Matrix representation in Quantum Computing

Masatsugu Sei Suzuki
Department of Physics, SUNY at Binghamton
Binghamton, NY

(Date: December 03, 2014)

What is the quantum computer?

Quantum parallelism is not much use if we cannot do anything more than encode the input. To build a computer we need to design physical devices that manipulate qubits to perform logical operations. These devices must be capable of perfectly reversible operation, that is to say, they must be unitary devices including CNOT gate, Hadamard gate, Toffoli gate, and Fredkin gate.

It has always been assumed that any computational step required energy. The first guess, and one that was a common belief for years, was that there was a minimum amount of energy required for each logical step taken by a machine. From what we have looked at so far, you should be able to appreciate the argument. The idea is that every logical state of a device must correspond to some physical state of the device, and whenever the device had to choose between 0 and 1 for its output - such as a transistor in an AND gate - there would be a compression of the available phase-space of the object from two

((**Reference**))

R.P. Feynman, Lectures on Quantum Computation (Addison Wesley, 1996)
G.J. Milburn, Feynman Proccessor (Perseus Book, Cambridge MA, 1998)

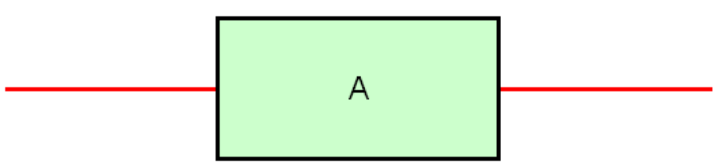
A quantum gate has an equal number of qubits and the output states are described by vectors in a Hibert space with the corresponding number of dimensions. The input/output state of a n-qubits quantum gate is calculated as the tensor product (Kronecker product) of the corresponding state vectors of the individual input/output qubits.

1. Quantum circuits

Suppose that all the matrices describing quantum gates are of the same size.

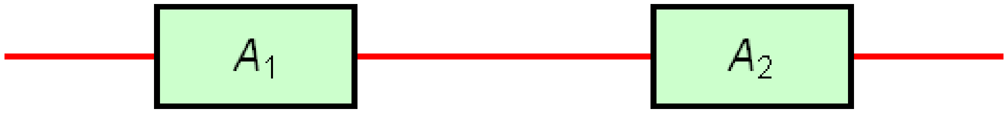
(a) $\hat{A}$

We introduce a notation of quantum circuit. We draw a one-qubit operator $\hat{A}$ like a box as shown below.

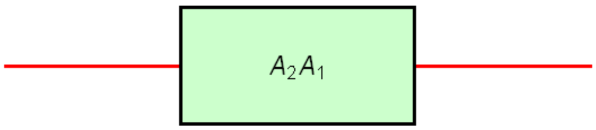


(b) Scalar product (inner product) $\hat{A}_2\hat{A}_1$

We consider two such gates by stringing them together,

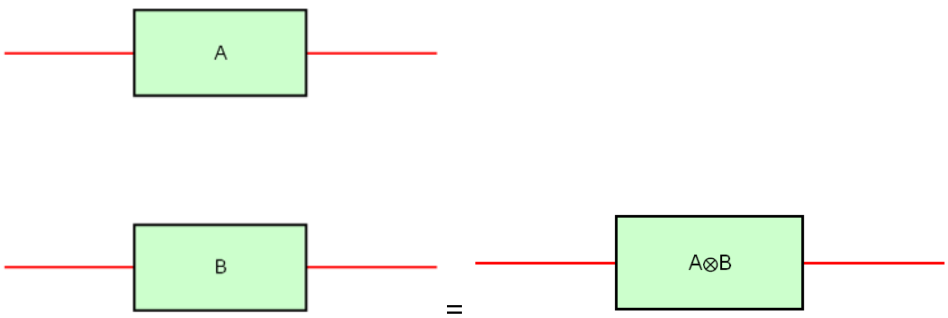


which is equivalent to the scalar product of two operators $\hat{A}_1\hat{A}_2$ in this order.



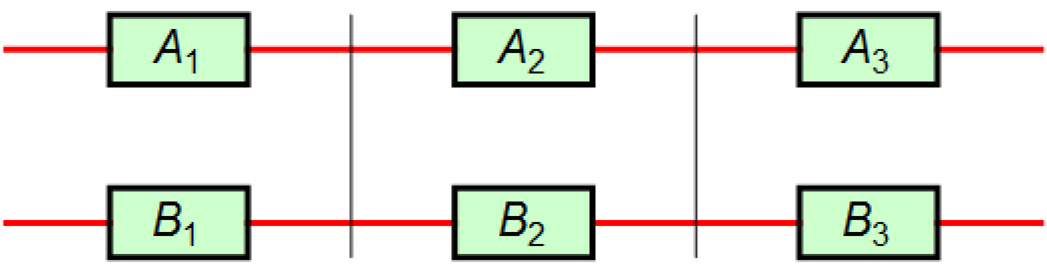
(c) Kronecker product $\hat{A}\otimes\hat{B}$

If we have two qubits, applying two operators in parallel (Fig.a) gives their Kronecker product of two operators, $\hat{A}\otimes\hat{B}$

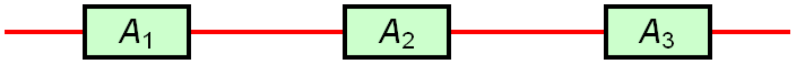


(d) $(\hat{A}_3\otimes\hat{B}_3)(\hat{A}_2\otimes\hat{B}_2)(\hat{A}_1\otimes\hat{B}_1)=\hat{A}_3\hat{A}_2\hat{A}_1\otimes\hat{B}_3\hat{B}_2\hat{B}_1$

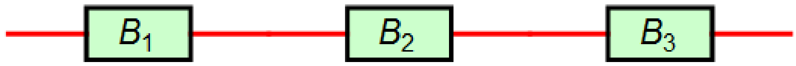
The quantum circuits of this figure is described by $(\hat{A}_3\otimes\hat{B}_3)(\hat{A}_2\otimes\hat{B}_2)(\hat{A}_1\otimes\hat{B}_1)$.



This is equivalent to the Kronecker product of two operators $\hat{A}_3\hat{A}_2\hat{A}_1$

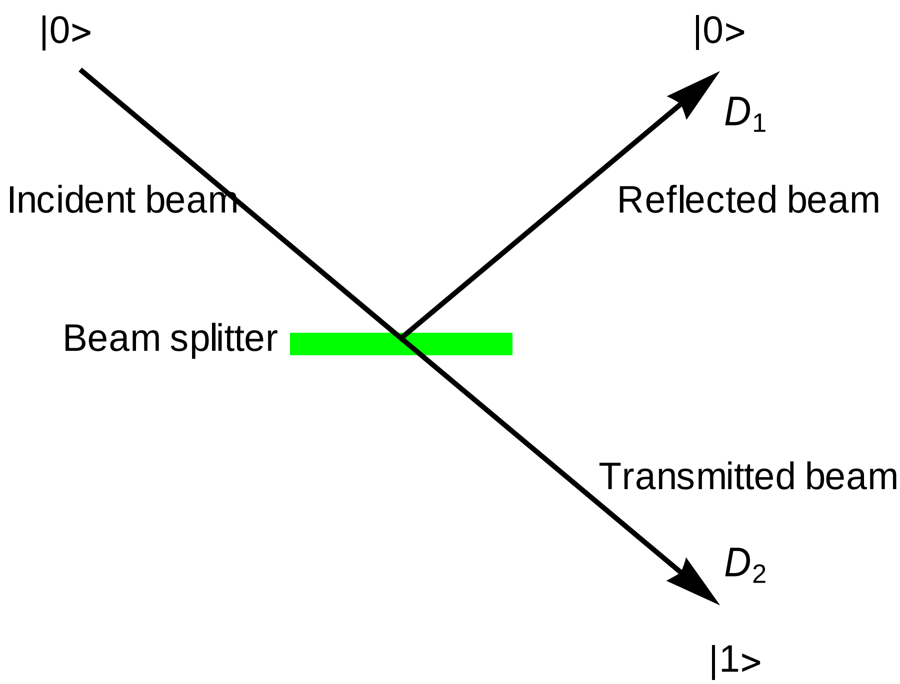


and $\hat{B}_3\hat{B}_2\hat{B}_1$



2. Hadamard gate, beam splitter

We consider a device called a beam splitter, a half-silvered mirror. A beam of light falling on a beam splitter is split into two components, one transmitted and one reflected. A beam splitter may transmit a larger or a smaller fraction of the incident light depending upon the characteristics of the silver deposition. For the experiments discussed here, the two components are of equal intensity. The color of the light is not altered by a beam splitter, a behavior consistent with a wave.



We consider a 50-50 beam splitter where an incident particle coming from above or from below has the same probability of emerging as an upwards or a downwards beam. The transformation performed by the beam splitter is described by the Walsh-Hadamard transform.

$$\hat{H} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

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

Similarly

$$\hat{H}|1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0\\ 1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ -1\end{pmatrix} = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

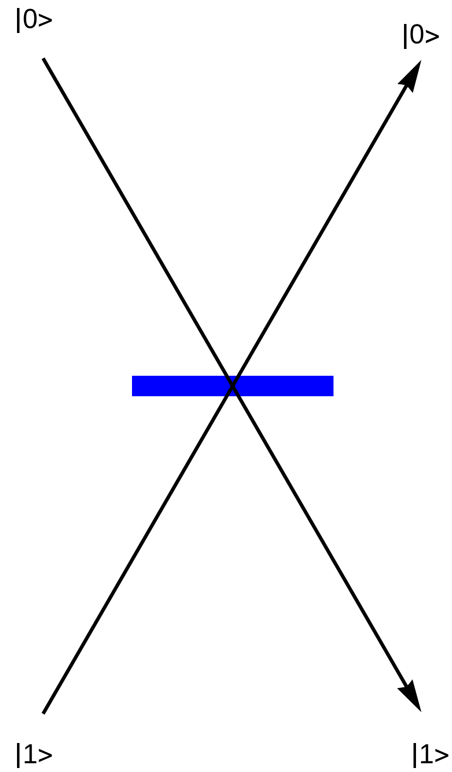


Fig. A beam splitter performs a transformation described by a Hamadard gate.

Let us call the input to a Hadamard gate as $|\psi\rangle = c_0|0\rangle + c_1|1\rangle = \begin{pmatrix}c_0\\ c_1\end{pmatrix}$ and call its output as $|\varphi\rangle = \hat{H}|\psi\rangle$. Using the matrix of the Hadamard operator

$$\hat{H} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}.$$

we have

$$
\begin{aligned}
|\varphi\rangle &= \hat{H}|\psi\rangle \\
&= \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} c_0 \\ c_1 \end{pmatrix} \\
&= \frac{1}{\sqrt{2}}\begin{pmatrix} c_0 + c_1 \\ c_0 - c_1 \end{pmatrix} \\
&= \frac{1}{\sqrt{2}}(c_0 + c_1)|0\rangle + \frac{1}{\sqrt{2}}(c_0 - c_1)|1\rangle
\end{aligned}
$$

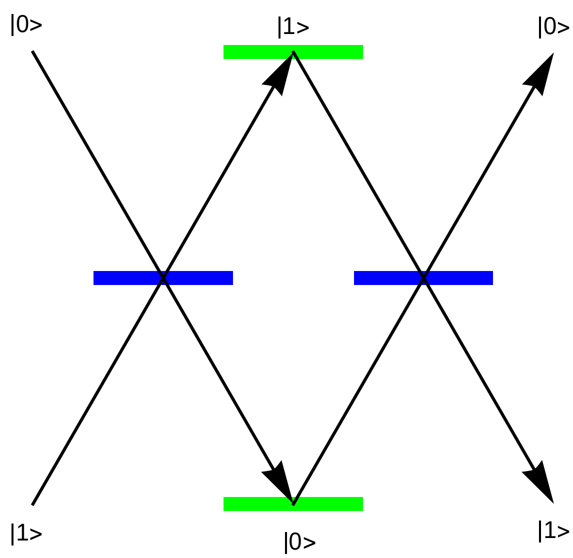
or

$$
|\varphi\rangle = \frac{c_0}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} + \frac{c_1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{c_0}{\sqrt{2}}(|0\rangle + |1\rangle) + \frac{c_1}{\sqrt{2}}((|0\rangle - |1\rangle)
$$

The probability amplitude for finding the particle in the outgoing beam directed upward is $\frac{1}{\sqrt{2}}(c_0 + c_1)$ and the probability amplitude for finding the particle in the outgoing beam directed downwards is $\frac{1}{\sqrt{2}}(c_0 - c_1)$.

We now consider a system consisting of two cascaded beam splitters. In this case the output is given by

$$
|\varphi\rangle = \hat{H}^2|\psi\rangle
$$



Here we note that

$$\hat{H}^2 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = \hat{1}$$

Thus we get

$$|\varphi\rangle = \hat{H}^2|\psi\rangle = \hat{1}|\psi\rangle = |\psi\rangle .$$

In general,

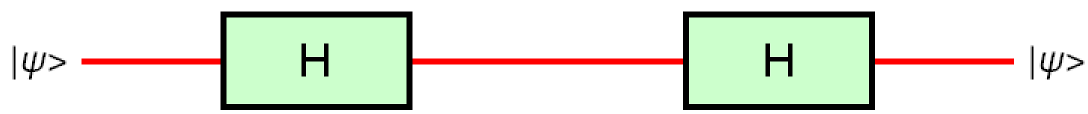
$$|\varphi\rangle = \hat{H}^{2n}|\psi\rangle = |\psi\rangle, \qquad |\varphi\rangle = \hat{H}^{2n+1}|\psi\rangle = \hat{H}|\psi\rangle .$$

3. Arrangement of Hadamard gates in parallel and in series

$$\hat{H}|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \qquad \hat{H}|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

We now apply to an arbitrary qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

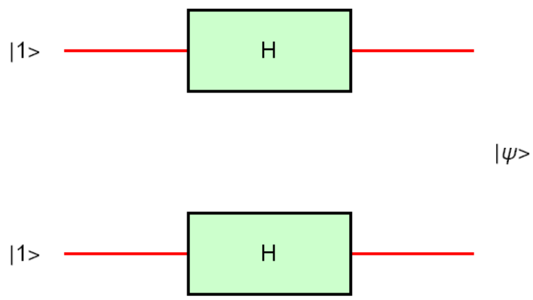
(a) Hadamard gates in series



$$\hat{H}|\psi\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} \alpha+\beta \\ \alpha-\beta \end{pmatrix}$$

$$\hat{H}^2|\psi\rangle = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} \alpha+\beta \\ \alpha-\beta \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = |\psi\rangle$$

(b) Hadamard gates in parallel



$$(\hat{H}\otimes\hat{H})(|1\rangle\otimes|1\rangle)=\hat{H}|1\rangle\otimes\hat{H}|1\rangle=\frac{1}{2}(|0\rangle-|1\rangle)\otimes(|0\rangle-|1\rangle)=\frac{1}{2}(|00\rangle-|01\rangle-|10\rangle+|11\rangle)$$

Similarly, we have

$$(\hat{H}\otimes\hat{H})(|0\rangle\otimes|0\rangle)=\hat{H}|0\rangle\otimes\hat{H}|0\rangle=\frac{1}{2}(|0\rangle+|1\rangle)\otimes(|0\rangle+|1\rangle)=\frac{1}{2}(|00\rangle+|01\rangle+|10\rangle+|11\rangle)$$

$$(\hat{H}\otimes\hat{H})(|0\rangle\otimes|1\rangle)=\hat{H}|0\rangle\otimes\hat{H}|0\rangle=\frac{1}{2}(|0\rangle+|1\rangle)\otimes(|0\rangle-|1\rangle)=\frac{1}{2}(|00\rangle-|01\rangle+|10\rangle-|11\rangle)$$

$$(\hat{H}\otimes\hat{H})(|1\rangle\otimes|0\rangle)=\hat{H}|1\rangle\otimes\hat{H}|0\rangle=\frac{1}{2}(|0\rangle-|1\rangle)\otimes(|0\rangle+|1\rangle)=\frac{1}{2}(|00\rangle+|01\rangle-|10\rangle-|11\rangle)$$

4. Quantum CNOT gate

We consider the property of the operator $\hat{U}_{CNOT}$

$$|W_{CNOT}\rangle=\hat{G}_{CNOT}|V_{CNOT}\rangle$$

where

$$\hat{G}_{CNOT}=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}$$

The input state vector is

$$\begin{aligned}|V_{CNOT}\rangle&=(\alpha_0|0\rangle+\alpha_1|1\rangle)\otimes(\beta_0|0\rangle+\beta_1|1\rangle)\\&=\alpha_0\beta_0|00\rangle+\alpha_0\beta_1|01\rangle+\alpha_1\beta_0|10\rangle+\alpha_1\beta_1|11\rangle\end{aligned}$$

The components of the input vector are transformed by the CNOT quantum gate as follows,

$$\hat{G}_{CNOT}|00\rangle = |00\rangle, \qquad \hat{G}_{CNOT}|01\rangle = |01\rangle,$$

$$\hat{G}_{CNOT}|10\rangle = |11\rangle, \qquad \hat{G}_{CNOT}|11\rangle = |10\rangle$$

where

$$\hat{G}_{CNOT}|xy\rangle = |x, y \oplus x\rangle.$$

We note that

$$\begin{aligned}
\hat{G}_{CNOT} &= \hat{G}_{CNOT}(|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| + |11\rangle\langle 11|) \\
&= |00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11|) \\
&= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}
\end{aligned}$$

Then the output state vector is obtained as

$$\begin{aligned}
|W_{CNOT}\rangle &= \hat{G}_{NOT}|V_{CNOT}\rangle \\
&= \hat{G}_{NOT}[\alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|10\rangle + \alpha_1\beta_1|11\rangle] \\
&= \alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|11\rangle + \alpha_1\beta_1|10\rangle \\
&= \alpha_0|0\rangle \otimes [\beta_0|0\rangle + \beta_1|1\rangle] + \alpha_1|1\rangle \otimes [\beta_0|1\rangle + \beta_1|0\rangle]
\end{aligned}$$

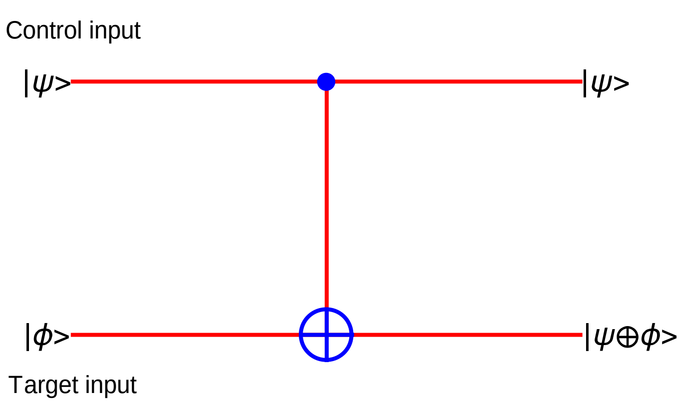


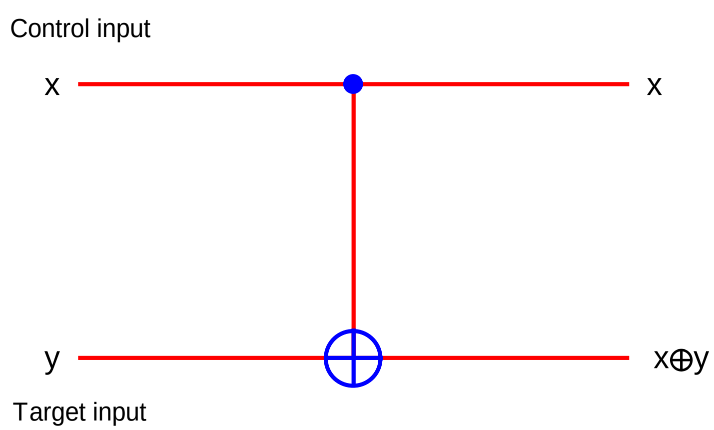
Fig. Quantum CNOT gate has two inputs as well; the control input is a qubit in state $|\psi\rangle$ and the target input is a qubit in state $|\phi\rangle$.

$$
\begin{aligned}
|W_{CNOT}\rangle &= \hat{G}_{NOT}|V_{CNOT}\rangle \\
&= \hat{G}_{NOT}[\alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|10\rangle + \alpha_1\beta_1|11\rangle] \\
&= \alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|11\rangle + \alpha_1\beta_1|10\rangle \\
&= \alpha_0|0\rangle \otimes [\beta_0|0\rangle + \beta_1|1\rangle] + \alpha_1|1\rangle \otimes [\beta_0|1\rangle + \beta_1|0\rangle]
\end{aligned}
$$

5. Possibility of cloning

(a) Classical CNOT gate

One can show that it is possible to replicate an input signal using classical gate. If the target input of a classical CNOT gate is 0, the circuit simply replicates input x on both output lines since $x \oplus 0 = x$. Thus the classical CNOT gate allows one to replicate an input bit.



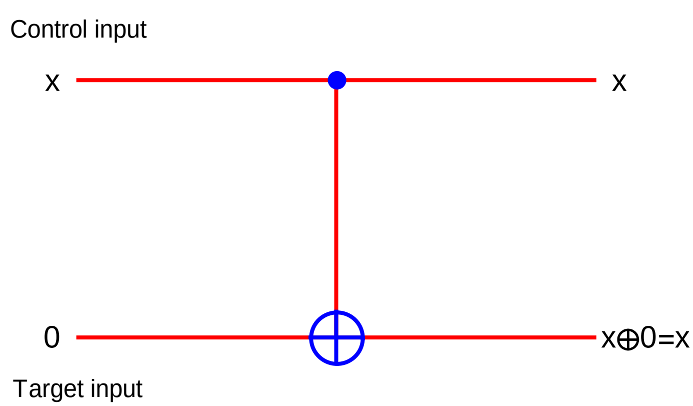
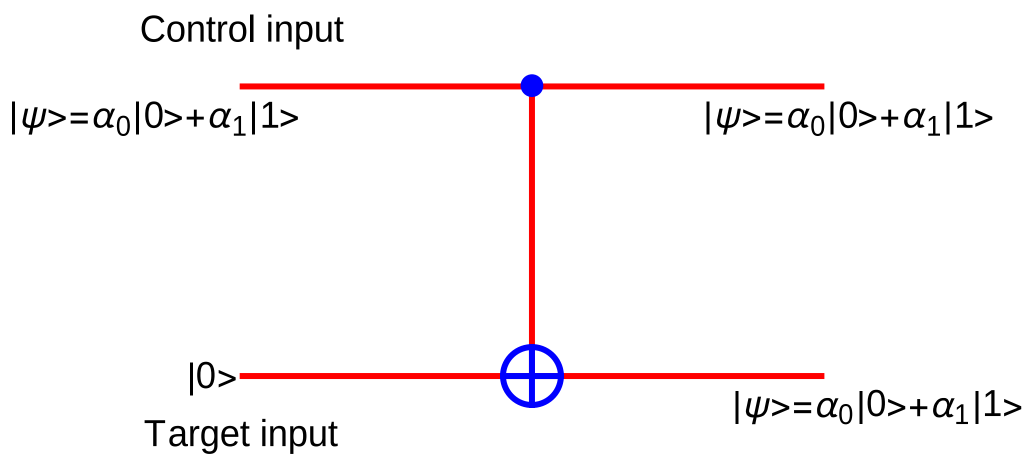


Fig. Classical CNOT gate. The target output is equal to the target input if the control input is zero and it is flipped if the control input is 1.

(b) Quantum CNOT gate

It is a single-qubit quantum NOT gate that can be activated or deactivated by the state of another qubit. This gate is sometimes called the measurement gate because it can be used to measure one qubit by looking at the other one. Here we show that the above method used for the classical CNOT gate is not applicable to the quantum CNOT gate.



From the analogy with the classical case, we assume that the target input is given by $|0\rangle$. Then the input vector is obtained as

$$
\begin{aligned}
|V\rangle &= (\alpha_0|0\rangle + \alpha_1|1\rangle)\otimes|0\rangle \\
&= \alpha_0|00\rangle + \alpha_1|10\rangle \\
&= \begin{pmatrix} \alpha_0 \\ 0 \\ \alpha_1 \\ 0 \end{pmatrix}
\end{aligned}
$$

The actual output state vector is

$$
\begin{aligned}
|W_{CNOT}\rangle &= \hat{G}_{CNOT}|V\rangle \\
&= \hat{G}_{CNOT}[\alpha_0|00\rangle + \alpha_1|10\rangle] \\
&= \alpha_0|00\rangle + \alpha_1|11\rangle \\
&= \begin{pmatrix} \alpha_0 \\ 0 \\ 0 \\ \alpha_1 \end{pmatrix}
\end{aligned}
$$

The desired state (in the vase of possible cloning) is

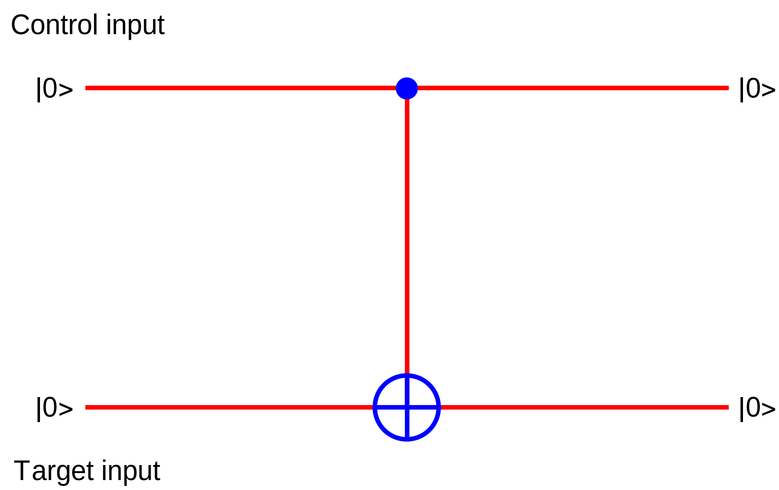
$$|W_{desired}\rangle = [\alpha_0|00\rangle + \alpha_1|10\rangle] \otimes [\alpha_0|00\rangle + \alpha_1|10\rangle]$$
$$= \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} \otimes \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$$
$$= \begin{pmatrix} \alpha_0{}^2 \\ \alpha_0\alpha_1 \\ \alpha_1\alpha_0 \\ \alpha_1{}^2 \end{pmatrix}$$

((**Example**))

This gate has two inputs and two outputs. The top input is the control qubit. It controls what the output will be. If $|c\rangle = |0\rangle$, then the bottom output will be the same as the input. f $|c\rangle = |1\rangle$, then the bottom output will be the same as the input. Then the bottom output will be the opposite.

