2.1 Quantum Arithmetic & Gates

① $|a\rangle \otimes |b\rangle \otimes |c\rangle \equiv |abc\rangle \qquad a, b, c \in \{0, 1\}$

E.g. $|0\rangle \otimes |1\rangle \otimes |1\rangle \otimes |0\rangle \equiv |0110\rangle$

② $(\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha'|0\rangle + \beta'|1\rangle)$

$= \alpha\alpha'|00\rangle + \alpha\beta'|01\rangle + \beta\alpha'|10\rangle + \beta\beta'|11\rangle$

E.g. $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |1\rangle$

$= \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|11\rangle$

Note that, sometimes "$\otimes$" may be ignored and you read

$|a\rangle|b\rangle \equiv |ab\rangle$

There is a matrix flavor expression of qubit(s).

$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \ : \quad [\alpha, \beta]$

$|\psi\rangle|\psi'\rangle = (\alpha|0\rangle + \beta|1\rangle)(\alpha'|0\rangle + \beta'|1\rangle) \ : \ [\alpha, \beta] \ [\alpha', \beta']$

$= [\alpha\alpha', \alpha\beta', \beta\alpha', \beta\beta']$

A quantum computer is built on quantum gates, and gates form up circuits. Now, it's time for us to know more gates and their corresponding logics. Let's start from single qubit gates:

① X Gate

$\alpha|0\rangle + \beta|1\rangle \ — \boxed{X} — \ \beta|0\rangle + \alpha|1\rangle$

The logic can be expressed using.

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

$$X \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix}$$

② Z Gate

$$\alpha|0\rangle + \beta|1\rangle \;-\!\!\boxed{Z}\!\!-\; \alpha|0\rangle - \beta|1\rangle$$

$$Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$Z \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \alpha \\ -\beta \end{bmatrix}$$

③ Hadamard Gate

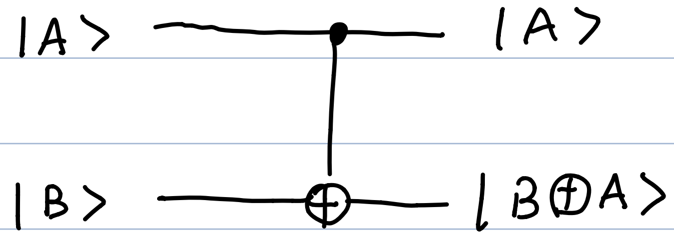
$$\alpha|0\rangle + \beta|1\rangle \;-\!\!\boxed{H}\!\!-\; \frac{\alpha+\beta}{\sqrt{2}}|0\rangle + \frac{\alpha-\beta}{\sqrt{2}}|1\rangle$$

$$H \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

It can be visualize by rotating y axis by 90° in counterclock-wise, and rotate x axis by 180° by counterclockwise. It's a very important and useful gate

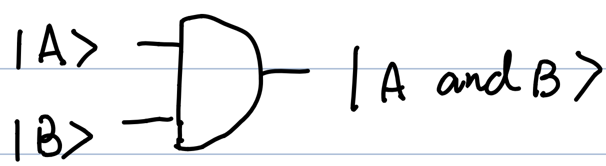
Now, we can talk about multiple qubit gates.

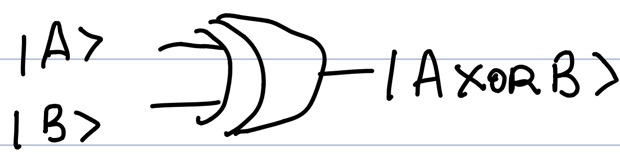
① Controlled - NOT , CNOT

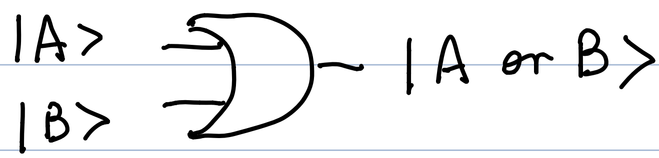


|B⊕A> follows XOR rule
$$\begin{cases} |0\rangle \oplus |0\rangle = |0\rangle \\ |0\rangle \oplus |1\rangle = |1\rangle \\ |1\rangle \oplus |0\rangle = |1\rangle \\ |1\rangle \oplus |1\rangle = |0\rangle \end{cases}$$

