Quantum State Transformation II

State Transition in Multi-Qubit System

- We start with a 2-qubit systems in standard or computational basis.
- The basis of such system is the tensor product of two 1-qubit bases -

$$
\begin{aligned}
& \{|0\rangle, |1\rangle\} \otimes \{|0\rangle, |1\rangle\} \\
= & \{|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle\} \\
= & \{|0\rangle |0\rangle, |0\rangle |1\rangle, |1\rangle |0\rangle, |1\rangle [|1\rangle\} \\
= & \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}
\end{aligned}
$$

.

2-Qubit Representation

- If we represent $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$,

$$|00\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \begin{bmatrix} 1 \\ 0 \end{bmatrix} \\ 0 \begin{bmatrix} 1 \\ 0 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

2-Qubit Representation

- Similarly,

$$|01\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \ |10\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \ |11\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}.$$

2-Qubit Unitary Transformation

- One may think of a 2-qubit unitary transformation as a tensor product of two 1-qubit unitary transformations.
- As an example consider

$$X \otimes Y = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} = \begin{bmatrix} 0 \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} & 1 \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \\ 1 \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} & 0 \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \end{bmatrix}$$

2-Qubit Unitary Transformation

$$X \otimes Y = \begin{bmatrix} 0 & 0 & 0 & -i \\ 0 & 0 & i & 0 \\ 0 & -i & 0 & 0 \\ i & 0 & 0 & 0 \end{bmatrix}$$

The effect of $X \otimes Y$ on a two qubit state $|pq\rangle$ is same as $|(Xp) \otimes (Yq)\rangle$.
We consider an example where $p = \left[\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right]$ and $q = \left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right]$.

2-Qubit Unitary Transformation

$$
\begin{aligned}
(X \otimes Y)\,|10\rangle &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \left(\begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} \right) \\
&= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ i \end{bmatrix} \\
&= \begin{bmatrix} 0 \\ i \\ 0 \\ 0 \end{bmatrix} = i\,|01\rangle = |0\rangle \otimes i\,|1\rangle
\end{aligned}
$$

Negation of the 1st qubit and Y on the second qubit. This is same as -

2-Qubit Unitary Transformation

$$(X \otimes Y)\,|10\rangle = \begin{bmatrix} 0 & 0 & 0 & -i \\ 0 & 0 & i & 0 \\ 0 & -i & 0 & 0 \\ i & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$$

$$= \begin{bmatrix} 0 \\ i \\ 0 \\ 0 \end{bmatrix}.$$

2-Qubit Unitary Transformation

In general, if $p = \begin{bmatrix} a \\ b \end{bmatrix}$ and $q = \begin{bmatrix} c \\ d \end{bmatrix}$,

$$
\begin{aligned}
(X \otimes Y)\,|pq\rangle &= \begin{bmatrix} 0 & 0 & 0 & -i \\ 0 & 0 & i & 0 \\ 0 & -i & 0 & 0 \\ i & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} ac \\ ad \\ bc \\ bd \end{bmatrix} = \begin{bmatrix} -ibd \\ ibc \\ -iad \\ iac \end{bmatrix} \\
&= \begin{bmatrix} b \\ a \end{bmatrix} \otimes \begin{bmatrix} -id \\ ic \end{bmatrix} = (Xp) \otimes (Yq).
\end{aligned}
$$

Note

- This type of transformations do not create any new dependency (entanglement) of qubits.
- But there are 2-qubit transformations that cannot be expressed as a tensor product of two 1-qubit transformations.

CNOT Gate

One of the most important of such transformations is CNOT. We have already shown (Boolean) that it cannot be expressed as a tensor product of two 1-qubit transformations.

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \otimes \begin{bmatrix} p & q \\ r & s \end{bmatrix} = \begin{bmatrix} ap & aq & bp & bq \\ ar & as & br & bs \\ cp & cq & dp & dq \\ cr & cs & dr & ds \end{bmatrix} \neq \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

$dp = 0$ implies that either $d = 0$ or $p = 0$. If $d = 0$, then $dq = 0$ - not possible. If $p = 0$, then $ap = 0$ - also not possible; so a contradiction.

CNOT Gate

The CNOT transformation can be expressed as

$$
\begin{aligned}
|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X &= \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \\
&= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \\
&= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}
\end{aligned}
$$

CNOT Gate

We have $p = \left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right]$ and $q = \left[\begin{smallmatrix} c \\ d \end{smallmatrix}\right]$.

$$CNOT\,|pq\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} ac \\ ad \\ bc \\ bd \end{bmatrix} = \begin{bmatrix} ac \\ ad \\ bd \\ bc \end{bmatrix}.$$

$$\left(\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \right) \begin{bmatrix} ac \\ ad \\ bc \\ bd \end{bmatrix} = \begin{bmatrix} ac \\ ad \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ bd \\ bc \end{bmatrix} = \begin{bmatrix} ac \\ ad \\ bd \\ bc \end{bmatrix}$$

Note

- We have seen that the effect of $X \otimes Y$ on a pair of qubits is an application of X on the first qubit and an application of Y on the second qubit. One action does not influence the other.
- On the other hand in case of CNOT, the first qubit influences the action on the second qubit - it is either identity or NOT.

Note

- If $p = \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$, the new state comes from $\begin{bmatrix} ac \\ ad \\ 0 \\ 0 \end{bmatrix}$, and no change in the order of c, d.
- If $p = \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$, the new state comes from $\begin{bmatrix} 0 \\ 0 \\ bd \\ bc \end{bmatrix}$, and the order of c, d are reversed.

CNOT versus $X \otimes Y$

Consider the state $|x\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$.

- $(X \otimes Y)\left(\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)\right) = \frac{i}{\sqrt{2}}(|11\rangle + |01\rangle)$.
- $CNOT\,|x\rangle = CNOT\left(\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)\right) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

The initial state was not entangled. The state after the transformation $X \otimes Y$ is also not entangled, but CNOT creates an entangled state.

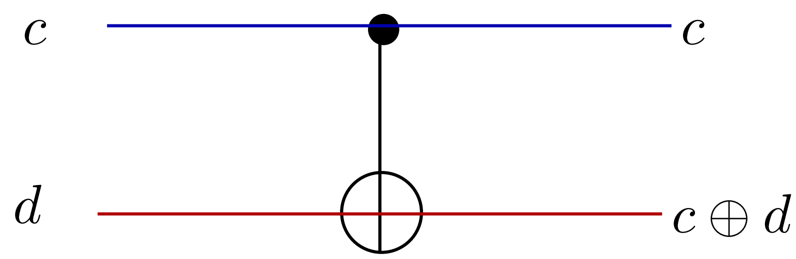
CNOT versus $X \otimes Y$

If we start with $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, we get

- $(X \otimes Y)\left(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\right) = \frac{i}{\sqrt{2}}(-|00\rangle + |11\rangle)$.
- $CNOT(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$

The input state was entangled. The entanglement remains after the transformation $X \otimes Y$, but it is not there after CNOT.

Graphical Notation: CNOT



CNOT

Controlled U Gate

For every 1-qubit transformation U we can have a controlled-U gate, U^c.

$$U^c\,|ab\rangle = \begin{cases} |ab\rangle & \text{if } a = 0, \\ |a(Ub)\rangle & \text{if } a = 1. \end{cases}$$

So $U^c = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U$.