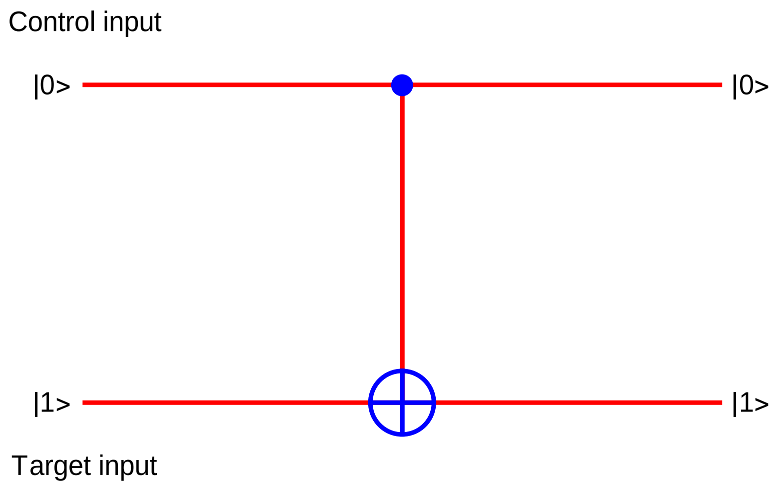
We examine the several cases whether output state vector may or may not be the same as the input state vector.

(i) The case-1



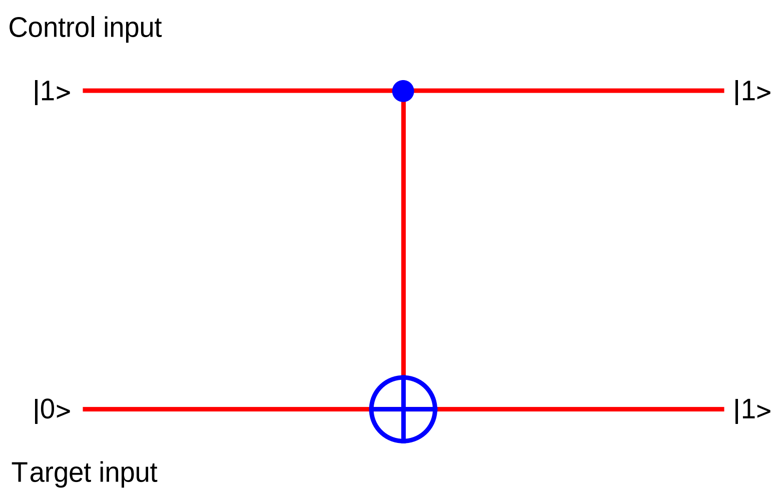
$|V\rangle = |00\rangle$, $|W_{CNOT}\rangle = \hat{G}_{CNOT}|00\rangle = |00\rangle$ (replicable)

(ii) The case 2



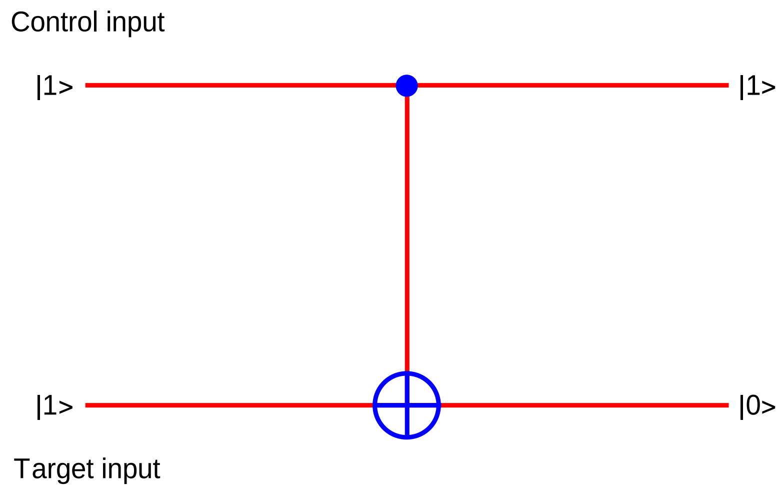
$|V\rangle = |01\rangle$, $|W_{CNOT}\rangle = \hat{G}_{CNOT}|01\rangle = |01\rangle$ (not replicable, the desired output state vector is $|00\rangle$)

(iii) The case-3



$|V\rangle = |10\rangle$, $|W_{CNOT}\rangle = \hat{G}_{NOT}|10\rangle = |11\rangle$ (replicable)

(iv) The case 4



$|V\rangle = |11\rangle$, $|W_{CNOT}\rangle = \hat{G}_{NOT}|11\rangle = |10\rangle$ (not replicable, the desired output state vector is $|11\rangle$)

((**Note**))

The CNOT gate can be reversed by itself. We consider the following figure: The state $|x, y\rangle$ goes to $|x, x \oplus y\rangle$, which further goes to $|x, x \oplus (x \oplus y)\rangle$. This last state is equal to $|x, (x \oplus x) \oplus y\rangle$. Because $x \oplus x = 0$ (always), this state reduces to its original $|x, y\rangle = |x\rangle \otimes |y\rangle$.

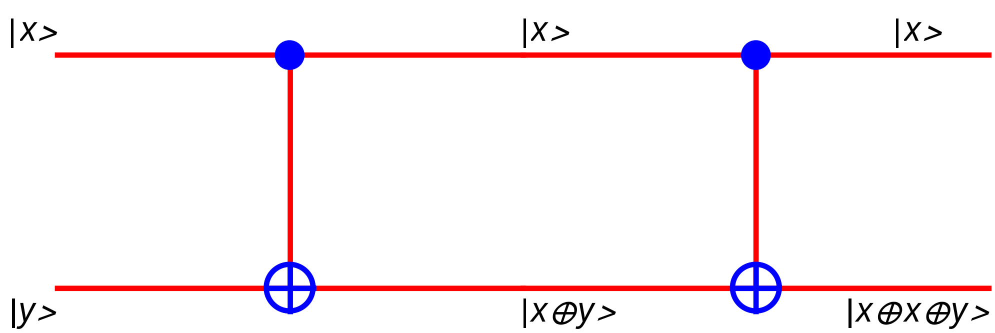
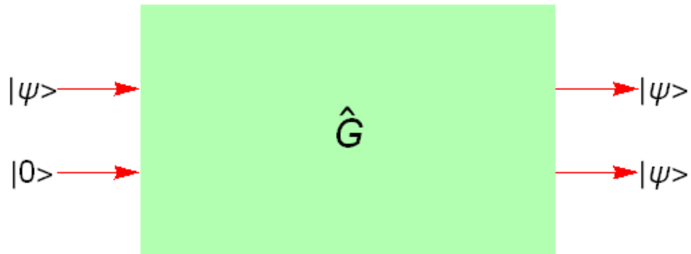


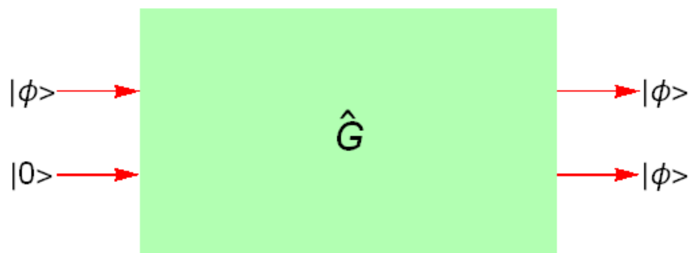
Fig. the output state is given by $|x\rangle$ and $|x \oplus x \oplus y\rangle = |0 \oplus y\rangle = |y\rangle$

6. Non-cloning theorem

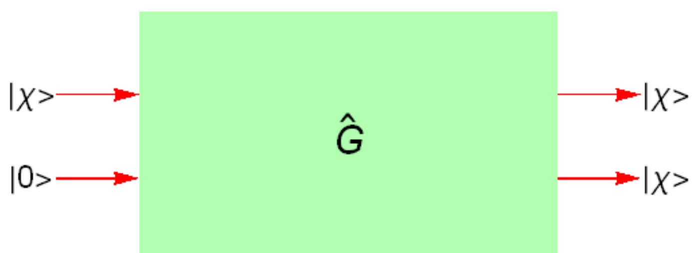
The transformation carried out by the quantum gate are unitary. As a consequence of this, unknown quantum states cannot be copied or cloned. We show this theorem as follows.



$$\hat{G}(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle$$



$$\hat{G}(|\phi\rangle \otimes |0\rangle) = |\phi\rangle \otimes |\phi\rangle$$



$$\hat{G}(|\chi\rangle \otimes |0\rangle) = |\chi\rangle \otimes |\chi\rangle,$$

where

$$|\chi\rangle = \frac{1}{\sqrt{2}}(|\psi\rangle + |\phi\rangle).$$

Then we have

$$\begin{aligned}\hat{G}(|\chi\rangle \otimes |0\rangle) &= \frac{1}{\sqrt{2}}\hat{G}(|\psi\rangle \otimes |0\rangle) + \frac{1}{\sqrt{2}}\hat{G}|\phi\rangle \otimes |0\rangle \\ &= \frac{1}{\sqrt{2}}(|\psi\rangle \otimes |\psi\rangle + |\phi\rangle \otimes |\phi\rangle)\end{aligned} \qquad (1)$$

On the other hand,

$$\begin{aligned} |\chi\rangle \otimes |\chi\rangle &= \frac{1}{2}(|\psi\rangle + |\phi\rangle) \otimes (|\psi\rangle + |\phi\rangle) \\ &= \frac{1}{2}(|\psi\rangle \otimes |\psi\rangle + |\psi\rangle \otimes |\phi\rangle + |\phi\rangle \otimes |\psi\rangle + |\phi\rangle \otimes |\phi\rangle) \end{aligned} \tag{2}$$

Eqs.(1) and (2) are clearly different. This implies that there is no linear operation that reliably clones unknown quantum states.

7. Non Cloning theorem

In physics, the no-cloning theorem is a no-go theorem of quantum mechanics that forbids the creation of identical copies of an arbitrary unknown quantum state. It was stated by Wootters and Zurek and Dieks in 1982, and has profound implications in quantum computing and related fields. The state of one system can be entangled with the state of another system. For instance, one can use the controlled NOT gate and the Walsh-Hadamard gate to entangle two qubits. This is not cloning. No well-defined state can be attributed to a subsystem of an entangled state. Cloning is a process whose result is a separable state with identical factors. According to Asher Peres and David Kaiser, the publication of the no-cloning theorem was prompted by a proposal of Nick Herbert for a superluminal communication device using quantum entanglement.

The no-cloning theorem is normally stated and proven for pure states; the no-broadcast theorem generalizes this result to mixed states. The no-cloning theorem has a time-reversed dual, the no-deleting theorem. Together, these underpin the interpretation of quantum mechanics in terms of category theory, and, in particular, as a dagger compact category. This formulation, known as categorical quantum mechanics, allows, in turn, a connection to be made from quantum mechanics to linear logic as the logic of quantum information theory (in the same sense that classical logic arises from Cartesian closed categories).
http://en.wikipedia.org/wiki/No-cloning_theorem

((**Note**))
No cloning theorem

$$\hat{Q}(a|\psi\rangle + b|\phi\rangle) = a\hat{Q}|\psi\rangle + b\hat{Q}|\phi\rangle$$

We define the cloning operator $\hat{C}$

$$\hat{C}|\phi,\psi\rangle = |\phi,\phi\rangle \qquad \text{for arbitrary } |\psi\rangle$$

$$\hat{C}|+z,\psi\rangle = |+z,+z\rangle$$

$$\hat{C}|-z,\psi\rangle = |-z,-z\rangle$$

Suppose that

$$\hat{C}|+x,\psi\rangle = |+x,+x\rangle \tag{1}$$

We note that

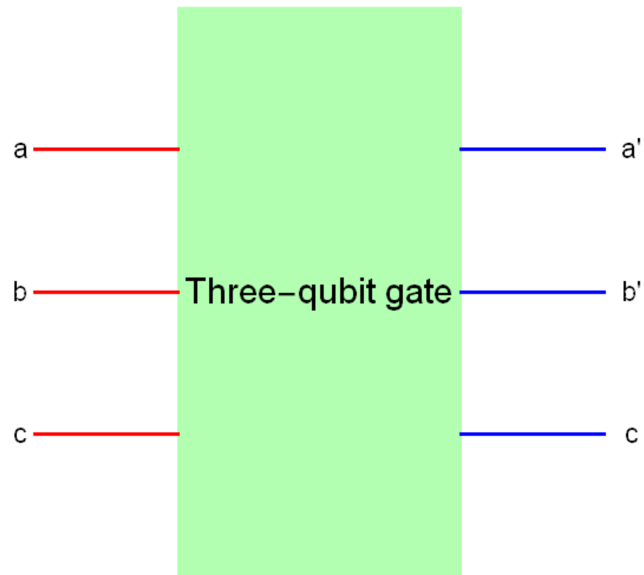
$$\begin{aligned}|+x,+x\rangle &= \frac{1}{2}(|+z\rangle + |-z\rangle)(|+z\rangle + |-z\rangle) \\ &= \frac{1}{2}(|+z,+z\rangle + |+z,-z\rangle + |-z,+z\rangle + |-z,-z\rangle)\end{aligned}$$

We also have

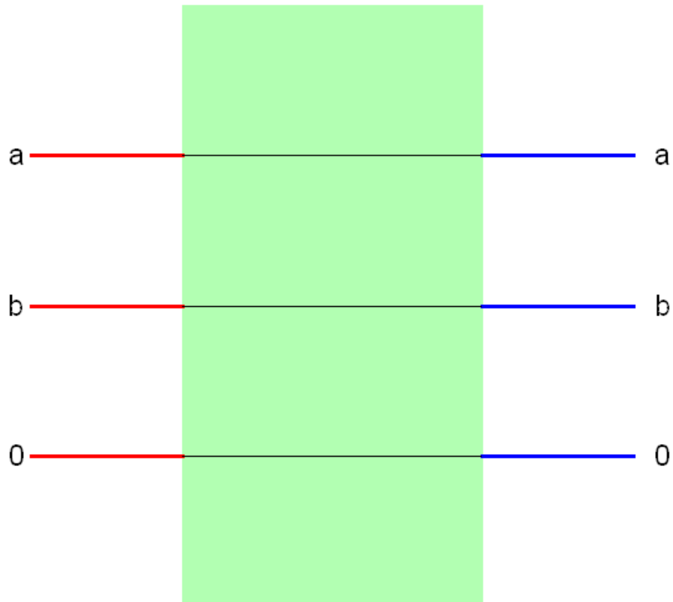
$$\begin{aligned}\hat{C}|+x,\psi\rangle &= \hat{C}|+x\rangle|\psi\rangle \\ &= \frac{1}{\sqrt{2}}[\hat{C}|+z,\psi\rangle + \hat{C}|-z,\psi\rangle] \\ &= \frac{1}{\sqrt{2}}[|+z,+z\rangle + |-z,-z]\rangle\end{aligned}$$

So Eq.(1) is not valid, implying that no clone can exist.

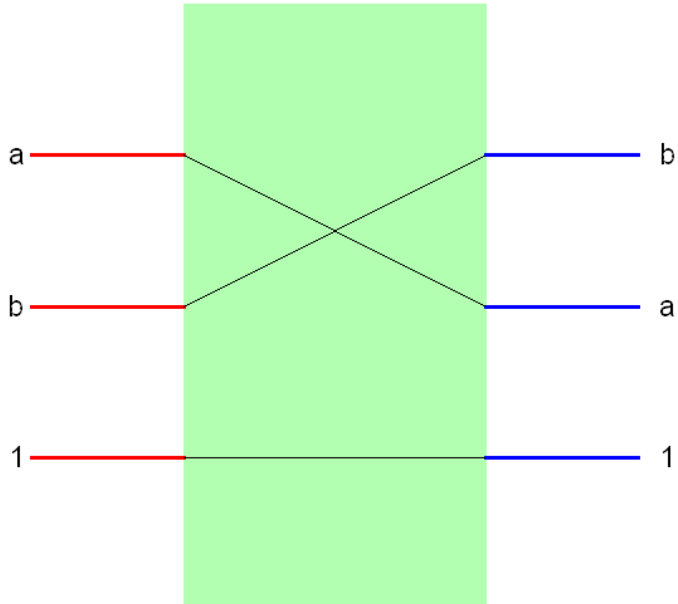
8. Fredkin gate



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**	1	0	**1**
1	0	**0**	1	0	**0**
1	0	**1**	0	1	**1**
1	1	**0**	1	1	**0**
1	1	**1**	1	1	**1**



Input			Output		
a	b	c	a'	b'	c'
0	0	**0**	0	0	**0**
0	1	**0**	0	1	**0**
1	0	**0**	1	0	**0**
1	1	**0**	1	1	**0**



Input			Output		
a	b	c	a'	b'	c'
0	0	**1**	0	0	**1**
0	1	**1**	1	0	**1**
1	0	**1**	0	1	**1**
1	1	**1**	1	1	**1**

$$|000\rangle = \begin{pmatrix}1\\0\\0\\0\\0\\0\\0\\0\end{pmatrix}, \quad |001\rangle = \begin{pmatrix}0\\1\\0\\0\\0\\0\\0\\0\end{pmatrix}, \quad |010\rangle = \begin{pmatrix}0\\0\\1\\0\\0\\0\\0\\0\end{pmatrix}, \quad |011\rangle = \begin{pmatrix}0\\0\\0\\1\\0\\0\\0\\0\end{pmatrix}$$

$$|100\rangle=\begin{pmatrix}1\\0\\0\\0\\1\\0\\0\\0\end{pmatrix},\qquad |101\rangle=\begin{pmatrix}0\\1\\0\\0\\0\\1\\0\\0\end{pmatrix},\qquad |110\rangle=\begin{pmatrix}0\\0\\1\\0\\0\\0\\1\\0\end{pmatrix},\qquad |111\rangle=\begin{pmatrix}0\\0\\0\\0\\0\\0\\0\\1\end{pmatrix},$$

$$\hat{G}_{Fredkin}|000\rangle=|000\rangle\,,$$
$$\hat{G}_{Fredkin}|001\rangle=|001\rangle\,,$$
$$\hat{G}_{Fredkin}|010\rangle=|010\rangle\,,$$
$$\hat{G}_{Fredkin}|011\rangle=|101\rangle\,,$$
$$\hat{G}_{Fredkin}|100\rangle=|100\rangle,$$
$$\hat{G}_{Fredkin}|101\rangle=|011\rangle,$$
$$\hat{G}_{Fredkin}|110\rangle=|110\rangle,$$
$$\hat{G}_{Fredkin}|111\rangle=|111\rangle\,.$$

We use the closure relation,

$$\begin{aligned}\hat{G}_{Fredkin} &= \hat{G}_{Fredkin}(|000\rangle\langle 000|+|001\rangle\langle 001|+|010\rangle\langle 010|+|011\rangle\langle 011| \\ &\quad +|100\rangle\langle 100|+|101\rangle\langle 101|+|110\rangle\langle 110|+|111\rangle\langle 111|) \\ &= |000\rangle\langle 000|+|001\rangle\langle 001|+|010\rangle\langle 010|+|101\rangle\langle 011| \\ &\quad +|100\rangle\langle 100|+|011\rangle\langle 101|+|110\rangle\langle 110|+|111\rangle\langle 111|\end{aligned}$$

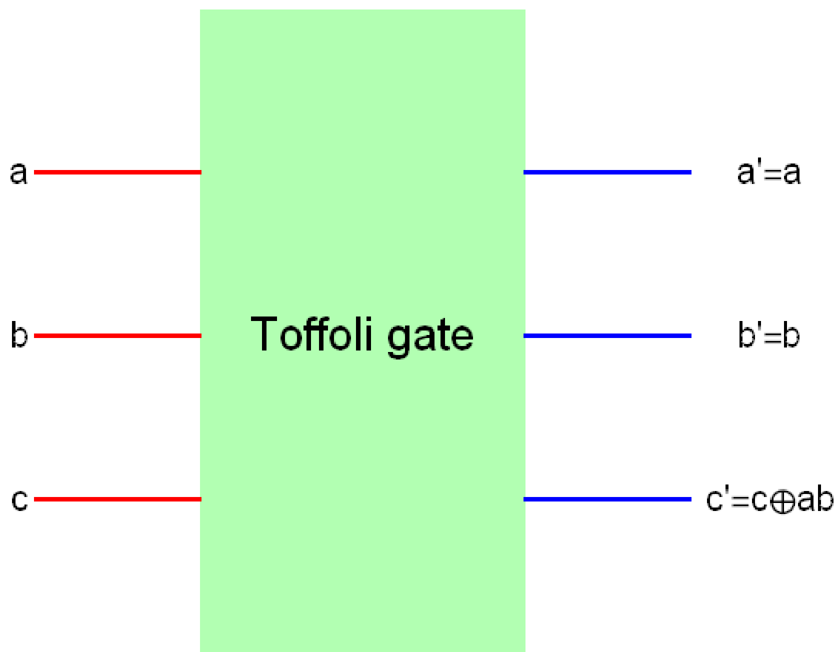
$$\hat{U}_{Fredkin}=\begin{pmatrix}1&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&1&0&0&0&0&0\\0&0&0&0&0&1&0&0\\0&0&0&0&1&0&0&0\\0&0&0&1&0&0&0&0\\0&0&0&0&0&0&1&0\\0&0&0&0&0&0&0&1\end{pmatrix}$$

$$
|V_{Fredkin}\rangle = \begin{pmatrix} \alpha_{000} \\ \alpha_{001} \\ \alpha_{010} \\ \alpha_{011} \\ \alpha_{100} \\ \alpha_{101} \\ \alpha_{110} \\ \alpha_{111} \end{pmatrix},
$$

$$
|W_{Fredkin}\rangle = \hat{G}_{Fredkin}|V_{Fredkin}\rangle .
$$

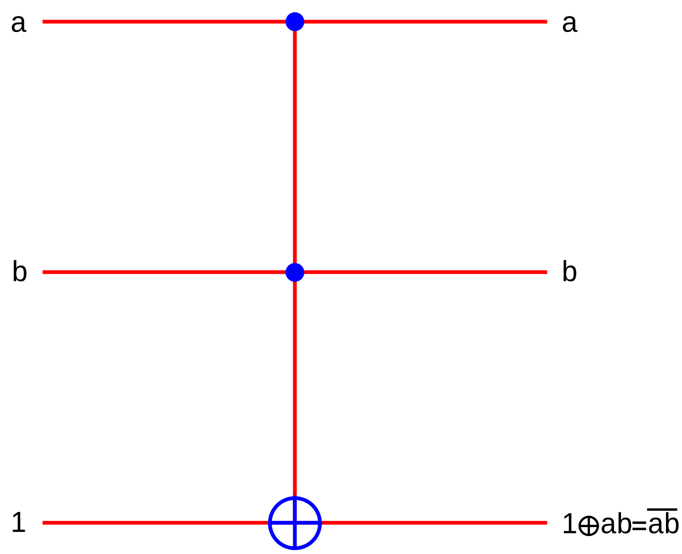
9. The Toffoli gate

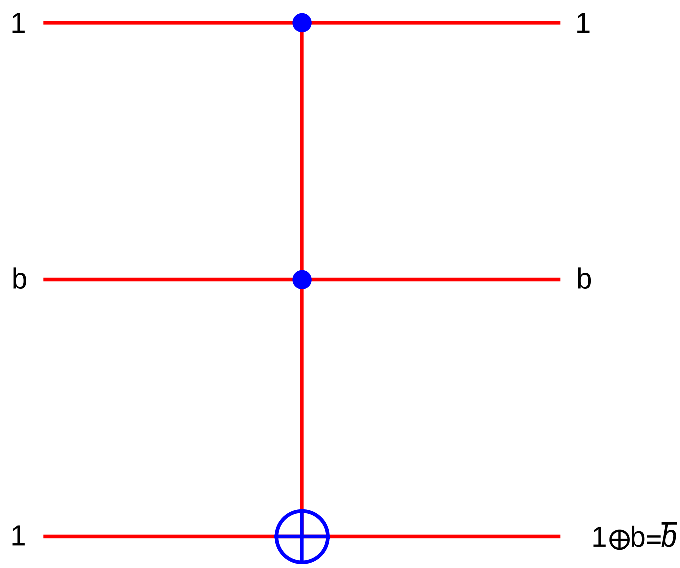
The Toffoli gate is a reversible gate. This is similar to the CNOT gate, but with two controlling qubits. The bottom bit flips only when both of the top two bits are in the state $|1\rangle$.



