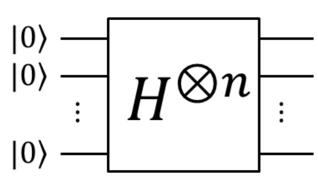
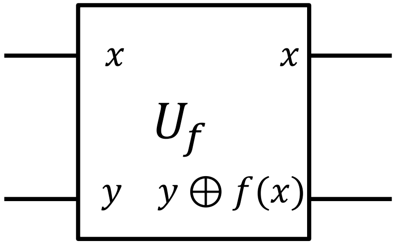
Summary of previous lecture

- Quantum entanglement
  - Typical example: $|\psi^{-}\rangle = [|H\rangle_A|V\rangle_B - |V\rangle_A|H\rangle_B]/\sqrt{2}$
  - Can we implement communication faster than the speed of light by using EPR pair (i.e. Bell basis)? NO!!!
  - Schrödinger's cat state
- Quantum teleportation
  - An arbitrary quantum state can be teleported by using an entangled state
  - No violation of no-cloning theorem
- Reversible gate
  - Unitary gate is reversible
  - Example: Toffoli gate
- Quantum parallelism
  - A superposition of all the possible combinations of input bits can be used as an input to a quantum circuit
  - $\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle$

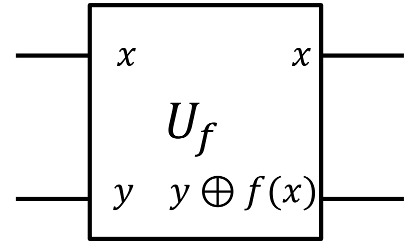


Deutsch's Algorithm I

- Section 1.4.3
- Assumption: $f(x)\colon \{0,1\} \to \{0,1\}$, i.e. the result of $f(x)$ is either 0 or 1 depending on the input value x, but we don't know the actual value of $f(0)$ and $f(1)$. Also, calculation of $f(x)$ takes a long time, so we want to minimize the number of $f(x)$ calculation.
- Challenge: can we decide whether the value of $f(0)$ and $f(1)$ are the same ($f(0) = f(1)$) or different ($f(0) \neq f(1)$) only through a single calculation?
- Answer: Yes, if we use the quantum superposition of the input state and quantum interference
- Assume that we are given the following quantum circuit U_f that accepts two input values (x, y) and produce two output values $(x, y \oplus f(x))$. Here, $\oplus$ means modulo 2 addition.



Deutsch's Algorithm II

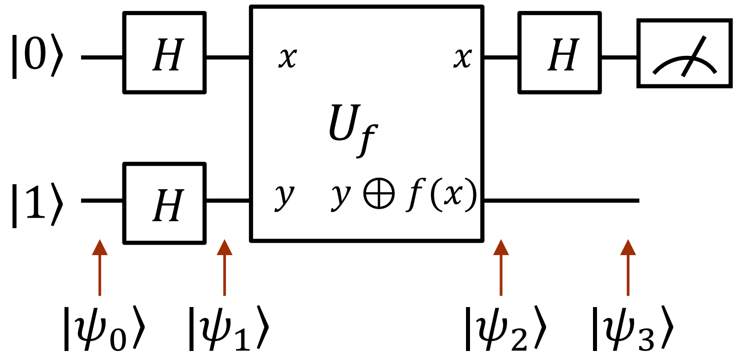


- For input $|x\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$, we can generalize the result of U_f operation.
  - When $f(x)=0$, $\frac{|x,0+f(x)\rangle-|x,1+f(x)\rangle}{\sqrt{2}}=\frac{|x,0\rangle-|x,1\rangle}{\sqrt{2}}=|x\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$
  - When $f(x)=1$, $\frac{|x,0+f(x)\rangle-|x,1+f(x)\rangle}{\sqrt{2}}=\frac{|x,1\rangle-|x,0\rangle}{\sqrt{2}}=|x\rangle\left[\frac{|1\rangle-|0\rangle}{\sqrt{2}}\right]$
  - Therefore, for input state $|x\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$, the output is $(-1)^{f(x)}|x\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$

