공지사항

- 기말고사 일정
  - 기말고사1: 6/8 (월) 17:00~18:15
    - 장소: 302-106/107
  - 기말고사2: 6/15(월) 17:00~18:15
    - 장소: 302-105

- 성적
  - 절대평가 기준

과제 (%)	기말고사1 (%)	기말고사2 (%)	출석 (%)	합계 (%)
35	30	30	5	100

Summary of previous lecture

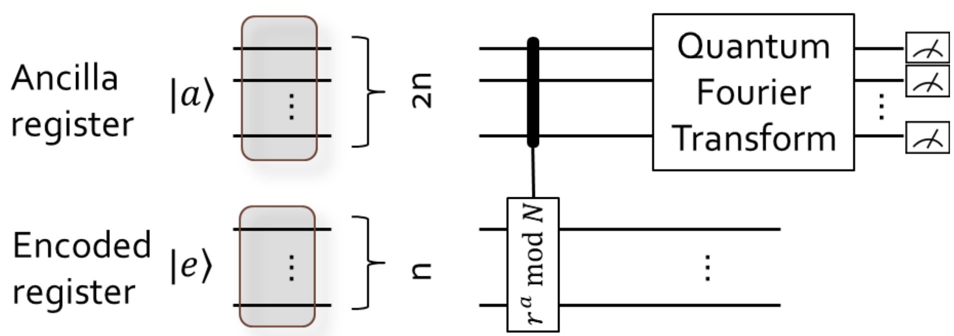
- Deutsch's algorithm
  - Pattern of the algorithm: Initialization ➔ **Superposition** of multiple possibilities ➔ Processing ➔ **Interference** of the multiple outputs ➔ Measurement of the output
- Reversible gate
  - Conversion of digital gates with reversible gates generally incurs the **auxiliary qubits** and **garbage qubits**.
  - Garbage qubit generally gets entangled with other qubits and can be detrimental to the overall circuits.
  - By **un-computing**, the garbage qubits can be un-entangled and the auxiliary qubits can be re-cycled.
- Factoring algorithm (Shor's algorithm)
  - Origin of quantum speed-up
    - Simultaneous calculation of $a^x \pmod{N}$ for x from 0 to $2^{2\cdot\mathrm{ceil}(\log_2 N)}$
    - Fast Fourier transform

Shor's Algorithm (Factoring algorithm)

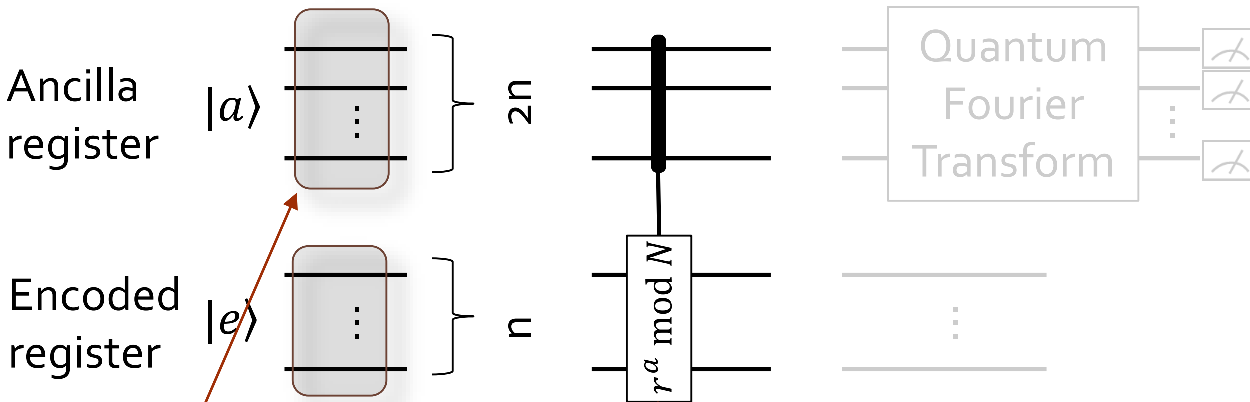
- Chapter 5
- Example for factorization of number 15
  - Choose a random number that has the following properties
    - No common divisor with 15 (target of factorization)
    - Smaller than 15 (target of factorization)
    - Ex) $r = 7$
  - Calculate $r^a (\mathrm{mod}\ 15)$ for all a between 0 and 255
  - Find the period among these values
    - Ex)