where

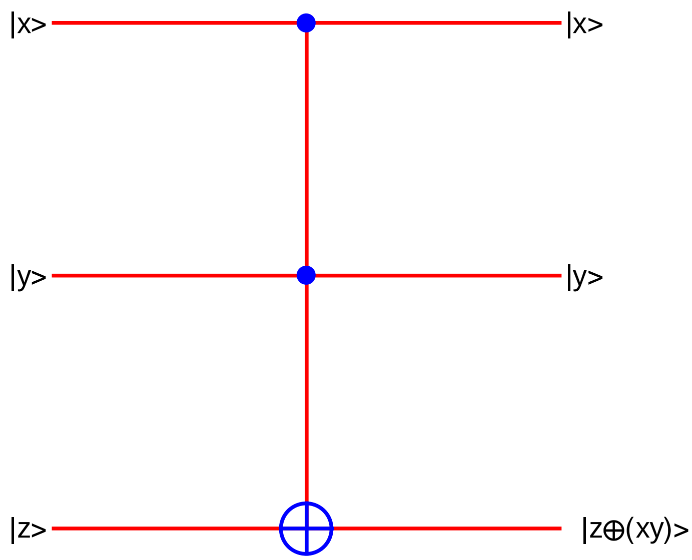
$$
1 \oplus a = \bar{a}, \qquad 0 \oplus a = a
$$





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

We can write the above operation as taking the state $|x,y,z\rangle \rightarrow |x,y,z\oplus(xy)\rangle$



$$\hat{G}_{Toffolin}|000\rangle = |000\rangle,$$
$$\hat{G}_{Toffolin}|001\rangle = |001\rangle,$$
$$\hat{G}_{Toffolin}|010\rangle = |010\rangle,$$
$$\hat{G}_{Toffolin}|011\rangle = |011\rangle,$$
$$\hat{G}_{Toffolin}|100\rangle = |100\rangle,$$
$$\hat{G}_{Toffolin}|101\rangle = |101\rangle,$$
$$\hat{G}_{Toffolin}|110\rangle = |111\rangle,$$
$$\hat{G}_{Toffolin}|111\rangle = |110\rangle.$$

$$\begin{aligned}\hat{G}_{Toffolin} &= \hat{G}_{Toffolin}(|000\rangle\langle 000| + |001\rangle\langle 001| + |010\rangle\langle 010| + |011\rangle\langle 011| \\ &\quad + |100\rangle\langle 100| + |101\rangle\langle 101| + |110\rangle\langle 110| + |111\rangle\langle 111|) \\ &= |000\rangle\langle 000| + |001\rangle\langle 001| + |010\rangle\langle 010| + |011\rangle\langle 011| \\ &\quad + |100\rangle\langle 100| + |101\rangle\langle 101| + |111\rangle\langle 110| + |110\rangle\langle 111|\end{aligned}$$

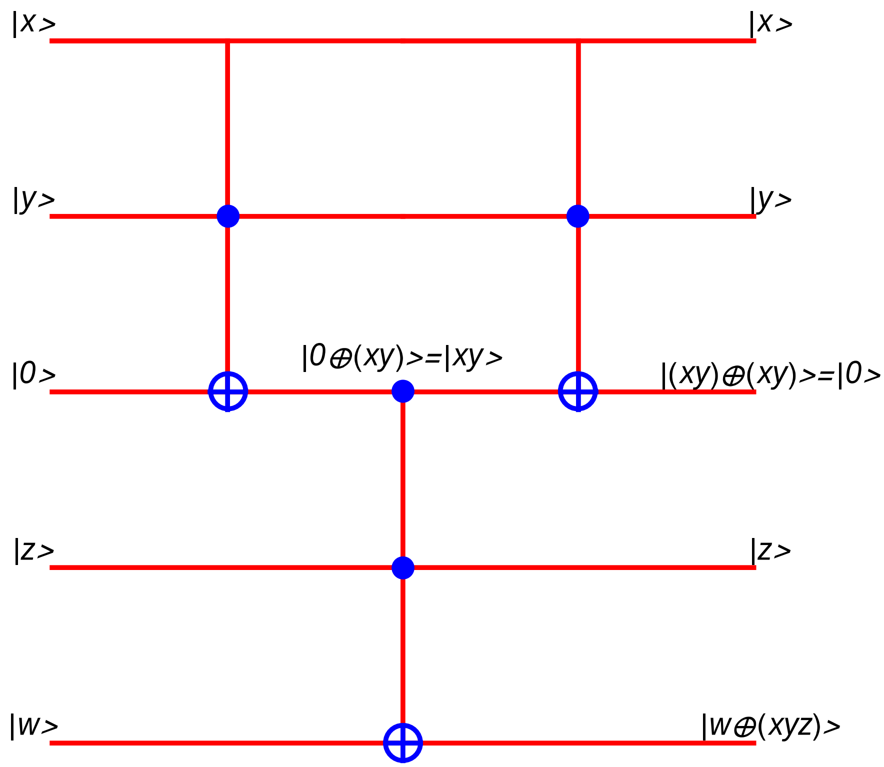
$$\hat{G}_{Toffolin} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

$$\left|V_{Toffolin}\right\rangle = \begin{pmatrix} \alpha_{000} \\ \alpha_{001} \\ \alpha_{010} \\ \alpha_{011} \\ \alpha_{100} \\ \alpha_{101} \\ \alpha_{110} \\ \alpha_{111} \end{pmatrix}$$

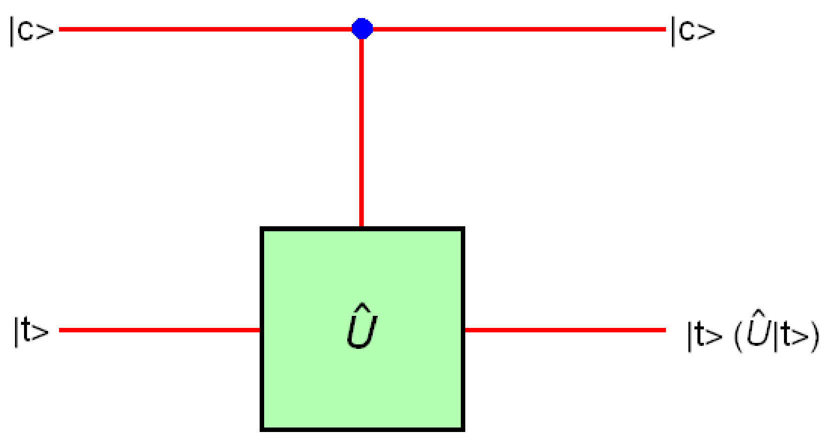
$$\left|W_{Toffolin}\right\rangle = \hat{G}_{Toffolin}\left|V_{Toffolin}\right\rangle .$$

((**Note**))

A gate with three controlling bits can be constructed from three Toffoli gates as follows.



10. The Controlled-*U* operation.



(i) When the control qubit is $|c\rangle = |0\rangle$, then the target qubit is transferred directly to the output.

$$|c\rangle = |0\rangle, \qquad |c'\rangle = |0\rangle$$

$$|t\rangle, \qquad |t'\rangle = |t\rangle$$

or

$$\hat{G}_U|00\rangle = |00\rangle, \qquad \hat{G}_U|01\rangle = |01\rangle$$

(ii) When the control qubit is $|c\rangle = |1\rangle$, then the transformation described by $\hat{U}$ is applied to the target;

$$|c\rangle = |1\rangle \qquad |c'\rangle = |1\rangle$$

$$|t\rangle \qquad |t'\rangle = \hat{U}|t\rangle$$

or

$$\begin{aligned}\hat{G}_U|10\rangle &= |1\rangle\hat{U}|0\rangle \\ &= |1\rangle[U_{11}|0\rangle + U_{21}|1\rangle], \\ &= U_{11}|10\rangle + U_{21}|11\rangle]\end{aligned}$$

$$\begin{aligned}\hat{G}_U|11\rangle &= |1\rangle\hat{U}|1\rangle \\ &= |1\rangle[U_{12}|0\rangle + U_{22}|1\rangle] \\ &= U_{12}|10\rangle + U_{22}|11\rangle\end{aligned}$$

where $\hat{U}$ is the unitary operator, and is defined by

$$\hat{U} = \begin{pmatrix} U_{11} & U_{12} \\ U_{21} & U_{22} \end{pmatrix}$$

and

$$\hat{U}|0\rangle = \begin{pmatrix} U_{11} & U_{12} \\ U_{21} & U_{22} \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} U_{11} \\ U_{21} \end{pmatrix}, \qquad \hat{U}|1\rangle = \begin{pmatrix} U_{11} & U_{12} \\ U_{21} & U_{22} \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} U_{12} \\ U_{22} \end{pmatrix}$$

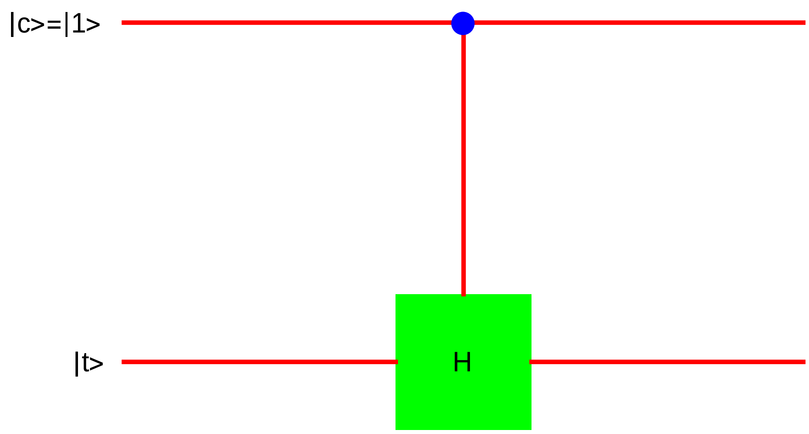
The matrix representing the controlled *U* is

$$\hat{G}_U = \hat{G}_U[|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| + |11\rangle\langle 11|]$$
$$= |00\rangle\langle 00| + |01\rangle\langle 01| + (U_{11}|10\rangle + U_{21}|11\rangle)\langle 10| + (U_{12}|10\rangle + U_{22}|11\rangle)\langle 11|]$$
$$= |00\rangle\langle 00| + |01\rangle\langle 01| + U_{11}|10\rangle\langle 10| + U_{21}|11\rangle\langle 10| + U_{12}|10\rangle\langle 11| + U_{22}|11\rangle\langle 11|$$

or

$$\hat{G}_U = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & U_{11} & U_{12} \\ 0 & 0 & U_{21} & U_{22} \end{pmatrix} = \begin{pmatrix} \boldsymbol{I} & 0 \\ 0 & \boldsymbol{U} \end{pmatrix}.$$

11. The Controlled-*H* operation



$$|00\rangle \rightarrow |0(0\oplus 0)\rangle = |00\rangle$$
$$|01\rangle \rightarrow |0(0\oplus 1)\rangle = |01\rangle$$
$$|10\rangle \rightarrow |1(1\oplus 0)\rangle = |11\rangle = |1\rangle\hat{H}|0\rangle = |1\rangle[\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle] = \frac{1}{\sqrt{2}}(|10\rangle + |11\rangle)$$
$$|11\rangle \rightarrow |1(1\oplus 1)\rangle = |10\rangle = |1\rangle\hat{H}|1\rangle = |1\rangle[\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle] = \frac{1}{\sqrt{2}}(|10\rangle - |11\rangle)$$

where

$$\hat{H}|0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}[|0\rangle + |1\rangle]$$

$$\hat{H}|1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{1}{\sqrt{2}}[|0\rangle - |1\rangle]$$

Then we have

$$\hat{G}_H = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & H_{11} & H_{12} \\ 0 & 0 & H_{21} & H_{22} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ 0 & 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$$

where

$$\hat{U} = \hat{H} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$\hat{G}_U = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ 0 & 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \boldsymbol{I} & 0 \\ 0 & \boldsymbol{H} \end{pmatrix}$$

Suppose that

$$|\psi_1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}, \qquad |\phi_1\rangle = \begin{pmatrix} \gamma \\ \delta \end{pmatrix}$$

Then we get

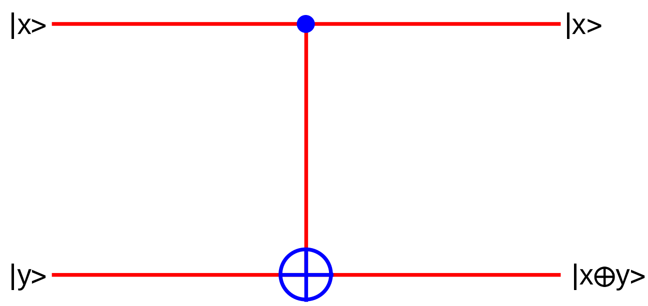
$$|\psi_1\rangle \otimes |\phi_1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \otimes \begin{pmatrix} \gamma \\ \delta \end{pmatrix} = \begin{pmatrix} \alpha\gamma \\ \alpha\delta \\ \beta\gamma \\ \beta\delta \end{pmatrix}$$

The output of this circuit is given by

$$\hat{C}(\hat{H})|\psi_1\rangle \otimes |\phi_1\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ 0 & 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \alpha\gamma \\ \alpha\delta \\ \beta\gamma \\ \beta\delta \end{pmatrix} = \begin{pmatrix} \alpha\gamma \\ \alpha\delta \\ \frac{\beta(\gamma+\delta)}{\sqrt{2}} \\ \frac{\beta(\gamma-\delta)}{\sqrt{2}} \end{pmatrix}$$

---

12. CNOT gate



$$|00\rangle \to |0(0\oplus 0)\rangle = |00\rangle$$

$$|01\rangle \to |0(0\oplus 1)\rangle = |01\rangle$$

$$|10\rangle \to |1(1\oplus 0)\rangle = |11\rangle = |1\rangle\hat{U}|0\rangle = |1\rangle[U_{11}|0\rangle + U_{21}|1\rangle] = U_{11}|10\rangle + U_{21}|11\rangle$$

$$|11\rangle \to |1(1\oplus 1)\rangle = |10\rangle = |1\rangle\hat{U}|1\rangle = |1\rangle[U_{12}|0\rangle + U_{22}|1\rangle] = U_{12}|10\rangle + U_{22}|11\rangle$$

where

$$\hat{U}|0\rangle = \begin{pmatrix} U_{11} & U_{12} \\ U_{21} & U_{22} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} U_{11} \\ U_{21} \end{pmatrix} = U_{11}|0\rangle + U_{21}|1\rangle$$

$$\hat{U}|1\rangle = \begin{pmatrix} U_{11} & U_{12} \\ U_{21} & U_{22} \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} U_{12} \\ U_{22} \end{pmatrix} = U_{12}|0\rangle + U_{22}|1\rangle$$

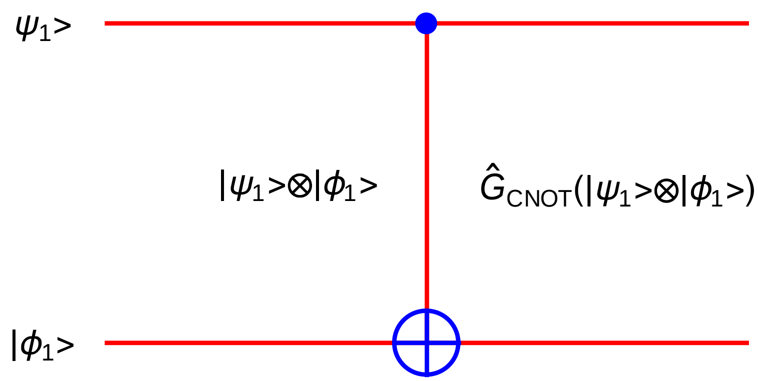
Thus we have

$$\hat{G}_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & U_{11} & U_{12} \\ 0 & 0 & U_{21} & U_{22} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

since

$$\hat{U}_{CNOT} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

What happens when the input kets are given in the general case?



Suppose that

$$|\psi_1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}, \qquad |\phi_1\rangle = \begin{pmatrix} \gamma \\ \delta \end{pmatrix}$$

Then we get

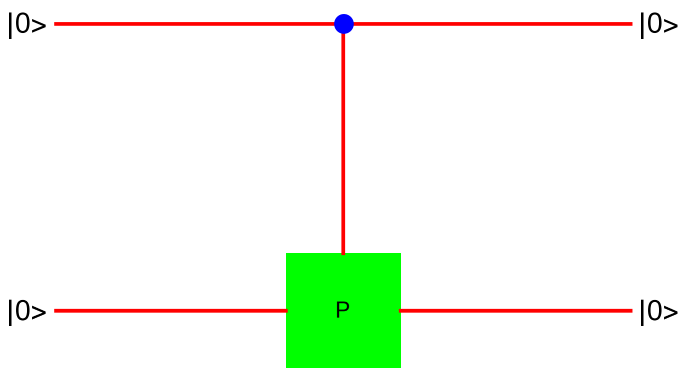
$$|\psi_1\rangle \otimes |\phi_1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \otimes \begin{pmatrix} \gamma \\ \delta \end{pmatrix} = \begin{pmatrix} \alpha\gamma \\ \alpha\delta \\ \beta\gamma \\ \beta\delta \end{pmatrix}$$

The output of this circuit is given by

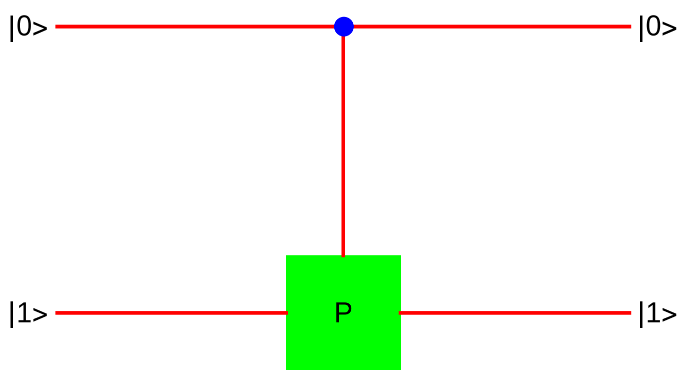
$$\hat{G}_{CNOT}|\psi_1\rangle\otimes|\phi_1\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}\begin{pmatrix} \alpha\gamma \\ \alpha\delta \\ \beta\gamma \\ \beta\delta \end{pmatrix} = \begin{pmatrix} \alpha\gamma \\ \alpha\delta \\ \beta\delta \\ \beta\gamma \end{pmatrix}$$
$$= \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\delta|10\rangle + \beta\gamma|11\rangle$$
$$= \alpha|0\rangle(\gamma|0\rangle + \beta|1\rangle) + \beta|1\rangle(\gamma|1\rangle + \delta|0\rangle)$$

13. Controlled-P operation

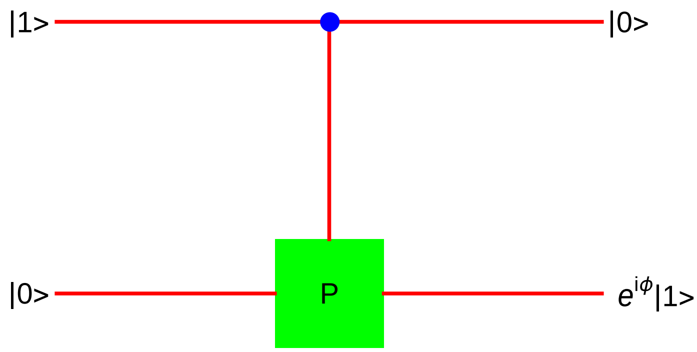
(i) $|00\rangle \rightarrow |00\rangle$



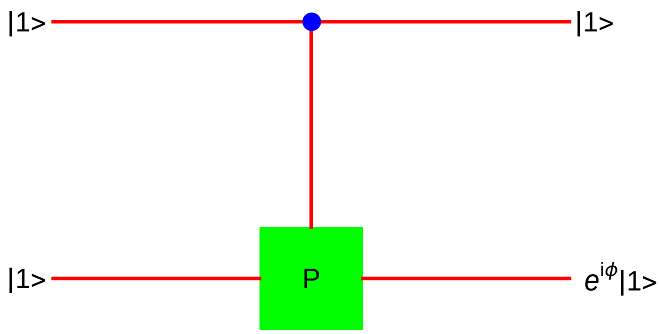
(ii) $|01\rangle \rightarrow |01\rangle$



(iii) $|10\rangle \rightarrow e^{i\varphi}|10\rangle$



(iv) $|11\rangle \rightarrow e^{i\varphi}|11\rangle$



$$|00\rangle \rightarrow |00\rangle,$$
$$|01\rangle \rightarrow |01\rangle,$$
$$|10\rangle \rightarrow e^{i\varphi}|10\rangle,$$
$$|11\rangle \rightarrow e^{i\varphi}|11\rangle,$$

$$\hat{G}_P = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e^{i\varphi} & 1 \\ 0 & 0 & 0 & e^{i\varphi} \end{pmatrix},$$

where

$$\hat{P}_\varphi = \begin{pmatrix} e^{i\varphi} & 0 \\ 0 & e^{i\varphi} \end{pmatrix}.$$

Suppose that

$$|\psi_1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}, \qquad |\phi_1\rangle = \begin{pmatrix} \gamma \\ \delta \end{pmatrix}$$

Then we get

$$|\psi_1\rangle \otimes |\phi_1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \otimes \begin{pmatrix} \gamma \\ \delta \end{pmatrix} = \begin{pmatrix} \alpha\gamma \\ \alpha\delta \\ \beta\gamma \\ \beta\delta \end{pmatrix}$$

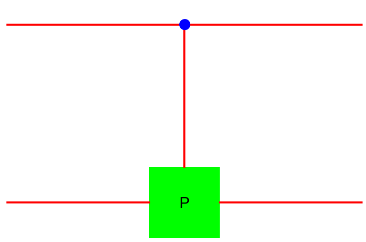
The output of this circuit is given by

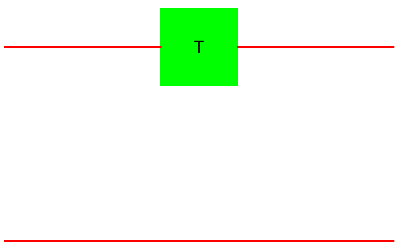
$$\begin{aligned} \hat{G}_P |\psi_1\rangle \otimes |\phi_1\rangle &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e^{i\varphi} & 0 \\ 0 & 0 & 0 & e^{i\varphi} \end{pmatrix} \begin{pmatrix} \alpha\gamma \\ \alpha\delta \\ \beta\gamma \\ \beta\delta \end{pmatrix} = \begin{pmatrix} \alpha\gamma \\ \alpha\delta \\ \beta\delta \\ \beta\gamma \end{pmatrix} \\ &= \alpha\gamma|00\rangle + \alpha\delta|01\rangle + e^{i\varphi}\beta\delta|10\rangle + \beta\gamma|11\rangle \\ &= \alpha|0\rangle(\gamma|0\rangle + \delta|1\rangle) + e^{i\varphi}\beta|1\rangle(\gamma|1\rangle + \delta|0\rangle) \\ &= (\alpha|0\rangle + e^{i\varphi}\beta|1\rangle)(\gamma|0\rangle + \delta|1\rangle) \end{aligned}$$

Here we introduce

$$\hat{T}_\varphi = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix}.$$

Then we have

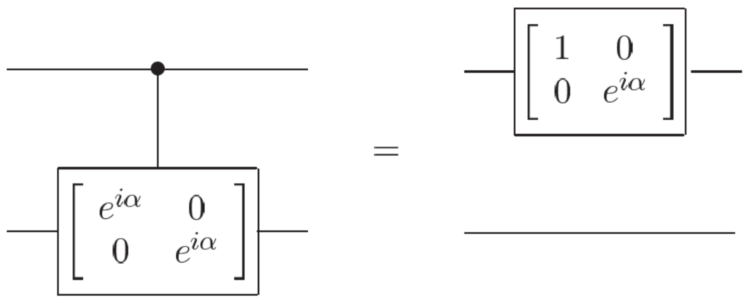




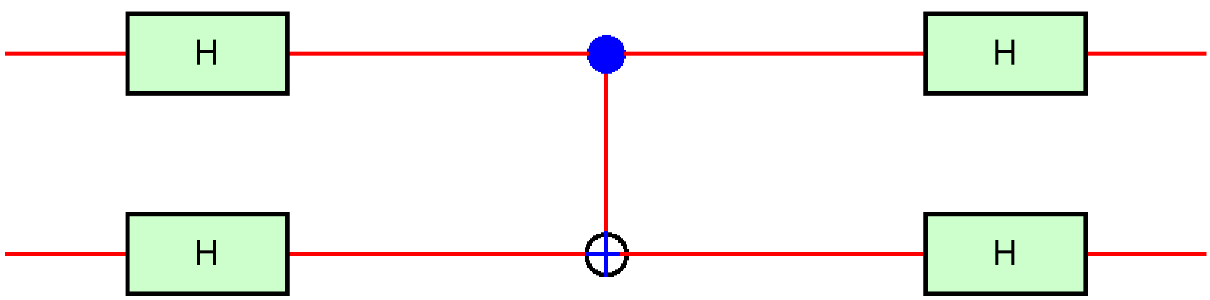
These two quantum circuits are equivalent.

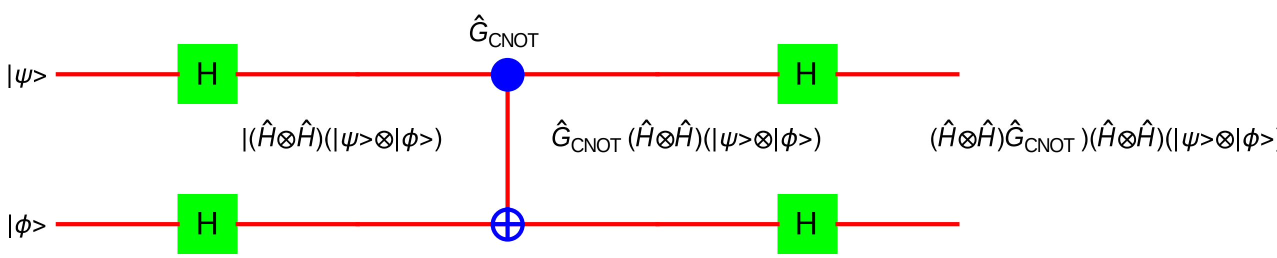
$$\hat{G}_P = \hat{T}_\varphi \otimes \hat{I}_2 = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e^{i\varphi} & 0 \\ 0 & 0 & 0 & e^{i\varphi} \end{pmatrix}.$$

((**Note**))



14. Application





$$\hat{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}; \qquad \hat{H} \otimes \hat{H} = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix},$$

$$\hat{G}_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$\hat{H} \otimes \hat{H} = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

Thus we have

$$(\hat{H} \otimes \hat{H})\hat{G}_{CNOT}(\hat{H} \otimes \hat{H}) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

This is equivalent to the reversed CNOT gate.

