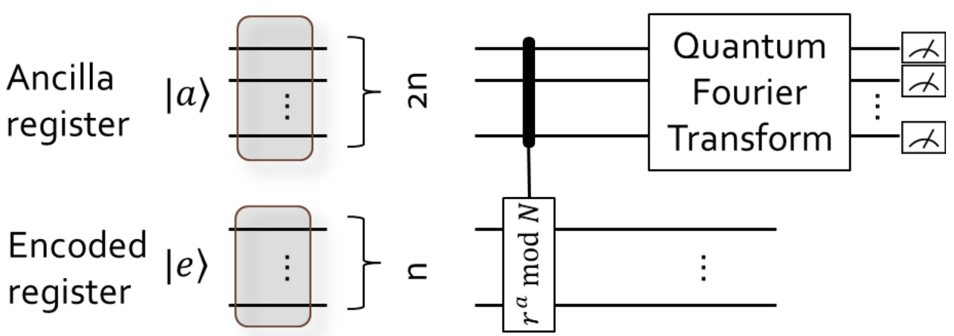
Shor's Algorithm (Factoring algorithm)

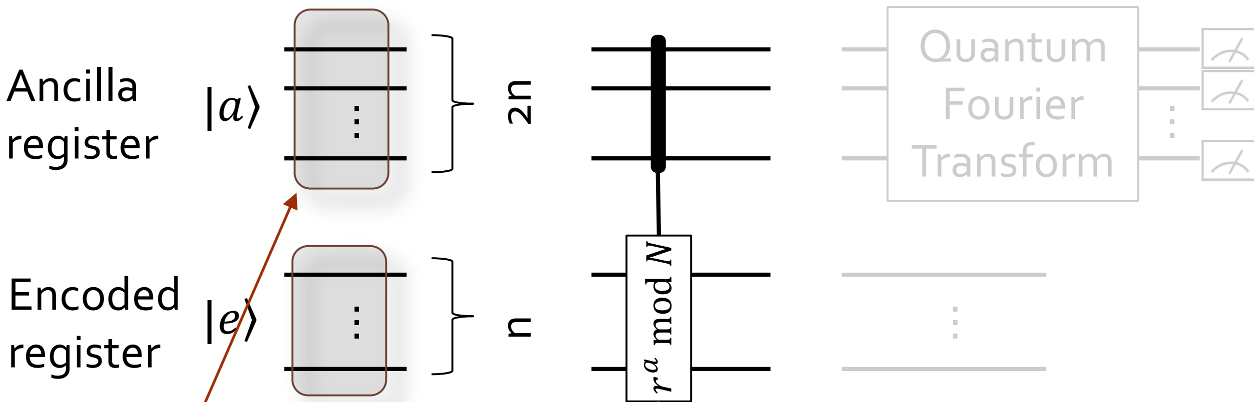
- Chapter 5
- Example for factorization of number 15
  - Choose a random number that has the following properties
    - No common divisor with 15 (target of factorization)
    - Smaller than 15 (target of factorization)
    - Ex) $r = 7$
  - Calculate $r^a (\mathrm{mod}\ 15)$ for all a between 0 and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