- For $\left[\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]=\frac{|0\rangle}{\sqrt{2}}\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]+\frac{|1\rangle}{\sqrt{2}}\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$,
  - $\frac{(-1)^{f(0)}|0\rangle}{\sqrt{2}}\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]+\frac{(-1)^{f(1)}|1\rangle}{\sqrt{2}}\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]=(-1)^{f(0)}\left[\frac{|0\rangle+(-1)^{f(1)-f(0)}|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$

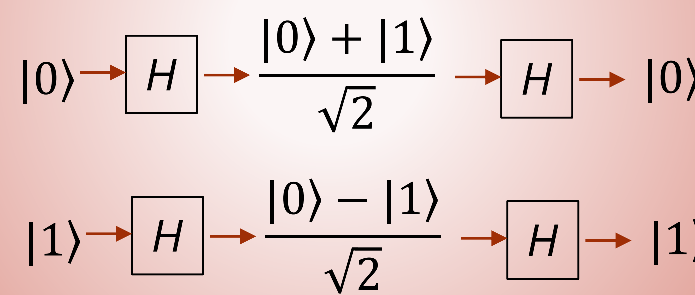
- In quantum mechanics, the global phase cannot be measured, so $(-1)^{f(0)}$ can be omitted. Therefore, depending on whether the values of $f(0)$ and $f(1)$ are the same, the result becomes:
  - When $f(0)=f(1)$, $\left[\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$
  - When $f(0)\neq f(1)$, $\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$

Deutsch's Algorithm III



- $|\psi_0\rangle = |01\rangle$
- $|\psi_1\rangle = \left[\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$
- $|\psi_2\rangle = \begin{cases} \left[\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] & if \;\; f(0) = f(1) \\ \left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] & if \;\; f(0) \neq f(1) \end{cases}$
- $|\psi_3\rangle = \begin{cases} |0\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] & if \;\; f(0) = f(1) \\ |1\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] & if \;\; f(0) \neq f(1) \end{cases}$
- Therefore we can decide whether $f(0) = f(1)$ or not only by a single calculation.

- Recall the property of Hadamard gate
  - $H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1 \\ 1 & -1\end{bmatrix}$, $H^2 = \begin{bmatrix}1 & 0 \\ 0 & 1\end{bmatrix}$



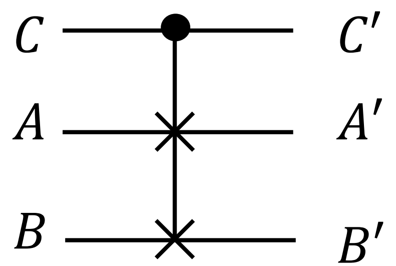
Deutsch-Jozsa Algorithm

- Please read section 1.4.4
- Especially check that $H^{\otimes n}|x\rangle = \sum_z (-1)^{x \cdot z} |z\rangle / \sqrt{2^n}$

Reversible gates

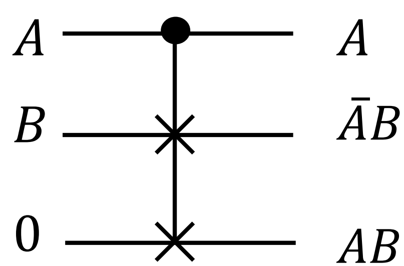
- Section 3.2.5 (pp.156~160)
- Fredkin gate

Input			Output		
C	A	B	C′	A′	B′
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	1	0
1	1	0	1	0	1
1	1	1	1	1	1

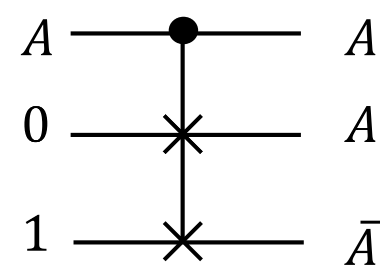


$$\left[\begin{array}{cccc|cccc} 1 & & & & & & & \\ & 1 & & & & & & \\ & & 1 & & & & & \\ & & & 1 & & & & \\ \hline & & & & 1 & 0 & 0 & 0 \\ & & & & 0 & 0 & 1 & 0 \\ & & & & 0 & 1 & 0 & 0 \\ & & & & 0 & 0 & 0 & 1 \end{array}\right]$$