Controlled-U Transformation

- Let $U = \begin{bmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{bmatrix}$ be a 1-qubit unitary transformation.
- The transformation matrix for

$$U^c = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{11} & u_{12} \\ 0 & 0 & u_{21} & u_{22} \end{bmatrix}.$$

Z^c, H and CNOT

We know that

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|)$$

and $I = |0\rangle\langle 0| + |1\rangle\langle 1|$. So,

$$\begin{aligned} I \otimes H &= (|0\rangle\langle 0| + |1\rangle\langle 1|) \otimes \\ &\quad \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|) \\ &= \frac{1}{\sqrt{2}}(|00\rangle\langle 00| + |00\rangle\langle 01| + |01\rangle\langle 00| - |01\rangle\langle 01| + \\ &\quad |10\rangle\langle 10| + |10\rangle\langle 11| + |11\rangle\langle 10| - |11\rangle\langle 11| \end{aligned}$$

Z^c, H and CNOT

$$I \otimes H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix}, \; Z^c = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

So $(I \otimes H) Z^c (I \otimes H)$ is

$$\frac{1}{2} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix}$$

Z^c, H and CNOT

So we have

$$(I \otimes H)Z^c(I \otimes H) = \frac{1}{2}\begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix}\begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & -1 & 1 \end{bmatrix}$$

$$= \frac{1}{2}\begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & 2 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

$$= CNOT$$

CNOT and Basis

- The 2-qubit CNOT gate behaves very similar to 2-bit Boolean gate, where the control bit remains unchanged and the other bit flips when the control bit is $|1\rangle$. This happens when the input state is in standard basis.
- But if the input state is not in standard basis, CNOT behaves differently.

CNOT On Hadamard Basis

The bases of a 2-qubit state space in Hadamard basis is $\{|{+}{+}\rangle, |{+}{-}\rangle, |{-}{+}\rangle, |{-}{-}\rangle\}$, where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

$$\begin{aligned} |{+}{+}\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ &= \frac{1}{2}\begin{bmatrix} 1 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}. \end{aligned}$$

CNOT On Hadamard Basis

Similarly,

$$|{+}{-}\rangle = \frac{1}{2}\begin{bmatrix} 1 \\ -1 \\ 1 \\ -1 \end{bmatrix}, |{-}{+}\rangle = \frac{1}{2}\begin{bmatrix} 1 \\ 1 \\ -1 \\ -1 \end{bmatrix}, |{-}{-}\rangle = \frac{1}{2}\begin{bmatrix} 1 \\ -1 \\ -1 \\ 1 \end{bmatrix}.$$

CNOT On Hadamard Basis

$$CNOT\,|{+}{+}\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = |{+}{+}\rangle\,.$$

Similarly,

$$CNOT\,|{+}{-}\rangle = |{-}{-}\rangle\,,\; CNOT\,|{-}{+}\rangle = |{-}{+}\rangle\,,\; CNOT\,|{-}{-}\rangle = |{+}{-}\rangle\,.$$

The second qubit remains unchanged, the first qubit flips when the second one is $|-\rangle$.

Superdense Coding: An Application

Alice can transmit two classical bits of information to Bob by sending only one qubit.

- Initially, Alice has the first qubit and Bob has the second qubit of an entangled pair of qubits - $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.
- Alice (Bob) can only transform her (his) qubit.

Superdense Coding: An Application

Alice encodes her classical bit pairs $00, 01, 10, 11$ as follows and sends to Bob.

$$00 \mapsto (I \otimes I)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle),$$
$$01 \mapsto (X \otimes I)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle),$$
$$10 \mapsto (Z \otimes I)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle),$$
$$11 \mapsto (iY \otimes I)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(-|10\rangle + |01\rangle).$$

Note that the second qubit is not touched. These transformations do not affect the entanglement.

Superdense Coding: An Application

After receiving the first qubit from Alice, Bob performs the following transformation on the entangled qubit pairs.

1. Applies CNOT that transformations the pair as follows:
$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \mapsto \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$,
$\frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) \mapsto \frac{1}{\sqrt{2}}(|11\rangle + |01\rangle)$,
$\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \mapsto \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$,
$\frac{1}{\sqrt{2}}(-|10\rangle + |01\rangle) \mapsto \frac{1}{\sqrt{2}}(-|11\rangle + |01\rangle)$.

Superdense Coding: An Application

2. Applies $H \otimes I$:
   $\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \mapsto |00\rangle$,
   $\frac{1}{\sqrt{2}}(|11\rangle + |01\rangle) \mapsto |01\rangle$,
   $\frac{1}{\sqrt{2}}(|00\rangle - |10\rangle) \mapsto |10\rangle$,
   $\frac{1}{\sqrt{2}}(-|11\rangle + |01\rangle) \mapsto |11\rangle$.
3. Bob measures the pair and recovers the two classical bits.

Superdense Coding: An Application

- The four qubit states produced by Alice are the orthonormal Bell basis - $\{\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, $\frac{1}{\sqrt{2}}(|10\rangle + |01\rangle)$, $\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$, $\frac{1}{\sqrt{2}}(-|10\rangle + |01\rangle)\}$.
- So Bob can perform suitable measurement and identify them directly.

Superdense Coding: Note

- Two qubits are involved, but Alice does not use the other qubit.
- Any third party may supply the entangled qubits to Alice and Bob.

Teleportation: An Application

Teleportation in a sense is reverse of superdense coding.
Alice has a qubit in some unknown state $|x\rangle = a\,|0\rangle + b\,|1\rangle$, where $|a|^2 + |b|^2 = 1$. She wishes to transmit the state information to Bob using two Boolean bits through a classical channel, so that Bob can reconstruct the qubit.

Teleportation: An Application

- To start with, the First qubit of an entangled pair $|y\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ is with Alice and the second qubit is with Bob.
- Alice starts with the 3-qubit state

$$\begin{aligned} |x\rangle \otimes |y\rangle &= (a\,|0\rangle + b\,|1\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ &= \frac{1}{\sqrt{2}}(a\,|000\rangle + a\,|011\rangle + b\,|100\rangle + b\,|111\rangle) \end{aligned}$$

- She can transform the first two qubits and Bob can transform the third qubit.

Teleportation: An Application

1. Alice applies $CNOT \otimes I$ on $|x\rangle \otimes |y\rangle$

$$
\begin{aligned}
& (CNOT \otimes I)(|x\rangle \otimes |y\rangle) \\
= \;& \frac{1}{\sqrt{2}}(CNOT \otimes I)(a\,|000\rangle + a\,|011\rangle + b\,|100\rangle + b\,|111\rangle) \\
= \;& \frac{1}{\sqrt{2}}(a\,|000\rangle + a\,|011\rangle + b\,|110\rangle + b\,|101\rangle).
\end{aligned}
$$

Teleportation: An Application

2. Then she applies $H \otimes I \otimes I$ on $(CNOT \otimes I)(|x\rangle \otimes |y\rangle)$ i.e.

$$\begin{aligned} & (H \otimes I \otimes I)(CNOT \otimes I)(|x\rangle \otimes |y\rangle) \\ = & \frac{1}{\sqrt{2}}(H \otimes I \otimes I)(a|000\rangle + a|011\rangle + b|110\rangle + b|101\rangle) \\ = & \frac{1}{2}(a(|000\rangle + |100\rangle + |011\rangle + |111\rangle) + \\ & b(|010\rangle - |110\rangle + |001\rangle - |101\rangle)) \\ = & \frac{1}{2}(|00\rangle (a|0\rangle + b|1\rangle) + |01\rangle (a|1\rangle + b|0\rangle) \\ & + |10\rangle (a|0\rangle - b|1\rangle) + |11\rangle (a|1\rangle - b|0\rangle)). \end{aligned}$$

Teleportation: An Application

3. Alice measures the first two qubits in standard basis. The outcomes of measurement are $|00\rangle, |01\rangle, |10\rangle$, or $|11\rangle$ with equal probability.

4. Alice transmits two Boolean bits $00, 01, 10, 11$ to Bob on classical channel, depending on the outcome of previous measurement.