((**Note**))

$$|\psi_1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}, \qquad |\phi_1\rangle = \begin{pmatrix} \gamma \\ \delta \end{pmatrix},$$

$$|\psi_1\rangle \otimes |\phi_1\rangle = \begin{pmatrix} \alpha\gamma \\ \alpha\delta \\ \beta\gamma \\ \beta\delta \end{pmatrix}$$

$$(\hat{H} \otimes \hat{H})|\psi_1\rangle \otimes |\phi_1\rangle = \hat{H}|\psi_1\rangle \otimes \hat{H}|\psi_1\rangle == \frac{1}{2}\begin{pmatrix} (\alpha+\beta)(\gamma+\delta) \\ (\alpha+\beta)(\gamma-\delta) \\ (\alpha-\beta)(\gamma+\delta) \\ (\alpha-\beta)(\gamma-\delta) \end{pmatrix}$$

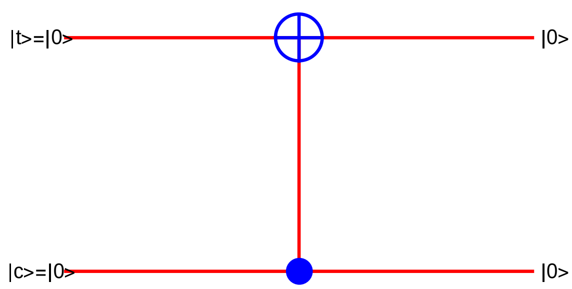
$$\hat{G}_{CNOT}(\hat{H}\otimes\hat{H})|\psi_1\rangle\otimes|\phi_1\rangle = \frac{1}{2}\begin{pmatrix}(\alpha+\beta)(\gamma+\delta)\\(\alpha+\beta)(\gamma-\delta)\\(\alpha-\beta)(\gamma-\delta)\\(\alpha-\beta)(\gamma+\delta)\end{pmatrix}$$

This implies that this output cannot be described by the form such as

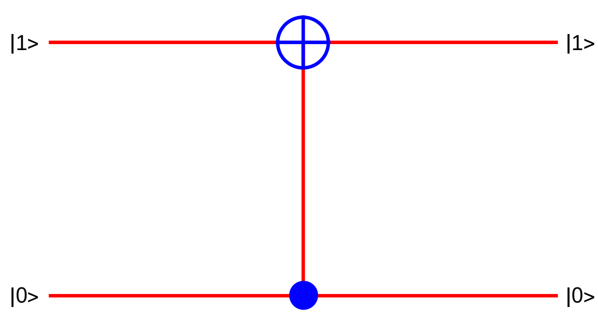
$$(\hat{H}\otimes\hat{H})\hat{G}_{CNOT}(\hat{H}\otimes\hat{H})|\psi_1\rangle\otimes|\phi_1\rangle = \begin{pmatrix}\alpha\gamma\\\beta\delta\\\beta\gamma\\\alpha\delta\end{pmatrix}$$

16. Reverse CNOT gate

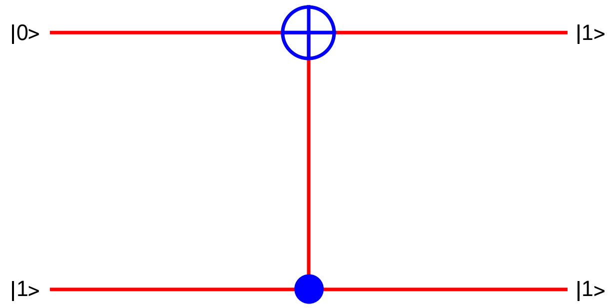
The role of control and target qubits can be reversed by an appropriate change of basis. The upper bar denotes the target qubit ($|t\rangle$).and lower bar denotes the control qubit ($|c\rangle$).



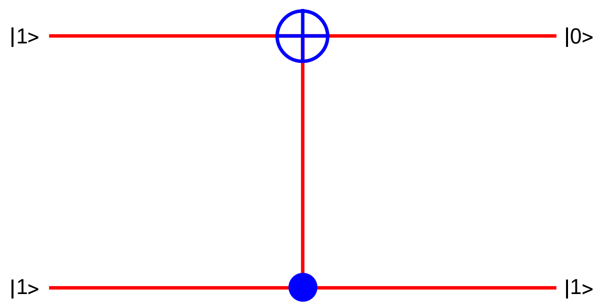
$$|00\rangle \rightarrow |00\rangle$$



$$|10\rangle \rightarrow |10\rangle$$



$$|01\rangle \rightarrow |11\rangle$$



$$|11\rangle \rightarrow |01\rangle$$

Then the matrix element for the reverse CNOT gate is given by

$$\hat{R}_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

Note that

$$\hat{G}_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} \boldsymbol{I} & 0 \\ 0 & \boldsymbol{X} \end{pmatrix}.$$

17. The ABC decomposition and controlled-*U*

One can show that a combination of controlled NOT and single-qubit gates can implement an arbitrary controlled-U gate where U is a unitary single qubit gate.

The quantum circuit in Fig.1(b) (below) simulates the general one-qubit controlled gate in Fig.1(a), where $\hat{A}$, $\hat{B}$, and $\hat{C}$ are the rotation matrices. When the control qubit is $|c\rangle = |0\rangle$, the target qubit becomes

$$|t\rangle \to \hat{C}\hat{B}\hat{A}|t\rangle = \hat{1}|t\rangle = |t\rangle .$$

When $|c\rangle = |1\rangle$, the target becomes

$$|t\rangle \to \hat{C}\hat{\sigma}_x\hat{B}\hat{\sigma}_x\hat{A}|t\rangle = \hat{U}|t\rangle$$

where

$$\hat{A} = \hat{R}_z(\frac{\delta-\beta}{2}), \qquad \hat{B} = \hat{R}_y(-\frac{\gamma}{2})\hat{R}_z(-\frac{\delta+\beta}{2}), \qquad \hat{C} = \hat{R}_z(\beta)\hat{R}_y(\frac{\gamma}{2}),$$

and

$$\hat{C}\hat{B}\hat{A} = \hat{1}$$

$$\hat{U} = \hat{C}\hat{\sigma}_x\hat{B}\hat{\sigma}_x\hat{A} = \hat{R}_z(\beta)\hat{R}_y(\gamma)\hat{R}_z(\delta)$$

where

$$\hat{\sigma}_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

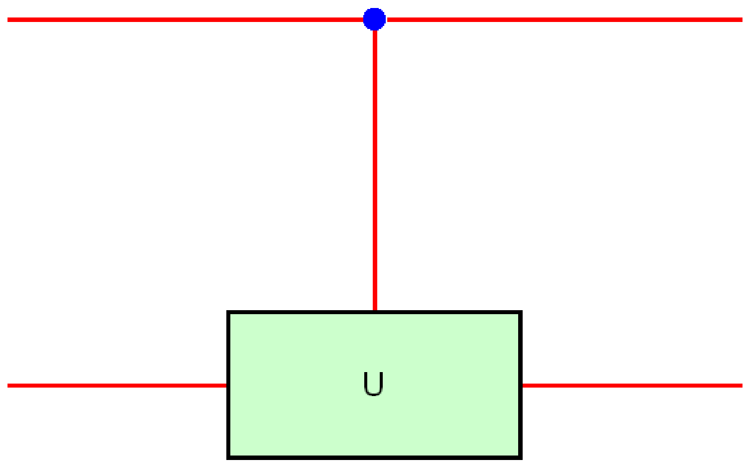


Fig. (a) Controlled U gate

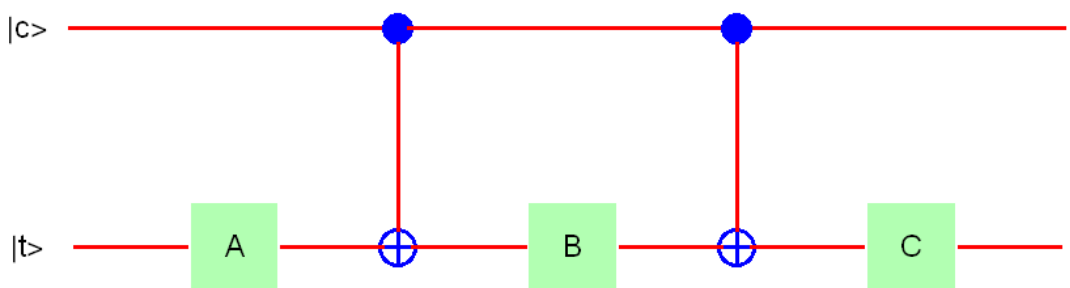


Fig.(b) Decomposition of an arbitrary single-qubit $\hat{U}$ into $\hat{U} = \hat{C}\hat{\sigma}_x\hat{B}\hat{\sigma}_x\hat{A}$ such that $\hat{C}\hat{B}\hat{A} = \hat{1}$.

((**Mathematica**))

```
Clear["Global`*"]; σx = PauliMatrix[1]; σy = PauliMatrix[2];
σz = PauliMatrix[3]; Sx = ℏ/2 σx; Sy = ℏ/2 σy; Sz = ℏ/2 σz;
Rx[β_] := MatrixExp[-ⅈ/ℏ Sx β] // Simplify ;
Ry[β_] := MatrixExp[-ⅈ/ℏ Sy β] // Simplify ;
Rz[β_] := MatrixExp[-ⅈ/ℏ Sz β] // Simplify;
```

```
Rx[β] // Simplify // MatrixForm
```

$$\begin{pmatrix} \mathrm{Cos}\left[\frac{\beta}{2}\right] & -i\,\mathrm{Sin}\left[\frac{\beta}{2}\right] \\ -i\,\mathrm{Sin}\left[\frac{\beta}{2}\right] & \mathrm{Cos}\left[\frac{\beta}{2}\right] \end{pmatrix}$$

```
Ry[β] // Simplify // MatrixForm
```

$$\begin{pmatrix} \mathrm{Cos}\left[\frac{\beta}{2}\right] & -\mathrm{Sin}\left[\frac{\beta}{2}\right] \\ \mathrm{Sin}\left[\frac{\beta}{2}\right] & \mathrm{Cos}\left[\frac{\beta}{2}\right] \end{pmatrix}$$

```
Rz[β] // Simplify // MatrixForm
```

$$\begin{pmatrix} e^{-\frac{i\beta}{2}} & 0 \\ 0 & e^{\frac{i\beta}{2}} \end{pmatrix}$$

```
Rz[ϕ].Ry[θ] // Simplify // MatrixForm
```

$$\begin{pmatrix} e^{-\frac{i\phi}{2}} \operatorname{Cos}\left[\frac{\theta}{2}\right] & -e^{-\frac{i\phi}{2}} \operatorname{Sin}\left[\frac{\theta}{2}\right] \\ e^{\frac{i\phi}{2}} \operatorname{Sin}\left[\frac{\theta}{2}\right] & e^{\frac{i\phi}{2}} \operatorname{Cos}\left[\frac{\theta}{2}\right] \end{pmatrix}$$

```
Rx[β].Rx[-β] // Simplify
```

{{1, 0}, {0, 1}}

```
Ry[β].Ry[-β] // Simplify
```

{{1, 0}, {0, 1}}

```
Rz[β].Rz[-β] // Simplify
```

{{1, 0}, {0, 1}}

```
Rx[β1].Rx[β2] - Rx[β1 + β2] // Simplify
```

{{0, 0}, {0, 0}}

```
Ry[β1].Ry[β2] - Ry[β1 + β2] // Simplify
```

{{0, 0}, {0, 0}}

```
Rz[β1].Rz[β2] - Rz[β1 + β2] // Simplify
```

{{0, 0}, {0, 0}}

```
C1 = Rz[β].Ry[γ/2];
B1 = Ry[-γ/2].Rz[-(δ + β)/2];
A1 = Rz[(δ - β)/2];
```

```
C1.B1.A1 // Simplify
```

{{1, 0}, {0, 1}}

```
C1.σx.B1.σx.A1 - Rz[β].Ry[γ].Rz[δ] // Simplify
```

{{0, 0}, {0, 0}}

```
Rz[β].Ry[γ].Rz[δ] // Simplify
```

$$\left\{\left\{e^{-\frac{1}{2}i(\beta+\delta)}\,\mathrm{Cos}\left[\frac{\gamma}{2}\right],\ -e^{-\frac{1}{2}i(\beta-\delta)}\,\mathrm{Sin}\left[\frac{\gamma}{2}\right]\right\},\ \left\{e^{\frac{1}{2}i(\beta-\delta)}\,\mathrm{Sin}\left[\frac{\gamma}{2}\right],\ e^{\frac{1}{2}i(\beta+\delta)}\,\mathrm{Cos}\left[\frac{\gamma}{2}\right]\right\}\right\}$$

15. Reversible operation

The controlled NOT gate and the Toffli gate are reversible.

(1) CNOT gate

$$\begin{aligned}|x,y\rangle &\to \hat{G}_{CNOT}|x,y\rangle = |x, x\oplus y\rangle \\ &\to \hat{G}_{CNOT}\hat{G}_{CNOT}|x,y\rangle = \hat{G}_{CNOT}|x, x\oplus y\rangle = |x, x\oplus(x\otimes y)\rangle = |x,y\rangle\end{aligned}$$

since $x \oplus x = 0$. Thus we have

$$\hat{G}_{CNOT}{}^2 = \hat{1}$$

(ii) Toffli gate

$$|x, y, z\rangle \to \hat{G}_{Toffli}|x, y, z\rangle = |x, y, z \oplus xy\rangle$$
$$\to \hat{G}_{Tofli}\hat{U}_{Tofli}|x, y, z\rangle = \hat{G}_{Tofli}|x, y, z \oplus xy\rangle = |x, y, z \oplus xy \otimes xy\rangle = |x, y, z\rangle$$

since $xy \oplus xy = 0$. Thus we have

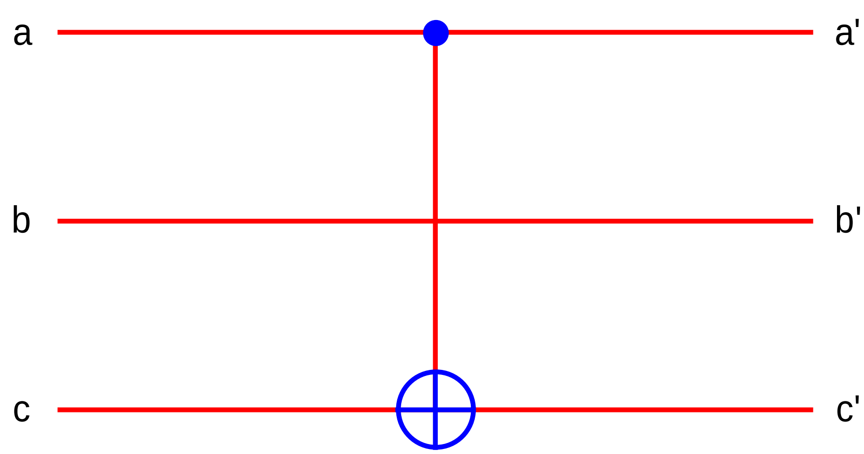
$$\hat{G}_{Tofli}{}^2 = \hat{1}$$

Such a gate is called the universal gate.

---

16. CNOT gate

(a) CNOT gate (modified case 1-3)



$a' = a$, $b' = b$, $c' = a \oplus c$

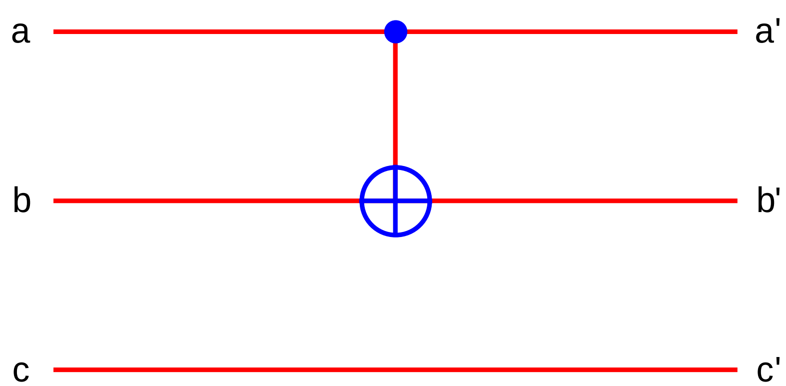
a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0

0	1	1	0	1	1
1	0	0	1	0	1
1	0	1	1	0	0
1	1	0	1	1	1
1	1	1	1	1	0

Then we have

$$\hat{U}_{CNOT}(1-3) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} \hat{I}_2 & 0 & 0 & 0 \\ 0 & \hat{I}_2 & 0 & 0 \\ 0 & 0 & \hat{\sigma}_x & 0 \\ 0 & 0 & 0 & \hat{\sigma}_x \end{pmatrix}$$

(b) CNOT gate (modified case1-2)



$a' = a$, $b' = a \oplus b$, $c' = c$

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	1	0
1	0	1	1	1	1
1	1	0	1	0	0

1 1 1 1 0 1

Then we have

$$\hat{U}_{CNOT}(1-2) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} \hat{I}_2 & 0 & 0 & 0 \\ 0 & \hat{I}_2 & 0 & 0 \\ 0 & 0 & 0 & \hat{I}_2 \\ 0 & 0 & \hat{I}_2 & 0 \end{pmatrix}$$

In fact, we have

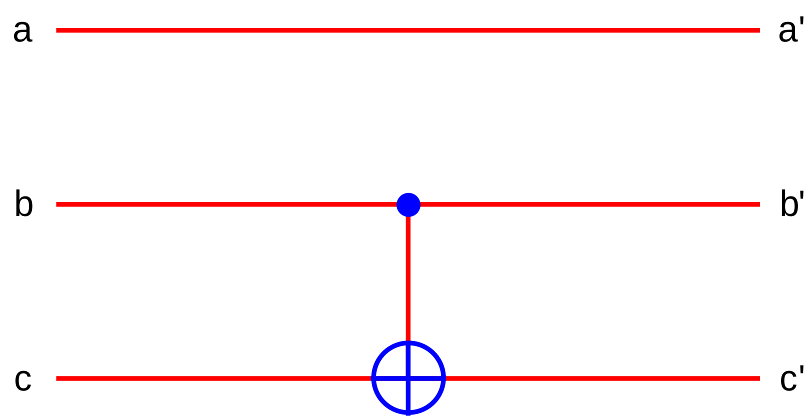
$$|\psi_{out}\rangle = (\hat{U}_{CNOT} \otimes \hat{I}_2)|\psi_{in}\rangle$$

$$\hat{U}_{CNOT} \otimes \hat{I}_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

where

$$\hat{U}_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

(c) CNOT gate (modified case2-3)



$a' = a,\ b' = b,\ c' = b \oplus c$

a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	1
0	1	1	0	1	0
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

Then we have

$$\hat{U}_{CNOT}(2-3) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} \hat{I}_2 & 0 & 0 & 0 \\ 0 & \hat{\sigma}_x & 0 & 0 \\ 0 & 0 & \hat{I}_2 & 0 \\ 0 & 0 & 0 & \hat{\sigma}_x \end{pmatrix}$$

In fact, we have

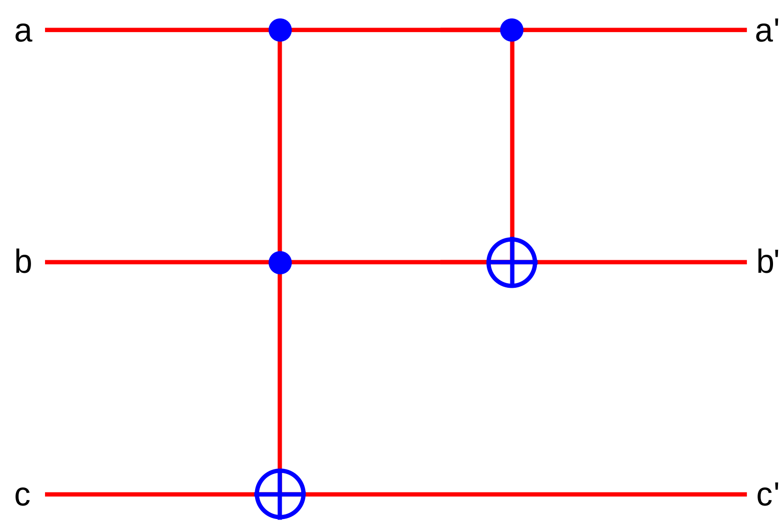
$$|\psi_{out}\rangle = (\hat{I}_2 \otimes \hat{U}_{CNOT})|\psi_{in}\rangle$$

$$\hat{I}_2 \otimes \hat{U}_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

where

$$\hat{U}_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

17. Series connection of Toffoli gate and CNOT gate



$a' = a$, $b' = a \oplus b$, $c' = c \oplus ab$

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	1	0
1	0	1	1	1	1
1	1	0	1	0	1
1	1	1	1	0	0

From this table, we get the corresponding matrix as

$$\hat{U} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

In fact

$$\left|\psi_{out}\right\rangle = (\hat{U}_{CNOT} \otimes I)\hat{U}_{Tofflis}\left|\psi_{in}\right\rangle$$

Note that

$$\hat{U}_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \qquad \hat{U}_{Toffolin} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

$$\hat{U}_{CNOT} \otimes I = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

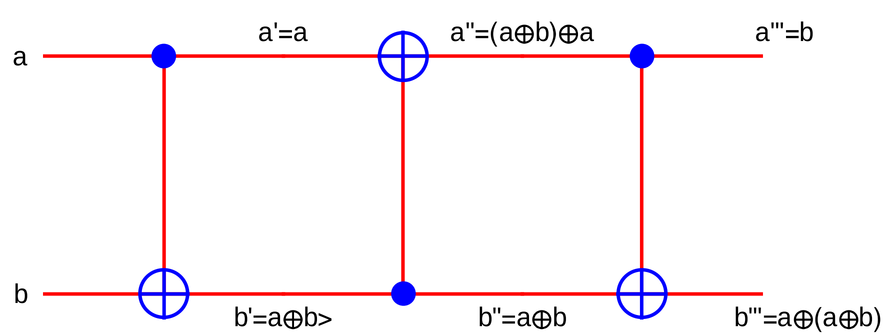
Then we have

$$(\hat{U}_{CNOT} \otimes I)\hat{U}_{Tofflis} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

which is the same as $\hat{U}$ obtained above.

---

18. Qubit swapping



$b'' = a \oplus (a \oplus b) = b$

since $a \oplus a = 0$ and $0 \oplus b = b$.

$$\hat{U}_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \qquad \hat{U}_{RCNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

where

$$\hat{U}_{CNOT}{}^2 = \hat{U}_{RCNOT}{}^2 = \hat{I}_4 .$$

The output is given by

$$|\psi_{out}\rangle = (\hat{U}_{CNOT}\hat{U}_{RCNOT}\hat{U}_{CNOT})|\psi_{in}\rangle$$

where

$$\begin{aligned} \hat{U}_{CNOT}\hat{U}_{RCNOT}\hat{U}_{CNOT} &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \\ &= \hat{U}_{swap} \end{aligned}$$

We note that for the qubit swapping,

a	b	a'	b'
0	0	0	0
0	1	1	0
1	0	0	1
1	1	1	1

Then we have

$$\hat{U}_{swap} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

We also note that

$$\begin{aligned} \hat{U}_{RCNOT}\hat{U}_{CNOT}\hat{U}_{RCNOT} &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \\ &= \hat{U}_{swap} \end{aligned}$$

$$\hat{1}_2 \otimes \hat{C} = \begin{pmatrix} \hat{C} & \hat{0} \\ \hat{0} & \hat{C} \end{pmatrix}, \qquad \hat{U}_{CNOT} = \begin{pmatrix} \hat{1}_2 & \hat{0} \\ \hat{0} & \hat{\sigma}_x \end{pmatrix}$$

$$\begin{aligned} (\hat{1}_2 \otimes \hat{C})\hat{U}_{CNOT}(\hat{1}_2 \otimes \hat{B})\hat{U}_{CNOT}(\hat{1}_2 \otimes \hat{A}) &= \begin{pmatrix} \hat{C} & \hat{0} \\ \hat{0} & \hat{C} \end{pmatrix}\begin{pmatrix} \hat{1}_2 & \hat{0} \\ \hat{0} & \hat{\sigma}_x \end{pmatrix}\begin{pmatrix} \hat{B} & \hat{0} \\ \hat{0} & \hat{B} \end{pmatrix}\begin{pmatrix} \hat{1}_2 & \hat{0} \\ \hat{0} & \hat{\sigma}_x \end{pmatrix}\begin{pmatrix} \hat{A} & \hat{0} \\ \hat{0} & \hat{A} \end{pmatrix} \\ &= \begin{pmatrix} \hat{C} & \hat{0} \\ \hat{0} & \hat{C} \end{pmatrix}\begin{pmatrix} \hat{B} & \hat{0} \\ \hat{0} & \hat{\sigma}_x\hat{B} \end{pmatrix}\begin{pmatrix} \hat{A} & \hat{0} \\ \hat{0} & \hat{\sigma}_x\hat{A} \end{pmatrix} \\ &= \begin{pmatrix} \hat{C} & \hat{0} \\ \hat{0} & \hat{C} \end{pmatrix}\begin{pmatrix} \hat{B}\hat{A} & \hat{0} \\ \hat{0} & \hat{\sigma}_x\hat{B}\hat{\sigma}_x\hat{A} \end{pmatrix} \\ &= \begin{pmatrix} \hat{C}\hat{B}\hat{A} & \hat{0} \\ \hat{0} & \hat{C}\hat{\sigma}_x\hat{B}\hat{\sigma}_x\hat{A} \end{pmatrix} \end{aligned}$$

Suppose that

$$\hat{C}\hat{B}\hat{A} = 1, \qquad \hat{C}\hat{\sigma}_x\hat{B}\hat{\sigma}_x\hat{A} = \hat{U}.$$

Then we have

$$(\hat{1}_2 \otimes \hat{C})\hat{U}_{CNOT}(\hat{1}_2 \otimes \hat{B})\hat{U}_{CNOT}(\hat{1}_2 \otimes \hat{A}) = \begin{pmatrix} \hat{1} & \hat{0} \\ \hat{0} & \hat{U} \end{pmatrix}$$

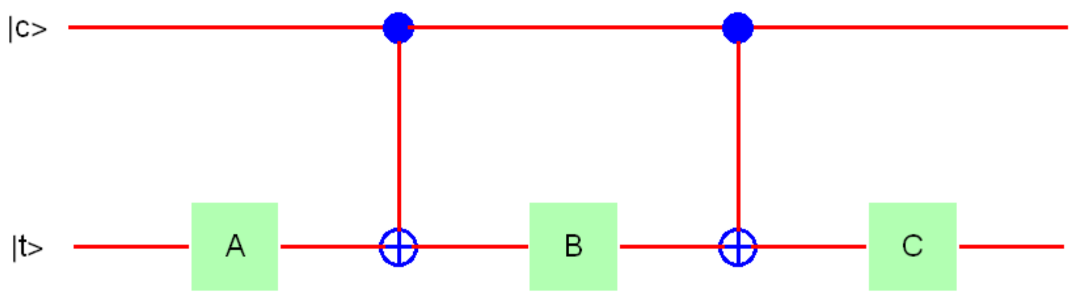
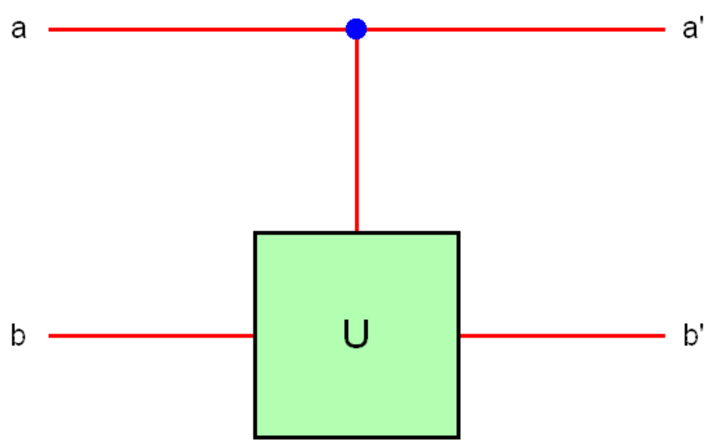


Fig.