② Other Gates

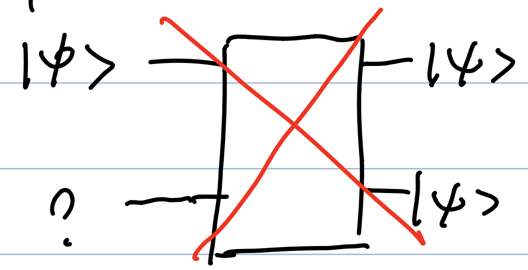






③ More generalized gates will be discussed later.

Here, we will show that qubits are impossible to be cloned (copied). There doesn't exist a circuit s.t.

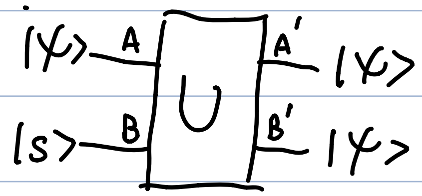


Non-cloning Theorem.

It's impossible to find an unitary operator to copy an unknown quantum state.

Proof:

Suppose there exists a quantum machine with two slots A & B. Slot A is fed with data $|\psi\rangle$, Slot B is fed with some pure state, $|s\rangle$. The output of the machine clones $|\psi\rangle$.



The initial state is. $|\psi\rangle \otimes |s\rangle$ or $|\psi\rangle|s\rangle$

$$|\psi\rangle|s\rangle \xrightarrow{U} |\psi\rangle|\psi\rangle$$

If we find in $|\varphi\rangle$ rather than $|\psi\rangle$ to A. we should have

$$|\varphi\rangle|s\rangle \xrightarrow{U} |\varphi\rangle|\varphi\rangle$$

So

$$U(|\psi\rangle|s\rangle) = |\psi\rangle|\psi\rangle$$

$$U(|\varphi\rangle|s\rangle) = |\varphi\rangle|\varphi\rangle$$

Then

$$(|\psi\rangle|s\rangle)^\dagger \underbrace{U^\dagger U^\dagger}_{=I} |\varphi\rangle|s\rangle = (|\varphi\rangle|\varphi\rangle)^\dagger (|\psi\rangle|\psi\rangle)$$

since it's scalar

$$\hookrightarrow \ |\psi\rangle^\dagger \underbrace{|s\rangle^\dagger |s\rangle}_{I} |\varphi\rangle = (|\psi\rangle^\dagger |\varphi\rangle)^2$$

$$\underbrace{\langle\psi|\varphi\rangle}_{\text{scalar}} = \underbrace{\langle\psi|\varphi\rangle}_{\text{scalar}}^2$$

$$x = x^2 \quad \text{for } x \in \mathbb{R}$$

$$x = 0 \text{ or } 1.$$

So $\psi = \varphi$ or $\psi \perp \varphi$.

So, only when φ & ψ are orthogonal, we can clone the qubit, which means it's not a general clone machine.

Proof end.

2.2. Measurements in bases other than the computational basis

For $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, if we measure it in $(|0\rangle, |1\rangle)$ basis, there will be $|\alpha|^2$ probability of seeing 0 and $|\beta|^2$ of seeing 1. It's also possible that the measurement basis is different from $(|0\rangle, |1\rangle)$.

One very useful and important basis is $|+\rangle \equiv \frac{(|0\rangle + |1\rangle)}{\sqrt{2}}$ and $|-\rangle \equiv \frac{|0\rangle - |1\rangle}{\sqrt{2}}$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \alpha \frac{|+\rangle + |-\rangle}{\sqrt{2}} + \beta \frac{|+\rangle - |-\rangle}{\sqrt{2}}$$

$$= \frac{\alpha+\beta}{\sqrt{2}}|+\rangle + \frac{\alpha-\beta}{\sqrt{2}}|-\rangle$$

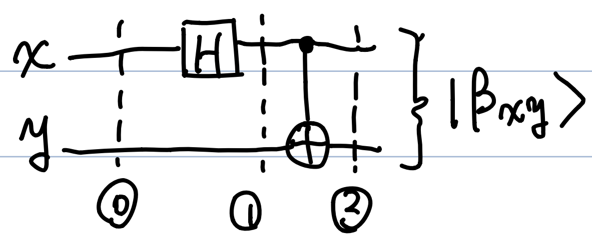
Measurement Circuit

2.3 Quantum Circuit

Quantum Circuit is generated by arranging quantum gates in some order. In 2.1 & 2.2, we cover how to deal with gates, here we only need to repeat what we have learnt several times.