Teleportation: An Application

As a result of Alice's measurement, the projected state of the third qubit of Bob is $(a|0\rangle + b|1\rangle), (a|1\rangle + b|0\rangle), (a|0\rangle - b|1\rangle)$, or $(a|1\rangle - b|0\rangle)$.

Teleportation: An Application

1. Bob receives the pair of bits and applies the following transformations on his qubit to bring it to the state of Alice's unknown qubit.

Boolean bits	Transformation
00	$I(a\|0\rangle + b\|1\rangle) = a\|0\rangle + b\|1\rangle$
01	$X(a\|1\rangle + b\|0\rangle) = a\|0\rangle + b\|1\rangle$
10	$Z(a\|0\rangle - b\|1\rangle) = a\|0\rangle + b\|1\rangle$
11	$iY(a\|1\rangle - b\|0\rangle) = a\|0\rangle + b\|1\rangle$

Controlled-U Transformation

- For every 1-qubit unitary transformation U, it is possible to implement a 2-qubit, controlled-U transformation, U^c, using CNOT gates and single qubit gates.
- We know that any single-qubit unitary transformation U can be decomposed as $e^{i\alpha}AXBXC$, where $ABC = I$.

Rotation gates

We know that

$$
\begin{aligned}
R_x(\alpha) &= \begin{bmatrix} \cos\left(\frac{\alpha}{2}\right) & -i\sin\left(\frac{\alpha}{2}\right) \\ -i\sin\left(\frac{\alpha}{2}\right) & \cos\left(\frac{\alpha}{2}\right) \end{bmatrix} \\
R_y(\alpha) &= \begin{bmatrix} \cos\left(\frac{\alpha}{2}\right) & -\sin\left(\frac{\alpha}{2}\right) \\ \sin\left(\frac{\alpha}{2}\right) & \cos\left(\frac{\alpha}{2}\right) \end{bmatrix} \\
R_z(\alpha) &= \begin{bmatrix} \cos\left(\frac{\alpha}{2}\right) - i\sin\left(\frac{\alpha}{2}\right) & 0 \\ 0 & \cos\left(\frac{\alpha}{2}\right) + i\sin\left(\frac{\alpha}{2}\right) \end{bmatrix}. \\
&= \begin{bmatrix} e^{-i\frac{\alpha}{2}} & 0 \\ 0 & e^{i\frac{\alpha}{2}} \end{bmatrix}.
\end{aligned}
$$

Hadamard Gate an Example

Observe that

$$
\begin{aligned}
& e^{i\pi/2} R_z(0) R_y(\pi/2) R_z(\pi) \\
= \;& i \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \cos\pi/4 & -\sin\pi/4 \\ \sin\pi/4 & \cos\pi/4 \end{bmatrix} \begin{bmatrix} e^{-i\pi/2} & 0 \\ 0 & e^{i\pi/2} \end{bmatrix} \\
= \;& i \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix} \\
= \;& i \frac{1}{\sqrt{2}} \begin{bmatrix} -i & -i \\ -i & i \end{bmatrix} = H.
\end{aligned}
$$

Hadamard Gate an Example

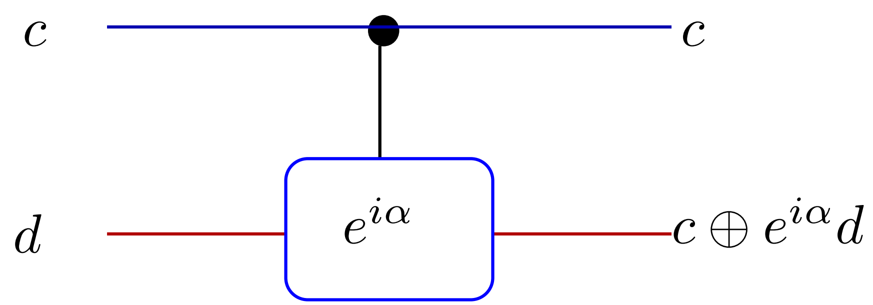
So we have $H = e^{i\pi/2}AXBXC$, where

$$\begin{aligned} A &= R_y(\pi/4), \\ B &= R_y(-\pi/4)R_z(-\pi/2), \\ C &= R_z(\pi/2), \end{aligned}$$

such that $ABC = I$.

Controlled-Phase Shift

If $U = e^{i\alpha}AXBXC$, where $ABC = I$, then in U^c the first operation is controlled phase shift, $(e^{i\alpha})^c$.



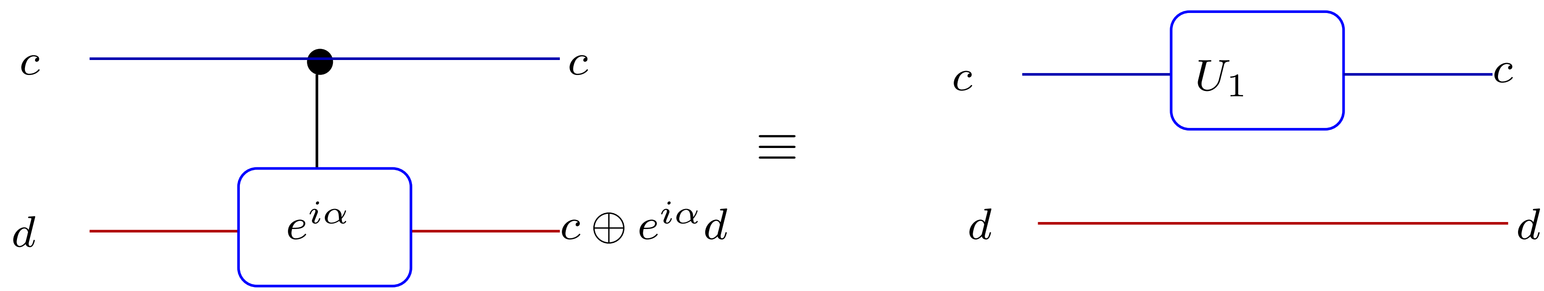
C-Phase-shift

$|00\rangle \mapsto |00\rangle$, $|01\rangle \mapsto |01\rangle$, $|10\rangle \mapsto |1\rangle \otimes e^{i\alpha}|0\rangle$, and $|11\rangle \mapsto |1\rangle \otimes e^{i\alpha}|1\rangle$.

Controlled-Phase Shift

- We observe that $|1\rangle \otimes e^{i\alpha}|x\rangle = e^{i\alpha}|1\rangle \otimes |x\rangle$, where $x \in \{0,1\}$.
- We need a 1-qubit transform U_1 so that $U_1|0x\rangle = |0x\rangle$ and $U_1|1x\rangle = e^{i\alpha}|1\rangle \otimes |x\rangle$. So $(e^{i\alpha})^c$ is implemented as $U_1 \otimes I$, where
$$U_1 = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{bmatrix} = e^{i\alpha/2} I R_z(\alpha).$$