AND



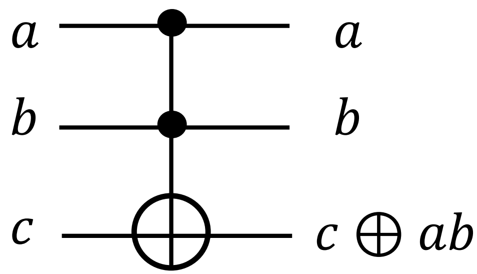
FANOUT & NOT



Similar to Toffoli gate, an arbitrary classical circuit can be simulated by reversible Fredkin circuits.

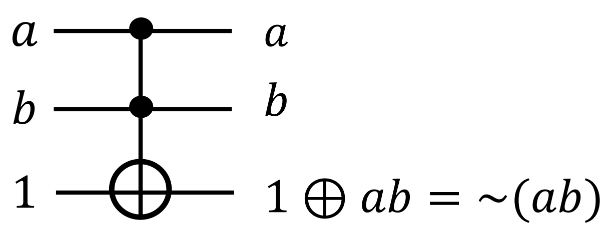
Reminder for Toffoli gate

Input			Output		
a	b	c	a′	b′	c′
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

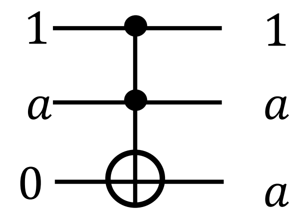


$$\begin{bmatrix} 1 & & & & & & & \\ & 1 & & & & & & \\ & & 1 & & & & & \\ & & & 1 & & & & \\ & & & & 1 & & & \\ & & & & & 1 & & \\ & & & & & & & 1 \\ & & & & & & 1 & \end{bmatrix}$$

NAND



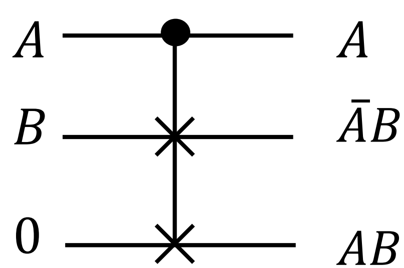
FANOUT



Overhead of reversible gates

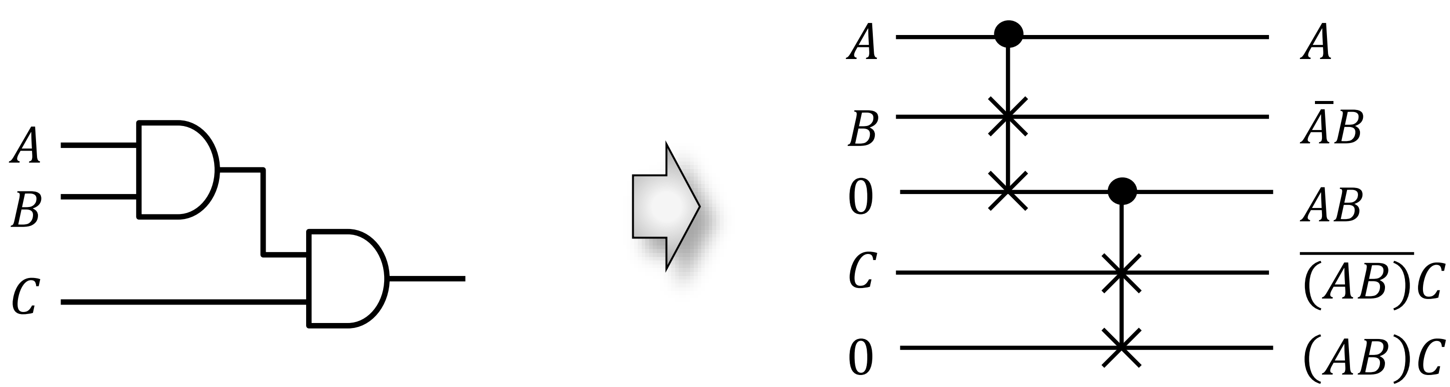
- When implementing $f(x)$ function using quantum gates, auxiliary (ancilla) qubit and/or garbage bits naturally occur with reversible gates.
  - For example, AND gate with Fredkin gate: $(A, B, 0) \rightarrow (A, \bar{A}B, AB)$