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



Analysis of Factorization Process I



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

$\otimes$

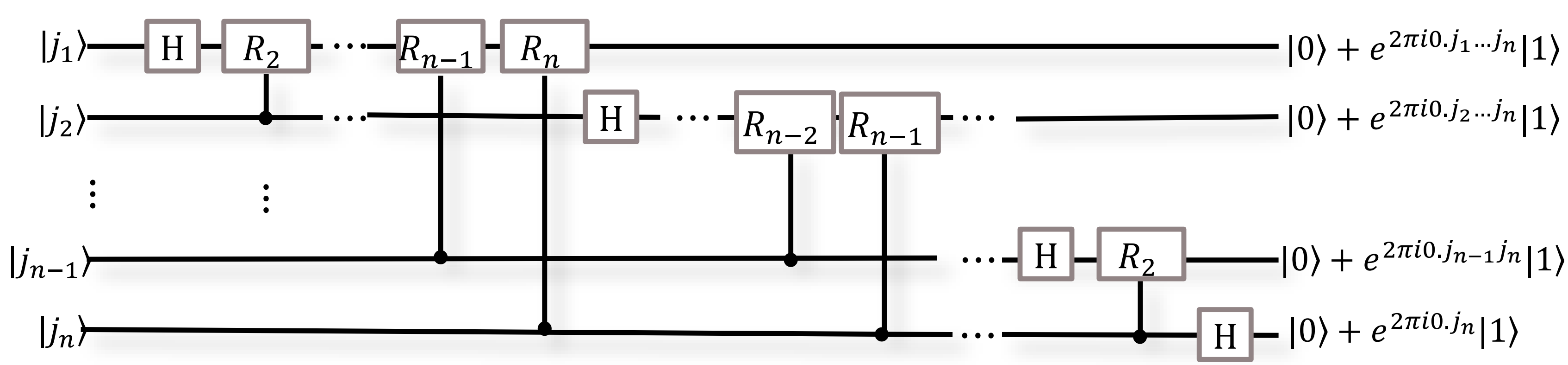
$|e\rangle = |1\rangle_e$

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

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

Summary of Quantum Fourier Transform

- Discrete Fourier transform (DFT)
  - Input data for DFT: $x_0, \dots, x_{N-1}$
  - 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 $|0\rangle, \dots, |N-1\rangle$ 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 $R_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix}$



Derivation of QFT circuit I

- Section 5.1
- $N = 2^n$
- $j = j_1 j_2 \dots j_n = j_1 2^{n-1} + j_2 2^{n-2} + \cdots + j_n 2^0$
- $0.j_l j_{l+1} \dots j_m = j_l/2 + j_{l+1}/2^2 + \cdots + j_m/2^{m-l+1}$
- QFT: $|j_1, \dots, j_n\rangle \rightarrow \frac{1}{2^{n/2}}\left(|0\rangle + e^{2\pi i 0.j_n}|1\rangle\right) \cdot \left(|0\rangle + e^{2\pi i 0.j_{n-1}j_n}|1\rangle\right) \dots \left(|0\rangle + e^{2\pi i 0.j_1 j_2 \dots j_n}|1\rangle\right)$

$$
\begin{aligned}
|j\rangle &\rightarrow \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{2\pi i jk/2^n} |k\rangle \\
&= \frac{1}{2^{n/2}} \sum_{k=0}^{1} \cdots \sum_{k_n=0}^{1} e^{2\pi i j \sum_{l=1}^{n} k_l 2^{-l}} |k_1 \dots k_n\rangle \\
&= \frac{1}{2^{n/2}} \sum_{k=0}^{1} \cdots \sum_{k_n=0}^{1} \bigotimes_{l=1}^{n} e^{2\pi i j k_l 2^{-l}} |k_l\rangle \\
&= \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \left[\sum_{k_l=0}^{1} e^{2\pi i j k_l 2^{-l}} |k_l\rangle\right] \\
&= \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \left[|0\rangle + e^{2\pi i j 2^{-l}} |1\rangle\right] \\
&= \frac{\left(|0\rangle + e^{2\pi i 0.j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_{n-1}j_n}|1\rangle\right) \cdots \left(|0\rangle + e^{2\pi i 0.j_1 j_2 \dots j_n}|1\rangle\right)}{2^{n/2}}
\end{aligned}
$$