This is equivalent to the controlled U gate;



a is the control qubit and *b* is the target qubit.

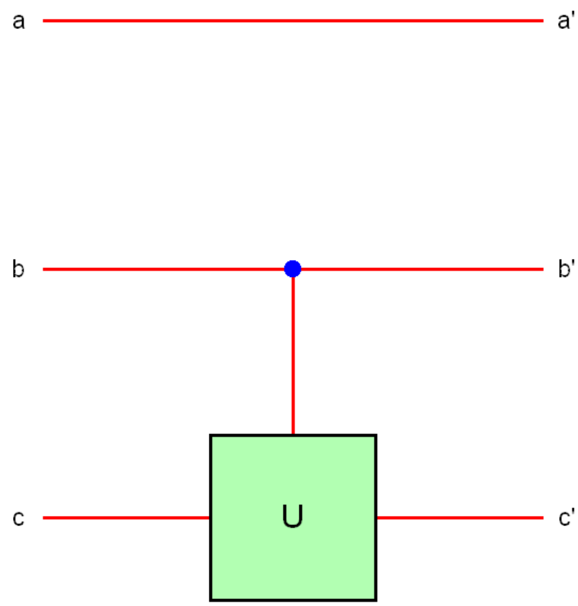
$$|00\rangle \to |00\rangle$$
$$|01\rangle \to |01\rangle$$
$$|10\rangle \to |1\rangle \hat{U}|0\rangle = U_{11}|10\rangle + U_{21}|11\rangle$$
$$|11\rangle \to |1\rangle \hat{U}|1\rangle = U_{12}|10\rangle + U_{22}|11\rangle$$

Then we have

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & U_{11} & U_{12} \\ 0 & 0 & U_{21} & U_{22} \end{pmatrix} = \begin{pmatrix} \hat{1} & 0 \\ 0 & \hat{U} \end{pmatrix}$$

---

19. Quantum gate related to controlled *U* gate



where *b* is the control qubit and *c* is the target qubit.

a	*b*	*c*	*a'*	*b'*	*c'*
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	1	1	$\hat{U}\vert 0\rangle$
0	1	1	1	1	$\hat{U}\vert 1\rangle$
1	0	0	0	0	0
1	0	1	0	0	1
1	1	0	1	1	$\hat{U}\vert 0\rangle$
1	1	1	1	1	$\hat{U}\vert 1\rangle$

Thus we get

$$\hat{C}(\hat{U}) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & U_{11} & U_{12} & 0 & 0 & 0 & 0 \\ 0 & 0 & U_{21} & U_{22} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & U_{11} & U_{12} \\ 0 & 0 & 0 & 0 & 0 & 0 & U_{21} & U_{22} \end{pmatrix} = \begin{pmatrix} \hat{I}_2 & 0 & 0 & 0 \\ 0 & \hat{U} & 0 & 0 \\ 0 & 0 & \hat{I}_2 & 0 \\ 0 & 0 & 0 & \hat{U} \end{pmatrix} = \hat{I}_2 \otimes \begin{pmatrix} \hat{I}_2 & 0 \\ 0 & \hat{U} \end{pmatrix}$$

Here we have the eight state;

$$\begin{aligned} \left|abc\right\rangle &= \left|000\right\rangle, \left|001\right\rangle, \left|010\right\rangle, \left|011\right\rangle, \left|100\right\rangle, \left|101\right\rangle, \left|110\right\rangle, \left|111\right\rangle \\ &= \left|1\right\rangle, \left|2\right\rangle, \left|3\right\rangle, \left|4\right\rangle, \left|5\right\rangle, \left|6\right\rangle, \left|7\right\rangle, \left|8\right\rangle \end{aligned}$$

We consider the case which is different from the above case. The role of *b* is replaced by that of *a*. In this case, the state is described by $\left|bac\right\rangle$;

$$\begin{aligned} \left|bac\right\rangle &= \left|000\right\rangle, \left|001\right\rangle, \left|100\right\rangle, \left|101\right\rangle, \left|010\right\rangle, \left|011\right\rangle, \left|110\right\rangle, \left|111\right\rangle \\ &= \left|1\right\rangle, \left|2\right\rangle, \left|5\right\rangle, \left|6\right\rangle, \left|3\right\rangle, \left|4\right\rangle, \left|7\right\rangle, \left|8\right\rangle, \end{aligned}$$

We need to replace both the row vectors and column vectors of the matrix $\hat{C}$ in the order of

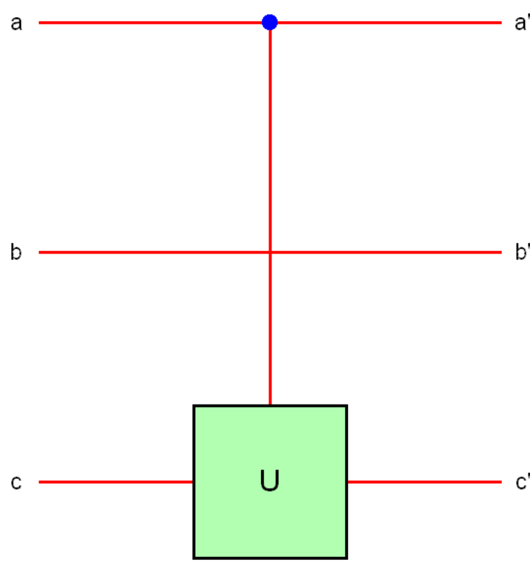
$$\begin{aligned} &\left|000\right\rangle, \left|001\right\rangle, \left|100\right\rangle, \left|101\right\rangle, \left|010\right\rangle, \left|011\right\rangle, \left|110\right\rangle, \left|111\right\rangle \\ &= \left|1\right\rangle, \left|2\right\rangle, \left|5\right\rangle, \left|6\right\rangle, \left|3\right\rangle, \left|4\right\rangle, \left|7\right\rangle, \left|8\right\rangle, \end{aligned}$$

((**Mathematica**))

```
Clear["Global`*"]; U = 
⎛1 0  0    0   0 0  0    0  ⎞
⎜0 1  0    0   0 0  0    0  ⎟
⎜0 0 u11  u12  0 0  0    0  ⎟
⎜0 0 u21  u22  0 0  0    0  ⎟ ;
⎜0 0  0    0   1 0  0    0  ⎟
⎜0 0  0    0   0 1  0    0  ⎟
⎜0 0  0    0   0 0 u11  u12 ⎟
⎝0 0  0    0   0 0 u21  u22 ⎠

U1 = {U[[All, 1]], U[[All, 2]], U[[All, 5]],
   U[[All, 6]], U[[All, 3]], U[[All, 4]],
   U[[All, 7]], U[[All, 8]] };
U11 = Transpose[U1];

U12 = {U11[[1]], U11[[2]], U11[[5]], U11[[6]],
   U11[[3]], U11[[4]], U11[[7]], U11[[8]]};
U12 // MatrixForm
```

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & u11 & u12 & 0 & 0 \\ 0 & 0 & 0 & 0 & u21 & u22 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & u11 & u12 \\ 0 & 0 & 0 & 0 & 0 & 0 & u21 & u22 \end{pmatrix}$$

In fact, we get this matrix fom the following basic consideration,



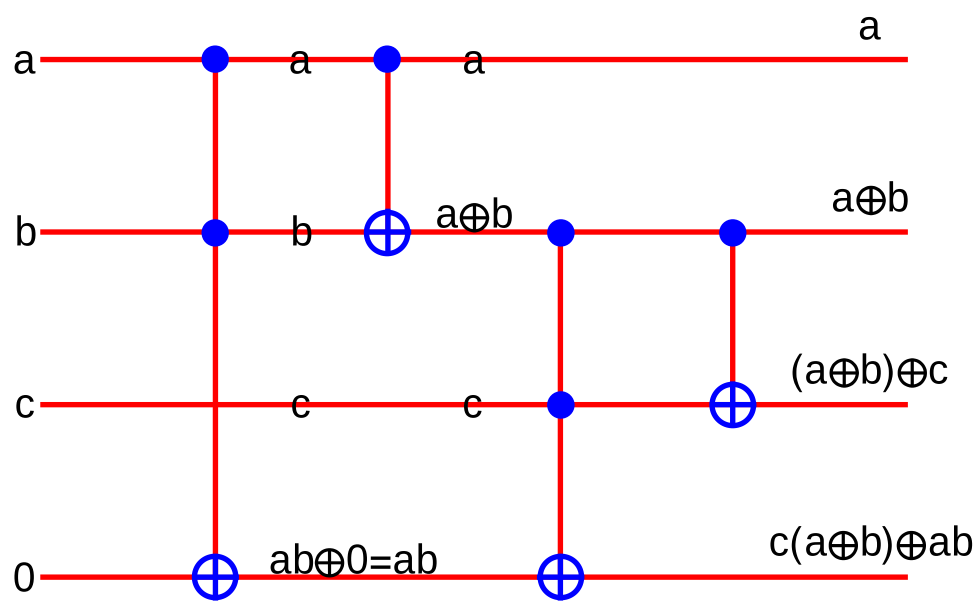
where *a* is the control qubit and *c* is the target qubit.

a	*b*	*c*	*a'*	*b'*	*c'*
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	1	1	0
0	1	1	1	1	1
1	0	0	0	0	$\hat{U}\lvert 0\rangle$
1	0	1	0	0	$\hat{U}\lvert 1\rangle$
1	1	0	1	1	$\hat{U}\lvert 0\rangle$
1	1	1	1	1	$\hat{U}\lvert 1\rangle$

Thus we get

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & U_{11} & U_{12} & 0 & 0 \\ 0 & 0 & 0 & 0 & U_{21} & U_{22} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & U_{11} & U_{12} \\ 0 & 0 & 0 & 0 & 0 & 0 & U_{21} & U_{22} \end{pmatrix} = \begin{pmatrix} \hat{I}_2 & 0 & 0 & 0 \\ 0 & \hat{I}_2 & 0 & 0 \\ 0 & 0 & \hat{U} & 0 \\ 0 & 0 & 0 & \hat{U} \end{pmatrix}$$

20. Example



Note that

$$(a \oplus b) \oplus c = a \oplus b \oplus c$$

$$c(a \oplus b) \otimes ab = ca \oplus ab \oplus bc$$

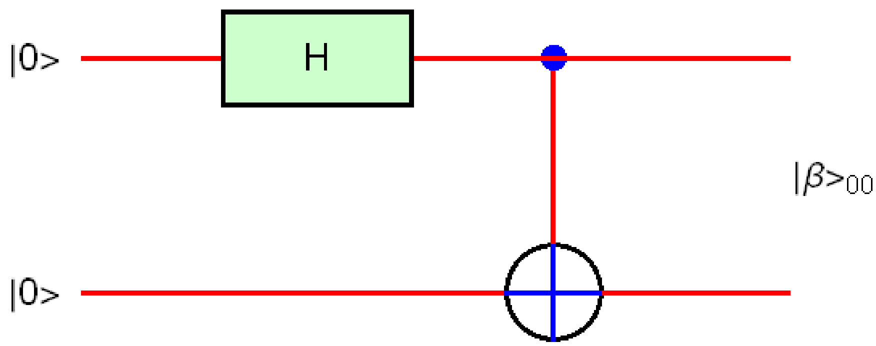
21. Generating entangled qubits (the Bell's state)

$$\hat{U}_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \qquad \hat{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$\hat{U}_{CNOT}(\hat{H} \otimes \hat{I}_2) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{pmatrix} ($$

The Hadamard gate (the H box) is the 2×2 unitary matrix, which takes a single qubit from the upper input and produces a single qubit output. The intermediate state after the Hadamard operation is displayed. The CNOT (Controlled NOT) gate uses a control input (the solid black circle) to affect the target input (the XOR symbol). If the control input is a |0>, then the target output is the same as the target input. If the control input is a |1>, then the target output is the target input inverted. Quantum wire coloring, unique for each qubit state. The dashed line indicates an entangled state, and the line coloring distinguishes the different cubit states.

(a)

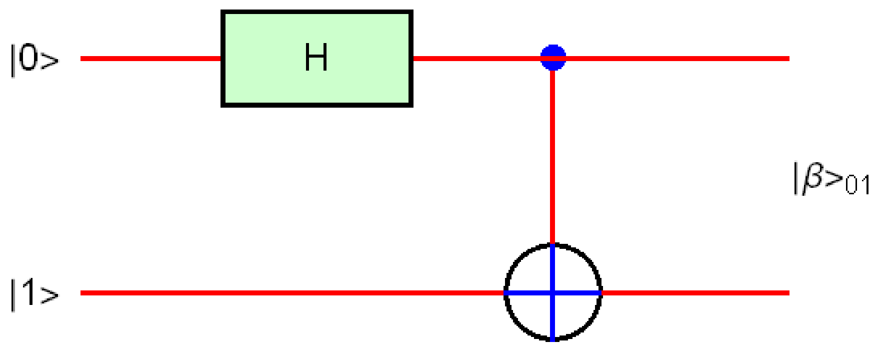


The initial state is

$$\left|\psi_{input}\right\rangle = \left|00\right\rangle = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}$$

$$\hat{U}_{CNOT}(\hat{H}\otimes\hat{I}_2)\begin{pmatrix}1\\0\\0\\0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\1\end{pmatrix} = \left|\beta\right\rangle_{00} \qquad \text{(Bell's state)}$$

(b)

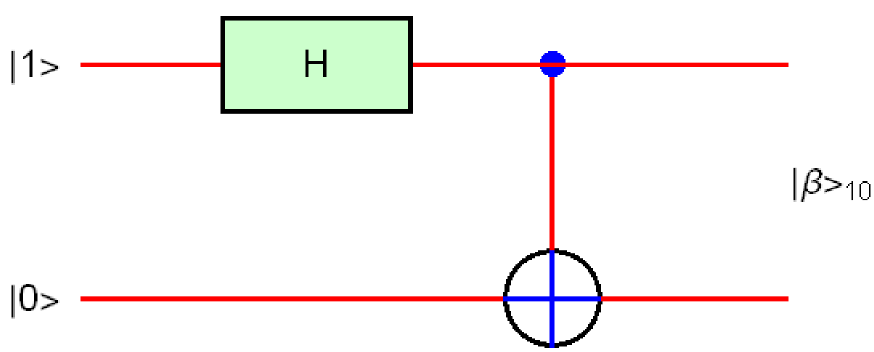


The initial state is

$$\left|\psi_{input}\right\rangle = \left|01\right\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$\hat{U}_{CNOT}(\hat{H}\otimes\hat{I}_2)\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \left|\beta\right\rangle_{01} \qquad \text{(Bell's state)}$$

(c)

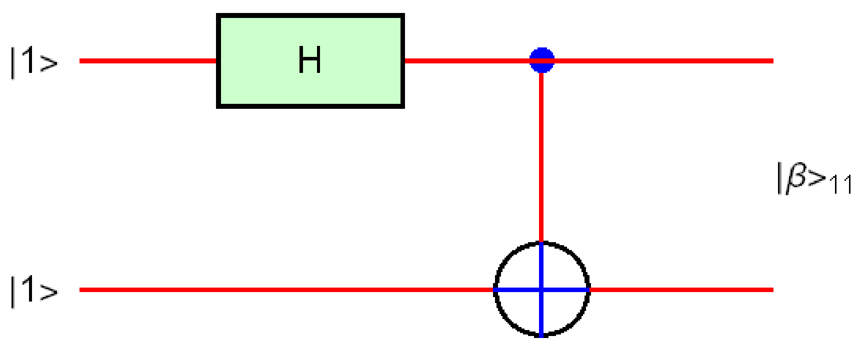


The initial state is

$$\left|\psi_{input}\right\rangle = \left|10\right\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

$$\hat{U}_{CNOT}(\hat{H} \otimes \hat{I}_2)\begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 0 \\ 0 \\ -1 \end{pmatrix} = \left|\beta\right\rangle_{10}$$ (Bell's state)

(d)



The initial state is

$$\left|\psi_{input}\right\rangle = \left|11\right\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Then we have

$$\hat{U}_{CNOT}(\hat{H} \otimes \hat{I}_2)\begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix} = \left|\beta\right\rangle_{11}.$$ (Bell's state)

---

22. Swapping qubit states

Select the states for two qubits. The quantum circuit consisting of three CNOT gates swaps the states as time progresses from left to right to produce the output.

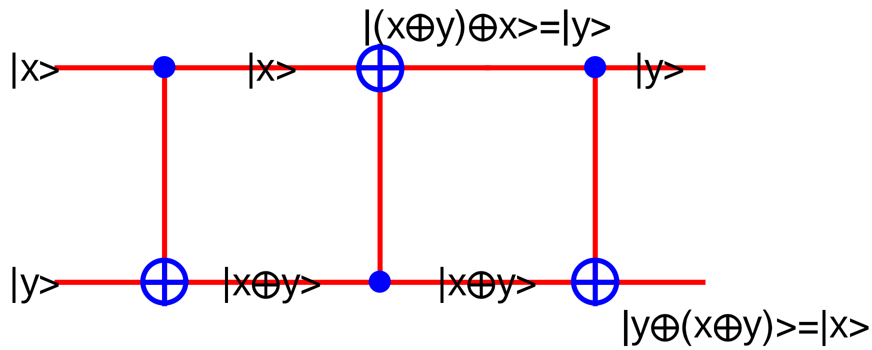


Fig. Swapping qubit states between $|x\rangle$ and $|y\rangle$. Note that $|y\rangle$ $x\oplus x=0$. $y\oplus y=0$

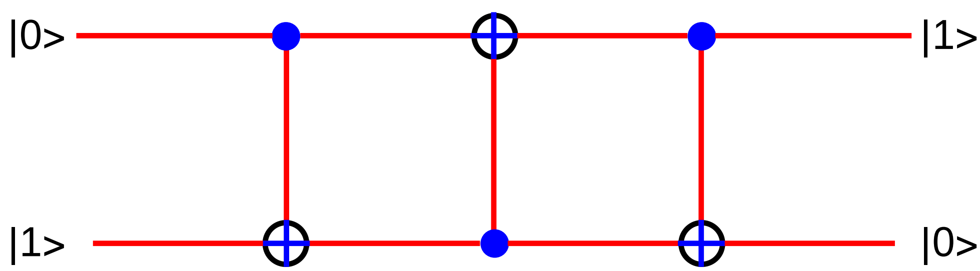


Fig. Swapping qubit states between $|0\rangle$ and $|1\rangle$. Note that $|y\rangle$ $x\oplus x=0$. $y\oplus y=0$

This can be proved by using the matrices of $\hat{U}_{CNOT}$ and $\hat{U}_{RCNOT}$, as follows.

$$\hat{U}_{CNOT}=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix},\qquad \hat{U}_{RCNOT}=\begin{pmatrix}1&0&0&0\\0&0&0&1\\0&0&1&0\\0&1&0&0\end{pmatrix}$$

$$\hat{U}_{CNOT}\hat{U}_{RCNOT}\hat{U}_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

The initial state is given by

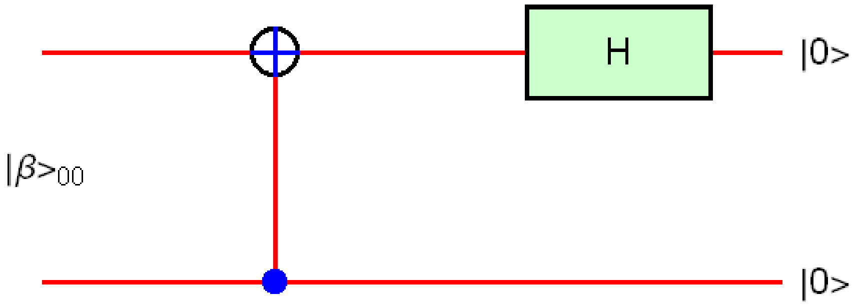
$$\left|\psi_{input}\right\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \left|+-\right\rangle$$

$$\hat{U}_{CNOT}\left|\psi_{input}\right\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix},$$

$$\hat{U}_{RCNOT}\hat{U}_{CNOT}\left|\psi_{input}\right\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

$$\left|\psi_{out}\right\rangle = \hat{U}_{CNOT}\hat{U}_{RCNOT}\hat{U}_{CNOT}\begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \left|-+\right\rangle$$

23. Measuring entangled qubits



$$\Phi_1 = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\1\end{pmatrix}, \qquad \Phi_2 = \frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\\1\\0\end{pmatrix}, \qquad \Phi_3 = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\-1\end{pmatrix}, \qquad \Phi_4 = \frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\\-1\\0\end{pmatrix}$$

$$(\hat{H}\otimes\hat{1})\hat{G}_{CNOT} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 0 & 0 & 1\\0 & 1 & 1 & 0\\1 & 0 & 0 & -1\\0 & 1 & -1 & 0\end{pmatrix}$$

$$(\hat{H}\otimes\hat{1})\hat{G}_{CNOT}\Phi_1 = \begin{pmatrix}1\\0\\0\\0\end{pmatrix} = |00\rangle,$$

$$(\hat{H}\otimes\hat{1})\hat{G}_{CNOT}\Phi_2 = \begin{pmatrix}0\\1\\0\\0\end{pmatrix} = |01\rangle,$$

$$(\hat{H}\otimes\hat{1})\hat{G}_{CNOT}\Phi_3 = \begin{pmatrix}0\\0\\1\\0\end{pmatrix} = |10\rangle,$$

$$(\hat{H}\otimes\hat{1})\hat{G}_{CNOT}\Phi_4 = \begin{pmatrix}0\\0\\0\\1\end{pmatrix} = |11\rangle.$$

We note that

$$(\hat{H}\otimes\hat{1})(\hat{H}\otimes\hat{1})\hat{G}_{CNOT}\Phi_1 = (\hat{H}\otimes\hat{1})|00\rangle$$

or

$$\hat{G}_{CNOT}\Phi_1 = (\hat{H}\otimes\hat{1})|00\rangle$$

and

$$\hat{G}_{CNOT}{}^2\Phi_1 = \hat{G}_{CNOT}(\hat{H}\otimes\hat{1})|00\rangle$$

or

$$\Phi_1 = \hat{G}_{CNOT}(\hat{H}\otimes\hat{1})|00\rangle$$

since

$$(\hat{H}\otimes\hat{1})(\hat{H}\otimes\hat{1}) = \hat{1}\otimes\hat{1} = \hat{1}, \qquad \hat{G}_{CNOT}\hat{G}_{CNOT} = \hat{1}$$