Auxiliary (ancilla) qubit



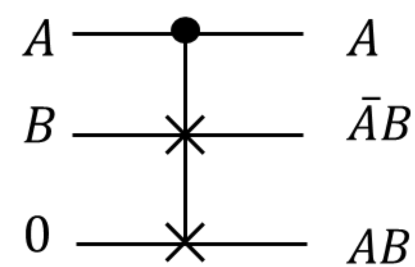
Garbage qubit for the case of AND gate

- The numbers of auxiliary qubits and garbage qubits increase as the number of gates increases.



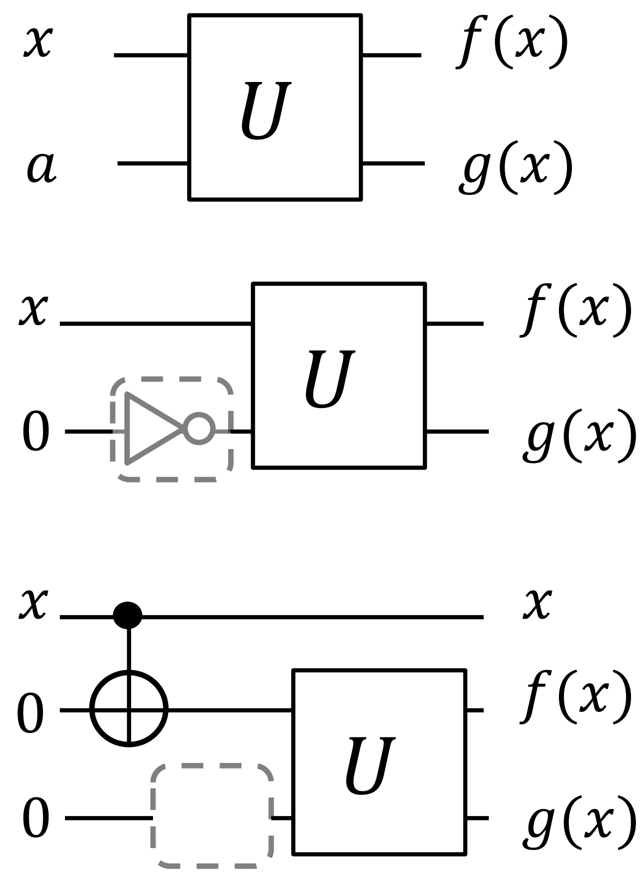
Overhead of reversible gates

- More serious problem is that the garbage qubit gets entangled with other results and accidental measurement of garbage qubit will destroy the superposition
  - $\frac{|0\rangle_1+|1\rangle_1}{\sqrt{2}} \otimes |1\rangle_2 \otimes |0\rangle_3$
    $= \frac{1}{\sqrt{2}}(|0\rangle_1 \otimes |1\rangle_2 \otimes |0\rangle_3 + |1\rangle_1 \otimes |1\rangle_2 \otimes |0\rangle_3)$
    $\xrightarrow{Fredkin\ gate} \frac{1}{\sqrt{2}}(|0\rangle_1 \otimes |1\rangle_2 \otimes |0\rangle_3 + |1\rangle_1 \otimes |0\rangle_2 \otimes |1\rangle_3)$
  - Measurement of qubit 2 will collapse the above superposed states.