Ex. 1. Bell states generation circuit.

This circuit is used to generate very useful and special states called Bell states.



Suppose inputs $x \otimes y = |00\rangle$

At point 0, the corresponding state $|\psi_0\rangle$ is

$$|\psi_0\rangle = x \otimes y$$
$$= |0\rangle|0\rangle$$

at point 1, since only x is processed by Hadamard gate the state $|\psi_1\rangle$ is

$$|\psi_1\rangle = (Hx) \otimes y$$
$$= (Hx) \otimes |0\rangle \qquad H(|0\rangle) = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$
$$= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle$$
$$= \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$$

at point ②, the state $|\psi_2\rangle$ is

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}\left(\mathrm{CNOT}(|00\rangle) + \mathrm{CNOT}(|10\rangle)\right)$$

$$\mathrm{CNOT}(|00\rangle) = |0\rangle \otimes |0 \oplus 0\rangle = |0\rangle|0\rangle = |00\rangle$$

$$\mathrm{CNOT}(|10\rangle) = |1\rangle \otimes |1 \oplus 0\rangle = |1\rangle|1\rangle = |11\rangle$$

So $|\psi_2\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\beta_{xy}\rangle$

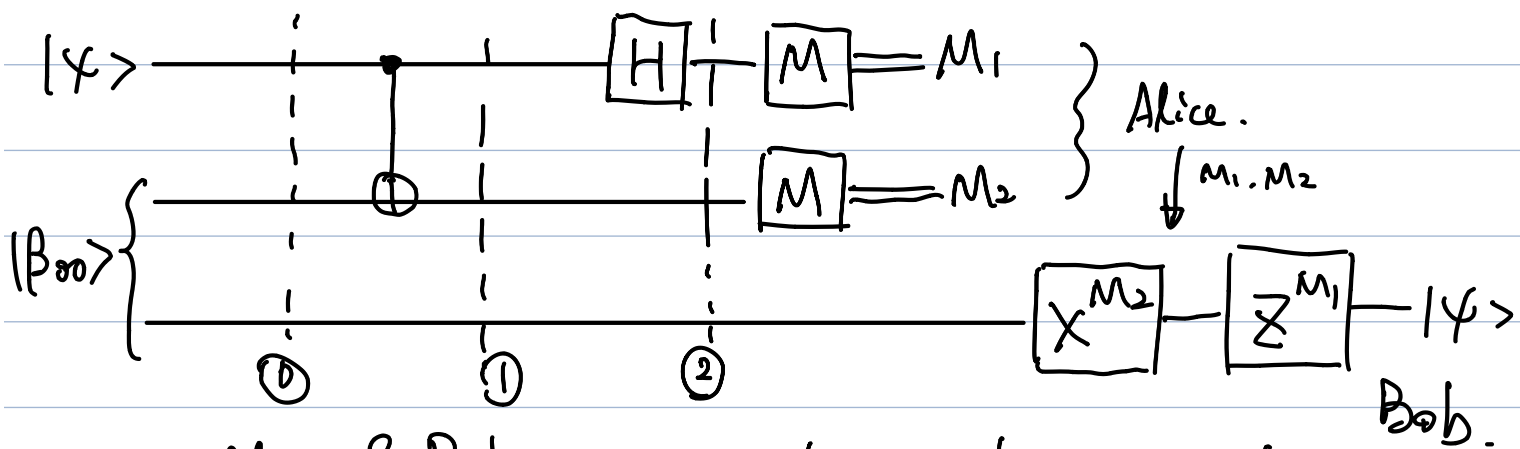
More general. $|\beta_{xy}\rangle = \frac{1}{\sqrt{2}}(|0,y\rangle + (-1)^x |1, \overset{\text{flip}}{\bar{y}}\rangle)$

2.4. Quantum teleportation

Alice & Bob are living in the same place but will separate in the future. Alice wants to deliver a qubit $|\psi\rangle$ to Bob via classic network. How could Alice achieve this?

