $N = p_1^{k_1} p_1^{k_2} \cdots p_m^{k_m}$: prime factorization of an odd positive integer N with $m \geq 2$
- x : an integer in Z_N^* chosen uniformly at random
- $r = o_N(x)$

$$\mathcal{P}(r \text{ is even and } x^{r/2} \not\equiv -1 \pmod{N}) \geq 1 - \frac{1}{2^m}$$

The Factoring Algorithm

- If N is even, return the factor 2 (to reduce the size of N by $N \leftarrow N/2$)
- Determine whether $N = a^b$ for integer $a \geq 3$ and $b \geq 2$ and if so, return the factor a (to reduce the size of N by $N \leftarrow a$)
- Randomly choose x in $[3, N-2]$, if $\gcd(x, N) > 1$, then return the factor $\gcd(x, N)$ (to reduce the size of N by $N \leftarrow N/\gcd(x, N)$)
- Use the order-finding algorithm to find $r = o_N(x)$
- If r is even and $x^{r/2} \not\equiv -1 \pmod N$, then compute $\gcd(x^{r/2} - 1, N)$ and $\gcd(x^{r/2} + 1, N)$, and test to see if one of these is a proper factor of N and return the factor if so. Otherwise, the algorithm fails

Factoring $N = 15$

- $L = \log_2 N = 4$
- $\epsilon = 1/4$
- $t = 2L + 1 + \lceil \log_2 \left(2 + \frac{1}{2\epsilon}\right) \rceil = 9 + 2 = 11$
- No factor of 2 : 15 is an odd number
- Not a power a^b with $a \geq 3$ and $b \geq 2$
- Randomly select an integer x in $[3, 13]$:
  - If x is a multiple of $3, 5$, then return $\gcd(x, N) = 3, 5 > 0$.
  - If x is not a multiple of $3, 5$, says $x = 7$, then $x \in Z_{15}^*$
- Compute $o_N(x) = o_{15}(7)$ (which is equal to 4, but we do not know it) by the quantum order-finding algorithm
  - Preparing the state $|0\rangle|1\rangle$ of the $(t + L)$-qubit composite system

- Applying Hadamard transform to the 1st register, the resulted state is

$$\frac{1}{\sqrt{2^t}}\sum_{k=0}^{2^t-1}|k\rangle|1\rangle$$

- Applying the controlled $U_{x,N}^k$ gate, the resulted state is

$$\begin{aligned}&\frac{1}{\sqrt{2^t}}\sum_{k=0}^{2^t-1}|k\rangle|x^k \pmod N\rangle\\ =\ &\frac{1}{\sqrt{2^t}}\{|0\rangle|1\rangle+|1\rangle|7\rangle+|2\rangle|4\rangle+|3\rangle|13\rangle+|4\rangle|1\rangle+|5\rangle|7\rangle+\cdots\}\end{aligned}$$

- Applying the inverse Fourier transform to the 1st register and measuring the resulted state

– Or before applying the inverse Fourier transform to the 1st register, we use the principle of implicit measurement by assuming that 2nd register is measured with result m

$$\mathcal{P}(m=1) = \mathcal{P}(m=7) = \mathcal{P}(m=4) = \mathcal{P}(m=13) = \frac{1}{4}$$

– Suppose $m = 4$ (any of the results works) is measured. The state of the 1st register input to the inverse FT is

$$\sqrt{\frac{4}{2^t}}\{|2\rangle + |6\rangle + |10\rangle + |14\rangle + \cdots\} = \sqrt{\frac{1}{2^{t-2}}}\sum_{j=0}^{2^{t-2}-1} |2+4j\rangle$$

– The output state after applying inverse FT to the 2nd register is

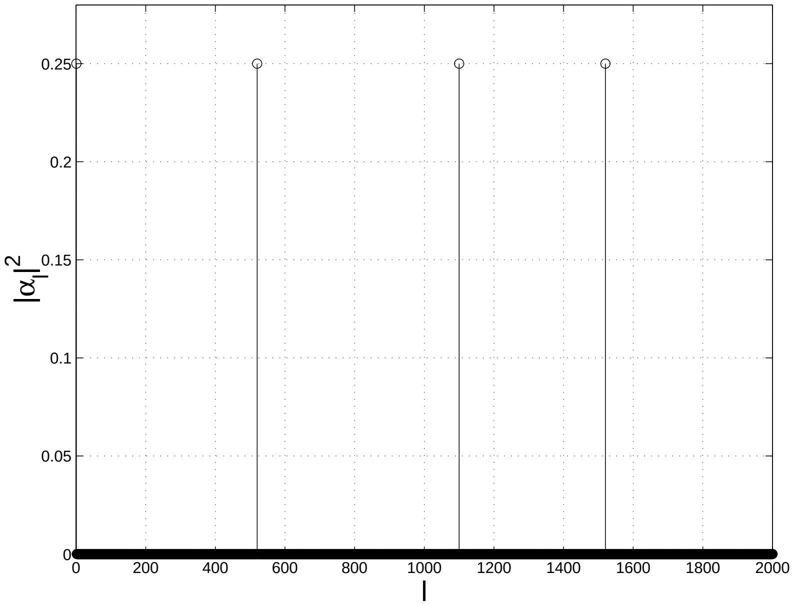
$$\frac{2}{\sqrt{2^t}}\sum_{j=0}^{2^{t-2}-1}\frac{1}{\sqrt{2^t}}\sum_{k=0}^{2^t-1} e^{-2\pi i(2+4j)k2^{-t}}|k\rangle = \sum_{l=0}^{2^t-1}\alpha_l|l\rangle$$