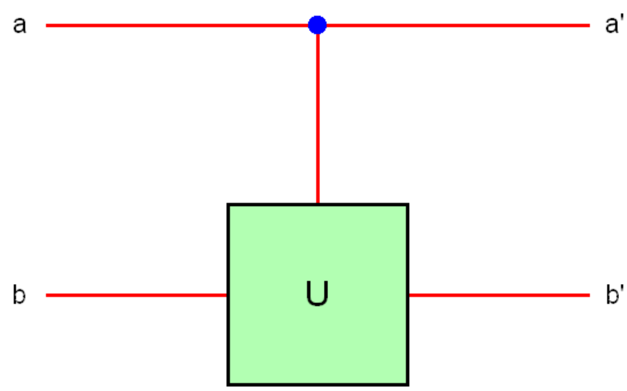
Similarly, we get

$$\Phi_2 = \hat{G}_{CNOT}(\hat{H}\otimes\hat{1})|01\rangle, \qquad \Phi_3 = \hat{G}_{CNOT}(\hat{H}\otimes\hat{1})|10\rangle,$$

$$\Phi_4 = \hat{G}_{CNOT}(\hat{H}\otimes\hat{1})|11\rangle$$

---

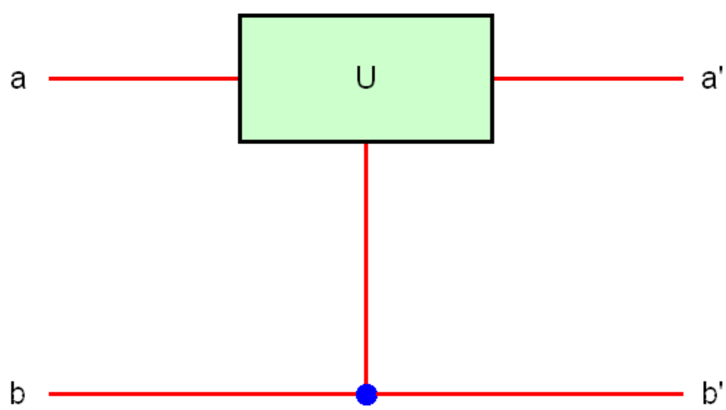
24. Quantum gates



$$\hat{G}_U = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{11} & u_{12} \\ 0 & 0 & u_{21} & u_{22} \end{pmatrix}$$

Here we have the four state;

$$\begin{aligned} |ab\rangle &= |00\rangle, |01\rangle, |10\rangle, |11\rangle \\ &= |1\rangle, |2\rangle, |3\rangle, |4\rangle \end{aligned}$$



We consider the case which is different from the above case. The role of *b* is replaced by that of *a*. In this case, the state is described by $|ba\rangle$;

$$|ba\rangle = |00\rangle, |10\rangle, |01\rangle, |11\rangle = |1\rangle, |3\rangle, |2\rangle, |4\rangle$$

We need to replace both the row vectors and column vectors of the matrix $\hat{C}$ in the order of

$$|00\rangle, |10\rangle, |01\rangle, |11\rangle = |1\rangle, |3\rangle, |2\rangle, |4\rangle$$

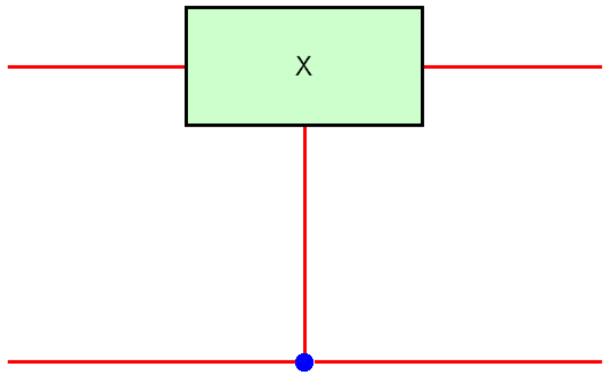
Then we have

$$\hat{R}_U = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & u_{11} & 0 & u_{12} \\ 0 & 0 & 1 & 0 \\ 0 & u_{21} & 0 & u_{22} \end{pmatrix}$$

((**Mathematica**))

```
Clear["Global`*"]; U = (1 0 0   0
                        0 1 0   0
                        0 0 u11 u12
                        0 0 u21 u22);

U1 = {U[[All, 1]], U[[All, 3]], U[[All, 2]],
   U[[All, 4]] }; U11 = Transpose[U1];
U12 = {U11[[1]], U11[[3]], U11[[2]], U11[[4]]};
U12 // MatrixForm

(1  0   0  0
 0  u11 0  u12
 0  0   1  0
 0  u21 0  u22)
```

(a) $\hat{U} = \hat{X}$

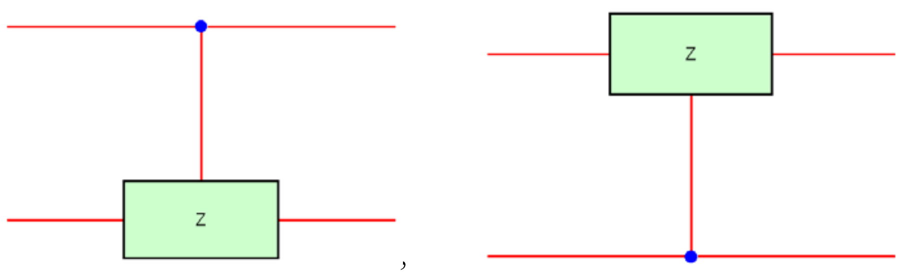


$$\hat{G}_X = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \hat{G}_{CNOT}$$

$$\hat{R}_X = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} = \hat{R}_{CNOT}$$

Note that $\hat{G}_X$ is the same as the matrix of $\hat{G}_{CNOT}$. and that $\hat{R}_X$ is the same as the matrix of $\hat{R}_{CNOT}$.

(b)



These two quantum circuits are equivalent.

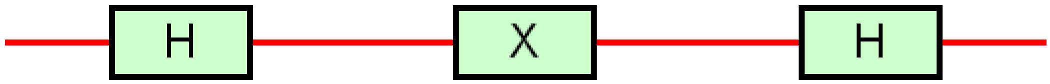
$$\hat{G}_Z = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \qquad \hat{R}_Z = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

25 Equivalence of *H*-*X*-*H* gate and *Z* gate

Since

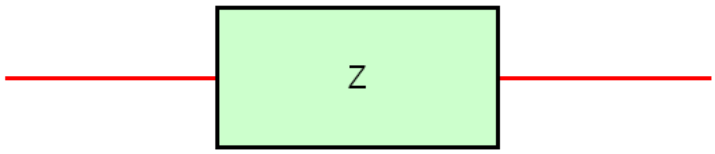
$$\hat{H}\hat{X}\hat{H} = \hat{Z}$$

this quantum circuit (1)



(1)

is equivalent to the *Z* gate (2)



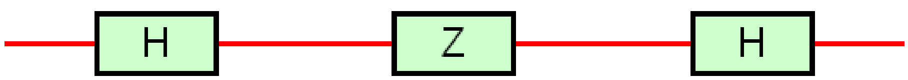
(2)

26. Series connection of H-Z-H

Since

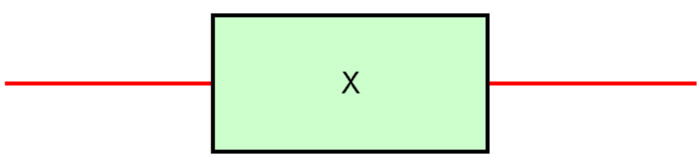
$$\hat{H}\hat{Z}\hat{H} = \hat{X}$$

this quantum circuit



(1)

is equivalent to the *X*-gate (2)



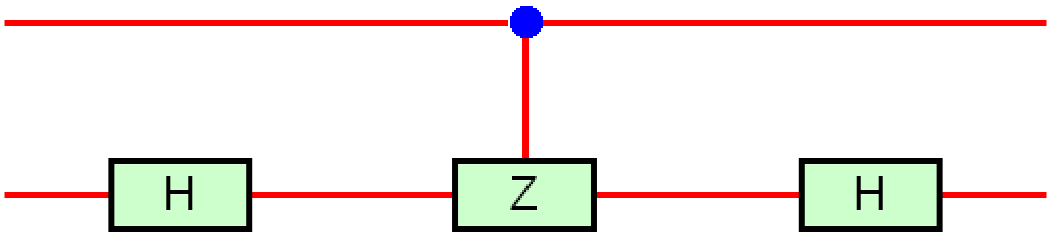
(2)

27 Equivalence

Since

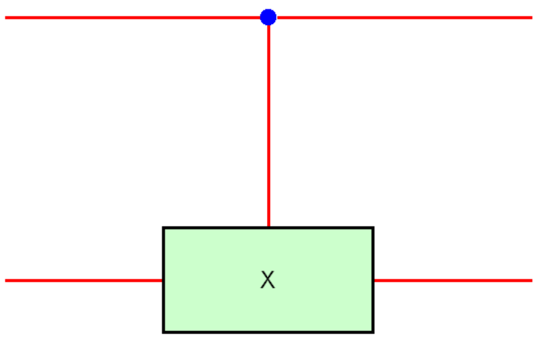
$$(\hat{1}\otimes\hat{H})\hat{G}_Z(\hat{1}\otimes\hat{H}) = \hat{G}_X$$

the quantum circuit (1)



(1)

is equivalent to the quantum gate $\hat{R}_X$ (2)



(2)

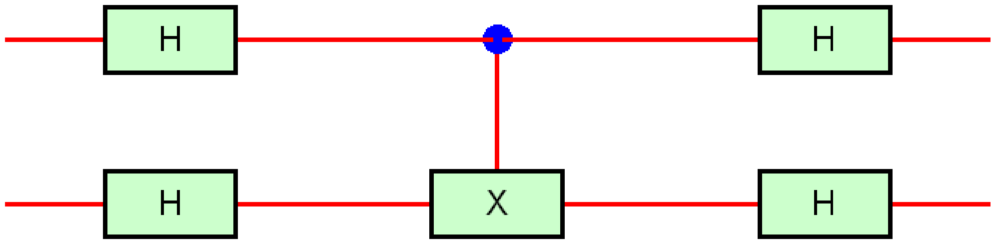
((**Mathematica**))

```
Clear["Global`*"]; CZ = (1 0 0 0
                         0 1 0 0
                         0 0 1 0
                         0 0 0 -1);

I2 = IdentityMatrix[2]; H1 = 1/Sqrt[2] (1 1
                                        1 -1);

H2 = KroneckerProduct[I2, H1];

M1 = H2.CZ.H2 // Simplify; M1 // MatrixForm
```

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

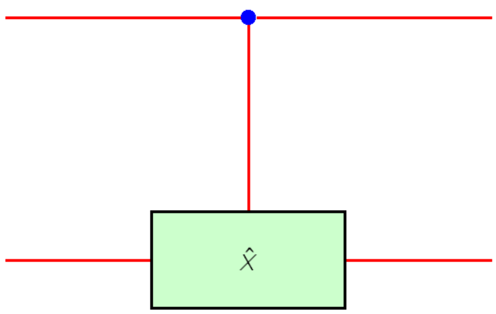
28. Equivalence

We now consider the quantum circuit equivalent to the circuit



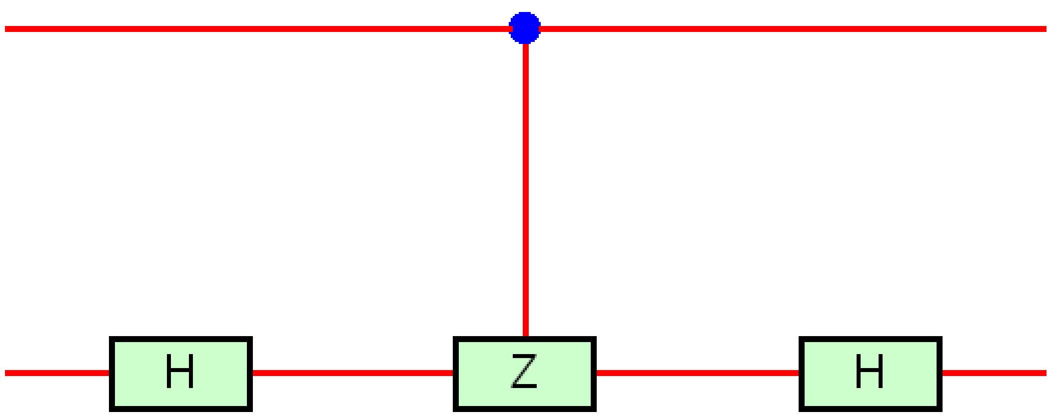
(1)

Here we use the following equivalence circuits. The quantum circuit (2)



(2)

is equivalent to the quantum circuit (3)

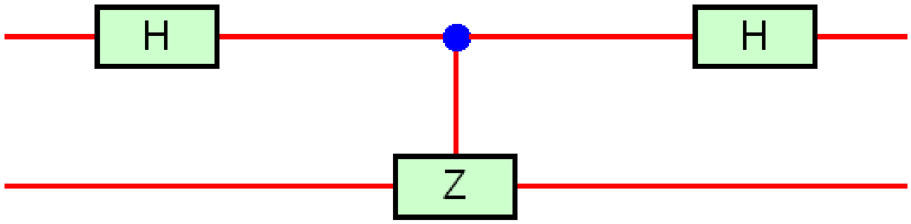


(3)

Noting that

$$\hat{H}^2 = \hat{1}$$

then the quantum circuit (1) is simplified into the quantum circuit

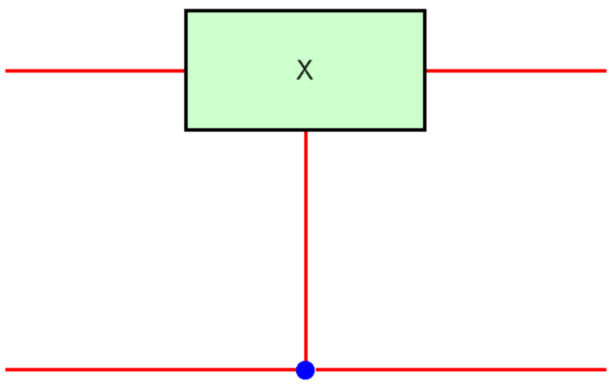


(4)

Since

$$(\hat{H}\otimes\hat{1})\hat{G}_Z(\hat{H}\otimes\hat{1}) = \hat{R}_X = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

the quantum circuit (4) is equivalent to the quantum circuit (5)



(5)

where

where

$$\hat{G}_X = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad \hat{R}_X = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

In conclusion. the quantum circuit (1) is equivalent to the quantum circuit (5).

((**Mathematica**))

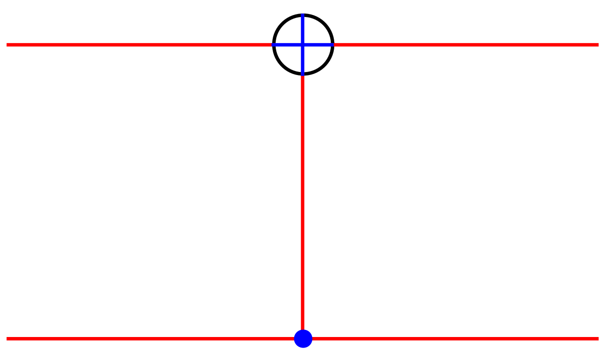
```
Clear["Global`*"]; CX = (1 0 0 0
                         0 1 0 0
                         0 0 0 1
                         0 0 1 0);

H1 = 1/Sqrt[2] (1  1
                1 -1); H2 = KroneckerProduct[H1, H1];

H2 // MatrixForm;

M1 = H2.CX.H2 // Simplify; M1 // MatrixForm
```

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

---

29. Construction of $\hat{G}_{RCNOT}$ from $\hat{R}_{CNOT}$

We consider the gate given by



For convenience we call the gate as the operator $\hat{R}_{CNOT}$ (for convenience), which is closely related to the CNOT operator $\hat{G}_{CNOT}$. We show that

$$\hat{R}_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

where

$$\hat{G}_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Here we have the four state;

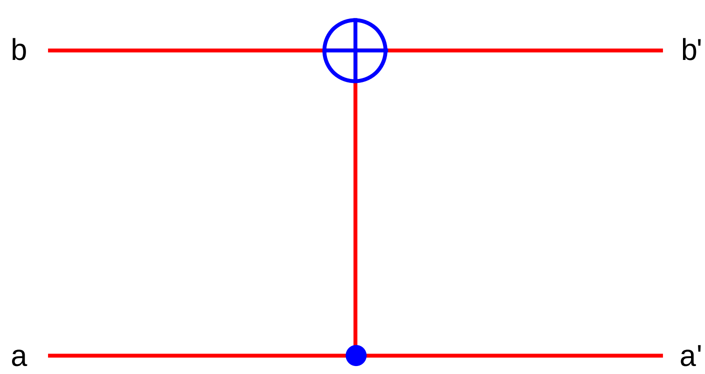
$$\begin{aligned} |ab\rangle &= |00\rangle, |01\rangle, |10\rangle, |11\rangle \\ &= |1\rangle, |2\rangle, |3\rangle, |4\rangle \end{aligned}$$

We consider $\hat{R}_{CNOT}$ which is different from $\hat{G}_{CNOT}$, where the role of *b* is replaced by that of *a*. In this case, the state is described by $|ba\rangle$;

$$|ba\rangle = |00\rangle, |10\rangle, |01\rangle, |11\rangle = |1\rangle, |3\rangle, |2\rangle, |4\rangle$$

Note that

$$\begin{array}{ll} |ab\rangle & |ba\rangle \\ |00\rangle = |1\rangle \rightarrow & |00\rangle = |1\rangle \\ |01\rangle = |2\rangle \rightarrow & |10\rangle = |3\rangle \\ |10\rangle = |3\rangle \rightarrow & |01\rangle = |2\rangle \\ |11\rangle = |4\rangle \rightarrow & |11\rangle = |4\rangle \end{array},$$



We need to replace both the row vectors and column vectors of the matrix $\hat{G}_{CNOT}$ in the order of

$|00\rangle, |10\rangle, |01\rangle, |11\rangle = |1\rangle, |3\rangle, |2\rangle, |4\rangle$

((**Mathematica**)) Construction of $\hat{R}_{CNOT}$ form $\hat{G}_{CNOT}$

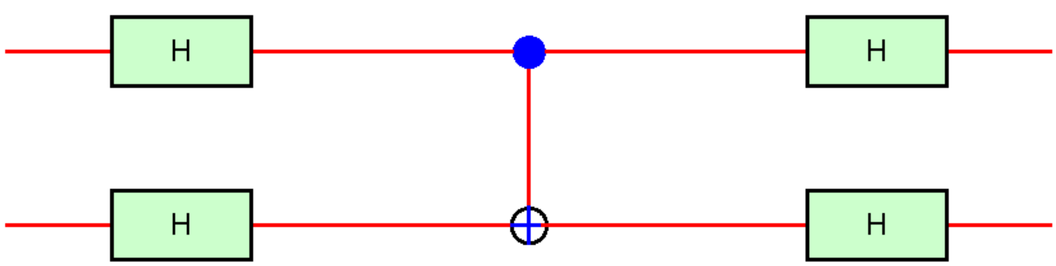
```
Clear["Global`*"]; U = (1 0 0 0
                        0 1 0 0
                        0 0 0 1
                        0 0 1 0);
U1 = {U[[All, 1]], U[[All, 3]], U[[All, 2]],
   U[[All, 4]] }; U11 = Transpose[U1];
U12 = {U11[[1]], U11[[3]], U11[[2]], U11[[4]]};
U12 // MatrixForm
```

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

30. Quantum gate equivalent to CNOT gate

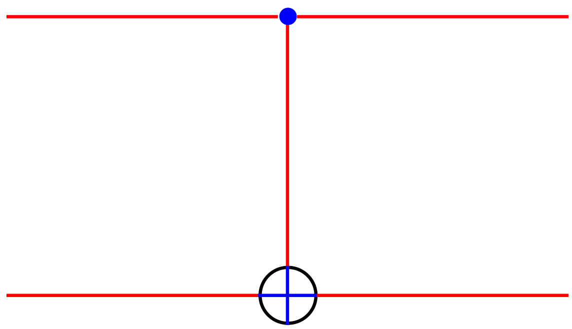
We show that the following circuit is equivalent to the CNOT gate. This shows that the control bit and the target bit is in a CNOT gate are interchangeable by introducing four Hadamard gates.

The quantum circuit (1)



(1)

is equivalent to the quantum gate (2)



(2)

((**Mathematica**)) This can be proved by using the Mathematica as follows.

$$(\hat{H}\otimes\hat{H})\hat{R}_{CNOT}(\hat{H}\otimes\hat{H})=\hat{G}_{CNOT}$$

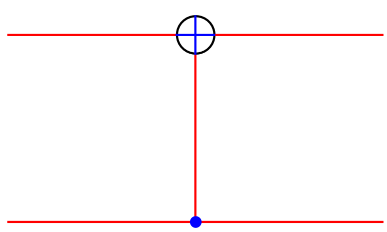
where

(a) Hadamard gate:

$$\hat{H}=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix},$$

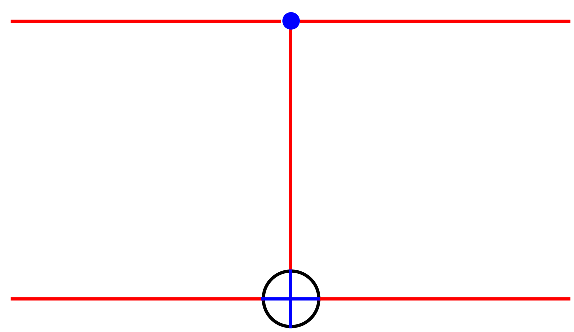
(b) RCNOT gate:

$$\hat{R}_{CNOT}=\begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\\ 0 & 1 & 0 & 0\end{pmatrix}$$



(c) CNOT gate:

$$\hat{G}_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

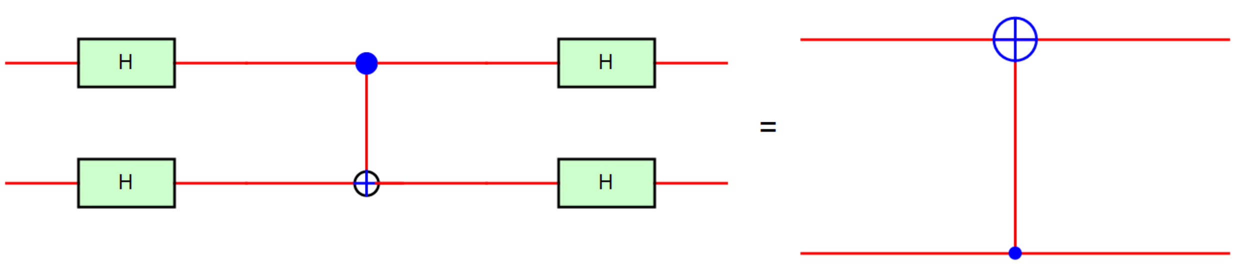


((**Mathematica**))

```
Clear["Global`*"]; UR = {{1, 0, 0, 0}, {0, 0, 0, 1}, {0, 0, 1, 0}, {0, 1, 0, 0}}; H1 = 1/Sqrt[2] {{1, 1}, {1, -1}};

H2 = KroneckerProduct[H1, H1];

M1 = H2.UR.H2 // Simplify; M1 // MatrixForm
```

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

31 Equivalence



$$\hat{G}_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \qquad H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \qquad \hat{R}_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

((**Mathematica**))

```
Clear["Global`*"]; H1 = 1/√2 (1  1
                              1 -1);

UCNOT = (1 0 0 0
         0 1 0 0
         0 0 0 1
         0 0 1 0);

H2 = KroneckerProduct[H1, H1];
eq1 = H2.UCNOT.H2 // FullSimplify;
eq1 // MatrixForm
```

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

28. X-CNOT-X

Empty circle if instead the target is flipped when the control is $|0\rangle$.