Controlled-Phase Shift

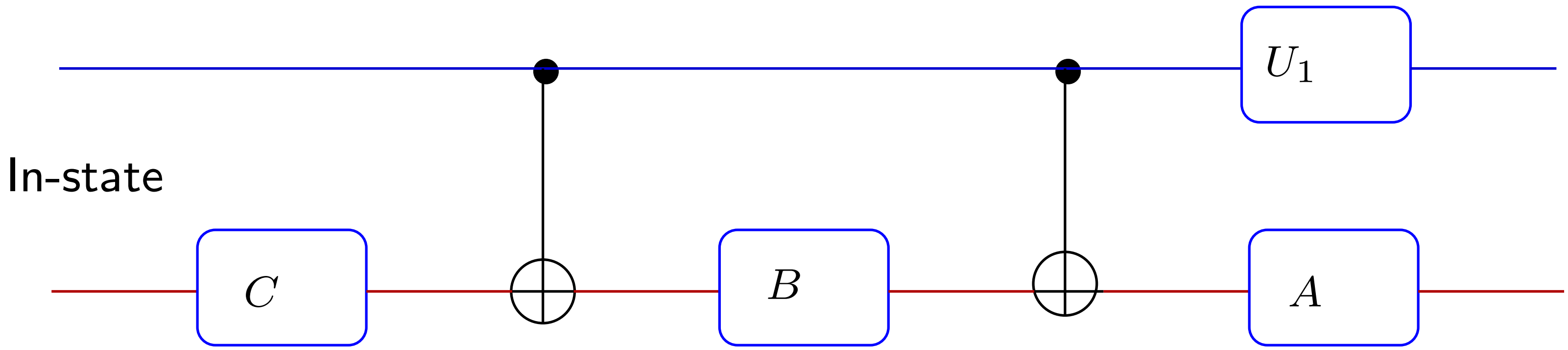


C-Phase-shift

Controlled-U Transformation

- If the control bit is $|1\rangle$, the state of the data bit is $Ud = (e^{i\alpha} AXBXC)d$.
- If the control bit is $|0\rangle$, the state of the data bit is $Id = (ABC)d$.
- The circuit is as follows:

Controlled-U Gate



Controlled-U (U^c)

Controlled-H Transformation: H^c

As we know
$H = e^{i\pi/2} R_z(0) R_y(\pi/2) R_z(\pi) = e^{i\pi/2} AXBXC$.
So we can construct controlled-H (H^c) gate.

Multi-qubit Control

- We can generalise the single-control 2-qubit unitary transformation to multiply-controlled multi-qubit unitary transformation.
- We have seen 3-bit reversible Boolean gates e.g. Toffoli gate and Fredkin gate, with two control-bits.

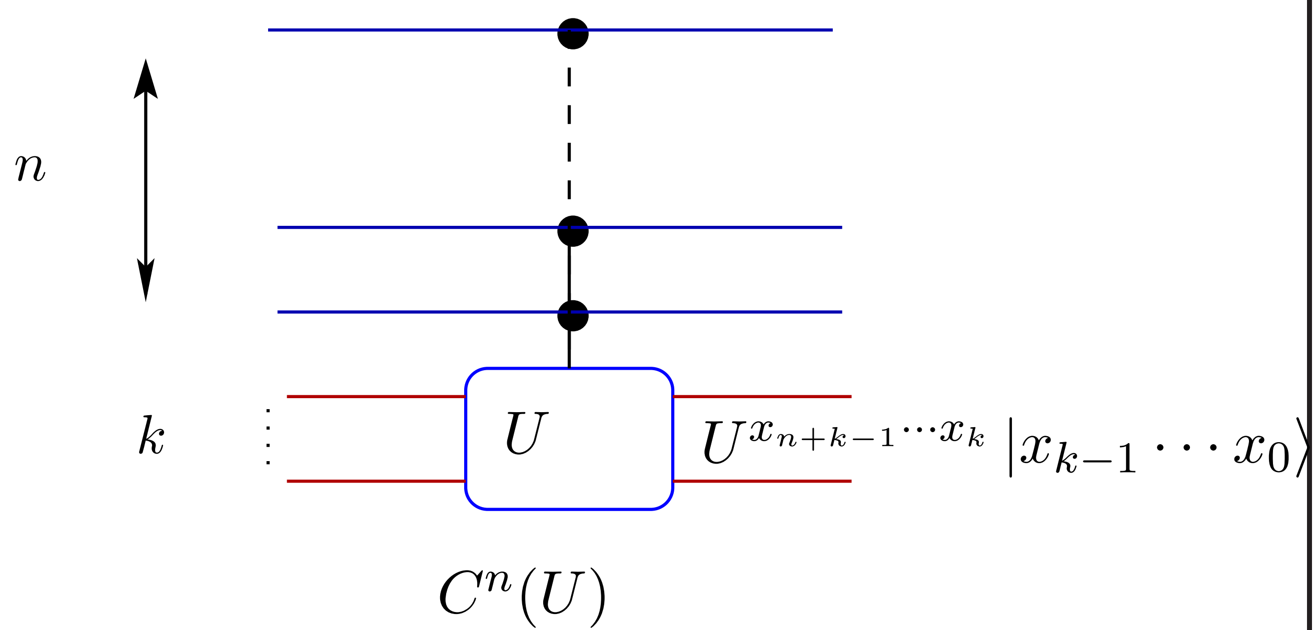
Multi-qubit Control

- Let U be a k-qubit unitary operator and there are n-control qubits.
- So we have a $(n+k)$-qubits unitary operator $C^n(U)$ controlled by n-qubits.

$$\begin{aligned} & C^n(U)\,|x_{n+k-1}\cdots x_k\rangle\,|x_{k-1}\cdots x_0\rangle \\ = & \;|x_{n+k-1}\cdots x_k\rangle\,U^{x_{n+k-1}\cdots x_k}\,|x_{k-1}\cdots x_0\rangle\,, \end{aligned}$$

U is applied on $|x_{k-1}\cdots x_0\rangle$ if $x_{n+k-1} = \cdots = x_k = 1$.

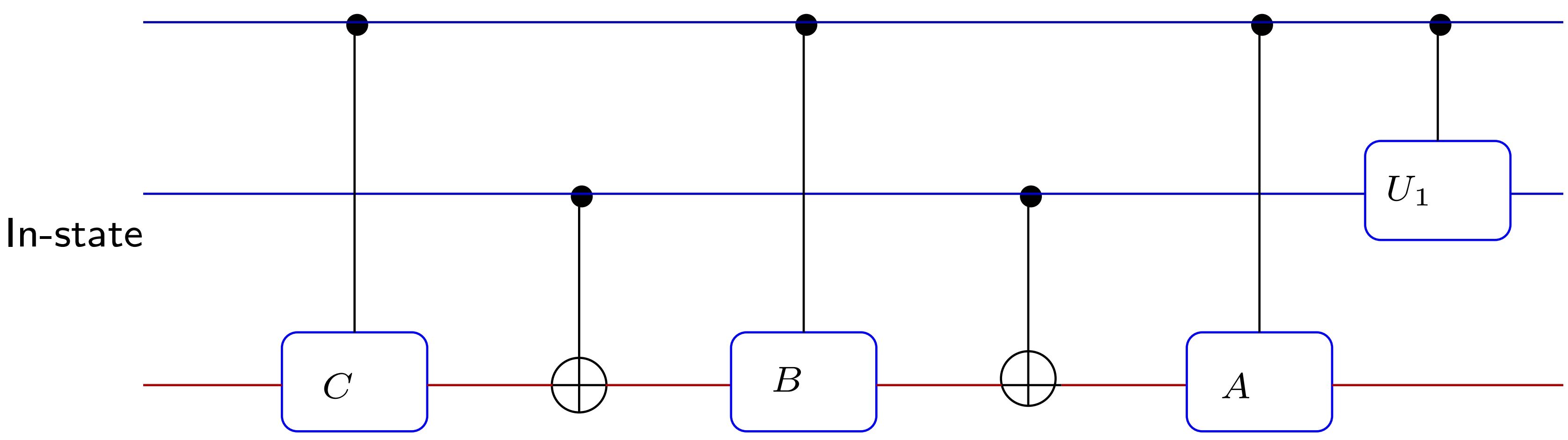
Multi-Qubit Controlled Circuit



Multi-qubit Control

- We shall consider $k = 1$ and $n \geq 1$.
- The circuit for $n = 1$ can be used for $n = 2$ by replacing the 1-qubit gates A, B, C and U_1 by the corresponding control gates.

