Quantum Fourier Transform

School on Quantum Computing @Yagami

Day 2, Lesson 1

9:00-10:00, March 23, 2005

Eisuke Abe

Department of Applied Physics and Physico-Informatics,
and CREST-JST, Keio University

Outline

- Quantum Fourier transform
  - Definition and examples
  - Power of QFT
  - Product representation
  - Quantum circuit for QFT
- Order finding algorithm
  - Order of permutation
  - Example
  - Remarks

Quantum Fourier transform

Definition

$$|j\rangle \xrightarrow{QFT_N} \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}\exp\left(2\pi i\frac{jk}{N}\right)|k\rangle$$

We treat only $N = 2^n$

Example; $N = 2$

$$|j\rangle \xrightarrow{QFT_2} \frac{1}{\sqrt{2}}\sum_{k=0}^{1}\exp(\pi ijk)|k\rangle$$

$$= \frac{1}{\sqrt{2}}\sum_{k=0}^{1}(-1)^{jk}|k\rangle = H$$

QFT_2 is Hadamard

$$\exp(\pi ijk) = \begin{cases} 1 & (jk = 0) \\ -1 & (jk = 1) \end{cases}$$

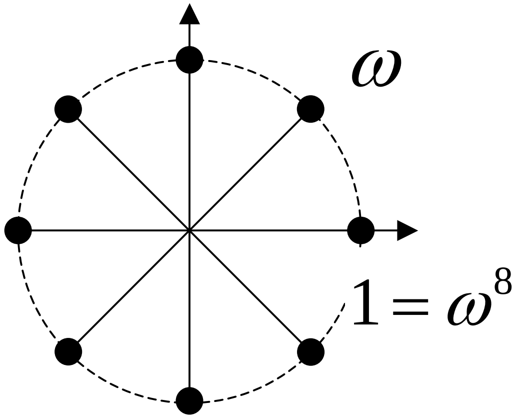
QFT_8

Example; $N = 8$

$$|j\rangle \xrightarrow{QFT_8} \frac{1}{\sqrt{8}}\sum_{k=0}^{7}\exp\left(2\pi i\frac{jk}{8}\right)|k\rangle = \frac{1}{\sqrt{8}}\sum_{k=0}^{7}\omega^{jk}|k\rangle$$

$$QFT_8 = \frac{1}{\sqrt{8}}\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega^1 & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 \\ 1 & \omega^2 & \omega^4 & \omega^6 & 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega^1 & \omega^4 & \omega^7 & \omega^2 & \omega^5 \\ 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 \\ 1 & \omega^5 & \omega^2 & \omega^7 & \omega^4 & \omega^1 & \omega^6 & \omega^3 \\ 1 & \omega^6 & \omega^4 & \omega^2 & 1 & \omega^6 & \omega^4 & \omega^2 \\ 1 & \omega^7 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega^1 \end{bmatrix}$$

$$\omega \equiv \exp(2\pi i/8) = \sqrt{i}$$



$$\omega^i + \omega^{i+4} = 0$$

QFT_8

$$\sum_{k=0}^{7}\alpha_j|j\rangle \xrightarrow{QFT_8} \sum_{k=0}^{7}\beta_k|k\rangle$$

r	input string $\{\alpha_j\}$									output string $\{\beta_k\}$								N/r
	0	1	2	3	4	5	6	7		0	1	2	3	4	5	6	7	
8	1	0	0	0	0	0	0	0	→	1	1	1	1	1	1	1	1	1
4	1	0	0	0	1	0	0	0	→	1	0	1	0	1	0	1	0	2
2	1	0	1	0	1	0	1	0	→	1	0	0	0	1	0	0	0	4
1	1	1	1	1	1	1	1	1	→	1	0	0	0	0	0	0	0	8

$$|0\rangle \rightarrow |0\rangle+|1\rangle+|2\rangle+|3\rangle+|4\rangle+|5\rangle+|6\rangle+|7\rangle$$

$$|0\rangle+|4\rangle \rightarrow |0\rangle+|2\rangle+|4\rangle+|6\rangle$$

$$|0\rangle+|2\rangle+|4\rangle+|6\rangle \rightarrow |0\rangle+|4\rangle$$

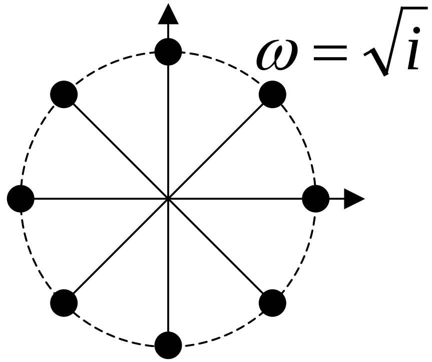
$$|0\rangle+|1\rangle+|2\rangle+|3\rangle+|4\rangle+|5\rangle+|6\rangle+|7\rangle \rightarrow |0\rangle$$

QFT inverts the periodicity

QFT_8

r	input string $\{\alpha_j\}$									output string $\{\beta_k\}$								N/r
	0	1	2	3	4	5	6	7		0	1	2	3	4	5	6	7	
4	1	0	0	0	1	0	0	0	→	1	0	1	0	1	0	1	0	2

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega^1 & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 \\ 1 & \omega^2 & \omega^4 & \omega^6 & 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega^1 & \omega^4 & \omega^7 & \omega^2 & \omega^5 \\ 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 \\ 1 & \omega^5 & \omega^2 & \omega^7 & \omega^4 & \omega^1 & \omega^6 & \omega^3 \\ 1 & \omega^6 & \omega^4 & \omega^2 & 1 & \omega^6 & \omega^4 & \omega^2 \\ 1 & \omega^7 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega^1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1+1 \\ 1+\omega^4 \\ 1+1 \\ 1+\omega^4 \\ 1+1 \\ 1+\omega^4 \\ 1+1 \\ 1+\omega^4 \end{bmatrix} // \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \end{bmatrix}$$



QFT_8

r	input string $\{\alpha_j\}$									output string $\{\beta_k\}$								N/r
	0	1	2	3	4	5	6	7		0	1	2	3	4	5	6	7	
2	1	0	1	0	1	0	1	0	→	1	0	0	0	1	0	0	0	4

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega^1 & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 \\ 1 & \omega^2 & \omega^4 & \omega^6 & 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega^1 & \omega^4 & \omega^7 & \omega^2 & \omega^5 \\ 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 \\ 1 & \omega^5 & \omega^2 & \omega^7 & \omega^4 & \omega^1 & \omega^6 & \omega^3 \\ 1 & \omega^6 & \omega^4 & \omega^2 & 1 & \omega^6 & \omega^4 & \omega^2 \\ 1 & \omega^7 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega^1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1+1+1+1 \\ 1+\omega^2+\omega^4+\omega^6 \\ 1+\omega^4+1+\omega^4 \\ 1+\omega^6+\omega^4+\omega^2 \\ 1+1+1+1 \\ 1+\omega^2+\omega^4+\omega^6 \\ 1+\omega^4+1+\omega^4 \\ 1+\omega^6+\omega^4+\omega^2 \end{bmatrix} // \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

$$\omega^i + \omega^{i+4} = 0$$

QFT_8

input string $\{\alpha_j\}$									output string $\{\beta_k\}$							
0	1	2	3	4	5	6	7		0	1	2	3	4	5	6	7
1	0	0	0	1	0	0	0	$\to$	1	0	1	0	1	0	1	0
0	1	0	0	0	1	0	0	$\to$	1	0	i	0	–1	0	i	0
0	0	1	0	0	0	1	0	$\to$	1	0	–1	0	1	0	–1	0
0	0	0	1	0	0	0	1	$\to$	1	0	$-i$	0	–1	0	i	0