Derivation of QFT circuit II

- Example for $N = 2^2 = 4$
- $|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i \frac{k \cdot j}{N}} |k\rangle = \frac{1}{2}\left(e^{2\pi i \frac{0 \cdot j}{4}} |00_2\rangle + e^{2\pi i \frac{1 \cdot j}{4}} |01_2\rangle + e^{2\pi i \frac{2 \cdot j}{4}} |10_2\rangle + e^{2\pi i \frac{3 \cdot j}{4}} |11_2\rangle\right)$
- $|j = 0\rangle \rightarrow \frac{1}{2}(|0\rangle|0\rangle + |0\rangle|1\rangle + |1\rangle|0\rangle + |1\rangle|1\rangle) = \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)$
- $|j = 1\rangle \rightarrow \frac{1}{2}\left(e^{2\pi i \frac{(0 \cdot 2^1 + 0 \cdot 2^0) \cdot 1}{4}} |0\rangle|0\rangle + e^{2\pi i \frac{(0 \cdot 2^1 + 1 \cdot 2^0) \cdot 1}{4}} |0\rangle|1\rangle + e^{2\pi i \frac{(1 \cdot 2^1 + 0 \cdot 2^0) \cdot 1}{4}} |1\rangle|0\rangle + e^{2\pi i \frac{(1 \cdot 2^1 + 1 \cdot 2^0) \cdot 1}{4}} |1\rangle|1\rangle\right)$

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

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

- $|j\rangle \rightarrow \frac{1}{2}\left(|0\rangle + e^{2\pi i \frac{2^1 \cdot j}{4}} |1\rangle\right)\left(|0\rangle + e^{2\pi i \frac{2^0 \cdot j}{4}} |1\rangle\right)$

Derivation of QFT circuit III

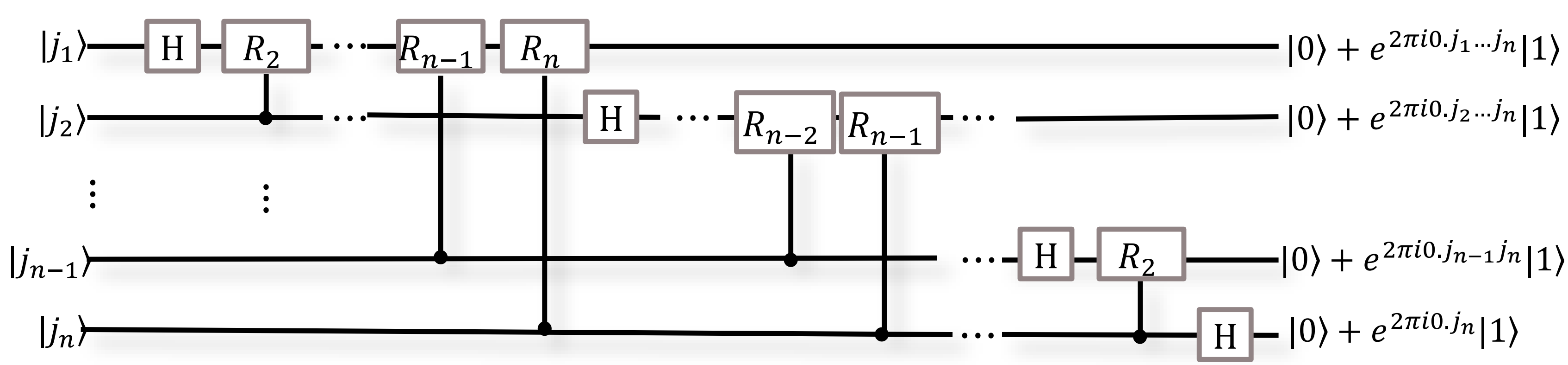
- Generally we want $|j\rangle \rightarrow \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1} e^{2\pi i\frac{k\cdot j}{N}}|k\rangle$
- From the previous page, for $n = 2$ and $N = 2^n = 4$, $|j\rangle \rightarrow \frac{1}{2}\left(|0\rangle + e^{2\pi i\frac{2^1\cdot j}{4}}|1\rangle\right)\left(|0\rangle + e^{2\pi i\frac{2^0\cdot j}{4}}|1\rangle\right)$
- For $n = 3$, $|j\rangle \rightarrow \frac{1}{\sqrt{8}}\left(|0\rangle + \boxed{e^{2\pi i\frac{2^2\cdot j}{8}}}|1\rangle\right)\left(|0\rangle + e^{2\pi i\frac{2^1\cdot j}{8}}|1\rangle\right)\left(|0\rangle + e^{2\pi i\frac{2^0\cdot j}{8}}|1\rangle\right)$
  - When $j = 111_2$, $\frac{2^2\cdot j}{8} = \frac{2^2\cdot(1\cdot 2^2+1\cdot 2^1+1\cdot 2^0)}{2^3} = \frac{\boxed{1\cdot 2^4+1\cdot 2^3}+1\cdot 2^2}{2^3}$.
  - As the exponent of $e^{2\pi i\frac{2^2\cdot j}{8}}$, $1 \cdot 2^4 + 1 \cdot 2^3$ in the numerator is meaningless. Why?
  - Therefore, when $j = j_1 j_2 j_3$,