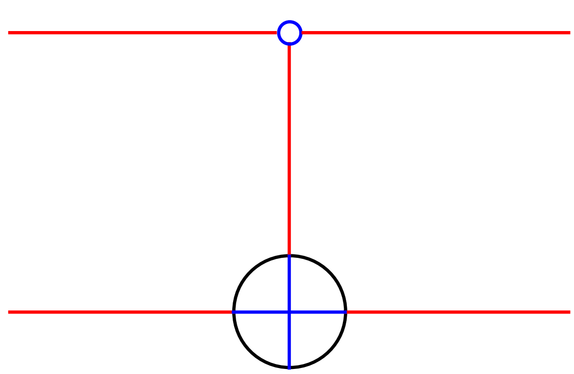
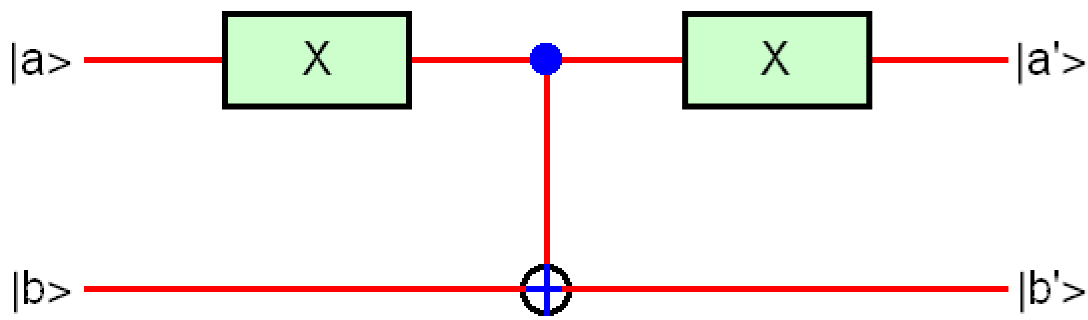


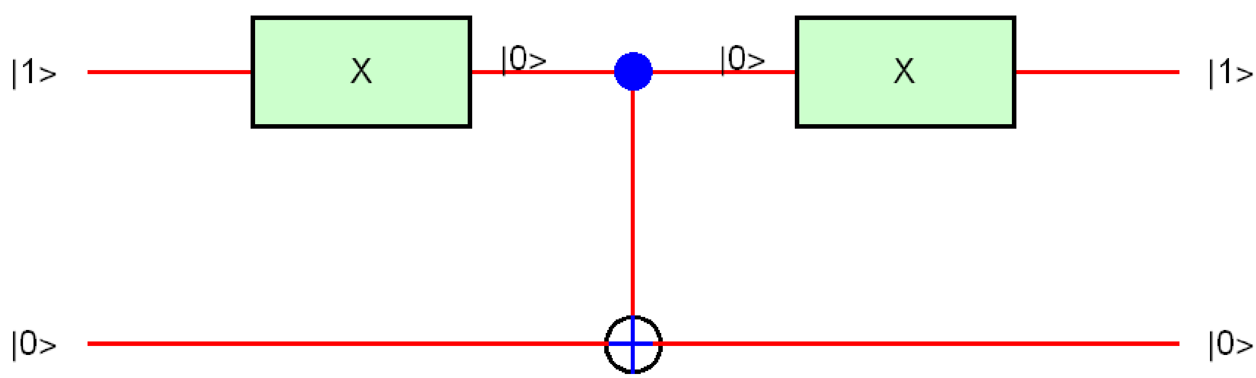
Fig. Controlled operation with a NOT gate being performed on the second qubit, conditional on the first being set to zero. This quantum circuit is equivalent to the following circuit.
Note that

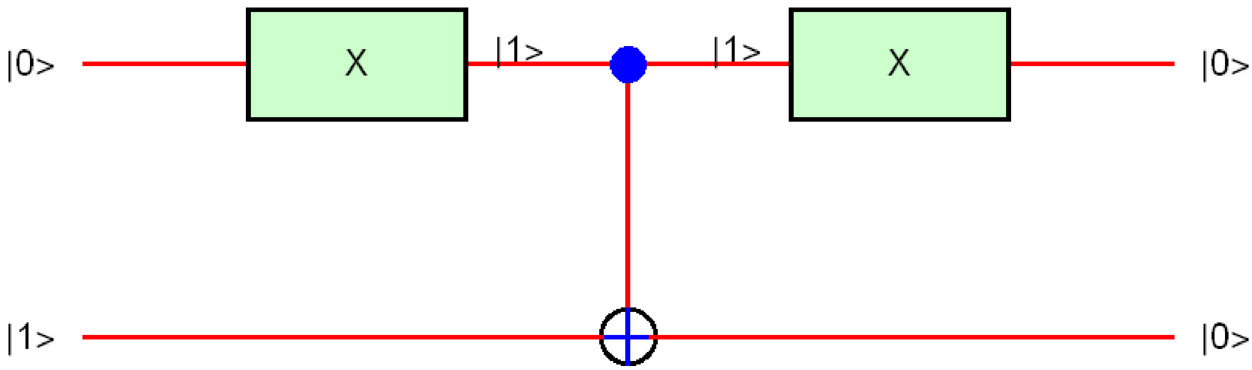
$$(\hat{X} \otimes \hat{1})\hat{G}_{CNOT}(\hat{X} \otimes \hat{1}) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$



Truth table:

a	b	a'	b'
1	0	1	0
1	1	1	1
0	0	0	1
0	1	0	0





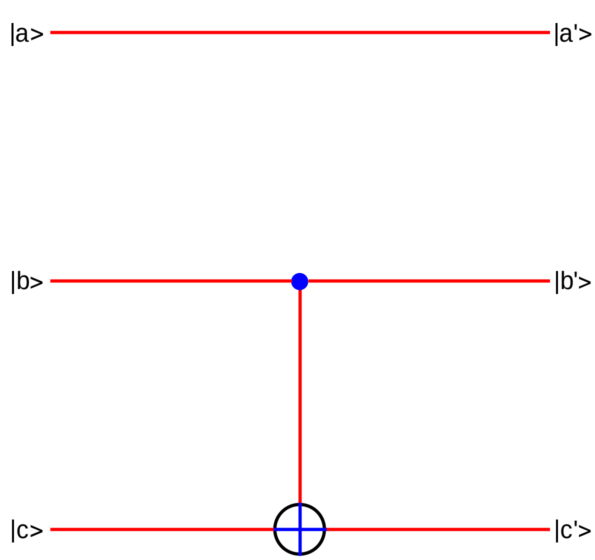
32. Three qubits systems

(a) $\hat{G}_{CNOT23}$

The quantum circuit $\hat{G}_{CNOT23}$ consists of the Identity operator $\hat{1}$ and the CNOT operator in parallel connection.

$$\hat{G}_{CNOT\,23} = \hat{1} \otimes \hat{G}_{CNOT}$$

$$= \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} \boldsymbol{I} & 0 & 0 & 0 \\ 0 & \boldsymbol{X} & 0 & 0 \\ 0 & 0 & \boldsymbol{I} & 0 \\ 0 & 0 & 0 & \boldsymbol{X} \end{pmatrix}$$



(b) $\hat{G}_{CNOT13}$

We show that the $\hat{G}_{CNOT13}$ is given by

$$\hat{G}_{CNOT13} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} \boldsymbol{I} & 0 & 0 & 0 \\ 0 & \boldsymbol{I} & 0 & 0 \\ 0 & 0 & \boldsymbol{I} & 0 \\ 0 & 0 & 0 & \boldsymbol{X} \end{pmatrix}$$

where the quantum circuit of $\hat{G}_{CNOT13}$ is schematically shown by

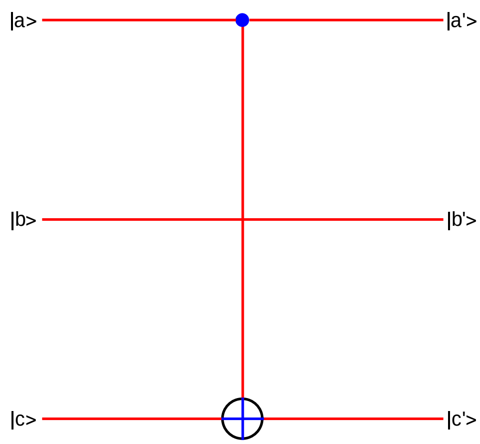


Fig. For convenience this is called $\hat{G}_{CNOT13}$). The qubits 1 ($|a\rangle$) and 3 ($|c\rangle$) form the CNOT gate, while $|b\rangle = |b'\rangle$

The quantum circuit of $\hat{G}_{CNOT13}$ is compared with that of $\hat{G}_{CNOT23}$, where the state is switched as $|abc\rangle \rightarrow |bac\rangle$. The roles of $|a\rangle$ and $|b\rangle$ are replaced by those of $|b\rangle$ and $|a\rangle$. So we need to replace both the row vectors and column vectors of the matrix $\hat{G}_{CNOT23}$ in the order of

$|abc\rangle \qquad |bac\rangle$

$|000\rangle = |1\rangle \to \quad |000\rangle = |1\rangle$

$|001\rangle = |2\rangle \to \quad |001\rangle = |2\rangle$

$|010\rangle = |3\rangle \to \quad |100\rangle = |5\rangle$

$|011\rangle = |4\rangle \to \quad |101\rangle = |6\rangle$

$|100\rangle = |5\rangle \to \quad |010\rangle = |3\rangle$

$|101\rangle = |6\rangle \to \quad |011\rangle = |4\rangle$

$|110\rangle = |7\rangle \to \quad |110\rangle = |7\rangle$

$|111\rangle = |8\rangle \to \quad |111\rangle = |8\rangle$

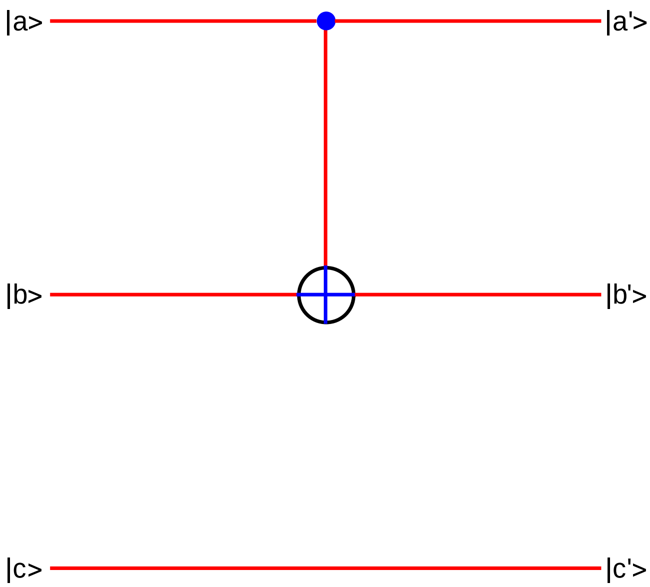
((**Mathematica**))

```
Clear["Global`*"]; UCNOT = (1 0 0 0
                            0 1 0 0
                            0 0 0 1
                            0 0 1 0); I2 = (1 0
                                            0 1);
U = KroneckerProduct[I2, UCNOT];
U1 = {U[[All, 1]], U[[All, 2]], U[[All, 5]],
  U[[All, 6]], U[[All, 3]], U[[All, 4]],
  U[[All, 7]], U[[All, 8]] }; U11 = Transpose[U1];
U12 = {U11[[1]], U11[[2]], U11[[5]], U11[[6]],
  U11[[3]], U11[[4]], U11[[7]], U11[[8]]};
U12 // MatrixForm
```

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

(c) $\hat{G}_{CNOTI2}$

The quantum circuit $\hat{G}_{CNOTI2}$ consists of the Identity operator I_2 and the CNOT operator in parallel connection. The quantum circuit of $\hat{G}_{CNOTI2}$ is schematically shown by



$$\hat{G}_{CNOT12} = \hat{G}_{CNOT} \otimes \hat{1} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

33. Equivalence of quantum circuit

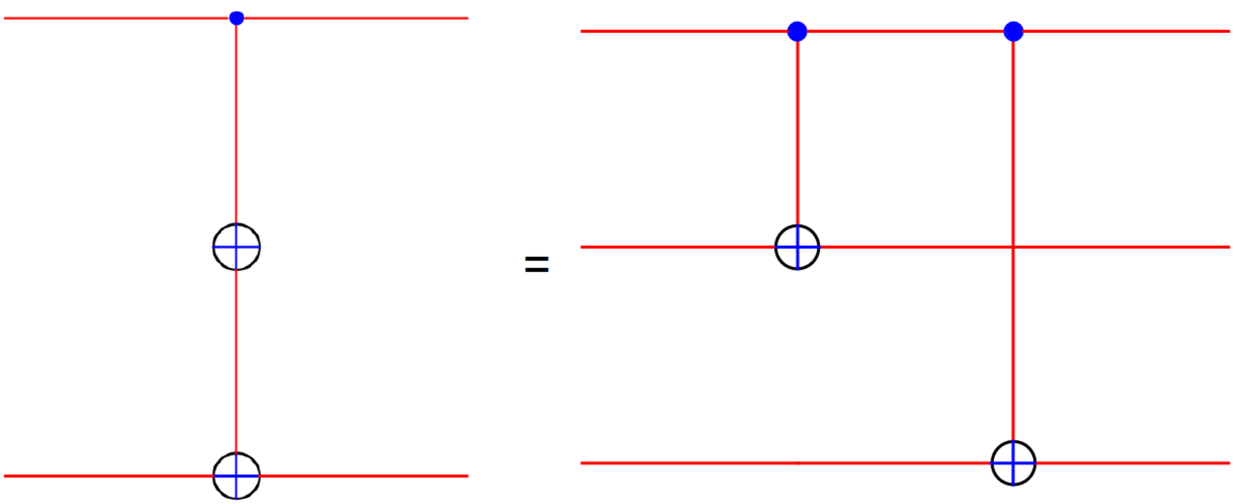
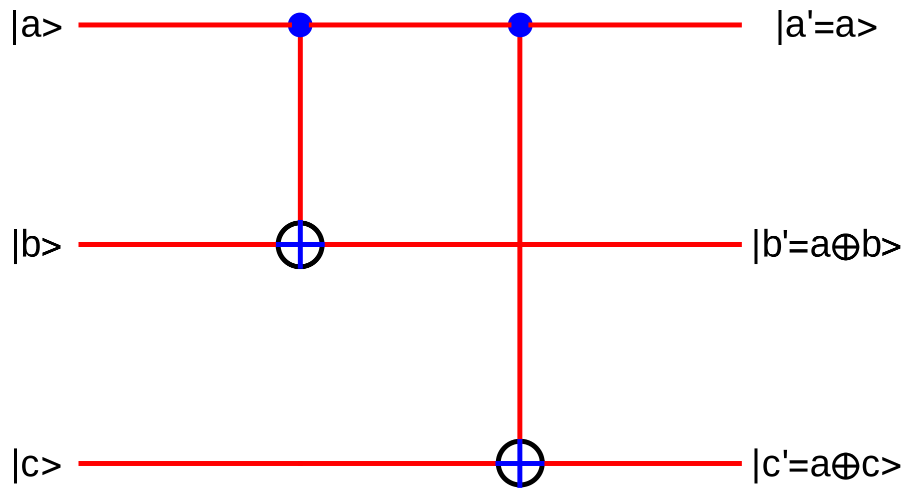


Fig. Controlled NOT gate with multiple targets.



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	1	1
1	0	1	1	1	0
1	1	0	1	0	1
1	1	1	1	0	0

$$\hat{G}_{CNOT12}\hat{G}_{CNOT13} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

In fact, using two matrices $\hat{G}_{CNOT13}$ and $\hat{G}_{CNOT12}$

$$\hat{G}_{CNOT13} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

$$\hat{G}_{CNOT12} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

we can evaluate

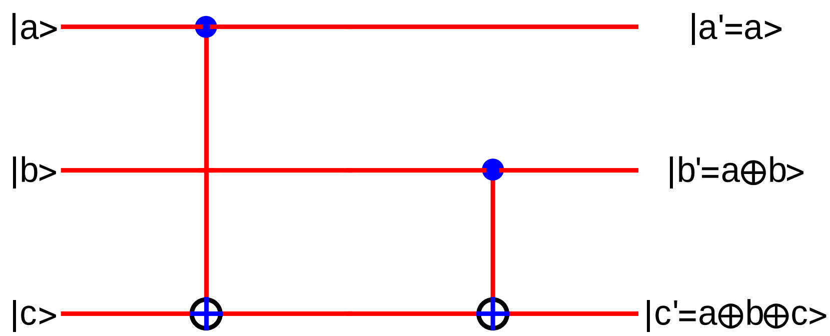
$$\hat{G}_{CNOT}(1-2)\hat{G}_{CNOT}(1-3) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

or

$$\hat{G}_{CNOT12}\hat{G}_{CNOT13} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} \boldsymbol{I} & 0 & 0 & 0 \\ 0 & \boldsymbol{I} & 0 & 0 \\ 0 & 0 & 0 & \boldsymbol{X} \\ 0 & 0 & \boldsymbol{X} & 0 \end{pmatrix}$$

which is the same as that derived from the truth table listed above.

34. Combination of two three qubits circuit



$$\hat{G}_{CNOT13}\hat{G}_{CNOT23}=\begin{pmatrix}1&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&1&0&0&0&0&0\\0&0&0&1&0&0&0&0\\0&0&0&0&0&1&0&0\\0&0&0&0&1&0&0&0\\0&0&0&0&0&0&0&1\\0&0&0&0&0&0&1&0\end{pmatrix}\begin{pmatrix}1&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&0&1&0&0&0&0\\0&0&1&0&0&0&0&0\\0&0&0&0&1&0&0&0\\0&0&0&0&0&1&0&0\\0&0&0&0&0&0&0&1\\0&0&0&0&0&0&1&0\end{pmatrix}$$

$$=\begin{pmatrix}1&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&0&1&0&0&0&0\\0&0&1&0&0&0&0&0\\0&0&0&0&0&1&0&0\\0&0&0&0&1&0&0&0\\0&0&0&0&0&0&1&0\\0&0&0&0&0&0&0&1\end{pmatrix}$$

In fact we have

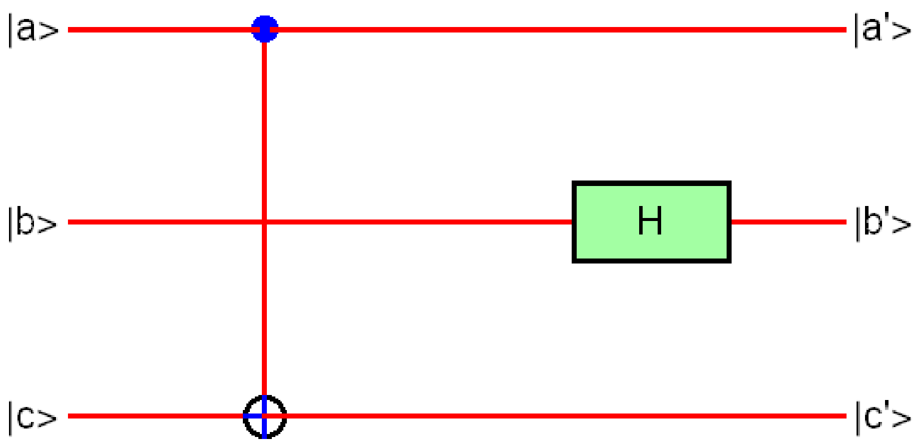
a	b	c	a’	b’	c’
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	1
0	1	1	0	1	0
1	0	0	1	0	1
1	0	1	1	0	0
1	1	0	1	1	0
1	1	1	1	1	1

Then the matrix can be obtained as

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

which is the same as that derived from the matrix calculation by using the Mathematica.

35. Quantum circuit with CNOT (1-3) and *H* gates



$$
\hat{G}_{CNOT13} =
\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0
\end{pmatrix}
=
\begin{pmatrix}
\boldsymbol{I} & 0 & 0 & 0 \\
0 & \boldsymbol{I} & 0 & 0 \\
0 & 0 & \boldsymbol{X} & 0 \\
0 & 0 & 0 & \boldsymbol{X}
\end{pmatrix}
$$

$$\hat{1}\otimes\hat{H}\otimes\hat{1}=\frac{1}{\sqrt{2}}\begin{pmatrix}1&0&1&0&0&0&0&0\\0&1&0&1&0&0&0&0\\1&0&-1&0&0&0&0&0\\0&1&0&-1&0&0&0&0\\0&0&0&0&1&0&1&0\\0&0&0&0&0&1&0&1\\0&0&0&0&1&0&-1&0\\0&0&0&0&0&1&0&-1\end{pmatrix}$$

$$\hat{G}_{CNOT13}[\hat{1}\otimes\hat{H}\otimes\hat{1}]=\frac{1}{\sqrt{2}}\begin{pmatrix}1&0&1&0&0&0&0&0\\0&1&0&1&0&0&0&0\\1&0&-1&0&0&0&0&0\\0&1&0&-1&0&0&0&0\\0&0&0&0&0&1&0&1\\0&0&0&0&1&0&1&0\\0&0&0&0&0&1&0&-1\\0&0&0&0&1&0&-1&0\end{pmatrix}$$

Note that

$$[\hat{1}\otimes\hat{H}\otimes\hat{1}]\hat{G}_{CNOT13}=\hat{G}_{CNOT13}[\hat{1}\otimes\hat{H}\otimes\hat{1}] \qquad \text{(reversible)}$$

---

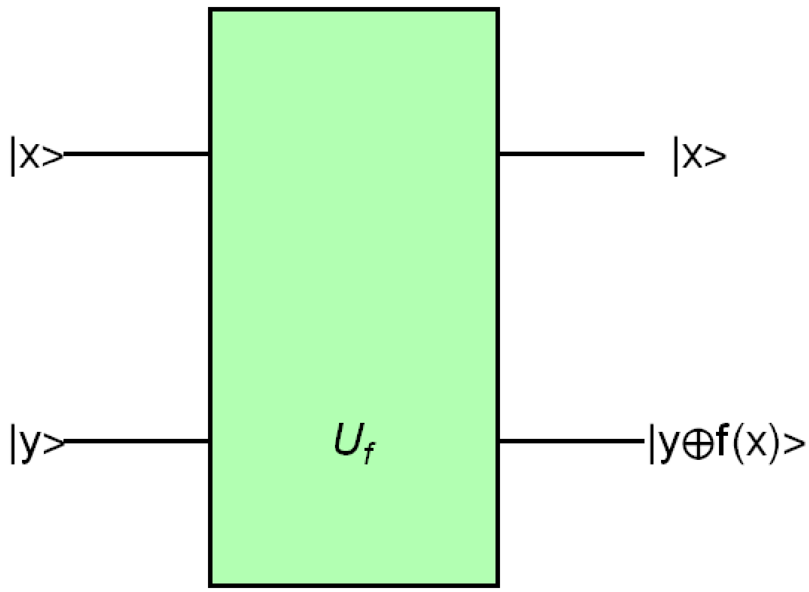
36. Quantum gate with the operator $\hat{U}_f$

N.D. Mermin, Quantum Computer Science, An Introduction (Cambridge University Press, 2007)

"Deutsch's problem is the simplest example of a quantum tradeoff that sacrifices particular information to acquire relational information. A crude version of it appeared in a 1985 paper by David Deutsch that, together with a 1982 paper by Richard Feynman, launched the whole field. In that early version the trick could be executed successfully only half the time. It took a while for people to realize that the trick could be accomplished every single time. Here is how it works.

Suppose that we are given a black box that calculates one of four functions (as shown in table) in the usual quantum-computational format, by performing the unitary transformation

$$\hat{U}_f|x\rangle\otimes|y\rangle=|x\rangle\otimes|y\oplus f(x)\rangle .$$



((**Note**))

$\hat{U}_f$ is the universal operator.

$$\hat{U}_f{}^2|x,y\rangle = \hat{U}_f|x, y\oplus f(x)\rangle = |x, y\oplus f(x)\oplus f(x)\rangle$$

Noting that

$$f(x)\oplus f(x) = 0$$

then we have

$$\hat{U}_f{}^2|x,y\rangle = |x, y\oplus 0\rangle = |x,y\rangle$$

or

$$\hat{U}_f{}^2 = \hat{1}$$

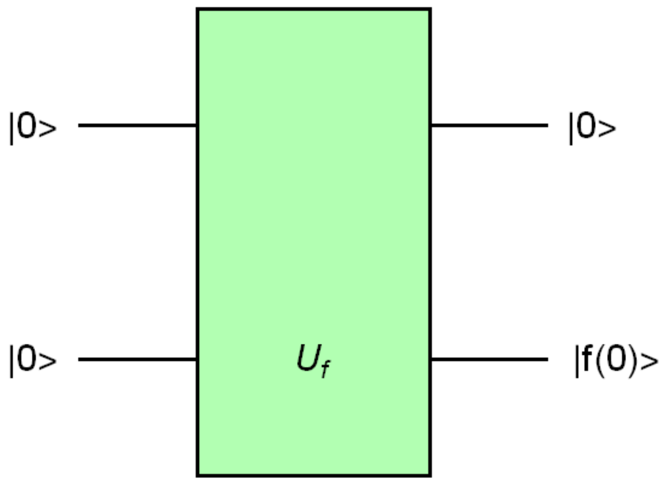
We consider the four types operations [*f*(0) and *f*(1)].
Table

Type	*f*(0)	*f*(1)
a	0	0
b	0	1
c	1	0

d 1 1

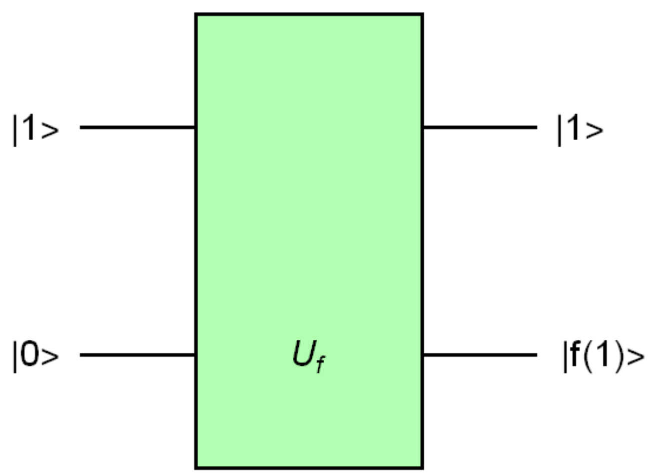
But we are not told which of the four operations the black box carries out. We can, of course, find out by letting the black box act twice, first on $|0\rangle \otimes |0\rangle = |0,0\rangle$ and then on $|1\rangle \otimes |0\rangle = |1,0\rangle$.

(i) The input as $|0\rangle \otimes |0\rangle = |0,0\rangle$. The second qubit of the output is $|f(0)\rangle$.



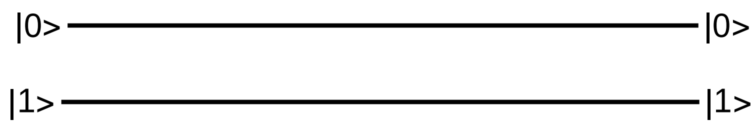
,

(ii) The input as $|1\rangle \otimes |0\rangle = |1,0\rangle$. The second qubit of the output is $|f(1)\rangle$.



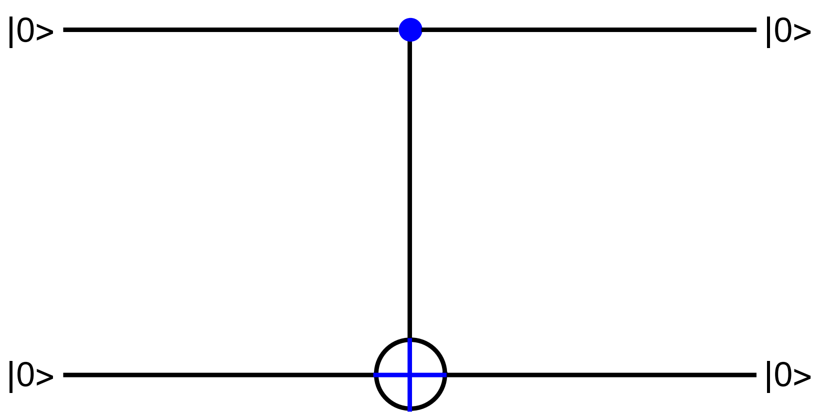
From the two queries, we can find the values of $f(0)$ and $f(1)$.

