Lecture 7

The Quantum Gates are basically represented by operators, ~~t~~ and they must be unitary operators, i.e. $U^{\dagger}U = I$.

Generally, classical computers are not reversible. They could be sometimes made ~~so~~ ~~reves~~ reversible by storing lots of garbage information, which is extremely energy inefficient. A Quantum computer, on the other hand, has to be reversible. In the case of classical computer NOT gate is reversible

$$0 \longrightarrow 1$$
$$1 \longrightarrow 0$$

Because if we know the output, then we automatically know what is the input or vice-versa.

Elementary Quantum Gates

Unitary operations on a single qubit:

Because of unitary operations, each state on the Bloch sphere goes to another point on the Bloch sphere, keeping the length of the vector (i.e. the radius of the sphere) preserved. Geometrically, it corresponds to rigid rotations on the unit sphere. So any point can be transformed to any other point by a sequence of operations which are either rotations or reflections or both.

Operators must be represented by a unitary 2×2 matrix.

P.T.O.

$$|\psi\rangle \xrightarrow{A} |\phi\rangle$$

$$A|\psi\rangle = |\phi\rangle \Rightarrow A\begin{pmatrix}\psi_1\\ \psi_2\end{pmatrix} = \begin{pmatrix}\phi_1\\ \phi_2\end{pmatrix}$$

$$\Rightarrow A \equiv \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

In general, we can write:

$$U = e^{i\alpha} \exp\left[-i\theta\, \hat{n}\cdot\vec{\sigma}/2\right] \quad , \quad \alpha, \theta \in \mathbb{R}$$

Recall from an earlier class:

$$e^{i\theta\, \hat{n}\cdot\vec{\sigma}} = \cos\theta\, I + i\,(\hat{n}\cdot\vec{\sigma})\sin\theta$$

Thus,

$$U = e^{i\alpha}\left[\cos\frac{\theta}{2}\, I - i\,(\hat{n}\cdot\vec{\sigma})\sin\frac{\theta}{2}\right]$$

$$\cancel{= e^{i\alpha}\left[\begin{pmatrix} \cos\frac{\theta}{2} & 0 \\ 0 & \cos\frac{\theta}{2} \end{pmatrix} - i\sin\frac{\theta}{2}\begin{pmatrix} n_z & n_x - i n_y \\ n_x + i n_y & -n_z \end{pmatrix}\right]}$$

$$\cancel{= e^{i\alpha}\left[\left(\cos\frac{\theta}{2} - i\sin\frac{\theta}{2}\, n_z\right.\right.}$$

$$\boxed{\begin{aligned} U &= e^{i\alpha}\cos\frac{\theta}{2}\, I - i\sigma_x n_x e^{i\alpha}\sin\frac{\theta}{2} \\ &\quad - i\sigma_y n_y e^{i\alpha}\sin\frac{\theta}{2} - i\sigma_z n_z e^{i\alpha}\sin\frac{\theta}{2} \\ &= a I + b\sigma_x + c\sigma_y + d\sigma_z \end{aligned}}$$

with

$$a = e^{i\alpha}\cos\frac{\theta}{2}$$

$$b = -ie^{i\alpha} n_x \sin\frac{\theta}{2}$$

$$c = -ie^{i\alpha} n_y \sin\frac{\theta}{2}$$

$$d = -ie^{i\alpha} n_z \sin\frac{\theta}{2}$$

Prove that an arbitrary single qubit unitary operator can be written in the form

$$U = e^{i\alpha} \exp\left[-i\theta \, \hat{n}.\vec{\sigma}/2\right] \quad , \quad \alpha \text{ and } \theta \text{ are real numbers}$$

Proof

Say, $U = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

Let us express it in terms of Pauli matrices and Identity matrix :

$$U = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \alpha_0 I + \beta \sigma_x + \gamma \sigma_y + \delta \sigma_z$$

$$= \begin{pmatrix} \alpha_0 + \delta & \beta - i\gamma \\ \beta + i\gamma & \alpha_0 - \delta \end{pmatrix}$$

$$\Rightarrow \quad a = \alpha_0 + \delta$$
$$b = \beta - i\gamma$$
$$c = \beta + i\gamma$$
$$d = \alpha_0 - \delta$$

$$\Rightarrow \quad \alpha_0 = \frac{a+d}{2}$$
$$\beta = \frac{b+c}{2}$$
$$\gamma = \frac{c-b}{2i}$$
$$\delta = \frac{a-d}{2}$$