$$\frac{1}{\sqrt{8}}\left(|0\rangle + e^{2\pi i\frac{j_3}{2}}|1\rangle\right)\left(|0\rangle + e^{2\pi i\frac{j_2 j_3}{4}}|1\rangle\right)\left(|0\rangle + e^{2\pi i\frac{j_1 j_2 j_3}{8}}|1\rangle\right)$$

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

Summary of Quantum Fourier Transform

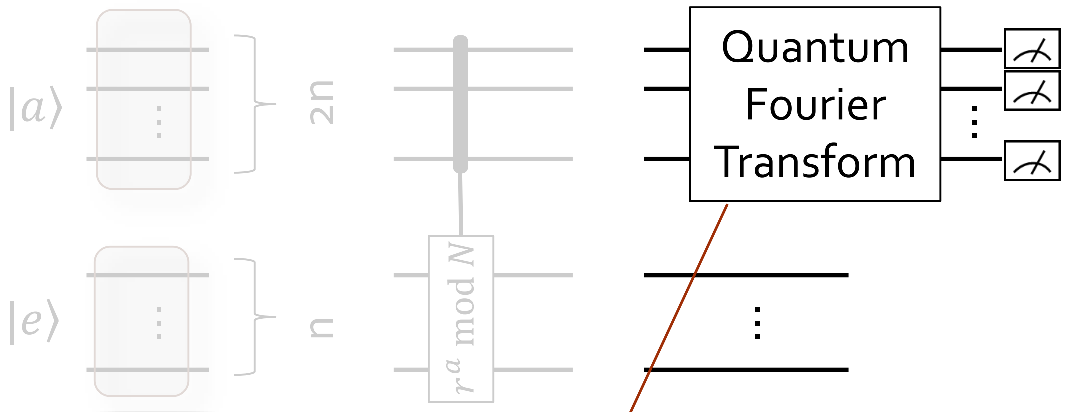
- Discrete Fourier transform (DFT)
  - Input data for DFT: $x_0, \dots, x_{N-1}$
  - Output data of DFT: $y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi ijk/N}$
- Quantum Fourier transform (QFT)
  - Input quantum state: each input data is used as the probability amplitude of the corresponding 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 $|0\rangle, \dots, |N-1\rangle$ 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 $R_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix}$