$C^2(U)$ Gate: Diagram

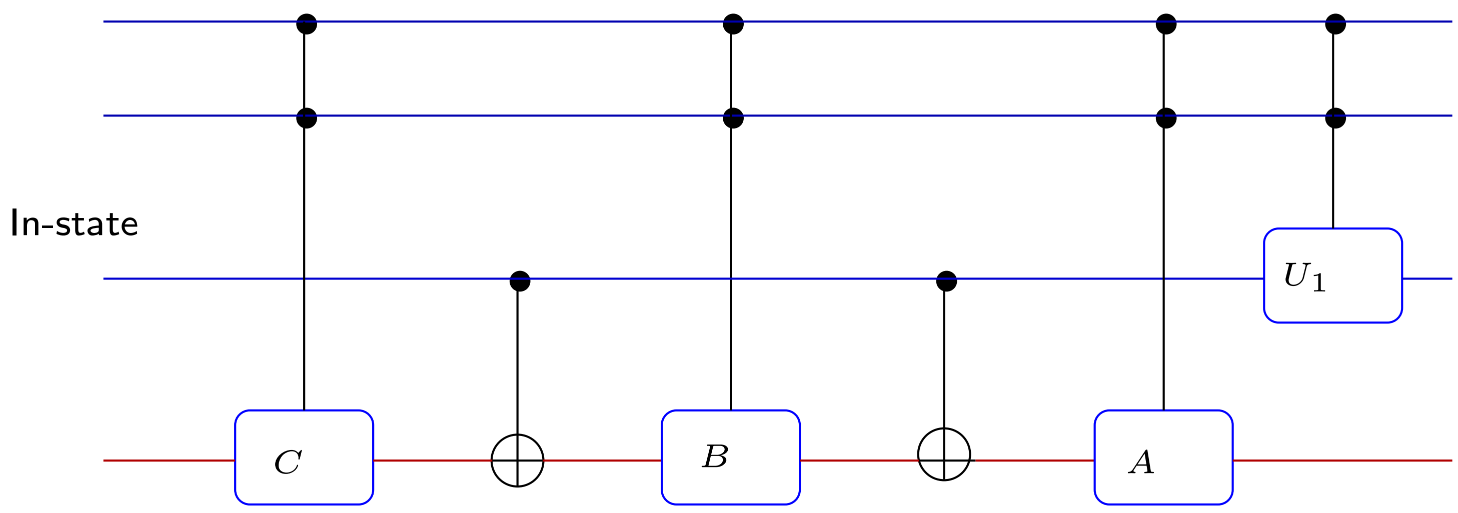


Controlled-Controlled-U ($C^2(U)$)

$C^2(U)$ Gate count

Each single-qubit control gate require two CNOT and four single-qubit unitary gates. So all together the requirement is $4^2 = 16$, single-qubit gates and $2 + 2 \cdot 4 = 10$, CNOT gates.

$C^3(U)$ Gate: Diagram



Controlled^3-U ($C^3(U)$)

$C^k(U)$ Gate count

The number of 1-qubit gates are 4^k and the number of CNOT gates are $2 + 2 \cdot 4 + \cdots + 2 \cdot 4^{k-1} = \frac{2}{3}(4^k - 1)$.

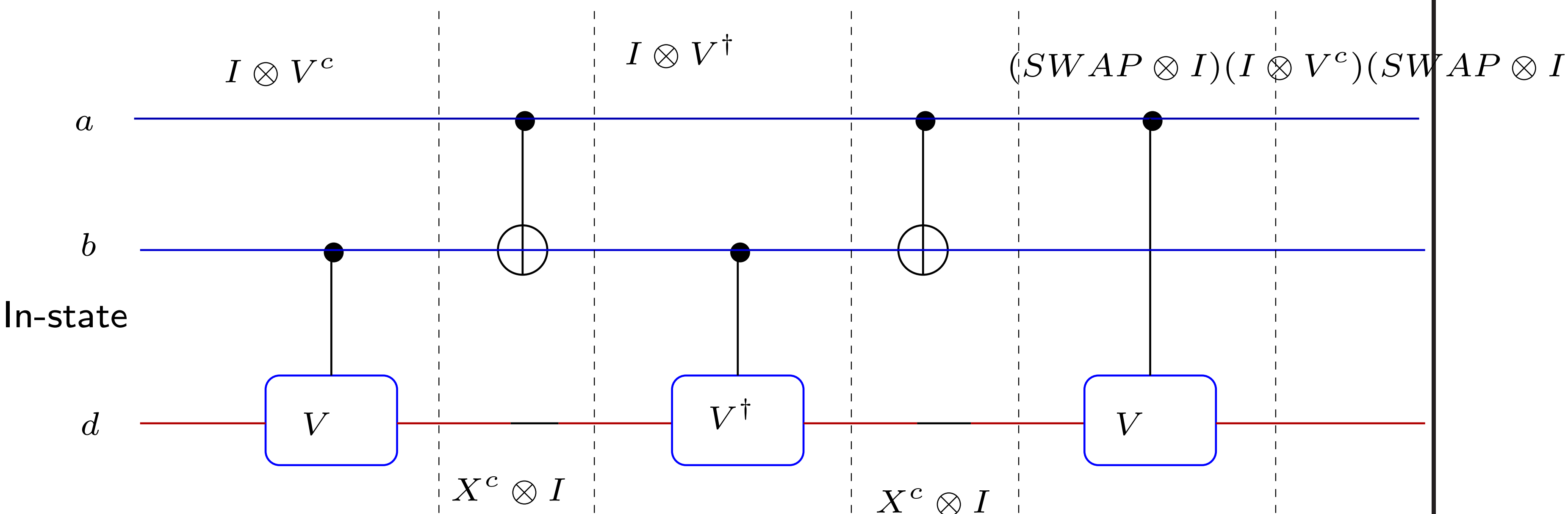
$C^2(U)$ where $U = V^2$

If the 1-qubit unitary operator $U = V^2$ where V is also unitary, then

$$\begin{aligned} C^2(U) &= (SWAP \otimes I)(I \otimes V^c)(SWAP \otimes I)(X^c \otimes I) \\ &\quad (I \otimes (V^\dagger)^c)(X^c \otimes I)(I \otimes V^c) \end{aligned}$$

This scheme uses $3 \times 4 = 12$ single-qubit gates and $3 \times 2 + 2 = 8$ CNOT gates.

$C^2(U)$ where $U = V^2$: Diagram



$C^2(U)$ where $U = V^2$

$C^2(U)$ where $U = V^2$

We apply the given sequence of transformations on $|00d\rangle, |01d\rangle, |10d\rangle$ and $|11d\rangle$, where $d \in \{0, 1\}$.