7^0	7^1	7^2	7^3	7^4	7^5	7^6	7^7	7^8	7^9	7^{10}	7^{11}	7^{12}	…
1	7	4	13	1	7	4	13	1	7	4	13	1	…

    - $7^4 = 1$ (mod 15) => $7^4 - 1 = (7^2 - 1)(7^2 + 1) = N * 15$
    - $\gcd(7^2 - 1, 15) = 3$, $\gcd(7^2 + 1, 15) = 5$



Analysis of Factorization Process I



$$|a\rangle = |0\rangle_a + |1\rangle_a + |2\rangle_a + \cdots + |255\rangle_a$$

$$\otimes$$

$$|e\rangle = |1\rangle_e$$

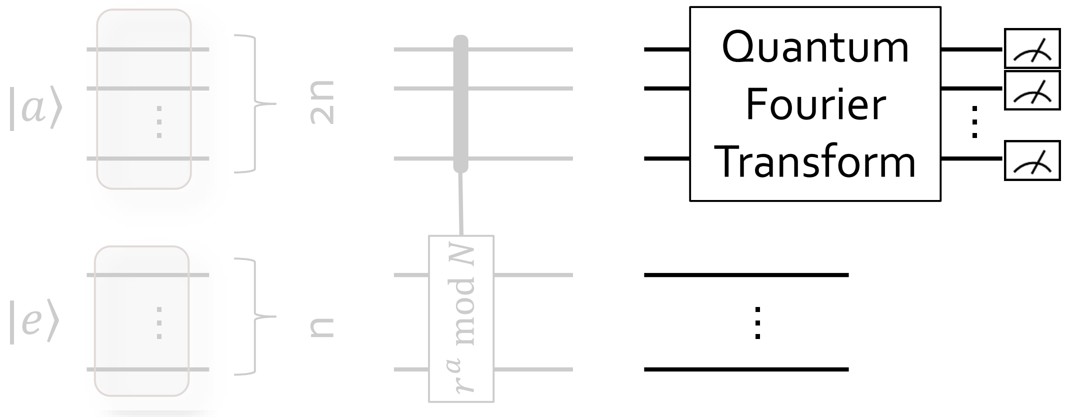
$$\begin{aligned}
&|0\rangle_a|1\rangle_e + |1\rangle_a|7\rangle_e + |2\rangle_a|4\rangle_e + |3\rangle_a|13\rangle_e \\
&+|4\rangle_a|1\rangle_e + |5\rangle_a|7\rangle_e + |6\rangle_a|4\rangle_e + |7\rangle_a|13\rangle_e \\
&+|8\rangle_a|1\rangle_e + |9\rangle_a|7\rangle_e + |10\rangle_a|4\rangle_e + |11\rangle_a|13\rangle_e \\
&+ \quad \cdots \\
&+|252\rangle_a|1\rangle_e + |253\rangle_a|7\rangle_e + |254\rangle_a|4\rangle_e + |255\rangle_a|13\rangle_e
\end{aligned}$$

$$\begin{aligned}
&= (|0\rangle_a + |4\rangle_a + |8\rangle_a + \cdots + |252\rangle_a)|1\rangle_e \\
&+(|1\rangle_a + |5\rangle_a + |9\rangle_a + \cdots + |253\rangle_a)|7\rangle_e \\
&+(|2\rangle_a + |6\rangle_a + |10\rangle_a + \cdots + |254\rangle_a)|4\rangle_e \\
&+(|3\rangle_a + |7\rangle_a + |11\rangle_a + \cdots + |255\rangle_a)|13\rangle_e
\end{aligned}$$