Amazingly, Alice can send Bob merely two bits of information to let Bob know $|\psi\rangle$. But Alice will no longer have $|\psi\rangle$ because of the Non-cloning Theorem.

The circuit for teleportation is as follows:



When Alice & Bob are together, they use the Bell state generation circuit (in previous section) to generate $|\beta_{00}\rangle$ and each of them hold one qubit.

The first to lines belong to Alice's circuit. When Alice use the circuit to get M_1 & M_2, she sends M_1 & M_2 to Bob. Then Bob use the third line's circuit to reproduce $|\psi\rangle$. Here is the process.

At ⓪, the initial state of $|\psi\rangle$, $|\beta_{00}\rangle$ is

$$|\psi_0\rangle = |\psi\rangle|\beta_{00}\rangle$$
$$= (\alpha|0\rangle + \beta|1\rangle)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Now, we regroup Alice's part and separate out Bob's part

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}(\alpha|0\rangle|00\rangle + \alpha|0\rangle|11\rangle + \beta|100\rangle + \beta|111\rangle)$$
$$= \frac{1}{\sqrt{2}}[\alpha(|00\rangle|0\rangle + |01\rangle|1\rangle) + \beta(|10\rangle|0\rangle + |11\rangle|1\rangle)]$$

at ①,

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}[\alpha\cdot(CNOT(|00\rangle)|0\rangle + CNOT(|01\rangle)|1\rangle)$$
$$+ \beta\cdot(CNOT(|10\rangle)|0\rangle + CNOT(|11\rangle)|1\rangle)]$$
$$= \frac{1}{\sqrt{2}}[\alpha(|0\rangle|0\oplus 0\rangle|0\rangle + |0\rangle|0\oplus 1\rangle|1\rangle)$$
$$+ \beta(|1\rangle|1\oplus 0\rangle|0\rangle + |1\rangle|1\oplus 1\rangle|1\rangle)]$$
$$= \frac{1}{\sqrt{2}}[\alpha|0\rangle(|00\rangle + |11\rangle)$$
$$+ \beta|1\rangle(|10\rangle + |01\rangle)]$$

At ②

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}\Big[\alpha\, H(|0\rangle)\,(|00\rangle + |11\rangle) + \beta\, H(|1\rangle)\,(|10\rangle + |01\rangle)\Big]$$

$$= \frac{1}{\sqrt{2}}\Big[\alpha \cdot \frac{|0\rangle+|1\rangle}{\sqrt{2}}\,(|00\rangle+|11\rangle) + \beta\,\frac{|0\rangle-|1\rangle}{\sqrt{2}}\,(|10\rangle+|01\rangle)\Big]$$

$$= \frac{1}{2}\alpha\big[|000\rangle+|011\rangle+|100\rangle+|111\rangle\big] + \frac{1}{2}\beta\big[|010\rangle+|001\rangle-|110\rangle-|101\rangle\big]$$

rearrange terms

$$|\psi_2\rangle = \frac{1}{2}\Big[|00\rangle(\alpha|0\rangle+\beta|1\rangle) + |01\rangle(\alpha|1\rangle+\beta|0\rangle) + |10\rangle(\alpha|0\rangle-\beta|1\rangle) + |11\rangle(\alpha|1\rangle-\beta|0\rangle)\Big]$$

and.

$$\alpha|0\rangle+\beta|1\rangle \longrightarrow |\psi\rangle$$

$$\alpha|1\rangle+\beta|0\rangle \longrightarrow \boxed{X} \longrightarrow |\psi\rangle$$

$$\alpha|0\rangle-\beta|1\rangle \longrightarrow \boxed{Z} \longrightarrow |\psi\rangle$$

$$\alpha|1\rangle-\beta|0\rangle \longrightarrow \boxed{X} \longrightarrow \boxed{Z} \longrightarrow |\psi\rangle$$

So, Alice only needs to measure her qubits and send the M_1, M_2 to Bob. By doing $X^{M_2} Z^{M_1}$, Bob can regenerate $|\psi\rangle$.