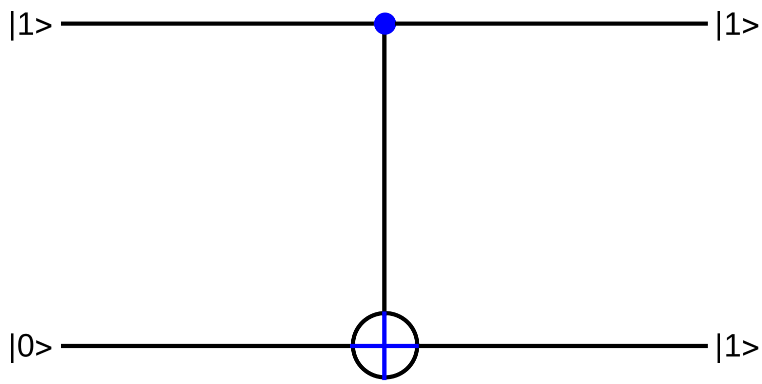
(a) $f(0) = 0$, $f(1) = 0$



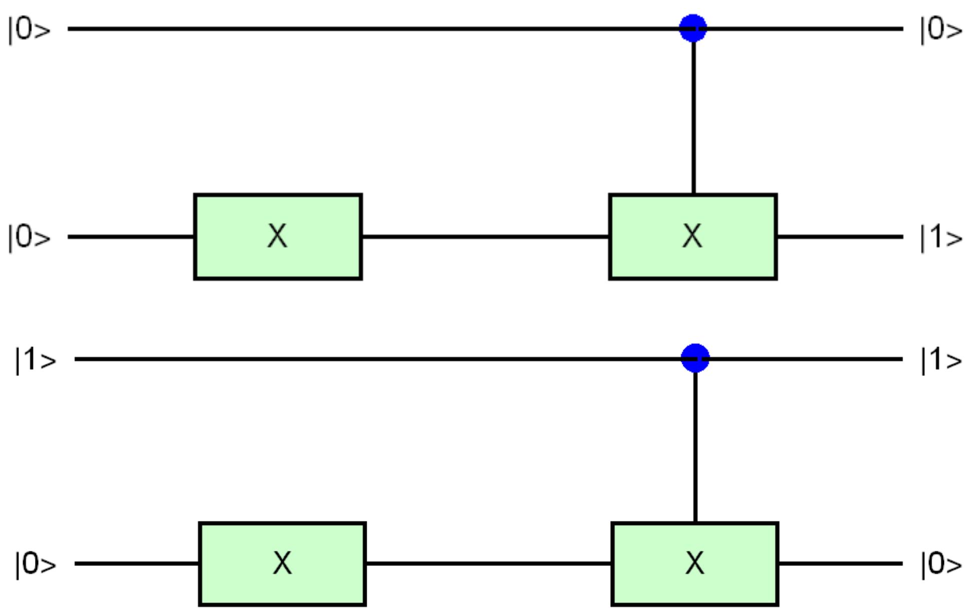
(b) $f(0) = 0$, $f(1) = 1$

Controlled NOT (CNOT) gate

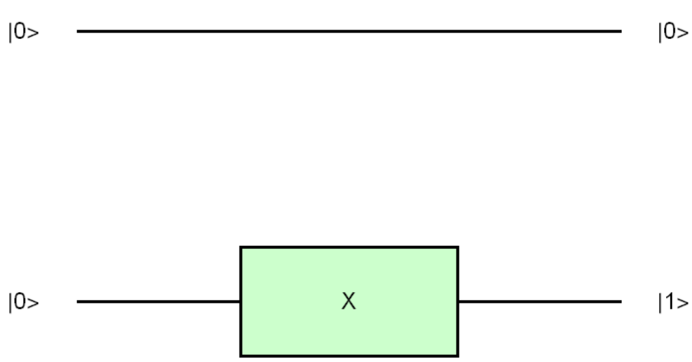


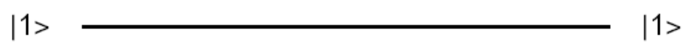


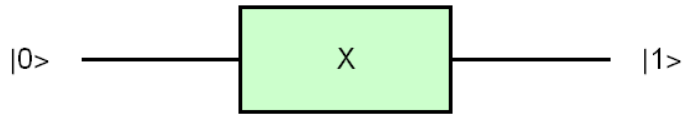
(c) $f(0) = 1$, $f(1) = 0$



(d) $f(1) = 1$, $f(1) = 1$

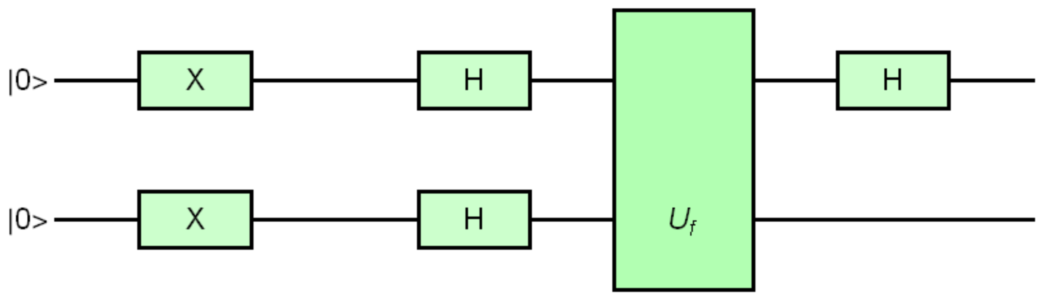






37. Deutsch problem (I)

We consider the following problem, which was first proposed in 1985 by David Deutsch. Are *f*'s two values *f*(0) and *f*(1) the same or different? Equivalently what is their parity. Classically, in order to solve this problem, we need to query *f*(0) and *f*(1) separately. But quantum mechanically a single query suffices.



We consider the quantum circuits where the input is given by $|0\rangle \otimes |0\rangle = |0,0\rangle$.

((**The first and second stages**))

$$
\begin{aligned}
(\hat{H} \otimes \hat{H})(\hat{X} \otimes \hat{X})|00\rangle &= (\hat{H} \otimes \hat{H})(\hat{X}|0\rangle \otimes \hat{X}|0\rangle) \\
&= (\hat{H} \otimes \hat{H})(|1\rangle \otimes |1\rangle) \\
&= \hat{H}|1\rangle \otimes \hat{H}|1\rangle \\
&= \frac{1}{2}(|0\rangle - |1\rangle) \otimes (|0\rangle - |1\rangle) \\
&= \frac{1}{2}[|00\rangle - |01\rangle - |10\rangle + |11\rangle]
\end{aligned}
$$

((**Third stage**))

We get

$$\hat{U}_f\left(\hat{H}\otimes\hat{H}\right)\left(\hat{X}\otimes\hat{X}\right)|00\rangle = \frac{1}{2}[\hat{U}_f|00\rangle - \hat{U}_f|01\rangle - \hat{U}_f|10\rangle + \hat{U}_f|11\rangle]$$
$$= \frac{1}{2}[|0,0\oplus f(0)\rangle - |0,1\oplus f(0)\rangle - |1,0\oplus f(1)\rangle + |1,1\oplus f(1)\rangle]$$
$$= \frac{1}{2}[|0, f(0)\rangle - |0, \tilde{f}(0)\rangle - |1, f(1)\rangle + |1, \tilde{f}(1)\rangle]$$

We consider the four cases.

	$f(0)$	$f(1)$	$f(0)\oplus f(1)$
a.	0	0	0
b	0	1	1
c	1	0	1
d	1	1	0

(a)

Suppose that $f(0)=f(1)$ corresponding to the cases (a) and (d). Then we get

$$\hat{U}_f\left(\hat{H}\oplus\hat{H}\right)\left(\hat{X}\oplus\hat{X}\right)|00\rangle = \frac{1}{2}[|0, f(0)\rangle - |0, \tilde{f}(0)\rangle - |1, f(0)\rangle + |1, \tilde{f}(0)\rangle]$$
$$= \frac{1}{2}(|0\rangle - |1\rangle)(|f(0)\rangle - |\tilde{f}(0)\rangle)$$

Furthermore, we apply $(\hat{H}\otimes\hat{1})$ to this result,

$$\frac{1}{2}(\hat{H}\otimes\hat{1})(|0\rangle - |1\rangle)(|f(0)\rangle - |\tilde{f}(0)\rangle) = \frac{1}{2}(\hat{H})(|0\rangle - |1\rangle)\otimes\hat{1}(|f(0)\rangle - |\tilde{f}(0)\rangle)$$
$$= \frac{1}{\sqrt{2}}|1\rangle(|f(0)\rangle - |\tilde{f}(0)\rangle)$$
$$= \frac{1}{\sqrt{2}}(|1, f(0)\rangle - |1, \tilde{f}(0)\rangle)$$

(b)

Suppose that $f(0)\neq f(1)$ corresponding to the cases (b) and (c). Then we get

$$f(0)=\tilde{f}(1), \quad f(1)=\tilde{f}(0)$$

$$\hat{U}_f\left(\hat{H}\oplus\hat{H}\right)\left(\hat{X}\oplus\hat{X}\right)|00\rangle = \frac{1}{2}[|0,f(0)\rangle - |0,\tilde{f}(0)\rangle - |1,f(1)\rangle + |1,\tilde{f}(1)\rangle]$$
$$= \frac{1}{2}(|0\rangle + |1\rangle)(|f(0)\rangle - |\tilde{f}(0)\rangle)$$

Furthermore, we apply a Hadamard operator $\hat{H}$ to this result. Then we have

$$|\psi\rangle = \frac{1}{2}(\hat{H}\otimes\hat{1})(|0\rangle - |1\rangle)(|f(0)\rangle - |\tilde{f}(0)\rangle) = \frac{1}{\sqrt{2}}|1\rangle(|f(0)\rangle - |\tilde{f}(0)\rangle) \quad [f(0) = f(1)]$$

$$|\psi\rangle = |1\rangle \otimes (\frac{|0\rangle - |1\rangle}{\sqrt{2}})$$ for the case (a)

$$|\psi\rangle = -|1\rangle \otimes (\frac{|0\rangle - |1\rangle}{\sqrt{2}})$$ for the case (d)

$$|\psi\rangle = \frac{1}{2}(\hat{H}\otimes\hat{1})(|0\rangle + |1\rangle)(|f(0)\rangle - |\tilde{f}(0)\rangle)$$
$$= \frac{1}{2}(\hat{H}(|0\rangle + |1\rangle)\otimes\hat{1}(|f(0)\rangle - |\tilde{f}(0)\rangle) \qquad [f(0) \neq f(1)]$$
$$= \frac{1}{\sqrt{2}}|0\rangle(|f(0)\rangle - |\tilde{f}(0)\rangle)$$

$$|\psi\rangle = |0\rangle \otimes (\frac{|0\rangle - |1)\rangle}{\sqrt{2}})$$ for the case (b)

$$|\psi\rangle = -|0\rangle \otimes (\frac{|0\rangle - |1\rangle}{\sqrt{2}})$$ for the case (c)

We note that

$f(0)\oplus f(1) = 0$ if $f(0) = f(1)$,

$f(0)\oplus f(1) = 1$ if $f(0) \neq f(1)$,

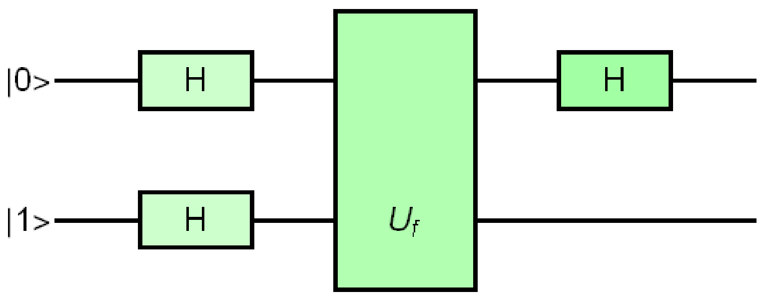
In summary, $|\psi\rangle$ can be rewritten as

$$|\psi\rangle = \pm|f(0)\oplus f(1)\rangle \otimes (\frac{|0\rangle - |1\rangle}{\sqrt{2}})$$

This expression tells us that by measuring the first output qubit of the quantum circuit, we are able to determine $f(0)\oplus f(1)$ after performing a single evaluation of the function *f*(*x*).

38 Deutsch's problem (II)

We consider a quantum circuit (shown below) for solving the Deutsch's problem. We show that the first output qubit of the circuit is $\pm|f(0)\oplus f(1)\rangle$. If $f(0) = f(1)$, the qubit is $|0\rangle$ and if $f(0) \neq f(1)$, the qubit is $|1\rangle$.



((**The second stage**))

$$\begin{aligned}(\hat{H}\otimes\hat{H})|01\rangle &= (\hat{H}|0\rangle \otimes \hat{H}|1\rangle) \\ &= \frac{1}{2}(|0\rangle + |1\rangle)\otimes(|0\rangle - |1\rangle) \\ &= |+\rangle \otimes |-\rangle \\ &= \frac{1}{2}[|00\rangle - |01\rangle + |10\rangle - |11\rangle]\end{aligned}$$

where

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

((**Third stage**))

We have

$$|\psi\rangle = \hat{U}_f \left(\hat{H}\otimes\hat{H})\right)|01\rangle$$
$$= \frac{1}{2}[\hat{U}_f|00\rangle - \hat{U}_f|01\rangle + \hat{U}_f|10\rangle - \hat{U}_f|11\rangle]$$
$$= \frac{1}{2}[|0,0\oplus f(0)\rangle - |0,1\oplus f(0)\rangle + |1,0\oplus f(1)\rangle - |1,1\oplus f(1)\rangle]$$
$$= \frac{1}{2}[|0,f(0)\rangle - \left|0,\tilde{f}(0)\right\rangle + |1,f(1)\rangle - \left|1,\tilde{f}(1)\right\rangle]$$

Now we consider the four cases.

	$f(0)$	$f(1)$
a.	0	0
b	0	1
c	1	0
d	1	1

(a) $f(0) = f(1) = 0$,

$$|\psi_3\rangle = \frac{1}{2}[|0,0\rangle - |0,1\rangle + |1,0\rangle - |1,1\rangle] = |+\rangle\otimes|-\rangle$$

(d) $f(0) = f(1) = 1$

$$|\psi_3\rangle = \frac{1}{2}[|0,1\rangle - |0,0\rangle + |1,1\rangle - |1,0\rangle] = -|+\rangle\otimes|-\rangle$$

(b) $f(0) = 0$, $f(1) = 1$

$$|\psi_3\rangle = \frac{1}{2}[|0,0\rangle - |0,1\rangle + |1,1\rangle - |1,0\rangle] = |-\rangle\otimes|-\rangle$$

(c) $f(0) = 1$, $f(1) = 0$

$$|\psi_3\rangle = \frac{1}{2}[|0,1\rangle - |0,0\rangle + |1,0\rangle - |1,1\rangle] = -|-\rangle\otimes|-\rangle$$

((Fourth stage))

$$|\psi_4\rangle = \frac{1}{2}(\hat{H}\otimes 1)[|0, f(0)\rangle - |0, \tilde{f}(0)\rangle + |1, f(1)\rangle - |1, \tilde{f}(1)\rangle]$$
$$= \frac{1}{2}[|+, f(0)\rangle - |+, \tilde{f}(0)\rangle + |-, f(1)\rangle - |-, \tilde{f}(1)\rangle$$

(a) $f(0) = f(1) = 0$, $f(0) \oplus f(1) = 0$

$$|\psi_4\rangle = \frac{1}{2}[|+,0\rangle - |+,1\rangle + |-,0\rangle - |-,1\rangle] = |0\rangle \otimes |-\rangle$$

(d) $f(0) = f(1) = 1$ $f(0) \oplus f(1) = 0$

$$|\psi_4\rangle == \frac{1}{2}[|+,1\rangle - |+,0\rangle + |-,1\rangle - |-,0\rangle] = -|0\rangle \otimes |-\rangle$$

(b) $f(0) = 0$, $f(1) = 1$, $f(0) \oplus f(1) = 1$

$$|\psi_4\rangle = \frac{1}{2}[|+,0\rangle - |+,1\rangle + |-,0\rangle - |-,1\rangle = |1\rangle \otimes |-\rangle$$

(c) $f(0) = 1$, $f(1) = 0$ $f(0) \oplus f(1) = 1$

$$|\psi_4\rangle = \frac{1}{2}[|+,1\rangle - |+,0\rangle + |-,0\rangle - |-,1\rangle] = -|1\rangle \otimes |-\rangle$$

Finally we get the expression for $|\psi_4\rangle$ as

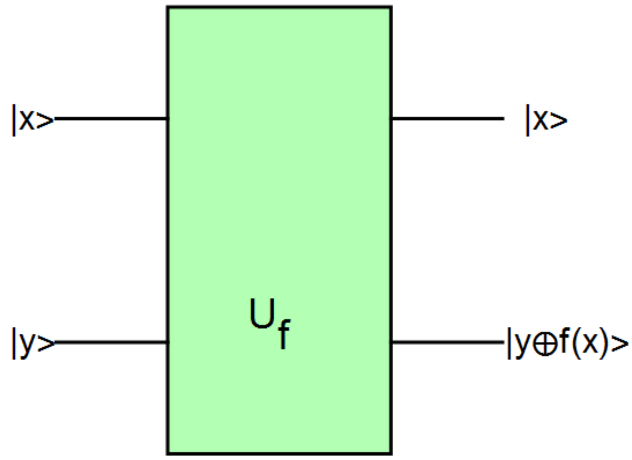
$$|\psi_4\rangle = \pm |f(0) \oplus f(1)\rangle \otimes |-\rangle$$

This expression tells us that by measuring the first output qubit of the quantum circuit, we are able to determine the value of $f(0) \oplus f(1)$ after performing a single evaluation of the function *f*(*x*).

---

39 Deutsch gate (III)
C. Moore and S. Mertens, The Nature of Computation (Oxford University Press, 2011).

We represent $\hat{U}_f$ in a quantum circuit as



If $f(0)=0$ and $f(1)=1$, then $\hat{U}_f$ is an ordinary controlled NOT (CNOT).

Suppose that

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

and

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle),$$

where

$$\hat{X}|+\rangle = |+\rangle, \qquad \hat{X}|-\rangle = -|-\rangle$$

Then we get

$$\begin{aligned}
\hat{U}_f|+\rangle \otimes |0\rangle &= \frac{1}{\sqrt{2}}\hat{U}_f|0\rangle \otimes |0\rangle + \frac{1}{\sqrt{2}}\hat{U}_f|1\rangle \otimes |0\rangle \\
&= \frac{1}{\sqrt{2}}|0\rangle \otimes |0 \oplus f(0)\rangle + \frac{1}{\sqrt{2}}\hat{U}_f|1\rangle \otimes |0 \oplus f(1)\rangle \\
&= \frac{1}{\sqrt{2}}|0\rangle \otimes |f(0)\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes |f(1)\rangle
\end{aligned}$$

With a single query, we create a state that contains information about both $f(0)$ and $f(1)$. It seems that we get two queries for the price of one. However, this state is less useful than one might hope.

In order to improve this situation, we can write the query operator $\hat{U}_f$ as

$$\hat{U}_f|x,y\rangle = \hat{U}_f|x\rangle \otimes |y\rangle = |x\rangle \otimes \hat{X}^{f(x)}|y\rangle$$

Suppose that

$$|y\rangle = |-\rangle .$$

Then we get

$$\hat{U}_f|x,-\rangle = |x\rangle \otimes \hat{X}^{f(x)}|-\rangle = |x\rangle \otimes (-1)^{f(x)}|-\rangle = (-1)^{f(x)}|x,-\rangle$$

When $|x\rangle = |+\rangle$,

$$\begin{aligned}\hat{U}_f|+\rangle \otimes |-\rangle &= \frac{1}{\sqrt{2}}|0\rangle \otimes (-1)^{f(0)}|-\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes (-1)^{f(1)}|-\rangle \\ &= (-1)^{f(0)}\frac{1}{\sqrt{2}}[|0\rangle \otimes |-\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle \otimes |-\rangle] \\ &= (-1)^{f(0)}\frac{1}{\sqrt{2}}[|0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle] \otimes |-\rangle\end{aligned}$$

Her e we note that

$$(-1)^{f(0)\oplus f(1)} = (-1)^{f(1)-f(1)}$$

when $f(0)$ and $f(1)$ are either 0 or 1, since

$f(0)$	$f(1)$	$(-1)^{f(0)\oplus f(1)}$	$(-1)^{f(1)-f(0)}$
0	0	1	1
0	1	-1	-1
1	0	-1	-1
1	1	1	1

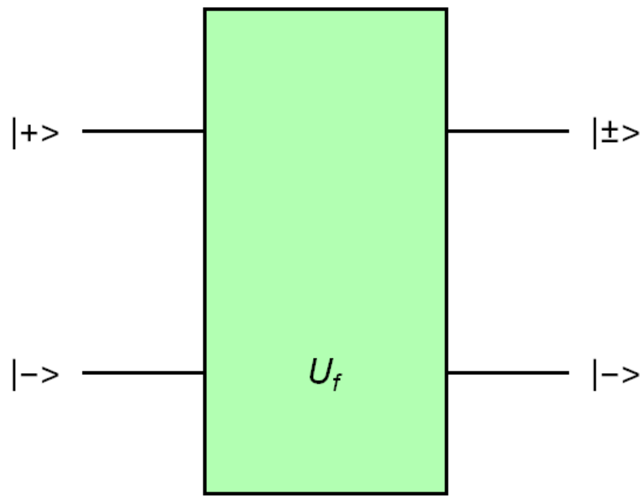
Since we ignore an overall phase, we can factor out $(-1)^{f(0)}$ and write the state of the first quibit as

$$|\psi\rangle = \frac{1}{\sqrt{2}}[|0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle]$$

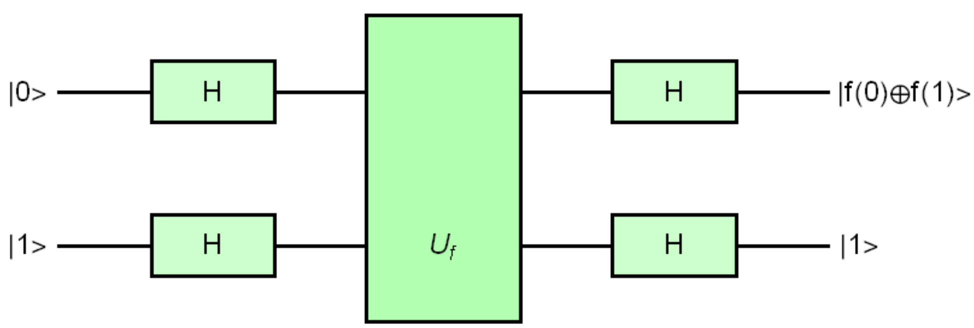
Then we have

$f(0)$	$f(1)$	$f(0) \oplus f(1)$	$\lvert\psi\rangle$
0	0	0	$\lvert+\rangle$
0	1	1	$\lvert-\rangle$
1	0	1	$\lvert-\rangle$
1	1	0	$\lvert+\rangle$

If we measure $\lvert\psi\rangle$ in the X-basis, we can learn the parity $f(0) \oplus f(1)$ without only calling the query operator once.



If we add the Hadamard gates on either side, we have



where

$$\hat{H}\lvert 0\rangle = \lvert+\rangle, \quad \hat{H}\lvert 1\rangle = \lvert-\rangle$$

This algorithm is the first example of a useful trick in quantum computing, called phase kickback.

REFERENCES

R.P. Feynman, Feynman Lectures on Computation (Addison-Wesley, 1996).

G.J. Milburn, The Feynman Processor (Perseus Books, 1998).

G.P. Berman, G.D. Doolen, R. Mainieri, and V.I. Tsifrinovich, Introduction to Quantum Computers (World Scientific, 1998).

J. Stolze and D. Suter, Quantum Computing A Short Course from Theory to Experiment (Wiley-VCH, 2004).

G. Bennet, G. Casati, and G. Strini, Principles of Quantum Computation and Information vol. I: Basic Concepts (World Scientific, 2005).

D.C. Marinescu and G.M. Marinescu, Approaching Quantum Computing (Peason Education, Inc., 2005).

M. Hayashi, Quantum Information An Introduction (Springer, 2006).

M. Pavičić, Quantum Computation and Quantum Communication: Theory and Experiments (Springer 2006).

P. Kaye, R. Laflamme, and M. Mosca, An Introduction to Quantum Computing (Oxford, 2007).

M.L. Bellac, A Short Introduction to Quantum Information (Oxford University Press, 2006).

N.D. Mermin, Quantum Computer Science An Introduction (Cambridge, 2007)

L. Diosi, A Short Course in Quantum Information Theory (Springer, 2007).

G. Bennet, G. Casati, and G. Strini, Principles of Quantum Computation and Information vol. II: Basic Tools and Special Topics (World Scientific, 2007).

G. Jaeger, Quantum Information An Overview (Springer, 2007).

D. McMahon, Quantum Computing Explained (Wiley-Interscience, 2008)

Z. Meglicki, Quantum Computing without Magic Devices (MIT Press, 2008).

N.S. Yanofsky and M.A. Mannucci, Quantum Computing for Computer Scientists (Cambridge, 2008).

S.M. Barnett, Quantum Information (Oxford University Press, 2009).

A.D. Vos Reversible Computing Fundamentals, Quantum Computing, and Applications (Wiley-VCH, 2010).

M.A. Nielsen and I.L. Chuang, Quantum Computation and Quantum Information (Cambridge, 2010).

D.C. Marinescu and G.M. Marinescu, Classical and Quantum Information (Elsevier, 2010).

C. Moore and S. Mertens, The Nature of Computation (Oxford University Press, 2011)

E. Rieffel and W. Polak, Quantum Computing A General Introduction (The MIT Press, 2011).

D.C. Marinescu and G.M. Marinescu, Classical and Quantum Information (Elsevir, 2012).

M. Fayngold and V. Fayngold, Quantum Mechanics and Quantum Information (Wiley-VCH, 2013).
S. Aaronson, Quantum Computing since Democritus (Cambridge University Press, 2013).