Analysis of Factorization Process II

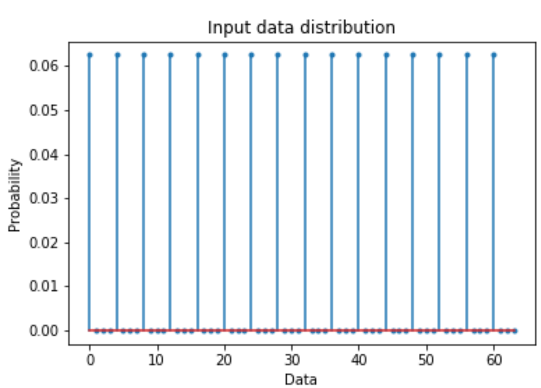
Ancilla register

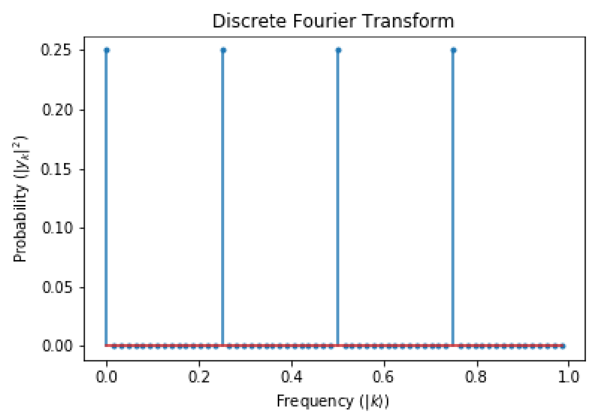
Encoded register



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

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



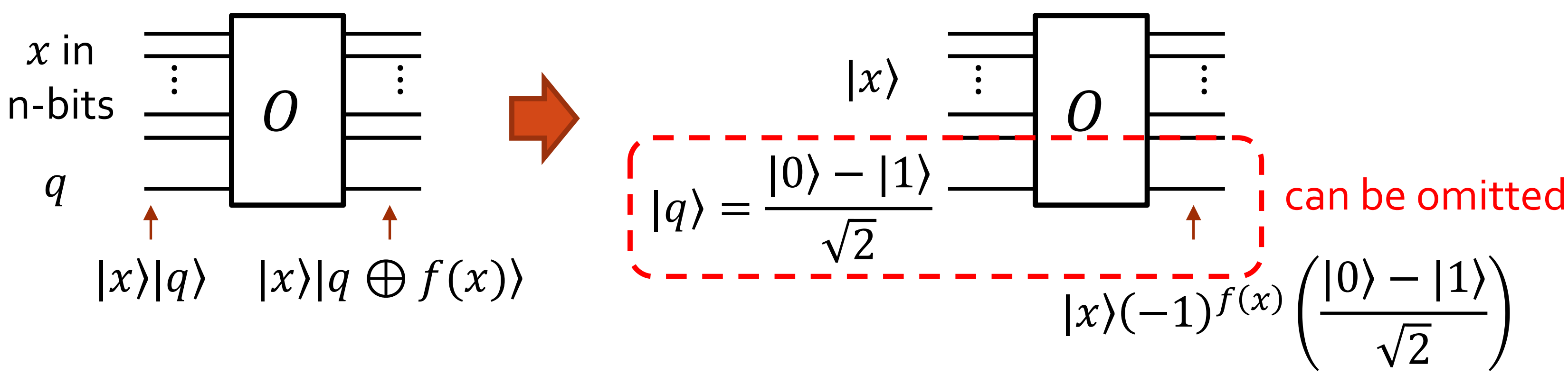


If $|k=192\rangle$ quantum state is measured, the corresponding frequency is 192/256=3/4. From this value, we can learn that there exist a high probability that the period is 4.