Period 4

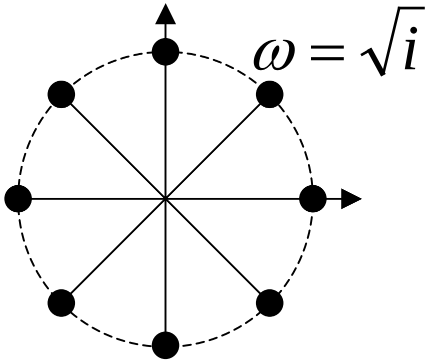
$$\begin{aligned}
|0\rangle+|4\rangle &\to |0\rangle+|2\rangle+|4\rangle+|6\rangle \\
|1\rangle+|5\rangle &\to |0\rangle+i|2\rangle-|4\rangle-i|6\rangle \\
|2\rangle+|6\rangle &\to |0\rangle-|2\rangle+|4\rangle-|6\rangle \\
|3\rangle+|7\rangle &\to |0\rangle-i|2\rangle-|4\rangle+i|6\rangle
\end{aligned}$$

Offsets in the input are converted into phase factors in the output (shift invariance)

QFT_8

input string $\{\alpha_j\}$									output string $\{\beta_k\}$							
0	1	2	3	4	5	6	7		0	1	2	3	4	5	6	7
0	1	0	0	0	1	0	0	→	1	0	i	0	–1	0	i	0

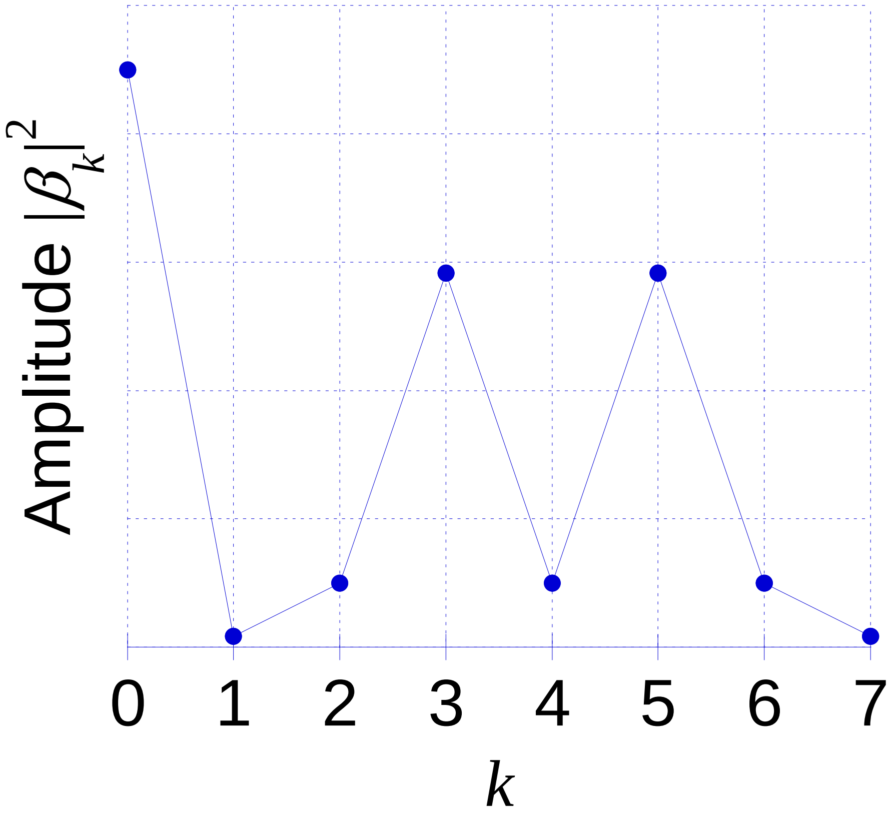
$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega^1 & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 \\ 1 & \omega^2 & \omega^4 & \omega^6 & 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega^1 & \omega^4 & \omega^7 & \omega^2 & \omega^5 \\ 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 \\ 1 & \omega^5 & \omega^2 & \omega^7 & \omega^4 & \omega^1 & \omega^6 & \omega^3 \\ 1 & \omega^6 & \omega^4 & \omega^2 & 1 & \omega^6 & \omega^4 & \omega^2 \\ 1 & \omega^7 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega^1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1+1 \\ \omega^1+\omega^5 \\ \omega^2+\omega^2 \\ \omega^3+\omega^7 \\ \omega^4+\omega^4 \\ \omega^5+\omega^1 \\ \omega^6+\omega^6 \\ \omega^7+\omega^3 \end{bmatrix} // \begin{bmatrix} 1 \\ 0 \\ i \\ 0 \\ -1 \\ 0 \\ -i \\ 0 \end{bmatrix}$$



$\omega = \sqrt{i}$

QFT_8

r	input string $\{\alpha_j\}$								N/r
	0	1	2	3	4	5	6	7	
3	1	0	0	1	0	0	1	0	2.67



If r does not divide N, the inverse of the period is approximate

Power of QFT

Our observation so far can be summarized as follows

$$\sqrt{\frac{r}{N}}\sum_{j=0}^{N/r-1}\left|\underbrace{jr}_{\text{Period}}+\underbrace{m}_{\text{Offset}}\right\rangle \xrightarrow{QFT_N} \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}\underbrace{\exp\left(2\pi i\frac{mk}{r}\right)}_{\text{Phase}}\left|\underbrace{\frac{N}{r}}_{\text{Inverse of the period}}k\right\rangle$$

In the next few slides, we simply assume r divides N

Power of QFT

Proof

$$\sqrt{\frac{r}{N}}\sum_{j=0}^{N/r-1}\left| jr+m\right\rangle$$

$$\left| j\right\rangle \to \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}\exp\left(2\pi i\frac{jk}{N}\right)\left| k\right\rangle$$

$$\to \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}\sqrt{\frac{r}{N}}\sum_{j=0}^{N/r-1}\exp\left(2\pi i\frac{(jr+m)k}{N}\right)\left| k\right\rangle$$

$$\to \frac{\sqrt{r}}{N}\sum_{k=0}^{N-1}\exp\left(2\pi i\frac{mk}{N}\right)\underline{\sum_{j=0}^{N/r-1}\exp\left(2\pi i\frac{jrk}{N}\right)\left| k\right\rangle}$$

2 cases; k divides N/r or not

Power of QFT

Case 1 $k = \frac{N}{r} k'$

Constructive interference

$$\sum_{j=0}^{N/r-1} \exp\left(2\pi i \frac{jrk}{N}\right) = \sum_{j=0}^{N/r-1} \exp(2\pi i j k') = \frac{N}{r}$$

$$\exp(2\pi i j k') = 1$$

$$\frac{\sqrt{r}}{N} \sum_{k=0}^{N-1} \exp\left(2\pi i \frac{mk}{N}\right) \sum_{j=0}^{N/r-1} \exp\left(2\pi i \frac{jrk}{N}\right) |k\rangle$$

$$= \frac{\sqrt{r}}{N} \sum_{k'=0}^{r-1} \exp\left(2\pi i \frac{m}{N} \frac{N}{r} k'\right) \times \frac{N}{r} \times \left| \frac{N}{r} k' \right\rangle$$

$$= \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\left(2\pi i \frac{mk}{r}\right) \left| \frac{N}{r} k \right\rangle$$