Now $U = \alpha_0 I + \beta \sigma_x + \gamma \sigma_y + \delta \sigma_z$ is unitary

if $U^{+} U = I$

$$U^\dagger U = (\alpha_0^* I + \beta^* \sigma_x + \gamma^* \sigma_y + \delta^* \sigma_z)(\alpha_0 I + \beta \sigma_x + \gamma \sigma_y + \delta \sigma_z)$$

$$= (|\alpha_0|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2) I$$
$$+ (\alpha_0^* \beta + \beta^* \alpha_0 + i\gamma^* \delta - i\delta^* \gamma)\sigma_x$$
$$+ (\alpha_0^* \gamma - i\beta^* \delta + \gamma^* \alpha_0 + i\beta\delta^*)\sigma_y$$
$$+ (\alpha_0^* \delta + i\beta^* \gamma - i\beta\gamma^* + \alpha_0 \delta^*)\sigma_z$$

$$\left[\begin{array}{l} \sigma_x^2 = \sigma_y^2 = \sigma_z^2 = I \\ \sigma_x \sigma_y + \sigma_y \sigma_x = 0 \\ \sigma_i \sigma_j + \sigma_j \sigma_i = 0 \\ [\sigma_x, \sigma_y] = i\sigma_z \end{array}\right.$$

\# $U^\dagger U = I$ requires that

$$|\alpha_0|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$$
$$\alpha_0^* \beta + \beta^* \alpha_0 + i\gamma^* \delta - i\delta^* \gamma = 0$$
$$\alpha_0^* \gamma - i\beta^* \delta + \gamma^* \alpha_0 + i\beta\delta^* = 0$$
$$\alpha_0^* \delta + i\beta^* \gamma - i\beta\gamma^* + \alpha_0 \delta^* = 0$$

Now define:

$\cancel{|\alpha|^2}$

$$|\alpha_0| = \cos\frac{\theta}{2}$$

[Please ~~don't confuse with 'α' in the problem~~]

then, $$|\beta|^2 + |\gamma|^2 + |\delta|^2 = \sin^2\frac{\theta}{2}$$

$$n_x = \frac{|\beta|}{\sin\frac{\theta}{2}}, \quad n_y = \frac{|\gamma|}{\sin\frac{\theta}{2}}, \quad n_z = \frac{|\delta|}{\sin\frac{\theta}{2}}$$

$$\Rightarrow \quad n_x^2 + n_y^2 + n_z^2 = 1$$

$\Rightarrow$ $\hat{n}$ is a three dimensional unit vector

Now define: $$e^{i\alpha} = \frac{\alpha_0}{\cos\frac{\theta}{2}}$$

say, the phase of β, γ and δ are α_1, α_2 and α_3 respectively.

Thus,

$$\alpha_0^* \beta + \beta^* \alpha_0 + i\gamma^* \delta - i\delta^* \gamma = 0$$

$$\Rightarrow \cos\frac{\theta}{2} \sin\frac{\theta}{2} n_x e^{i(\alpha_1 - \alpha)} + \cos\frac{\theta}{2} \sin\frac{\theta}{2} n_x e^{-i(\alpha_1 - \alpha)}$$

$$+ i \sin^2\left(\frac{\theta}{2}\right) n_y n_z e^{i(\alpha_3 - \alpha_2)} - i \sin^2\frac{\theta}{2} n_y n_z e^{-i(\alpha_3 - \alpha_2)} = 0$$

$$\Rightarrow 2\cos\frac{\theta}{2} \sin\frac{\theta}{2} \cos(\alpha - \alpha_1) n_x + 2\sin^2\frac{\theta}{2} n_y n_z \sin(\alpha_3 - \alpha_2) = 0$$

$$\Rightarrow \left.\begin{array}{l} \cos(\alpha - \alpha_1) = 0 \\ \sin(\alpha_3 - \alpha_2) = 0 \end{array}\right\} \Rightarrow \boxed{\begin{array}{l} \alpha_1 = \alpha - \frac{\pi}{2} \\ \alpha_2 = \alpha_3 \end{array}}$$

Similarly, we can find

$$\alpha_2 = \alpha_3 = \alpha - \frac{\pi}{2}$$

$$\alpha_1 = \alpha_2 = \alpha_3$$

Therefore,

$$\alpha_0 = e^{i\alpha} \cos\frac{\theta}{2}$$

$$\beta = -i e^{i\alpha} \sin\frac{\theta}{2} n_x$$

$$\gamma = -i e^{i\alpha} \sin\frac{\theta}{2} n_y$$

$$\delta = -i e^{i\alpha} \sin\frac{\theta}{2} n_z$$

$$\beta = |\beta| e^{i\alpha_1}$$

Hence,

$$U = e^{i\alpha} \cos\frac{\theta}{2} I - i e^{i\alpha} \sin\frac{\theta}{2} \left(n_x \sigma_x + n_y \sigma_y + n_z \sigma_z \right)$$

$$= e^{i\alpha} \left[\cos\frac{\theta}{2} I - i \sin\frac{\theta}{2} \hat{n}\cdot\vec{\sigma} \right]$$

$$\boxed{U = e^{i\alpha} \exp\left[-i\theta \frac{\hat{n}\cdot\vec{\sigma}}{2} \right]}$$

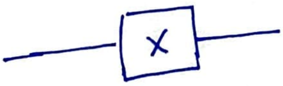
If our input is a single qubit and the output is also a single qubit state, then this operation has to be done by an 2×2 operator corresponding to a 2×2 matrix.