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

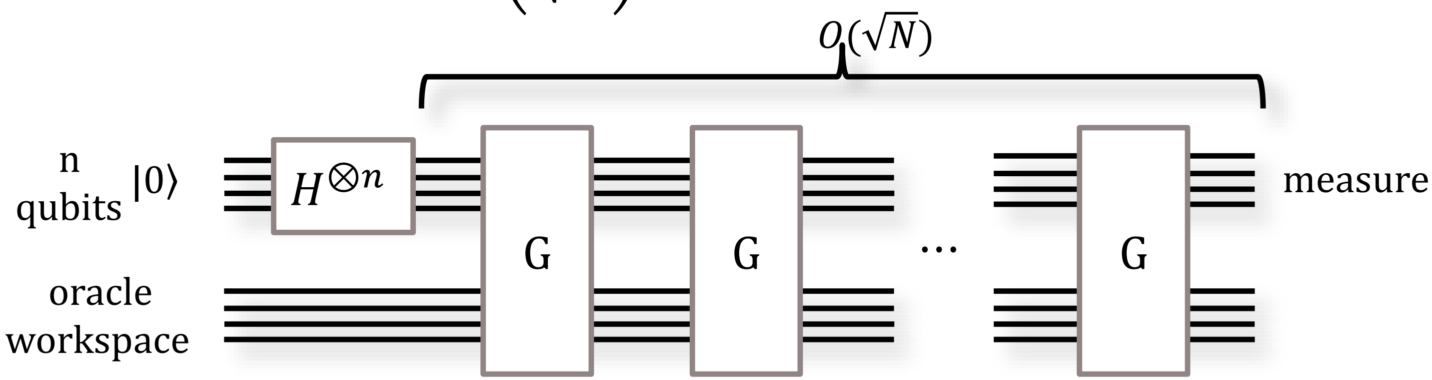
Grover search algorithm

- Section 6.1
- Search space: $N = 2^n$
- Number of solutions: M where $1 \leq M \leq N$
- $f(x) = \begin{cases} 1 & \text{if } x \text{ is a solution to the search problem} \\ 0 & \text{otherwise} \end{cases}$
- Quantum oracle O
  - $|x\rangle|q\rangle \xrightarrow{O} |x\rangle|q \oplus f(x)\rangle$
  - By feeding $|q\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$ as input and due to $|x\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) \xrightarrow{O} (-1)^{f(x)}|x\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$, we can implement quantum circuit which converts $|x\rangle \xrightarrow{O} (-1)^{f(x)}|x\rangle$.



Grover search algorithm

- In classical case: $O\left(\frac{N}{M}\right)$ oracle query
- In quantum case: $O\left(\sqrt{\frac{N}{M}}\right)$ oracle query



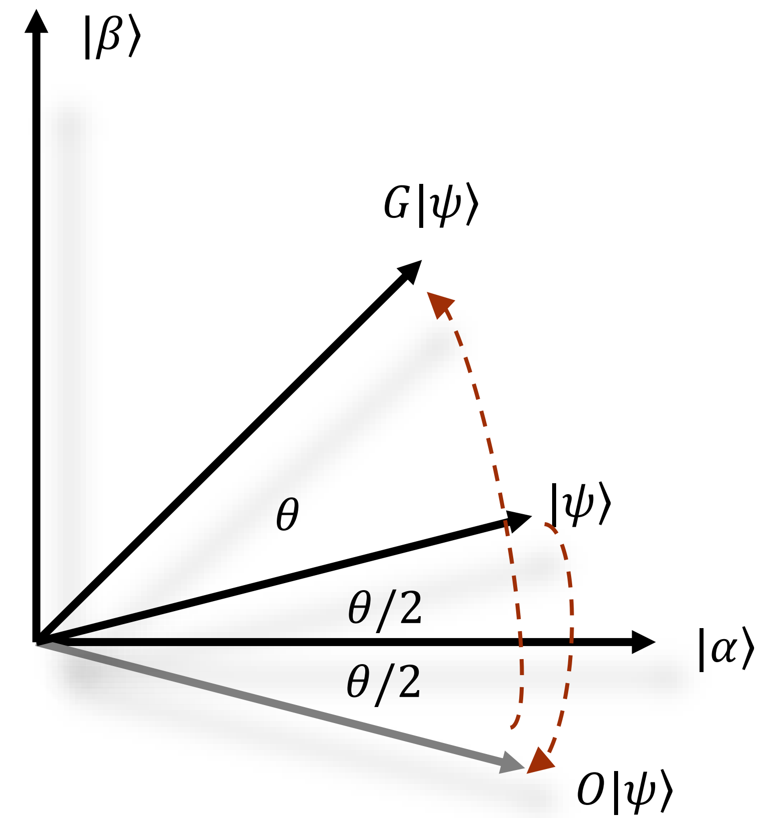
- Strategy for the quantum search
  - Create the superposition of all the inputs
  - Before the measurement, increase the probability amplitudes of the solutions and decrease the probability amplitudes of the wrong inputs
  - Measure the states