$k : 0 \rightarrow N - 1$

$k' : 0 \rightarrow r - 1$

Power of QFT

Case 2 $k \neq \frac{N}{r} k'$

$$\lambda \equiv \exp\left(2\pi i \frac{rk}{N}\right)$$

$$\sum_{j=0}^{N/r-1} \lambda^j = \frac{1-\lambda^{N/r}}{1-\lambda} = 0$$

$$\sum_{j=0}^{N/r-1} \exp\left(2\pi i \frac{jrk}{N}\right) = \sum_{j=0}^{N/r-1} \lambda^j = 0$$

Destructive interference

Combining Case 1 & 2, we obtain

$$\sqrt{\frac{r}{N}} \sum_{j=0}^{N/r-1} \left| jr + m \right\rangle \xrightarrow{QFT_N} \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\left(2\pi i \frac{mk}{r}\right) \left| \frac{N}{r} k \right\rangle$$

Again, quantum interference is the key

Product representation

$$\left|j_1 j_2 \cdots j_n\right\rangle$$

$$\rightarrow \frac{\left(\left|0\right\rangle + \exp(2\pi i 0.j_n)\left|1\right\rangle\right)\left(\left|0\right\rangle + \exp(2\pi i 0.j_{n-1}j_n)\left|1\right\rangle\right)\cdots\left(\left|0\right\rangle + \exp(2\pi i 0.j_1 j_2 \cdots j_n)\left|1\right\rangle\right)}{2^{n/2}}$$

Notation

$$j = j_1 j_2 \cdots j_n = j_1 2^{n-1} + j_2 2^{n-2} + \cdots + j_n 2^0 = \sum_{k=1}^{n} j_k 2^{n-k}$$

$$0.j_1 j_2 \cdots j_n = j_1 2^{-1} + j_2 2^{-2} + \cdots + j_n 2^{-n} = \sum_{k=1}^{n} j_k 2^{-k}$$

This representation provides a natural way to construct a quantum circuit for QFT, and a proof that QFT is unitary

Product representation

$$|j\rangle$$

$$\rightarrow \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} \exp(2\pi ijk/2^n)|k\rangle$$

$$= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} \exp(2\pi ij \sum_{l=1}^{n} k_l 2^{-l})|k_1 \cdots k_n\rangle$$

$$= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} \bigotimes_{l=1}^{n} \exp(2\pi ijk_l 2^{-l})|k_l\rangle$$

$$= \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \left[\sum_{k_l=0}^{1} \exp(2\pi ijk_l 2^{-l})|k_l\rangle \right]$$

$$= \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \left[|0\rangle + \exp(2\pi ij2^{-l})|1\rangle \right]$$

$$= \frac{1}{2^{n/2}} \left(|0\rangle + e^{2\pi i0.j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i0.j_{n-1}j_n}|1\rangle\right)\cdots\left(|0\rangle + e^{2\pi i0.j_1j_2\cdots j_n}|1\rangle\right)$$

$$\frac{k}{2^n} = \frac{1}{2^n} \sum_{l=1}^{n} k_l 2^{n-l} = \sum_{l=1}^{n} k_l 2^{-l}$$

$$\exp(\alpha_1 + \alpha_2)|k_1\rangle \otimes |k_2\rangle$$

$$= \left[\exp(\alpha_1)|k_1\rangle\right] \otimes \left[\exp(\alpha_2)|k_2\rangle\right]$$

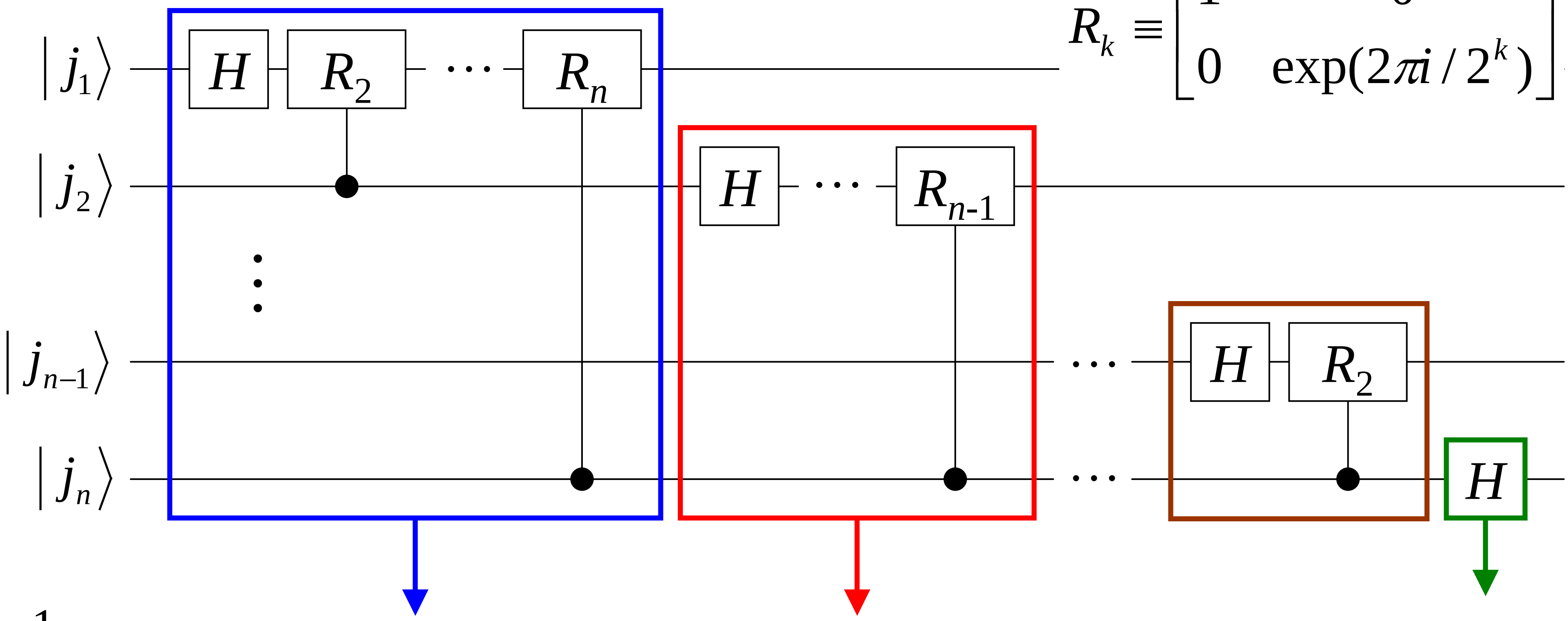
$$\sum_{k_1=0}^{1} \sum_{k_2=0}^{1} \left[\exp(\alpha_1)|k_1\rangle \otimes \exp(\alpha_2)|k_2\rangle\right]$$

$$= \left[\sum_{k_1=0}^{1} \exp(\alpha_1)|k_1\rangle\right] \otimes \left[\sum_{k_2=0}^{1} \exp(\alpha_2)|k_2\rangle\right]$$