Single qubit Quantum Gates

NOT Gate: $|0\rangle \longrightarrow |1\rangle \; ; \; |1\rangle \longrightarrow |0\rangle$

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

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



PH 441

Quantum computation and Quantum Cryptography

Quantum Gates

NOT : X Gate $-\boxed{X}-$ (pictorial representation)

$$|1\rangle \xrightarrow{X} |0\rangle \qquad\qquad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$
$$|0\rangle \xrightarrow{X} |1\rangle$$

Phase gate : It selectively provides a phase to one of the bits.

Examples

(i) Z-gate

$$|0\rangle \longmapsto |0\rangle$$
$$|1\rangle \longmapsto -|1\rangle$$

The corresponding operator is given by, what is called the Pauli σ_z matrices. That's why it is also called Z-gate.

$$Z : \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad -\boxed{Z}-$$

~~In general~~

$$\boxed{\text{In general, one can represent a phase gate with: } \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix} \quad \text{For Z gate } \phi = \pi}$$

(ii) T-gate

It is also a phase gate.

In this case, $\phi = \frac{\pi}{4}$

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

It is also called as $\frac{\pi}{8}$ gate!

Because :

$$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix} = e^{i\pi/8} \begin{pmatrix} e^{-i\pi/8} & 0 \\ 0 & e^{i\pi/8} \end{pmatrix}$$

Hadamard Gate

Its a very popular gate!

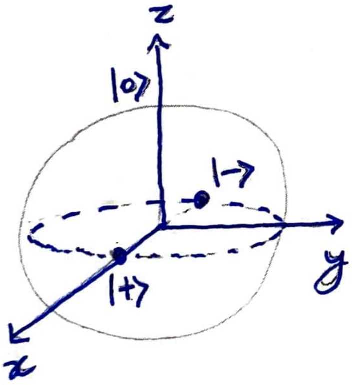
While in classical computing a '0' can go to either '0' or '1' or '1' can go to '0' or '1', in Quantum computing a '0' can go to a linear superposition of '0' and '1', similarly for '1'.

$$|0\rangle \longrightarrow \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

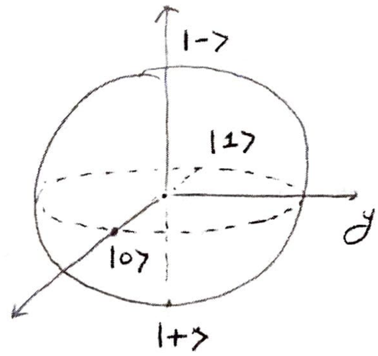
$$|1\rangle \longrightarrow \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

$$U_H = \frac{1}{\sqrt{2}} |0\rangle + |1\rangle \langle 0| + \frac{1}{\sqrt{2}} |0\rangle - |1\rangle \langle 1|$$

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

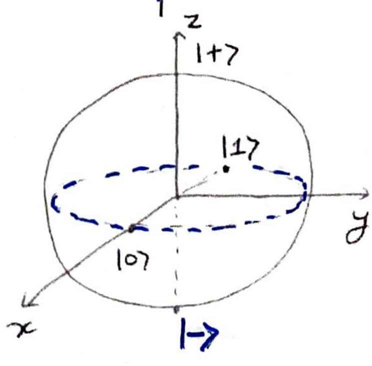


Rotation about y-axis in the counter clockwise direction



Reflection

~~Reflection~~ about x-y plane



Thus,

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

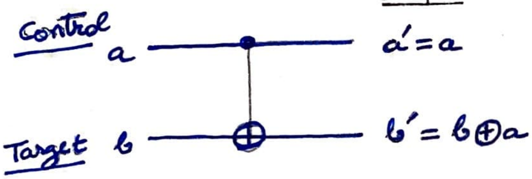
$$|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Geometrical representation of Hadamard gate

Two qubit gates

All quantum gates may be made to arbitrary degree of precision by one and two qubit gates alone.

CNOT gate : Controlled NOT gate is a 2 qubit gate.