Grover search algorithm

- $|\alpha\rangle \equiv \frac{1}{\sqrt{N-M}}\sum_x''|x\rangle$: sum over all x which are not solutions to the search problem
- $|\beta\rangle \equiv \frac{1}{\sqrt{M}}\sum_x'|x\rangle$: sum over all x which are solutions to the search problem
- $|\psi\rangle \equiv \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle = \frac{\sqrt{N-M}}{\sqrt{N}}|\alpha\rangle + \frac{\sqrt{M}}{\sqrt{N}}|\beta\rangle$: sum over all inputs
- Reflection about some arbitrary normalized vector $|\phi\rangle$: $(2|\phi\rangle\langle\phi| - I)$
  - Assume some initial state $|\gamma\rangle$ is given
  - Decompose $|\gamma\rangle$ into two components
  - Components along $|\phi\rangle$:$|\parallel\rangle = (|\phi\rangle\langle\phi|)|\gamma\rangle$
  - Components orthogonal to $|\phi\rangle$:$|\perp\rangle = (I - |\phi\rangle\langle\phi|)|\gamma\rangle$
  - Reflection with respect to $|\phi\rangle$ axis: $|\parallel\rangle - |\perp\rangle = (2|\phi\rangle\langle\phi| - I)|\gamma\rangle$

Grover search algorithm

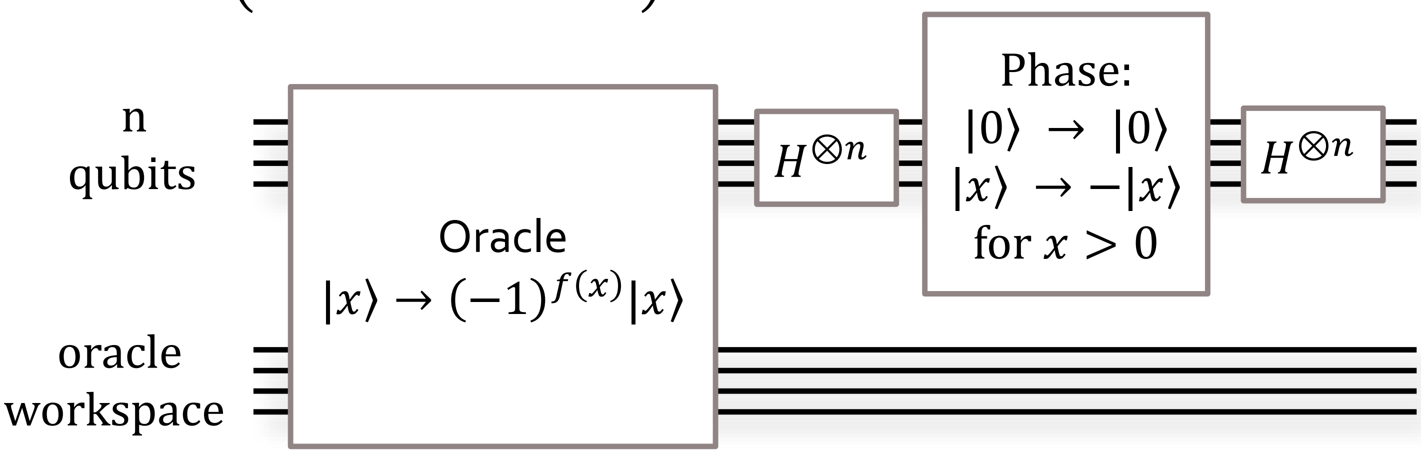
- Graphical interpretation of Grover operator
  - Reflection about $|\alpha\rangle$ which is the sum over all x which are not solutions to the search problem
  - Reflection about $|\psi\rangle$ which is the sum over all possible inputs
- The angle $\theta/2$ between $|\psi\rangle$ and $|\alpha\rangle$ can be obtained by calculating inner product.
- Single Grover operation can rotate the vector by θ w.r.t. the previous vector