$$j2^{-l} = j_1 \cdots j_{n-l}.j_{n-l+1} \cdots j_n$$

$$\exp(2\pi ij_1 \cdots j_{n-l}) = 1$$

Quantum circuit for QFT



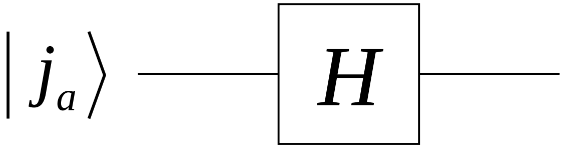
$$R_k \equiv \begin{bmatrix} 1 & 0 \\ 0 & \exp(2\pi i/2^k) \end{bmatrix}$$

$$\frac{1}{2^{n/2}}\underline{(|0\rangle+\exp(2\pi i0.j_1j_2\cdots j_n)|1\rangle)}\underline{(|0\rangle+\exp(2\pi i0.j_2\cdots j_n)|1\rangle)}\cdots\underline{(|0\rangle+\exp(2\pi i0.j_n)|1\rangle)}$$

SWAP

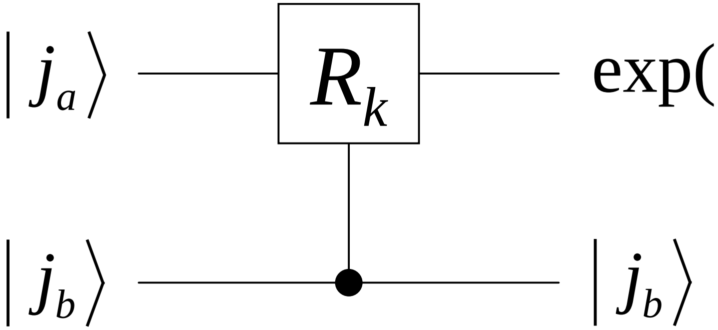
$$\frac{1}{2^{n/2}}\underline{(|0\rangle+\exp(2\pi i0.j_n)|1\rangle)}\underline{(|0\rangle+\exp(2\pi i0.j_{n-1}j_n)|1\rangle)}\cdots\underline{(|0\rangle+\exp(2\pi i0.j_1j_2\cdots j_n)|1\rangle)}$$

Quantum circuit for QFT



$$\frac{|0\rangle + \exp(2\pi i 0.j_a)|1\rangle}{\sqrt{2}}$$

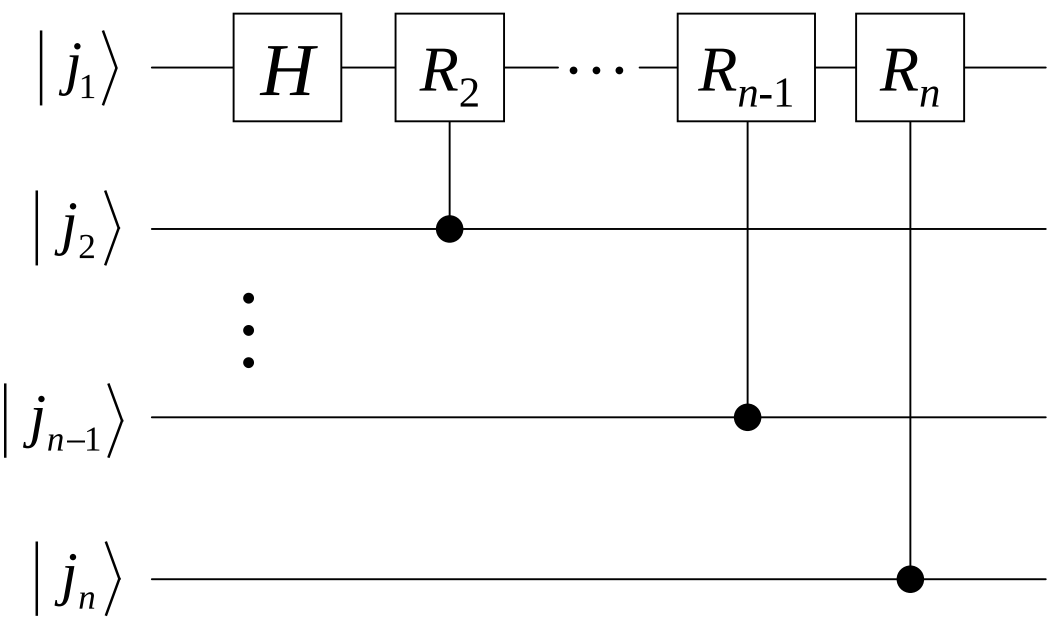
$$\exp(2\pi i 0.j_a) = \begin{cases} 1 & (j_a = 0) \\ -1 & (j_a = 1) \end{cases}$$



$$\exp(2\pi i 0.\underbrace{0\cdots 0\, j_b}_{k \text{ digits}})|j_a\rangle$$

$$\exp(2\pi i 0.0\cdots 0\, j_b) = \begin{cases} 1 & (j_a = 0) \\ \exp(2\pi i / 2^k) & (j_a = 1) \end{cases}$$

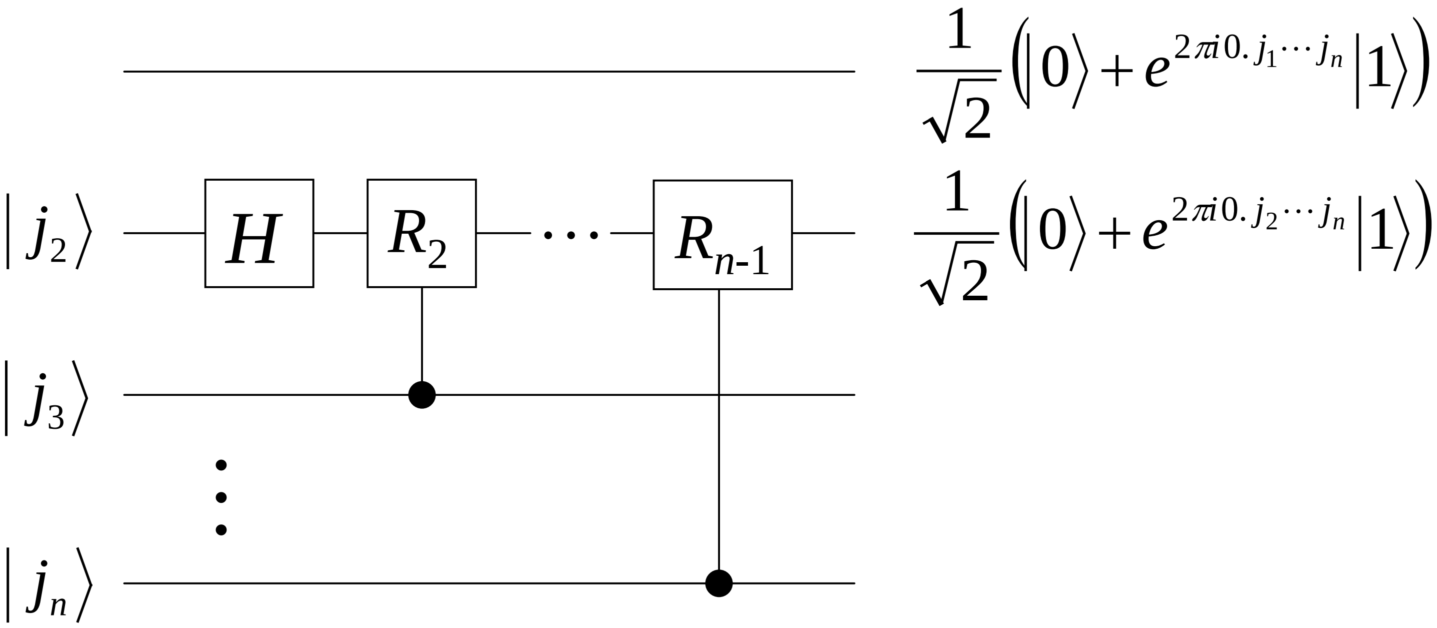
Quantum circuit for QFT



$$\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i 0.j_1\cdots j_n}|1\rangle\right)$$