Analysis of Factorization Process II

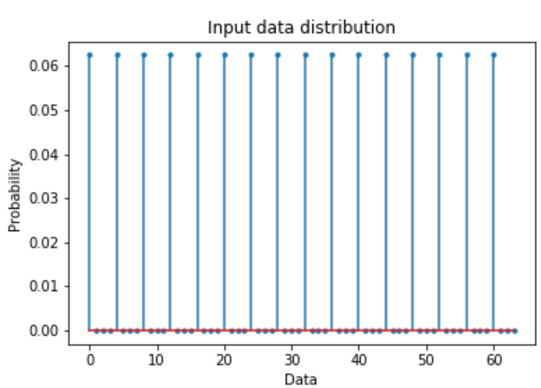
Ancilla register

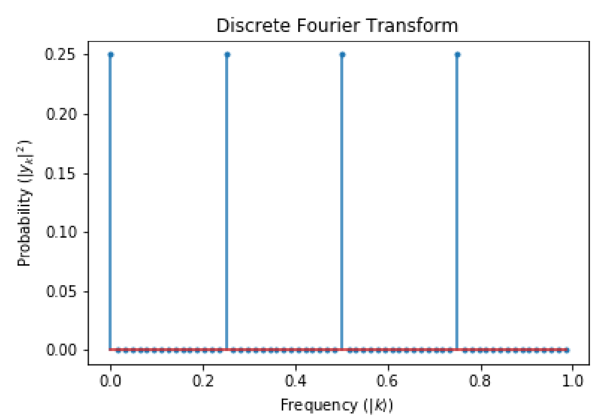
Encoded register



$$= (|0\rangle_a + |4\rangle_a + |8\rangle_a + \cdots + |252\rangle_a)|1\rangle_e$$
$$+(|1\rangle_a + |5\rangle_a + |9\rangle_a + \cdots + |253\rangle_a)|7\rangle_e$$
$$+(|2\rangle_a + |6\rangle_a + |10\rangle_a + \cdots + |254\rangle_a)|4\rangle_e$$
$$+(|3\rangle_a + |7\rangle_a + |11\rangle_a + \cdots + |255\rangle_a)|13\rangle_e$$

$$= (|k=0\rangle + |k=64\rangle + |k=128\rangle + |k=192\rangle)_y\,|1\rangle_e$$
$$+\big(|k=0\rangle + e^{i3\pi/2}|k=64\rangle + e^{i\pi}|k=128\rangle + e^{i\pi/2}|k=192\rangle\big)_y|7\rangle_e$$
$$+\big(|k=0\rangle + e^{i\pi}|k=64\rangle + e^{i2\pi}|k=128\rangle + e^{i\pi}|k=192\rangle\big)_y|4\rangle_e$$
$$+\big(|k=0\rangle + e^{i\pi/2}|k=64\rangle + e^{i\pi}|k=128\rangle + e^{i3\pi/2}|k=192\rangle\big)_y|13\rangle_e$$



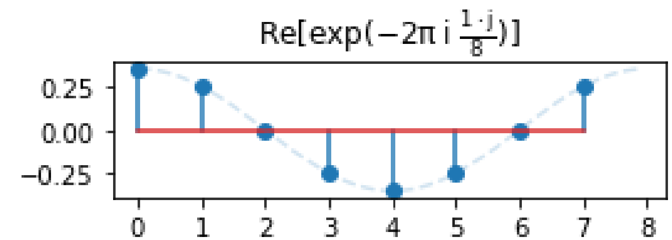


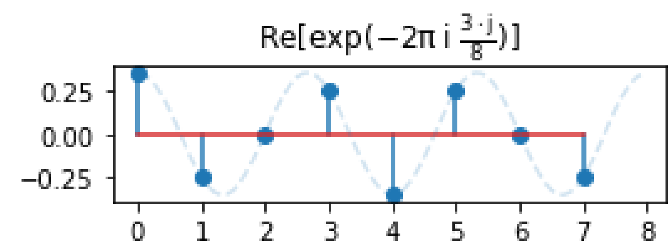
The above plots are generated using 64 inputs instead of 256 for readability

If $|k = 192\rangle$ quantum state is measured, the corresponding frequency is 192/256=3/4. From this value, we can learn that there exist a high probability that the period is 4.