0. $|00d\rangle \stackrel{I\otimes V^c}{\longrightarrow} |00d\rangle \stackrel{X^c\otimes I}{\longrightarrow} |00d\rangle \stackrel{I\otimes(V^\dagger)^c}{\longrightarrow} |00d\rangle \stackrel{X^c\otimes I}{\longrightarrow} |00d\rangle \stackrel{SWAP\otimes I}{\longrightarrow} |00d\rangle \stackrel{I\otimes V^c}{\longrightarrow} |00d\rangle \stackrel{SWAP\otimes I}{\longrightarrow} |00d\rangle$

1. $|01d\rangle \stackrel{I\otimes V^c}{\longrightarrow} |01\rangle V|d\rangle \stackrel{X^c\otimes I}{\longrightarrow} |01\rangle V|d\rangle \stackrel{I\otimes(V^\dagger)^c}{\longrightarrow} |01\rangle V^\dagger V|d\rangle = |01d\rangle \stackrel{X^c\otimes I}{\longrightarrow} |01d\rangle \stackrel{SWAP\otimes I}{\longrightarrow} |10d\rangle \stackrel{I\otimes V^c}{\longrightarrow} |10d\rangle \stackrel{SWAP\otimes I}{\longrightarrow} |01d\rangle$

$C^2(U)$ where $U = V^2$

2. $|10d\rangle \stackrel{I\otimes V^c}{\longrightarrow} |10d\rangle \stackrel{X^c\otimes I}{\longrightarrow} |11d\rangle \stackrel{I\otimes (V^\dagger)^c}{\longrightarrow} |11\rangle V^\dagger |d\rangle \stackrel{X^c\otimes I}{\longrightarrow} |10\rangle V^\dagger |d\rangle \stackrel{SWAP\otimes I}{\longrightarrow} |01\rangle V^\dagger |d\rangle \stackrel{I\otimes V^c}{\longrightarrow} |01\rangle V V^\dagger |d\rangle = |01d\rangle \stackrel{SWAP\otimes I}{\longrightarrow} |10d\rangle$

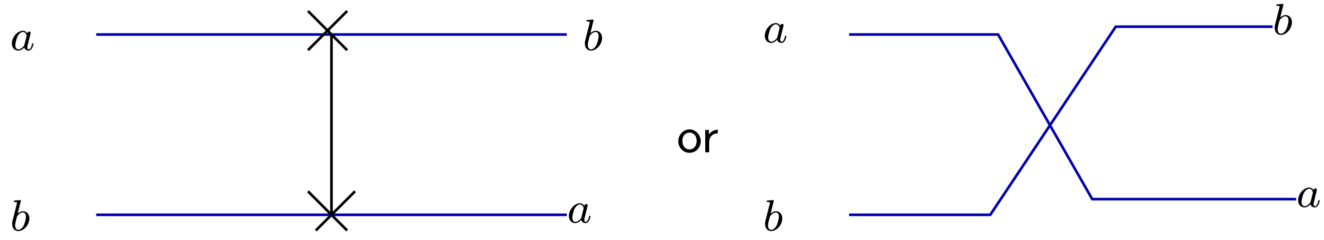
3. $|11d\rangle \stackrel{I\otimes V^c}{\longrightarrow} |11\rangle V |d\rangle \stackrel{X^c\otimes I}{\longrightarrow} |10\rangle V |d\rangle \stackrel{I\otimes (V^\dagger)^c}{\longrightarrow} |10\rangle V |d\rangle \stackrel{X^c\otimes I}{\longrightarrow} |11\rangle V |d\rangle \stackrel{SWAP\otimes I}{\longrightarrow} |11\rangle V |d\rangle \stackrel{I\otimes V^c}{\longrightarrow} |11\rangle V V |d\rangle = |11\rangle U |d\rangle \stackrel{SWAP\otimes I}{\longrightarrow} |11\rangle U |d\rangle$

SWAP Gate

An important 2-qubit gate is a SWAP gate. Its transition matrix is

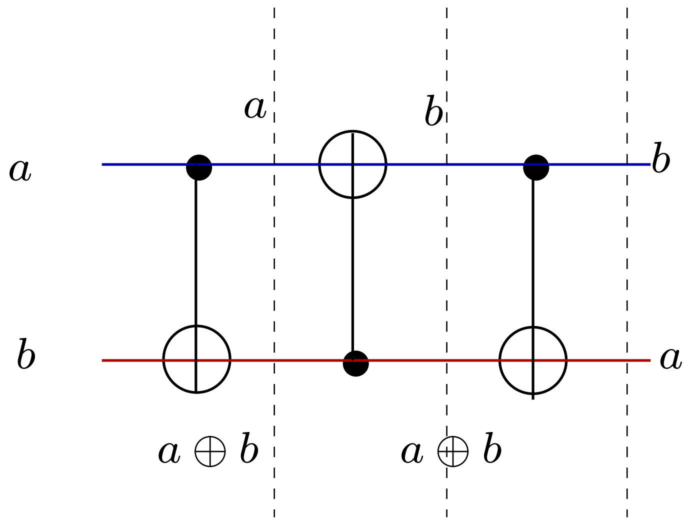
$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

SWAP Gate: Diagram

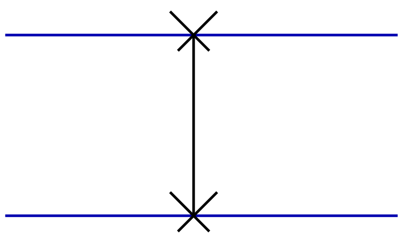


SWAP Gate

SWAP Gate using CNOT



$\equiv$



$$a \oplus (a \oplus b) = b, \; b \oplus (a \oplus b) = a$$

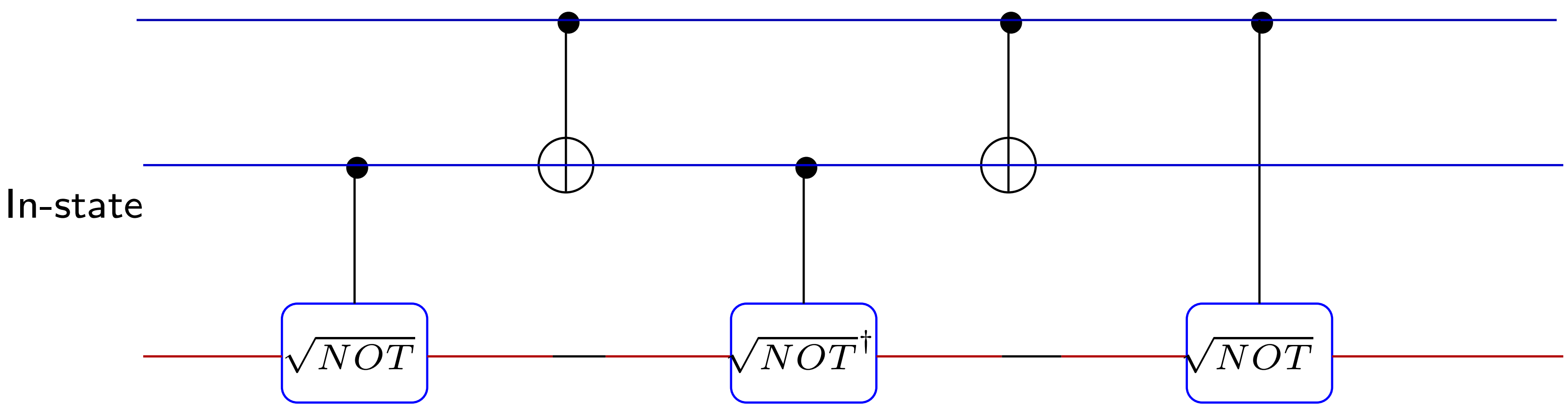
$\sqrt{NOT}$ Gate

The following gate is known as $\sqrt{NOT}$ such that $\sqrt{NOT} \cdot \sqrt{NOT} = NOT$.

$$\sqrt{NOT} = \frac{1}{2}\begin{bmatrix} 1+i & 1-i \\ 1-i & 1+i \end{bmatrix}.$$

This gate can be used to implement CCNOT or Toffoli gate.