$$\begin{aligned}
|\underline{j_1} j_2 \cdots j_n\rangle \quad &\rightarrow \quad \frac{1}{\sqrt{2}}\underline{\left(|0\rangle + \exp(2\pi i 0.j_1)|1\rangle\right)}|j_2 \cdots j_n\rangle \\
&\rightarrow \quad \frac{1}{\sqrt{2}}\left(|0\rangle + \exp(2\pi i \underline{0.j_1 j_2})|1\rangle\right)|j_2 \cdots j_n\rangle \\
&\vdots \\
&\rightarrow \quad \frac{1}{\sqrt{2}}\left(|0\rangle + \exp(2\pi i \underline{0.j_1 j_2 \cdots j_n})|1\rangle\right)|j_2 \cdots j_n\rangle
\end{aligned}$$

Quantum circuit for QFT



$$\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i 0.j_1 \cdots j_n}|1\rangle\right)$$

$$\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i 0.j_2 \cdots j_n}|1\rangle\right)$$

$$\frac{1}{\sqrt{2}}\left(|0\rangle + \exp(2\pi i 0.j_1 \cdots j_n)|1\rangle\right)|\underline{j_2}\, j_3 \cdots j_n\rangle$$

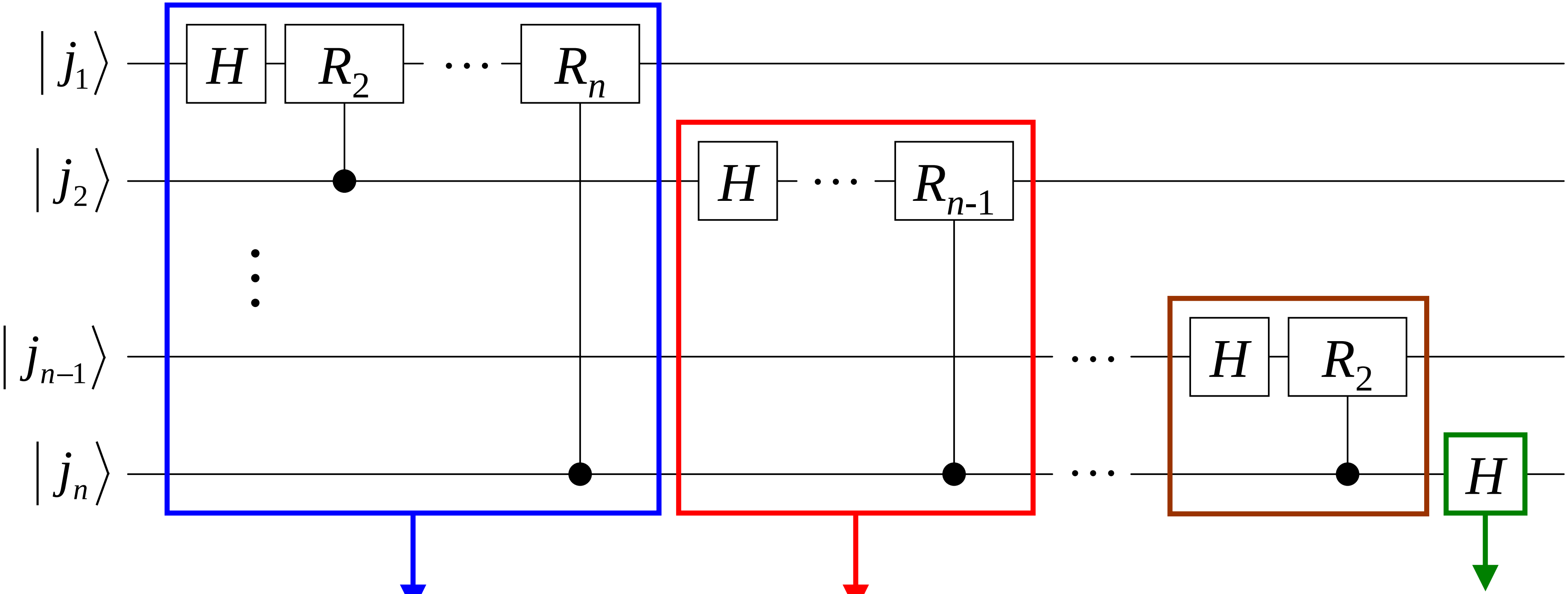
$$\to \quad \frac{1}{\sqrt{2}}\left(|0\rangle + \exp(2\pi i 0.j_1 \cdots j_n)|1\rangle\right)\frac{1}{\sqrt{2}}\underline{\left(|0\rangle + \exp(2\pi i 0.j_2)|1\rangle\right)}|j_3 \cdots j_n\rangle$$

$$\to \quad \frac{1}{2}\left(|0\rangle + \exp(2\pi i 0.j_1 \cdots j_n)|1\rangle\right)\left(|0\rangle + \exp(2\pi i \underline{0.j_2 j_3)}|1\rangle\right)|j_3 \cdots j_n\rangle$$

$$\vdots$$

$$\to \quad \frac{1}{2}\left(|0\rangle + \exp(2\pi i 0.j_1 \cdots j_n)|1\rangle\right)\left(|0\rangle + \exp(2\pi i \underline{0.j_2 \cdots j_n)}|1\rangle\right)|j_3 \cdots j_n\rangle$$