with

$$\alpha_l = \frac{1}{2^{t-1}} \sum_{j=0}^{2^{t-2}-1} e^{-2\pi i (2+4j) l 2^{-t}}$$

$$= \begin{cases} \frac{1}{2} e^{-k\pi i}, & \text{if } l = k2^{t-2}, k = 0, 1, 2, 3 \\ 0, & \text{otherwize} \end{cases}$$

– The probability distribution of $|\alpha_l|^2$ is



  - The measurement output is $l = 0, 512, 1024, 1536$ each with probability $1/4$
  - Suppose $l = 1536$. With continued fraction, we obtain $1536/2048 = 1(1 + (1/3)) = [0113]$ so that $3/4 = [0113]$ occurs as a convergent of $[0113]$. This gives $r' = 4$ and by checking $7^4 \equiv 1 \pmod{15}$, we conclude that $r = o_{15}(7) = 4$

- Since $r = 4$ is even and $x^{r/2} = 7^2 \not\equiv -1 \pmod{15}$, then compute $\gcd(7^2 - 1, 15) = 3$ and $\gcd(7^2 + 1, 15) = 5$, which tells us that $15 = 3 \times 5$

Period-Finding

Periodic Function

- f : periodic function from $N_0 = \{0, 1, 2, \ldots\}$ to $\{0, 1\}$
- r : period length of f, $1 \le r \le 2^L - 1$, to be evaluated

$$f(x + r) = f(x), \ \forall \ x \ge 0$$

- $\{|x\rangle\}$: computational basis of the state space of an t-qubit system
  - $\{|x\rangle\}$: served as (a subset of) the domain of the periodic function f
  - t : no less than L (at least to cover one period) and dependent on the desired accuracy for r
- $\{|y\rangle\}$: computational basis of the state space of a single qubit
  - $\{|y\rangle\}$: served as the co-domain of the periodic function f

- $[|\hat{f}(0)\rangle, |\hat{f}(1)\rangle, \ldots, |\hat{f}(r-1)\rangle]$: r-tuple representing the Inverse Fourier transform of the r-tuple $[|f(0)\rangle, |f(1)\rangle, \ldots, |f(r-1)\rangle]$ of states

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

  - $[|f(0)\rangle, |f(1)\rangle, \ldots, |f(r-1)\rangle]$: representing the dynamics of the periodic function f in one period

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

Simultaneous Evaluation of f

- U : unitary operator acting on the $(t+1)$-qubit composite system

$$U|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$$

- Quantum parallelism :

$$|0\rangle|0\rangle \xrightarrow{H^{\otimes t} \otimes I} \frac{1}{\sqrt{2^t}} \sum_{x=0}^{2^t-1} |x\rangle|0\rangle \xrightarrow{U} \frac{1}{\sqrt{2^t}} \sum_{x=0}^{2^t-1} |x\rangle|f(x)\rangle$$

Hidden Interaction Between t-qubit and 1-qubit Systems

$$
\begin{aligned}
\frac{1}{\sqrt{2^t}}\sum_{x=0}^{2^t-1}|x\rangle|f(x)\rangle &= \frac{1}{\sqrt{2^t}}\sum_{x=0}^{2^t-1}|x\rangle\frac{1}{\sqrt{r}}\sum_{l=0}^{r-1}e^{2\pi ilx/r}|\hat{f}(l)\rangle \\
&= \frac{1}{\sqrt{r}}\sum_{l=0}^{r-1}\left(\frac{1}{\sqrt{2^t}}\sum_{x=0}^{2^t-1}e^{2\pi ix(l/r)}|x\rangle\right)|\hat{f}(l)\rangle
\end{aligned}
$$