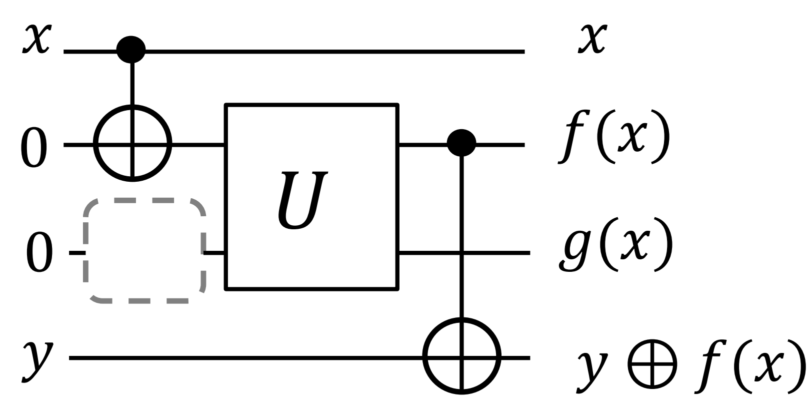
Un-computation I

- Can we recycle auxiliary qubits and un-entangle the garbage qubits?
  - Generally $(x, a) \rightarrow \big(f(x), g(x)\big)$
  - By using NOT gates to the auxiliary qubits, we can generalize that all the auxiliary qubits starts in 0's: $(x, 0) \rightarrow \big(f(x), g(x)\big)$
  - Make a copy of input x using C-NOT before the calculation of $f(x)$: $(x, 0, 0) \rightarrow \big(x, f(x), g(x)\big)$



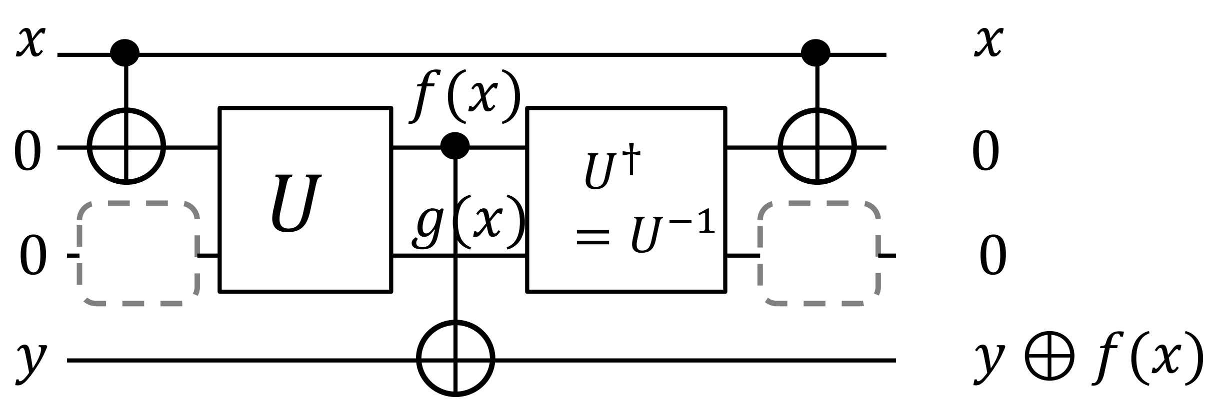
Un-computation II

- If we need to calculate $(x, y) \rightarrow (x, y \oplus f(x))$, we can recover all the auxiliary qubits back to its initial state after the calculation:



$$(x, 0,0, y) \rightarrow (x, f(x), g(x), y) \rightarrow (x, f(x), g(x), y \oplus f(x))$$

$$\xrightarrow{Uncompute} (x, 0,0, y \oplus f(x))$$



양자 컴퓨터를 이용한 소인수 분해

- 15의 소인수 분해 예
  - 소인수 분해하고자 하는 수(15)보다 작고 공통 인수가 없는 임의의 수를 선택
    - 예) a=7
  - 0~255 사이의 모든 x에 대하여 a^x (mod 15)를 계산후 그 결과값들의 주기를 찾음
    - 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