Quantum circuit for QFT



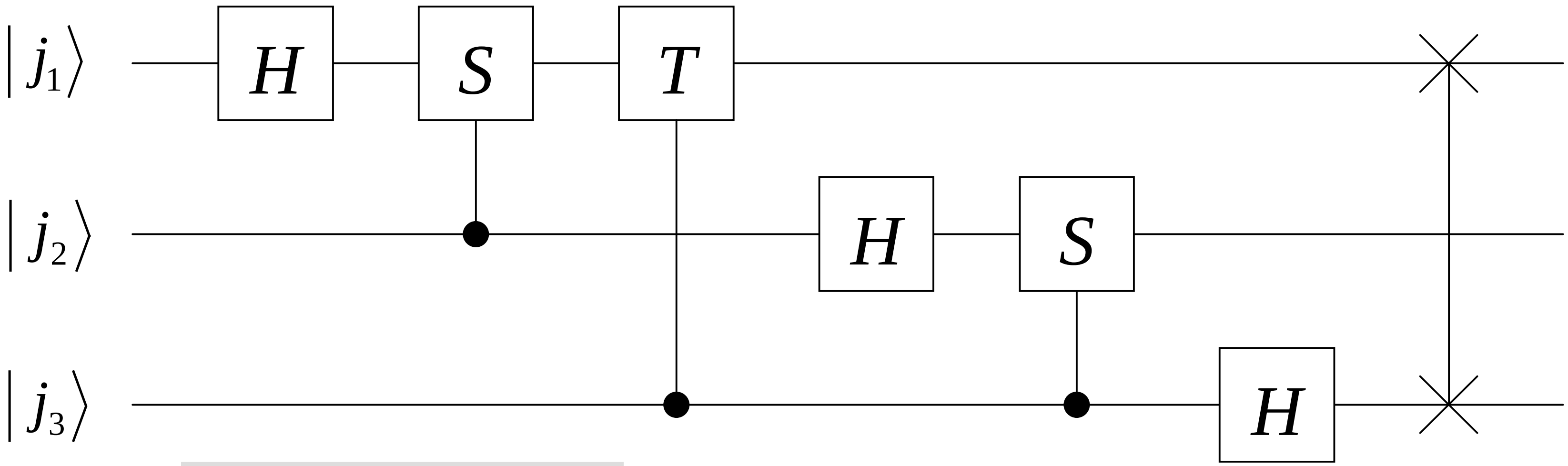
$$\frac{1}{2^{n/2}}\underline{\left(|0\rangle+\exp(2\pi i0.j_1j_2\cdots j_n)|1\rangle\right)}\underline{\left(|0\rangle+\exp(2\pi i0.j_2\cdots j_n)|1\rangle\right)}\cdots\underline{\left(|0\rangle+\exp(2\pi i0.j_n)|1\rangle\right)}$$

SWAP

$$\frac{1}{2^{n/2}}\underline{\left(|0\rangle+\exp(2\pi i0.j_n)|1\rangle\right)}\underline{\left(|0\rangle+\exp(2\pi i0.j_{n-1}j_n)|1\rangle\right)}\cdots\underline{\left(|0\rangle+\exp(2\pi i0.j_1j_2\cdots j_n)|1\rangle\right)}$$

Quantum circuit for QFT_8

$$\frac{1}{\sqrt{8}}\left(|0\rangle + e^{2\pi i 0.j_3}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_2 j_3}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_1 j_2 j_3}|1\rangle\right)$$



$$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} = R_2$$

$$T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix} = R_3$$

Order of permutation

y	$\pi(y)$
0	3
1	7
2	5
3	1
4	2
5	4
6	6
7	0

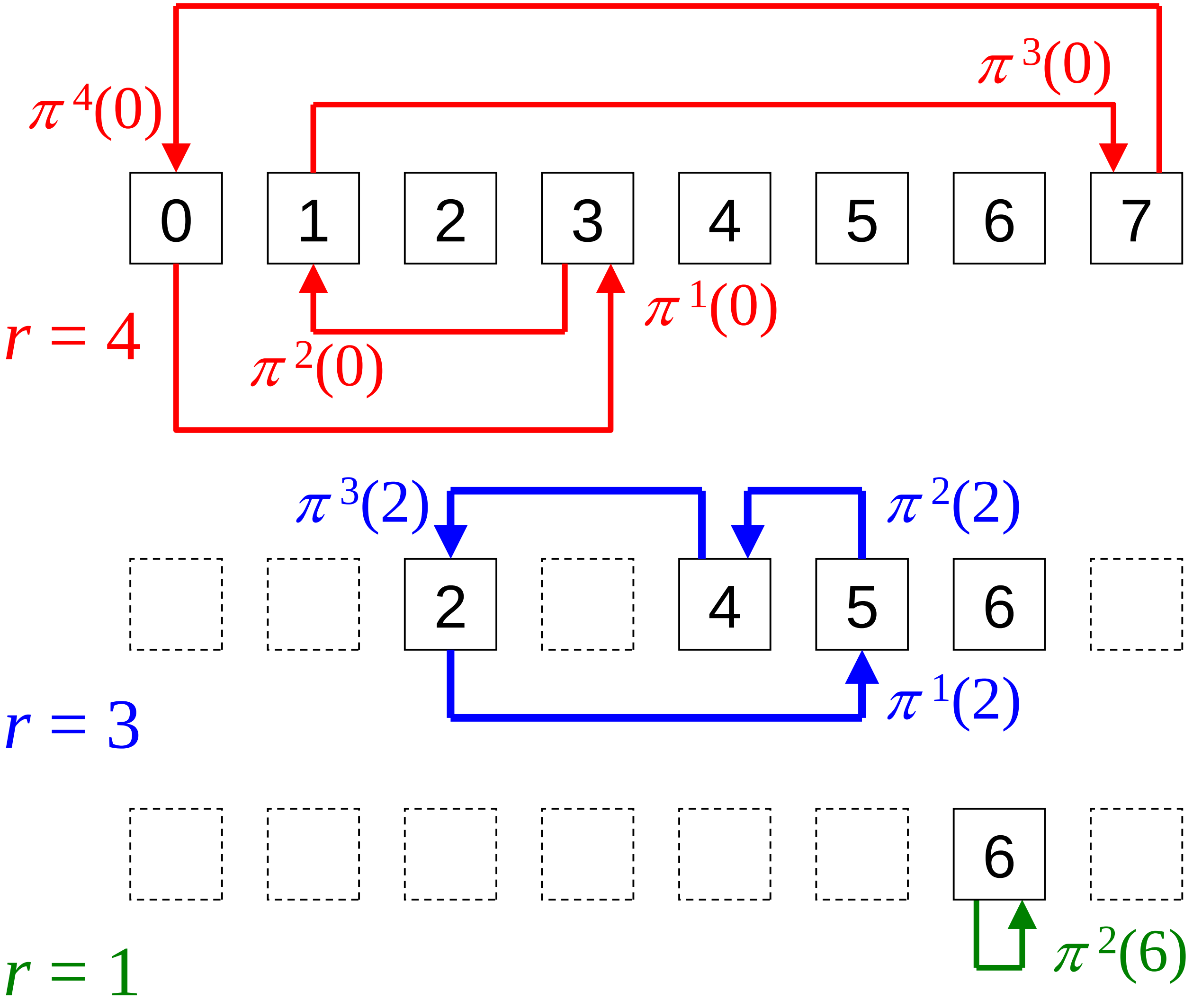
Order of the permutation $\pi(y)$; the least positive integer r that satisfies