Discrete Fourier Transform

- N-dimensional vector space composed of $[x_0, x_1, \cdots, x_{N-1}]$
  - One option for the basis is $[0, , \cdots, 0, 1, 0, \cdots, 0]$
  - Orthonormal basis: $|k\rangle \leftrightarrow \frac{1}{\sqrt{N}}\left[e^{-2\pi i\frac{k\cdot 0}{N}}, e^{-2\pi i\frac{k\cdot 1}{N}}, \cdots, e^{-2\pi i\frac{k\cdot(N-1)}{N}}\right]$ for $0 \leq k < N$
  - For example, if $N = 8$
    - $k = 1$ ➔ $\frac{1}{\sqrt{8}}\left[e^{-2\pi i\frac{1\cdot 0}{8}}, e^{-2\pi i\frac{1\cdot 1}{8}}, \cdots, e^{-2\pi i\frac{1\cdot 7}{8}}\right]$
    - $k = 3$ ➔ $\frac{1}{\sqrt{8}}\left[e^{-2\pi i\frac{3\cdot 0}{8}}, e^{-2\pi i\frac{3\cdot 1}{8}}, \cdots, e^{-2\pi i\frac{3\cdot 7}{8}}\right]$

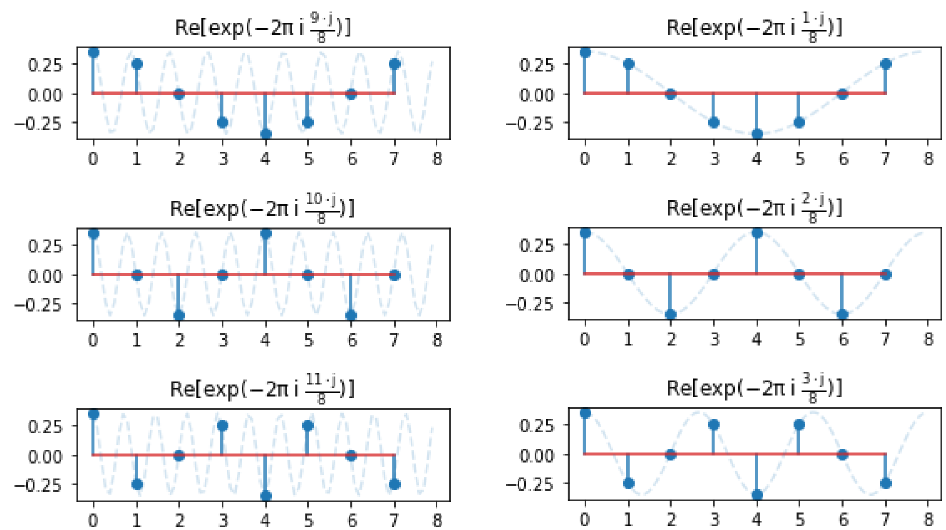




  - Inner product between $[x_0, x_1, \cdots, x_{N-1}]$ and $[y_0, y_1, \cdots, y_{N-1}]$ is defined as $\sum_{j=0}^{N-1} x_j^* y_j$.