Toffoli Gate using $\sqrt{NOT}$ Gate



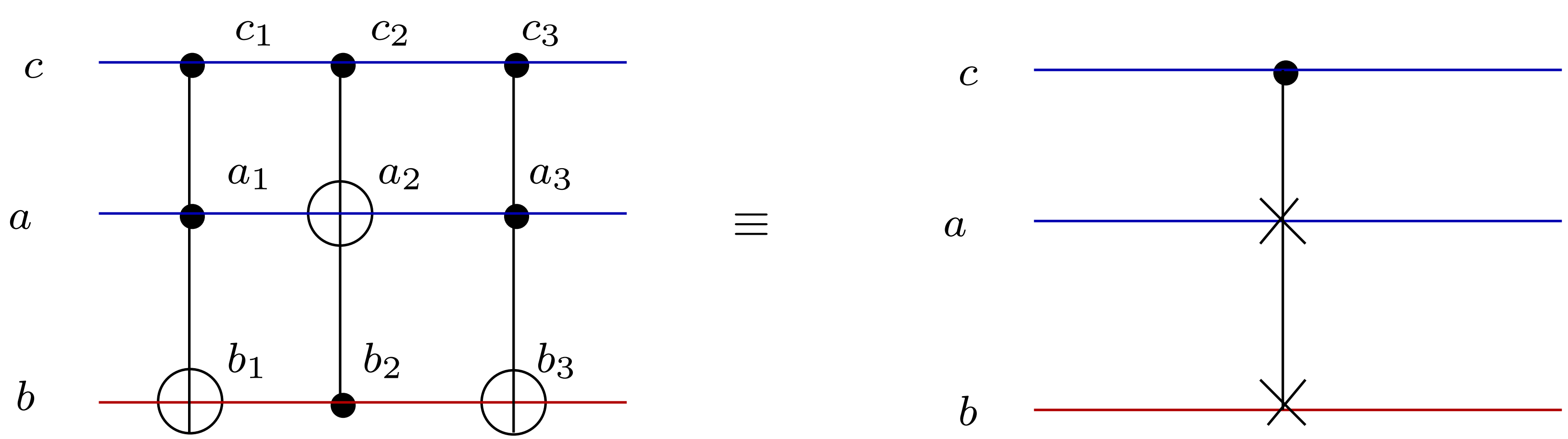
Note

Note that in Boolean logic, a Toffoli gate cannot be constructed using one-bit or two-bit gates. But a quantum Toffoli gate can be constructed using 2-qubit gates.

Fredkin or Controlled-Swap Gate

- We have already talked about the Fredkin or controlled-SWAP gate in connection to reversible Boolean logic.
- It is also known how a SWAP gate is implemented using 3 CNOT gates.
- So a Fredkin gate can be implemented as follows.

Fredkin or C-SWAP Gate using CCNOT



FREDKIN or Controlled-SWAP

Fredkin or C-SWAP Gate using CCCNOT

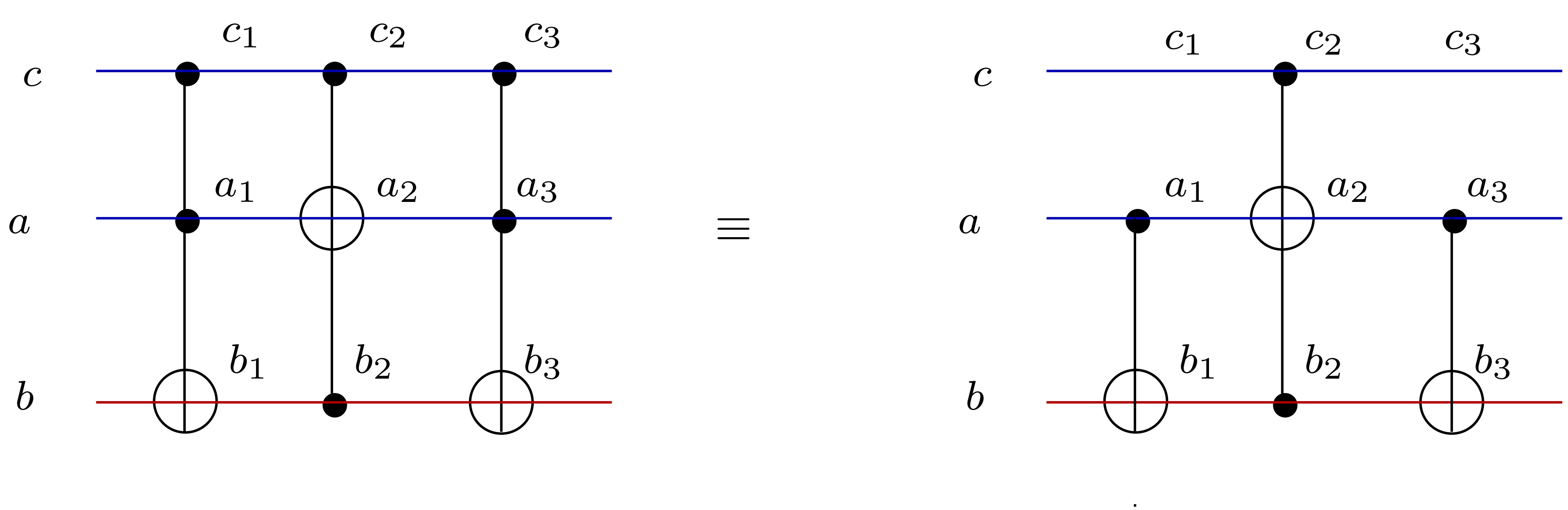
The computation of the left-hand circuit is

$$
\begin{aligned}
|c_1 a_1 b_1\rangle &= |c, a, b \oplus ca\rangle \\
|c_2 a_2 b_2\rangle &= |c, a \oplus c(b \oplus ca), b \oplus ca\rangle \\
|c_3 a_3 b_3\rangle &= |c, a \oplus c(b \oplus ca), (b \oplus ca) \oplus c(a \oplus c(b \oplus ca))\rangle
\end{aligned}
$$

- $c = 0$, $|c_3 a_3 b_3\rangle = |0, a, b\rangle$.
- $c = 1$, $|c_3 a_3 b_3\rangle = |1, b, a\rangle$ as $a \oplus (b \oplus a) = b$ and $(b \oplus a) \oplus (a \oplus (b \oplus a)) = a$.

Fredkin or Controlled-Swap Gate

We can replace the first and the third CCNOT gates by CNOT gates.



FREDKIN or Controlled-SWAP

The computation of the new circuit is

Fredkin Gate using CNOT and CCNOT

$$
\begin{aligned}
|c_1 a_1 b_1\rangle &= |c, a, b \oplus a\rangle \\
|c_2 a_2 b_2\rangle &= |c, a \oplus c(b \oplus a), b \oplus a\rangle \\
|c_3 a_3 b_3\rangle &= |c, a \oplus c(b \oplus a), (b \oplus a) \oplus (a \oplus c(b \oplus a))\rangle .
\end{aligned}
$$

- $c = 0$, $|c_3 a_3 b_3\rangle = |0, a, b\rangle$.
- $c = 1$, $|c_3 a_3 b_3\rangle = |1, b, a\rangle$ as $a \oplus (b \oplus a) = b$ and $(b \oplus a) \oplus (a \oplus (b \oplus a)) = a$.

Fredkin Gate using Only 2-Qubit Gates

- The CCNOT gate can be replaced by two CNOT, two $\sqrt{NOT}$ and one $\sqrt{NOT}^{\dagger}$ gate.
- So the Fredkin gate can be implemented using seven 2-qubit gates.
- This was impossible in classical Boolean logic.