$$\pi^r(y_0) = y_0$$

Generally, r depends on y_0, and finding r may be hard

Order of permutation

y	$\pi(y)$
0	3
1	7
2	5
3	1
4	2
5	4
6	6
7	0

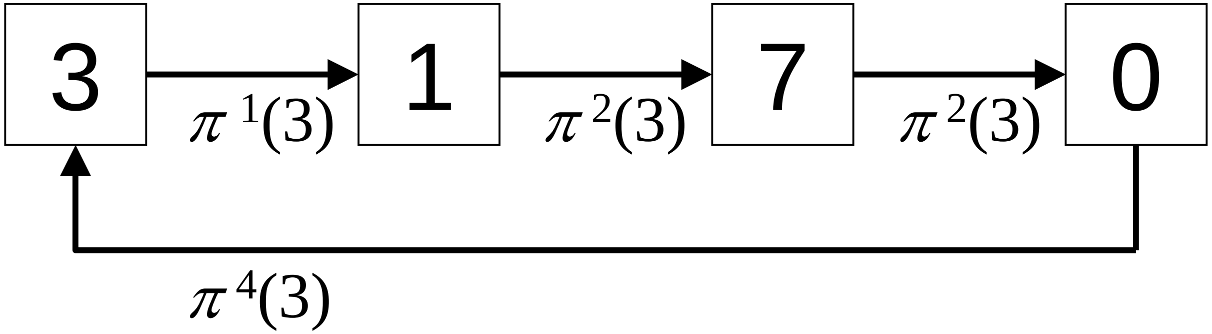


Order finding

y	$\pi(y)$
0	3
1	7
2	5
3	1
4	2
5	4
6	6
7	0

$r = 4$

Find r quantum mechanically



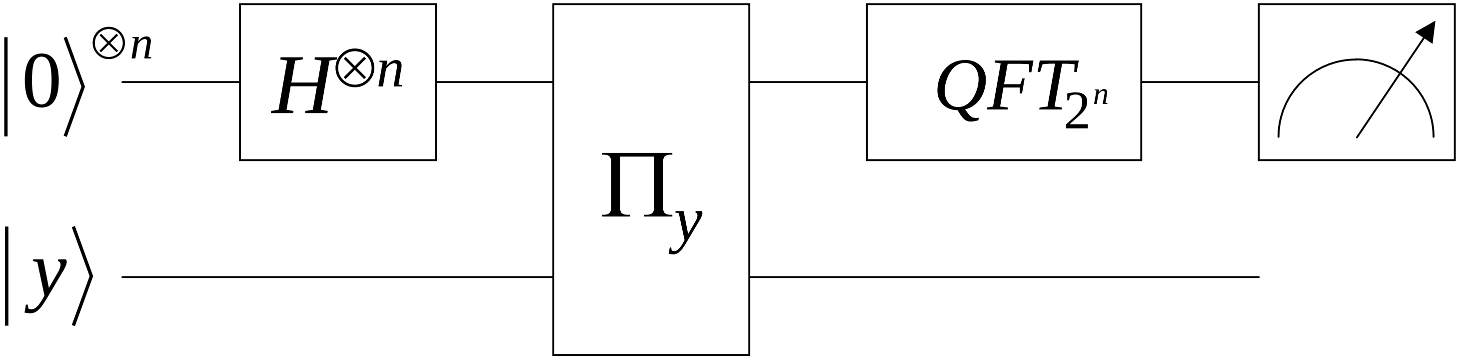
$$\pi^0(3) = \pi^4(3) = \pi^8(3) = \pi^{12}(3) = \cdots = 3$$

$$\pi^1(3) = \pi^5(3) = \pi^9(3) = \pi^{13}(3) = \cdots = 1$$

$$\pi^2(3) = \pi^6(3) = \pi^{10}(3) = \pi^{14}(3) = \cdots = 7$$

$$\pi^3(3) = \pi^7(3) = \pi^{11}(3) = \pi^{15}(3) = \cdots = 0$$

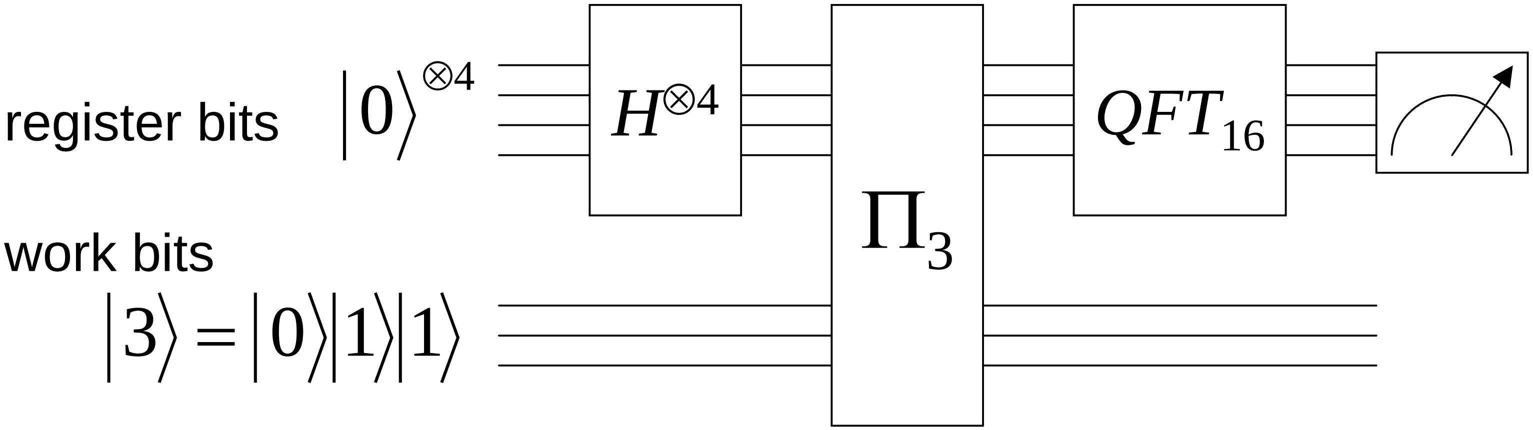
Order finding algorithm



$$\Pi_y |x\rangle |y\rangle = |x\rangle \left| \pi^x(y) \right\rangle$$

For now, we accept that Π_y is given as a ***black box***, or imagine a situation similar to ***Deutsch's problem*** (i.e., Alice wants to know the order, and Bob has $\pi(y)$)

Order finding algorithm



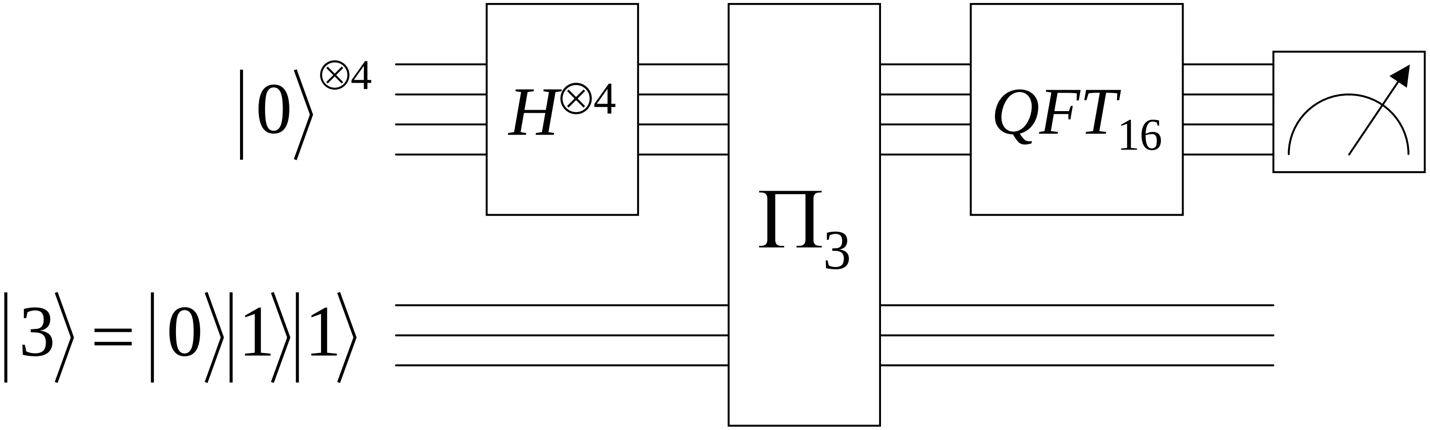
$$|0\rangle^{\otimes 4}|3\rangle \xrightarrow{H^{\otimes 4}} \frac{1}{4}\sum_{x=0}^{15}|x\rangle|3\rangle$$