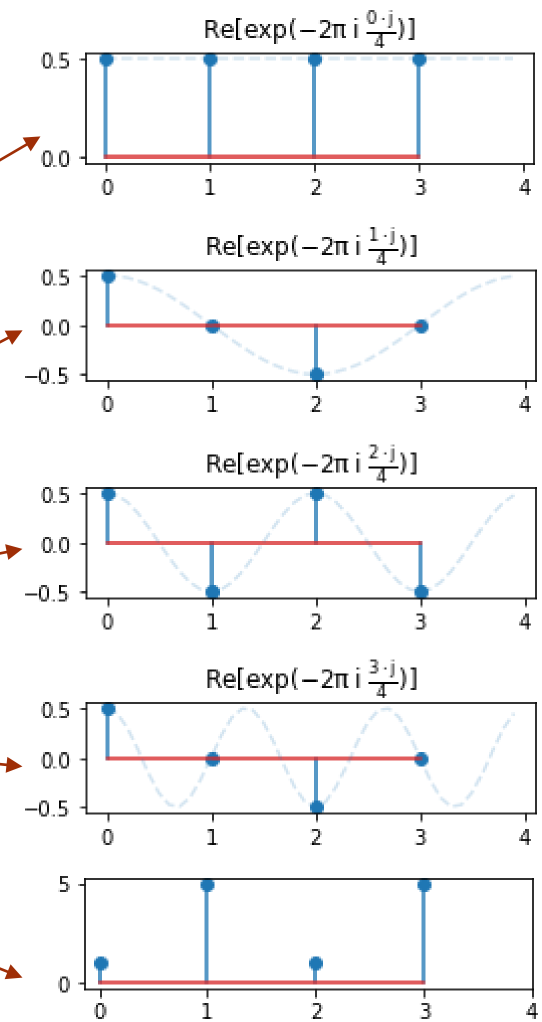
Discrete Fourier Transform

- Orthonormality between $|k\rangle$ and $|k'\rangle$
  - $\langle k|k'\rangle = \sum_{j=0}^{N-1} \frac{1}{\sqrt{N}} e^{2\pi i\frac{k\cdot j}{N}} \frac{1}{\sqrt{N}} e^{-2\pi i\frac{k'\cdot j}{N}} = \frac{1}{N}\sum_{j=0}^{N-1} e^{2\pi i\frac{(k-k')\cdot j}{N}} = \frac{1}{N}\sum_{j=0}^{N-1} \alpha^j$ where $\alpha = e^{2\pi i\frac{(k-k')}{N}}$
  - When $k = k'$: $\alpha = 1$ ➔ $\langle k|k'\rangle = \frac{1}{N}\sum_{j=0}^{N-1} \alpha^j = \frac{1}{N}\sum_{j=1}^{N} 1 = 1$
  - When $k \neq k'$: $\alpha \neq 1$ ➔$\langle k|k'\rangle = \frac{1}{N}\sum_{j=0}^{N-1} \alpha^j = \frac{1}{N}\frac{\alpha^N - 1}{\alpha - 1}$, but because $\alpha^N = \left(e^{2\pi i\frac{(k-k')}{N}}\right)^N = 1$, $\langle k|k'\rangle = 0$
- What about $k > N$?
  - It corresponds to the case for $0 \leq k' < N$ due to $e^{-2\pi i\frac{(k'+N)\cdot j}{N}} = e^{-2\pi i\frac{k'\cdot j}{N}} e^{-2\pi i\frac{N\cdot j}{N}} = e^{-2\pi i\frac{k'\cdot j}{N}}$



Discrete Fourier Transform

- Any arbitrary sequence of number $[x_0, x_1, \cdots, x_{N-1}] = |x\rangle$ can be decomposed into the weighted sum of basis $\frac{1}{\sqrt{N}}\left[e^{-2\pi i\frac{k\cdot 0}{N}}, e^{-2\pi i\frac{k\cdot 1}{N}}, \cdots, e^{-2\pi i\frac{k\cdot(N-1)}{N}}\right] = |k\rangle$
- $|x\rangle = \sum_{k=0}^{N-1} c_k |k\rangle$
- Example for $N = 4$
  - $|k=0\rangle = |0\rangle = \frac{1}{2}[1, 1, 1,1]$
  - $|k=1\rangle = |1\rangle = \frac{1}{2}[1, -i, -1, i]$
  - $|k=2\rangle = |2\rangle = \frac{1}{2}[1, -1, 1, -1]$
  - $|k=3\rangle = |3\rangle = \frac{1}{2}[1, i, -1, -i]$
  - $|x\rangle = [1,5,1,5] = 6|0\rangle - 4|2\rangle$