Rule

When $a = 0$ nothing happens to b

i.e. if $a = 0$, $b \to b$

But if $a = 1$, then $b \to \bar{b}$

Matrix representation :

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

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

$$|10\rangle \xrightarrow{U_{CNOT}} |11\rangle$$

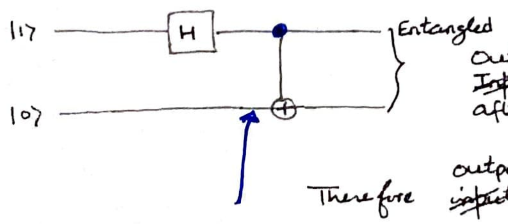
$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \underbrace{\begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}}_{|10\rangle} = \underbrace{\begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}}_{|11\rangle}$$

$$U_{CNOT} = |00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11|$$

$$= |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$$

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

Let us now design a quantum circuit which gives us a Bell state: $\dfrac{|00\rangle - |11\rangle}{\sqrt{2}}$



$$\frac{|0\rangle - |1\rangle}{\sqrt{2}} \otimes |0\rangle = \frac{|00\rangle - |10\rangle}{\sqrt{2}}$$

control bit : $\dfrac{|0\rangle - |1\rangle}{\sqrt{2}}$

Output ~~Input~~ after H : $\dfrac{|0\rangle - |1\rangle}{\sqrt{2}} \otimes |0\rangle = \boxed{\dfrac{|00\rangle - |10\rangle}{\sqrt{2}}}$

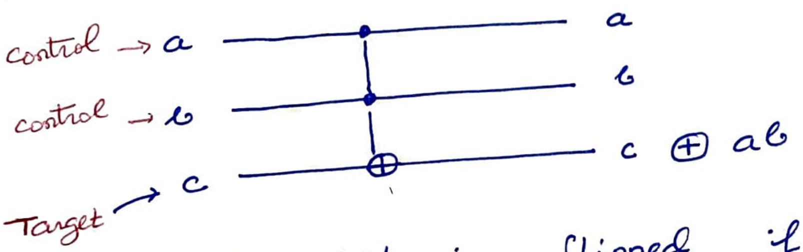
This is an input for CNOT

Therefore output ~~input~~ after CNOT is $\boxed{\dfrac{|00\rangle - |11\rangle}{\sqrt{2}}}$

Output

CCNOT Gate

control control NOT Gate. It is also known as Toffoli Gate. It is a three qubit gate. It has three inputs a, b, c and has double control.



The target bit is flipped if both a and b are equal to 1, i.e. if the product ab = 1, then only c gets flipped.

The matrix representation: $U_{CCNOT} = \left(|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| \right) \otimes I + \left(|11\rangle\langle 11| \right) \otimes X$

$$U_{CCNOT} = \begin{array}{c} \\ 000 \\ 001 \\ 010 \\ 011 \\ 100 \\ 101 \\ 110 \\ 111 \end{array} \begin{array}{c} \begin{array}{cccccccc} 000 & 001 & 010 & 011 & 100 & 101 & 110 & 111 \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \end{array}$$

SWAP Gate

It interchanges two states without entanglement.

$$U_s\,|\psi,\phi\rangle = U_s\left(|\psi\rangle \otimes |\phi\rangle\right) = |\phi,\psi\rangle$$

$$U_s\,|\psi\rangle \otimes |\phi\rangle = |\phi\rangle \otimes |\psi\rangle$$

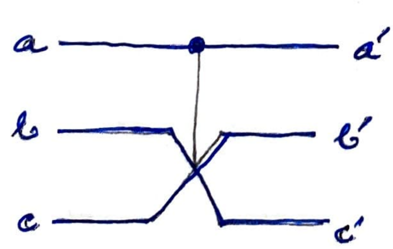
$$U_{SWAP} = U_s = |00\rangle\langle 00| + |01\rangle\langle 10| + |10\rangle\langle 01| + |11\rangle\langle 11|$$

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

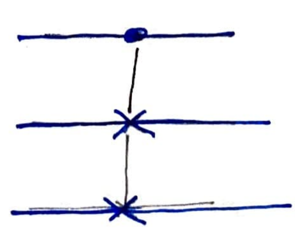
$$U_{SWAP} = \begin{array}{c} \\ 00 \\ 01 \\ 10 \\ 11 \end{array} \begin{array}{c} \begin{array}{cccc} 00 & 01 & 10 & 11 \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \end{array}$$

Note that the SWAP gate is a special gate which maps an arbitrary tensor product state to a tensor product state. In contrast most two-qubit gates map a tensor product state to an entangled state.

Controlled Swap gate (or Fredkin gate)



or



It flips the second (middle) and the third (bottom) qubits when and ~~when~~ only when the first (top) qubit is in the state $|1\rangle$. ~~The~~

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

Fig. Truth Table for Controlled Swap

$$U_{FREDKIN} = \begin{array}{c} \\ 000 \\ 001 \\ 010 \\ 011 \\ 100 \\ 101 \\ 110 \\ 111 \end{array} \begin{array}{c} \begin{array}{cccccccc} 000 & 001 & 010 & 011 & 100 & 101 & 110 & 111 \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \end{array}$$