- The period r is embedded in the phases l/r which will be estimated by the phase estimation algorithm on the t-qubit system
  - Applying inverse Fourier transform to the t-qubit system to obtain

$$\frac{1}{\sqrt{r}}\sum_{l=0}^{r-1}|\frac{\tilde{l}}{r}\rangle|\hat{f}(l)\rangle$$

where

$$|\frac{\tilde{l}}{r}\rangle = \sum_{x=-2^{t-1}+1}^{2^{t-1}} \frac{1}{2^t} \frac{1-e^{2\pi i(\delta_l 2^t - x)}}{1-e^{2\pi i(\delta_l - x2^{-t})}} |b_l + x\rangle$$

with $l/r = b_l 2^{-t} + \delta_l$ such that $0 \leq b_l \leq 2^t - 1$ and $0 < \delta_l < 2^{-t}$

– For each $0 \leq l \leq r-1$, $|\hat{f}(l)\rangle = u_{l0}|0\rangle + u_{l1}|1\rangle$ with

$$u_{l0} = \frac{1}{\sqrt{r}} \sum_{x \in P_0} e^{-2\pi i l x/r}, \quad u_{l1} = \frac{1}{\sqrt{r}} \sum_{x \in P_1} e^{-2\pi i l x/r}$$

where $P_0 = \{x \in [0, r-1] \mid f(x) = 0\}$ and $P_1 = \{x \in [0, r-1] \mid f(x) = 1\}$

- Resulted state after applying inverse Fourier transform

$$\left(\frac{1}{\sqrt{r}}\sum_{l=0}^{r-1} u_{l0}|\frac{\tilde{l}}{r}\rangle\right)|0\rangle + \left(\frac{1}{\sqrt{r}}\sum_{l=0}^{r-1} u_{l1}|\frac{\tilde{l}}{r}\rangle\right)|1\rangle$$

- With the principle of implicit measurement by assuming that 2nd register is measured with result m

$$\mathcal{P}(m=0) = \frac{|Q_0|}{2^t}, \quad \mathcal{P}(m=1) = \frac{|Q_1|}{2^t}$$

where $Q_0 = \{x \in [0, 2^t - 1] \mid f(x) = 0\}$ and $Q_1 = \{x \in [0, 2^t - 1] \mid f(x) = 1\}$

- Suppose that $m = 0$ is measured (which occurs with probability $|Q_0|/2^t$). Then the output state of the 1st register after applying inverse Fourier transform is

$$\sqrt{\frac{2^t}{r|Q_0|}}\sum_{l=0}^{r-1} u_{l0}|\frac{\tilde{l}}{r}\rangle$$

Discrete Logarithm

- a, b, N : positive integers with $1 < a, b < N$ and $(a, N) = 1$ such that

$$a^s = b \pmod{N}$$

  Note that $(b, N) = 1$, too

- Find the least positive integer s
  - $r = O_N(a)$: the order of a modulo N, which is assumed known by the order-finding algorithm
  - We must have $1 \leq b \leq r - 1$

Doubly Periodic Function

- f : a function from $N_0 \times N_0$ to (a), where $N_0 = \{0, 1, 2, \ldots\}$ and $(a) = \{a^k \pmod N \mid 0 \leq k \leq r-1\}$

$$f(x_1, x_2) = b^{x_1} a^{x_2} \pmod N = a^{sx_1 + x_2} \pmod N$$

- f : a doubly periodic function with 2-tuple periods
  - $(l, -sl)$ for each integer l :

$$f(x_1 + l, x_2 - sl) = f(x_1, x_2),\ \forall\ x_1, x_2 \geq 0$$

  - (r, r) :

$$f(x_1 + r, x_2 + r) = f(x_1, x_2),\ \forall\ x_1, x_2 \geq 0$$

- $L = \lceil \log_2 r \rceil$

- $\{|x\rangle\}$: computational basis of the state space of an t-qubit system
  - $\{|x\rangle\}$: served as (a subset of) a factor (N_0) of the domain of f
  - $t = L + \lceil \log_2 \left(2 + \frac{1}{2\epsilon}\right) \rceil$: no less than L (at least to cover one period) and dependent on the desired accuracy for s
  - Two registers of length t are needed
- $\{|y\rangle\}$: computational basis of the state space of an L-qubit system
  - $\{|y\rangle\}$: served as the co-domain of the function f through the following one-to-one correspondence

$$|y\rangle \leftrightarrow |a^y \pmod N\rangle$$

for $0 \le y \le r - 1$

- $\{|\hat{f}(l_1, l_2)\rangle, 0 \le l_1, l_2 \le r-1\}$: inverse Fourier transform of states $\{|f(x_1, x_2)\rangle, 0 \le x_1, x_2 \le r-1\}$

$$
\begin{aligned}
|\hat{f}(l_1, l_2)\rangle &= \frac{1}{r}\sum_{x_1=0}^{r-1}\sum_{x_2=0}^{r-1} e^{-2\pi i(l_1x_1+l_2x_2)/r}|f(x_1, x_2)\rangle \\
&= \begin{cases} \sum_{j=0}^{r-1} e^{-2\pi i l_2 j/r}|f(0, j)\rangle, & \text{if } l_1 = sl_2, \\ 0, & \text{othersiwe} \end{cases}
\end{aligned}
$$