Derivation of Quantum Fourier Transform I

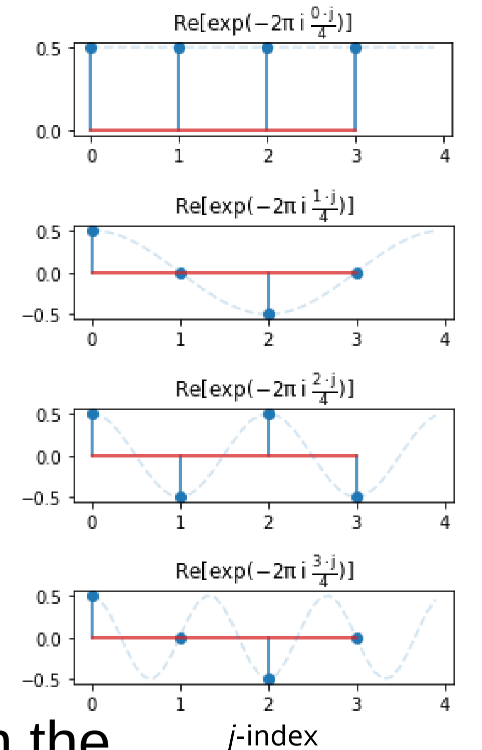
- Discrete Fourier transform finds the period embedded in the given random sequence $x_0, \dots, x_{\mathrm{N}-1}$
- Example: assume that we are given a sequence x_0, x_1, x_2, x_3 composed of 4 numbers. The following calculations allow us to find y_0, y_1, y_2, y_3 that is the relative importance of the signal with the corresponding period.

$$y_0 = \frac{1}{\sqrt{4}}\left(x_0 e^{2\pi i\frac{0\cdot 0}{4}} + x_1 e^{2\pi i\frac{0\cdot 1}{4}} + x_2 e^{2\pi i\frac{0\cdot 2}{4}} + x_3 e^{2\pi i\frac{0\cdot 3}{4}}\right)$$

$$y_1 = \frac{1}{\sqrt{4}}\left(x_0 e^{2\pi i\frac{1\cdot 0}{4}} + x_1 e^{2\pi i\frac{1\cdot 1}{4}} + x_2 e^{2\pi i\frac{1\cdot 2}{4}} + x_3 e^{2\pi i\frac{1\cdot 3}{4}}\right)$$

$$y_2 = \frac{1}{\sqrt{4}}\left(x_0 e^{2\pi i\frac{2\cdot 0}{4}} + x_1 e^{2\pi i\frac{2\cdot 1}{4}} + x_2 e^{2\pi i\frac{2\cdot 2}{4}} + x_3 e^{2\pi i\frac{2\cdot 3}{4}}\right)$$

$$y_3 = \frac{1}{\sqrt{4}}\left(x_0 e^{2\pi i\frac{3\cdot 0}{4}} + x_1 e^{2\pi i\frac{3\cdot 1}{4}} + x_2 e^{2\pi i\frac{3\cdot 2}{4}} + x_3 e^{2\pi i\frac{3\cdot 3}{4}}\right)$$



- Goal of quantum Fourier transform (QFT): when the input quantum state is $x_0|0\rangle + x_1|1\rangle + x_2|2\rangle + x_3|3\rangle$, the outcome of QFT should be $\boxed{y_0|0\rangle + y_1|1\rangle + y_2|2\rangle + y_3|3\rangle}$.

Derivation of Quantum Fourier Transform II

$$y_0|0\rangle \quad + \quad y_1|1\rangle \quad + \quad y_2|2\rangle \quad + \quad y_3|3\rangle$$