$$\Pi_3|x\rangle|3\rangle = |x\rangle|\pi^x(3)\rangle$$

$$\xrightarrow{\Pi_3} \frac{1}{4}\sum_{x=0}^{15}|x\rangle|\pi^x(3)\rangle$$

Encode information on $\pi^x(3)$ into the work bits

Order finding algorithm



$$\sum_{x=0}^{15}|x\rangle|\pi^{x}(3)\rangle = \left(|0\rangle+|4\rangle+|8\rangle+|12\rangle\right)|3\rangle+\left(|1\rangle+|5\rangle+|9\rangle+|13\rangle\right)|1\rangle$$

$$+\left(|2\rangle+|6\rangle+|10\rangle+|14\rangle\right)|7\rangle+\left(|3\rangle+|7\rangle+|11\rangle+|15\rangle\right)|0\rangle$$

$$\xrightarrow{QFT_{16}}$$

$$\left(|0\rangle+|4\rangle+|8\rangle+|12\rangle\right)|3\rangle+$$

$$\left(|0\rangle+i|4\rangle-|8\rangle-i|12\rangle\right)|1\rangle+$$

$$\left(|0\rangle-|4\rangle+|8\rangle-|12\rangle\right)|7\rangle+$$

$$\left(|0\rangle-i|4\rangle-|8\rangle+|12\rangle\right)|0\rangle$$

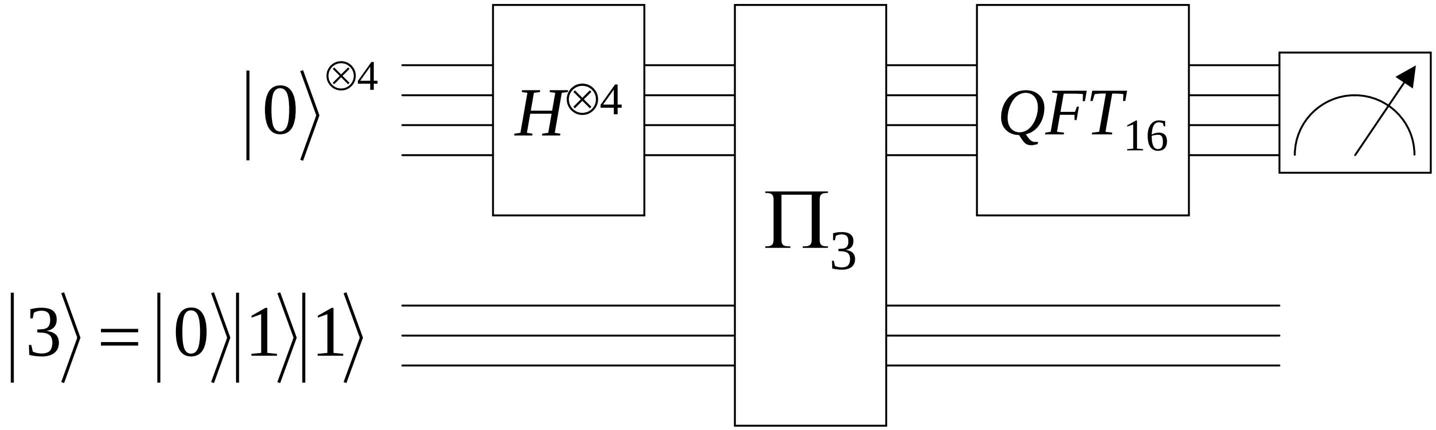
$$\pi^{0}(3)=\pi^{4}(3)=\pi^{8}(3)=\pi^{12}(3)=\cdots=3$$

$$\pi^{1}(3)=\pi^{5}(3)=\pi^{9}(3)=\pi^{13}(3)=\cdots=1$$

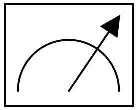
$$\pi^{2}(3)=\pi^{6}(3)=\pi^{10}(3)=\pi^{14}(3)=\cdots=7$$

$$\pi^{3}(3)=\pi^{7}(3)=\pi^{11}(3)=\pi^{15}(3)=\cdots=0$$

Order finding algorithm



$$\begin{aligned}&(|0\rangle+|4\rangle+|8\rangle+|12\rangle)|3\rangle+\\&(|0\rangle+i|4\rangle-|8\rangle-i|12\rangle)|1\rangle+\\&(|0\rangle-|4\rangle+|8\rangle-|12\rangle)|7\rangle+\\&(|0\rangle-i|4\rangle-|8\rangle+|12\rangle)|0\rangle\end{aligned}$$



$\longrightarrow$ Either 0, 4, 8, 12

$$\sqrt{\frac{r}{N}}\sum_{j=0}^{N/r-1}\left|jr+m\right\rangle \xrightarrow{QFT_N} \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}\exp\left(2\pi i\frac{mk}{r}\right)\left|\frac{N}{r}k\right\rangle$$

Order finding algorithm

$$\frac{16k}{r}=\begin{cases}0\\4\\8\\12\end{cases}\Rightarrow\quad\frac{k}{r}=\begin{cases}0 & \textbf{\textit{Fail}}\text{ (No info. on } r\text{)}\\1/4 & \textbf{\textit{Succeed}}\\1/2 & \textbf{\textit{Fail}}\text{ (Wrong } r\text{)}\\3/4 & \textbf{\textit{Succeed}}\end{cases}$$

The algorithm fails if $k=0$, or k and r have common divisors (Not so serious)

$$\mathrm{Prob}(\gcd(k/r)=1)\approx\frac{1}{\log\log r}$$

Remaining issues

- The measurement does not give us r itself, then how to obtain r out of the measurement result?
- What if r does not divide N?
- How to construct the Π_y gate?
- If it remains a black box, how can the algorithm be useful?

Quiz

Continued fraction expansion

Definition

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_{m-1} + \cfrac{1}{a_m}}}}$$

$$\equiv [a_0, a_1, \cdots, a_m]$$

"Convergent"

$$\frac{p_0}{q_0} = [a_0] = a_0$$

$$\frac{p_1}{q_1} = [a_0, a_1] = a_0 + \frac{1}{a_1}$$

$$\vdots$$

$$\frac{p_{m-1}}{q_{m-1}} = [a_0, a_1, \cdots, a_{m-1}]$$

$$\frac{p_m}{q_m} = [a_0, a_1, \cdots, a_{m-1}, a_m]$$

Quiz

Check that the continued fraction expansion for 31/13 and its convergents are given as follows

$$\frac{31}{13}=[2,2,1,1,2]=2+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{2}}}}$$

$$\frac{p_0}{q_0}=[2]=2$$

$$\frac{p_1}{q_1}=[2,2]=\frac{5}{2}$$

$$\frac{p_2}{q_2}=[2,2,1]=\frac{7}{3}$$

$$\frac{p_3}{q_3}=[2,2,1,1]=\frac{12}{5}$$

$$\frac{p_4}{q_4}=[2,2,1,1,2]=\frac{31}{13}$$

Also check the following

$$\frac{3413}{8192}=[0,2,2,2,170,4]$$