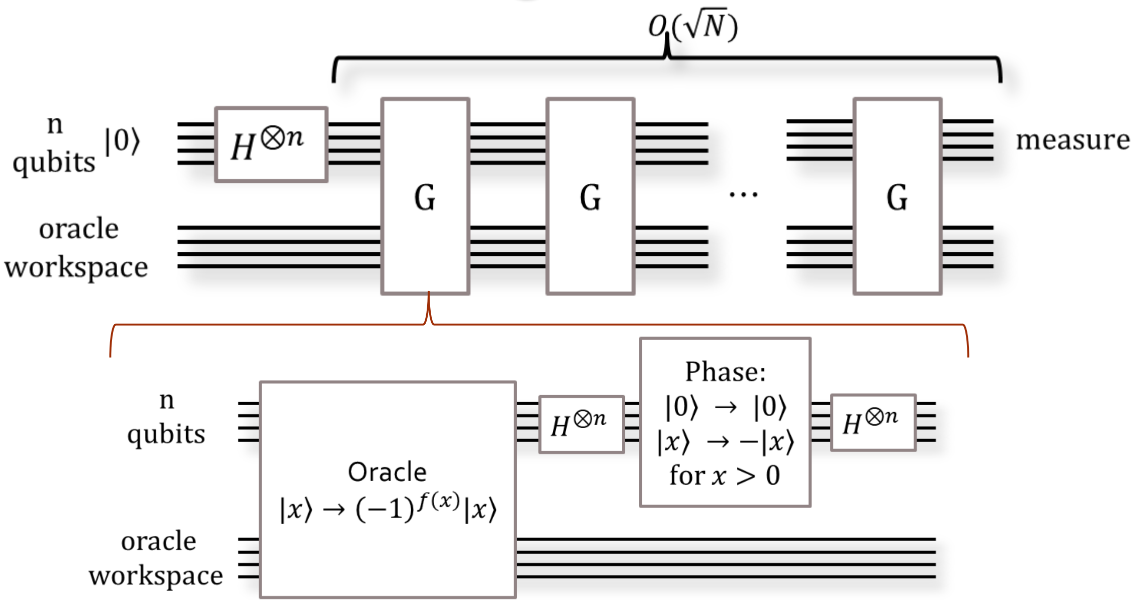
Grover search algorithm

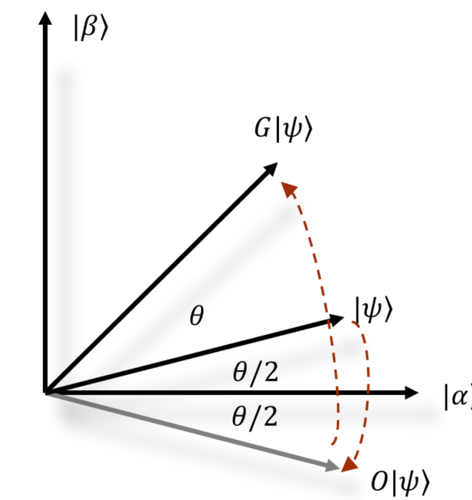
- Reflection about $|\alpha\rangle$
  - Oracle operator O: $|x\rangle \xrightarrow{O} (-1)^{f(x)}|x\rangle$ automatically reflects with respect to $|\alpha\rangle$
  - $O(a|\alpha\rangle + b|\beta\rangle) = a|\alpha\rangle - b|\beta\rangle$
- Reflection about $|\psi\rangle$
  - $2|\psi\rangle\langle\psi| - I$
  - $|\psi\rangle = H^{\otimes n}|0\rangle^{\otimes n}$
  - $2|\psi\rangle\langle\psi| - I = 2H^{\otimes n}|0\rangle^{\otimes n}\langle 0|^{\otimes n}H^{\otimes n} - I$

    $= H^{\otimes n}\left(2|0\rangle^{\otimes n}\langle 0|^{\otimes n} - I\right)H^{\otimes n}$



Grover search algorithm





- How many Grover operations are necessary?
  - $\theta/2$ is determined by inner product between $|\psi\rangle = \frac{\sqrt{N-M}}{\sqrt{N}}|\alpha\rangle + \frac{\sqrt{M}}{\sqrt{N}}|\beta\rangle$ and $|\alpha\rangle = \frac{1}{\sqrt{N-M}}\sum_x''|x\rangle$. ➔ $\cos\frac{\theta}{2} = \langle\alpha|\psi\rangle = \frac{\sqrt{N-M}}{\sqrt{N}}$.
  - Single application of Grover operation rotates the vector by θ w.r.t. the previous vector
  - We need to find m which will make $\left(m + \frac{1}{2}\right)\theta$ closest to $\frac{\pi}{2}$.