$$= \begin{pmatrix} x_0 e^{2\pi i\frac{0\cdot 0}{4}}|0\rangle \\ + \\ x_1 e^{2\pi i\frac{0\cdot 1}{4}}|0\rangle \\ + \\ x_2 e^{2\pi i\frac{0\cdot 2}{4}}|0\rangle \\ + \\ x_3 e^{2\pi i\frac{0\cdot 3}{4}}|0\rangle \end{pmatrix} + \begin{pmatrix} x_0 e^{2\pi i\frac{1\cdot 0}{4}}|1\rangle \\ + \\ x_1 e^{2\pi i\frac{1\cdot 1}{4}}|1\rangle \\ + \\ x_2 e^{2\pi i\frac{1\cdot 2}{4}}|1\rangle \\ + \\ x_3 e^{2\pi i\frac{1\cdot 3}{4}}|1\rangle \end{pmatrix} + \begin{pmatrix} x_0 e^{2\pi i\frac{2\cdot 0}{4}}|2\rangle \\ + \\ x_1 e^{2\pi i\frac{2\cdot 1}{4}}|2\rangle \\ + \\ x_2 e^{2\pi i\frac{2\cdot 2}{4}}|2\rangle \\ + \\ x_3 e^{2\pi i\frac{2\cdot 3}{4}}|2\rangle \end{pmatrix} + \begin{pmatrix} x_0 e^{2\pi i\frac{3\cdot 0}{4}}|3\rangle \\ + \\ x_1 e^{2\pi i\frac{3\cdot 1}{4}}|3\rangle \\ + \\ x_2 e^{2\pi i\frac{3\cdot 2}{4}}|3\rangle \\ + \\ x_3 e^{2\pi i\frac{3\cdot 3}{4}}|3\rangle \end{pmatrix} \quad /\sqrt{4}$$

$$= x_0\left(e^{2\pi i\frac{0\cdot 0}{4}}|0\rangle + e^{2\pi i\frac{1\cdot 0}{4}}|1\rangle + e^{2\pi i\frac{2\cdot 0}{4}}|2\rangle + e^{2\pi i\frac{3\cdot 0}{4}}|3\rangle\right)/\sqrt{4}$$

$$+$$

$$x_1\left(e^{2\pi i\frac{0\cdot 1}{4}}|0\rangle + e^{2\pi i\frac{1\cdot 1}{4}}|1\rangle + e^{2\pi i\frac{2\cdot 1}{4}}|2\rangle + e^{2\pi i\frac{3\cdot 1}{4}}|3\rangle\right)/\sqrt{4}$$

$$+$$

$$x_2\left(e^{2\pi i\frac{0\cdot 2}{4}}|0\rangle + e^{2\pi i\frac{1\cdot 2}{4}}|1\rangle + e^{2\pi i\frac{2\cdot 2}{4}}|2\rangle + e^{2\pi i\frac{3\cdot 2}{4}}|3\rangle\right)/\sqrt{4}$$

$$+$$

$$x_3\left(e^{2\pi i\frac{0\cdot 3}{4}}|0\rangle + e^{2\pi i\frac{1\cdot 3}{4}}|1\rangle + e^{2\pi i\frac{2\cdot 3}{4}}|2\rangle + e^{2\pi i\frac{3\cdot 3}{4}}|3\rangle\right)/\sqrt{4}$$

Note that the initial quantum state is $x_0|0\rangle + x_1|1\rangle + x_2|2\rangle + x_3|3\rangle$.

Then QFT is equivalent to unitary transformation

$|j\rangle \to \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1} e^{2\pi i\frac{k\cdot j}{N}}|k\rangle$.

Summary of Quantum Fourier Transform

- Discrete Fourier transform (DFT)
  - Input data for DFT: $x_0, \ldots, x_{N-1}$
  - Output data of DFT: $y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi i jk/N}$
- Quantum Fourier transform (QFT)
  - Input quantum state: each input data is used as the probability amplitude of the corresponding basis $\sum_{j=0}^{N-1} x_j |j\rangle$
  - Output quantum state: has the output of DFT as the probability amplitude of the corresponding basis $\sum_{k=0}^{N-1} y_k |k\rangle$
  - $\sum_{j=0}^{N-1} x_j |j\rangle \rightarrow \sum_{k=0}^{N-1} y_k |k\rangle$
- Implementation of QFT circuit
  - Need a quantum circuit that can transform the basis ket $|0\rangle, \ldots, |N-1\rangle$ of the input quantum state in the following way: $|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i \frac{k \cdot j}{N}} |k\rangle$
  - Circuit example for QFT where $R_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix}$