H, S, T and CNOT

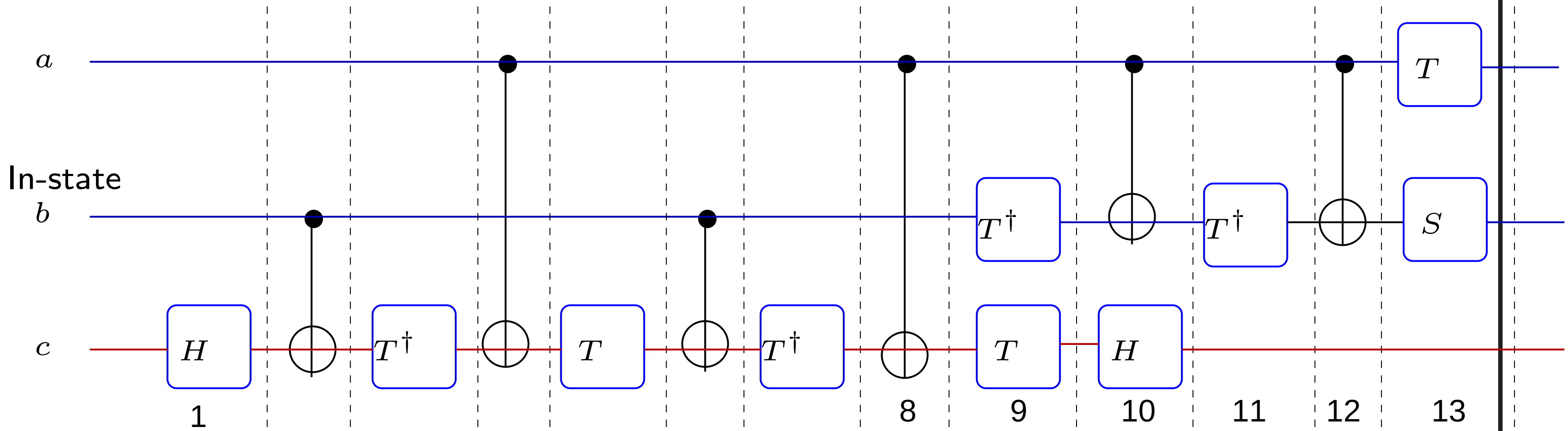
$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}, T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix},$$

and

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

These four gates can be used to approximate any unitary transformation.

CCNOT using H, S, T and CNOT



CCNOT using H, S, T and CNOT

$$|abc\rangle \xrightarrow{1} |ab\rangle H|c\rangle \xrightarrow{2} \cdots \xrightarrow{8} |ab\rangle X^aT^\dagger X^bTX^aT^\dagger X^bH|c\rangle,$$

$$\xrightarrow{9} \quad |a\rangle T^\dagger |b\rangle TX^aT^\dagger X^bTX^aT^\dagger X^bH|c\rangle$$

$$\xrightarrow{10} \quad |a\rangle X^aT^\dagger |b\rangle HTX^aT^\dagger X^bTX^aT^\dagger X^bH|c\rangle$$

$$\xrightarrow{11} \quad |a\rangle T^\dagger X^aT^\dagger |b\rangle HTX^aT^\dagger X^bTX^aT^\dagger X^bH|c\rangle$$

$$\xrightarrow{12} \quad |a\rangle X^aT^\dagger X^aT^\dagger |b\rangle HTX^aT^\dagger X^bTX^aT^\dagger X^bH|c\rangle$$

$$\xrightarrow{13} \quad T|a\rangle SX^aT^\dagger X^aT^\dagger |b\rangle HTX^aT^\dagger X^bTX^aT^\dagger X^bH|c\rangle$$

CCNOT using H, S, T and CNOT

- $a = 0$: $T\left|a\right\rangle = \left|0\right\rangle$, $SX^aT^\dagger X^aT^\dagger\left|b\right\rangle = S(T^\dagger)^2\left|b\right\rangle = \left|b\right\rangle$, $HTX^aT^\dagger X^bTX^aT^\dagger X^bH\left|c\right\rangle = \left|c\right\rangle$.
  So, $\left|0bc\right\rangle \stackrel{1\cdots12}{\rightarrow} \left|0bc\right\rangle$.
- $a = 1, b = 0$: $T\left|a\right\rangle = e^{i\pi/4}\left|1\right\rangle$, if we take the phase-factor $e^{i\pi/4}$ with the second term, we get $e^{i\pi/4}SX^aT^\dagger X^aT^\dagger\left|0\right\rangle = e^{i\pi/4}SXT^\dagger XT^\dagger\left|0\right\rangle = \left|0\right\rangle$.
  $HTX^aT^\dagger X^bTX^aT^\dagger X^bH\left|c\right\rangle = HTXT^\dagger TXT^\dagger H\left|c\right\rangle = \left|c\right\rangle$.
  So, $\left|10c\right\rangle \stackrel{1\cdots12}{\rightarrow} \left|10c\right\rangle$.

CCNOT using H, S, T and CNOT

- $a = 1 = b$: $T\,|a\rangle = e^{i\pi/4}\,|1\rangle$, if we take the phase-factor $e^{i\pi/4}$ with the second term, we get $e^{i\pi/4} S X^a T^\dagger X^a T^\dagger\,|1\rangle = e^{i\pi/4} S X T^\dagger X T^\dagger\,|1\rangle = i\,|1\rangle$.
  Transferring the phase-factor i to the third qubit state we get, $iHTX^aT^\dagger X^bTX^aT^\dagger X^bH\,|c\rangle = iH(TXT^\dagger X)(TXT^\dagger X)H\,|c\rangle = iH(-iZ)H\,|c\rangle = HZH\,|c\rangle = X\,|c\rangle$.
  So, $|11c\rangle \stackrel{1\cdots 12}{\rightarrow} |11\overline{c}\rangle$.
- So the circuit behaves like a CCNOT gate.

Controlled-U on $|0\rangle$

- The 1-qubit transformation U may be applied on the data-qubit when the control qubit is $|0\rangle$.
- The corresponding transformation matrix is

$$U^c_{|0\rangle} = \begin{bmatrix} u_{11} & u_{12} & 0 & 0 \\ u_{21} & u_{22} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

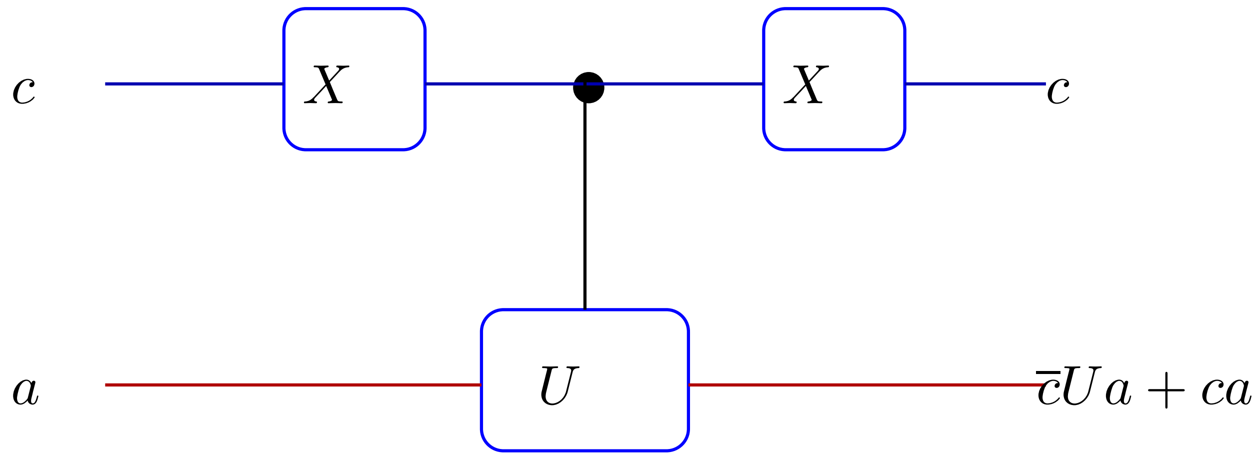
Controlled-U on $|0\rangle$

This can be achieved by $(X \otimes I) \circ U^c \circ (X \otimes I)$.

$$\begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{11} & u_{12} \\ 0 & 0 & u_{21} & u_{22} \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} u_{11} & u_{12} & 0 & 0 \\ u_{21} & u_{22} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Controlled-U on $|0\rangle$: Circuit



Controlled-U on $|0\rangle$