  - $\{|f(x_1, x_2)\rangle, 0 \le x_1, x_2 \le r-1\}$: representing the dynamics of the periodic function f in at least one period (r, r)

$$
\begin{aligned}
|f(x_1, x_2)\rangle &= \frac{1}{r}\sum_{l_1=0}^{r-1}\sum_{l_2=0}^{r-1} e^{2\pi i(l_1x_1+l_2x_2)/r}|\hat{f}(l_1, l_2)\rangle \\
&= \frac{1}{r}\sum_{l_2=0}^{r-1} e^{2\pi i(sl_2x_1+l_2x_2)/r}|\hat{f}(sl_2, l_2)\rangle
\end{aligned}
$$

Simultaneous Evaluation of f

- U : unitary operator acting on the $(2t + L)$-qubit composite system

$$U|x_1\rangle|x_2\rangle|y\rangle = |x_1\rangle|x_2\rangle|y \oplus f(x_1, x_2)\rangle$$

- Quantum parallelism :

$$|0\rangle|0\rangle|0\rangle \quad \xrightarrow{H^{\otimes t}\otimes H^{\otimes t}\otimes I} \quad \frac{1}{2^t}\sum_{x_1=0}^{2^t-1}\sum_{x_2=0}^{2^t-1}|x_1\rangle|x_2\rangle|0\rangle$$

$$\xrightarrow{U} \quad \frac{1}{2^t}\sum_{x_1=0}^{2^t-1}\sum_{x_2=0}^{2^t-1}|x_1\rangle|x_2\rangle|f(x_1, x_2)\rangle$$

Hidden Interaction Between $(2t + L)$-qubit Composite Systems

$$
\begin{aligned}
& \frac{1}{2^t}\sum_{x_1=0}^{2^t-1}\sum_{x_2=0}^{2^t-1}|x_1\rangle|x_2\rangle|f(x_1,x_2)\rangle \\
= \quad & \frac{1}{r2^t}\sum_{l_2=0}^{r-1}\sum_{x_1=0}^{2^t-1}\sum_{x_2=0}^{2^t-1} e^{2\pi i(sl_2x_1+l_2x_2)/r}|x_1\rangle|x_2\rangle|\hat{f}(sl_2,l_2)\rangle \\
= \quad & \frac{1}{r}\sum_{l_2=0}^{r-1}\left(\frac{1}{\sqrt{2^t}}\sum_{x_1=0}^{2^t-1} e^{2\pi i s l_2 x_1/r}|x_1\rangle\right)\left(\frac{1}{\sqrt{2^t}}\sum_{x_2=0}^{2^t-1} e^{2\pi i l_2 x_2/r}|x_2\rangle\right) \\
& |\hat{f}(sl_2,l_2)\rangle
\end{aligned}
$$

- The discrete logarithm s is embedded in the phases $(sl_2)/r$ and l_2/r which will be estimated by the phase estimation algorithm on each t-qubit system
  - Applying inverse Fourier transform to each t-qubit system to obtain

$$\frac{1}{r}\sum_{l_2=0}^{r-1}|\widetilde{\frac{sl_2}{r}}\rangle|\widetilde{\frac{l_2}{r}}\rangle|\hat{f}(sl_2, l_2)\rangle$$

where

$$|\widetilde{\frac{sl_2}{r}}\rangle = \sum_{x=-2^{t-1}+1}^{2^{t-1}} \frac{1}{2^t}\frac{1-e^{2\pi i(\delta_{sl_2}2^t - x)}}{1-e^{2\pi i(\delta_{sl_2}-x2^{-t})}}|b_{sl_2}+x\rangle$$

$$|\widetilde{\frac{l_2}{r}}\rangle = \sum_{x=-2^{t-1}+1}^{2^{t-1}} \frac{1}{2^t}\frac{1-e^{2\pi i(\delta_{l_2}2^t - x)}}{1-e^{2\pi i(\delta_{l_2}-x2^{-t})}}|b_{l_2}+x\rangle$$

with $(sl_2)/r = b_{sl_2}2^{-t} + \delta_{sl_2}$, $l_2/r = b_{l_2}2^{-t} + \delta_{l_2}$ such that $0 \leq b_{sl_2}, b_{l_2} \leq 2^t - 1$ and $0 < \delta_{sl_2}, \delta_{l_2} < 2^{-t}$