Introduction to Quantum Computing

Sugata Gangopadhyay

Quantum bits or Qubits

- The set $\{0, 1\}$ is a classical bit. If $x \in \{0, 1\}$, we say that x is the state of a classical ***bit***.

- The set $\left\{ \begin{pmatrix} a \\ b \end{pmatrix} : a, b \in \mathbb{C}, |a|^2 + |b|^2 = 1 \right\}$ is a quantum bit, or a ***qubit***.

- Example 1: the space of all possible polarization states of a photon is a single qubit. state

- Example 2: the space of all possible spins of an electron is said to be a qubit.

- ✓ Superposition – quantum state → qubits
- ✓ Entanglement – of $\boxed{\text{qubit}}$

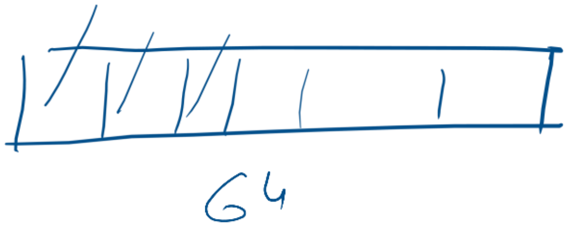
A Single

☐ bit is a system that can exist in two states.

- 0 'zero' state
- 1 'one' state

What can we do with bits?

- × Read
- × Write
- × Store → without and error for a very time.



- On a quantum computer there are issues with
  - × reading · × storing

- Bit → Binary Digits $\boxed{0, 1}$ → Quantum Bits

A quantum bit is a quantum mechanical system that exist in infinite number of states. A single qubit state can be specified by a pair of complex number a, b. $\begin{pmatrix} a \\ b \end{pmatrix}$ where $|a|^2 + |b|^2 = 1$

$\begin{pmatrix} a \\ b \end{pmatrix}$ $|a|^2+|b|^2=1$

Unit of information:

The single qubit state space

$\mathbb{C}$

ket zero

$\boxed{|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}}$

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

$|\psi\rangle = a|0\rangle + b|1\rangle$

$$|\psi\rangle = \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ b \end{pmatrix} = a\begin{pmatrix} 1 \\ 0 \end{pmatrix} + b\begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$\begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$, $\begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$

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

$\boxed{\begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle}$ $\mathbb{C}$

ket one

$|a|^2+|b|^2=1$

$|\psi\rangle$

ket psi.

$a = a_0 + i a_1$ $|a|^2 = a_0^2 + a_1^2$

$b = b_0 + i b_1$ $|b|^2 = b_0^2 + b_1^2$.

Vector spaces over $\mathbb{C}$ and qubits

- A single-qubit state space is a two-dimensional vector space over the field of complex numbers $\mathbb{C}$.
- We represent it as

$$\boxed{\mathbb{C}^2 = \left\{ \begin{pmatrix} a \\ b \end{pmatrix} : a, b \in \mathbb{C}, \boxed{|a|^2 + |b|^2 = 1} \right\}}$$

- The computational basis is

$$\boxed{|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}}, \boxed{|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}}$$

- A qubit state is written as

$$|\psi\rangle = a|0\rangle + b|1\rangle$$

We can write → and single-qubit state as a linear combinatn of $|0\rangle$ (ket 0) and $|1\rangle$ (ket 1)

$\left\{ \begin{pmatrix} a \\ b \end{pmatrix} : a, b \in \mathbb{C} \quad |a|^2 + |b|^2 = 1 \right\}$

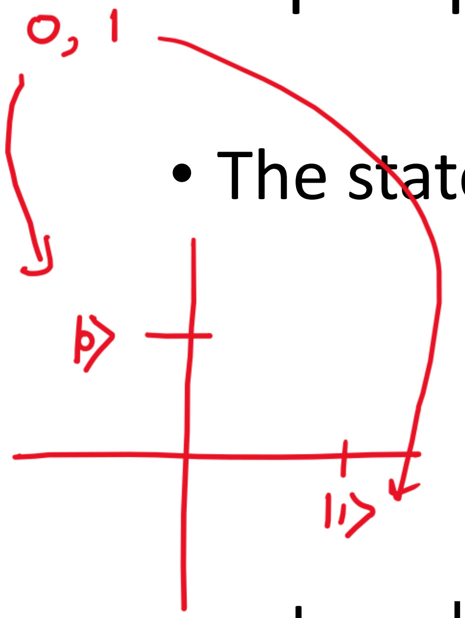
- It is possible to ~~a~~ single qubit to a particular single qubit state.] Write ✓
- Reading a qubit ✗ – Measurement

~~Storing a qubit~~ ✗

Quantum memory

Superposition of states

What is a superposition of states?
If I am construction a single qubit state by taking a (linear) combination of



- The state of a single-qubit is of the form

$$\boxed{|\psi\rangle = \begin{pmatrix} a \\ b \end{pmatrix} = a\begin{pmatrix} 1 \\ 0 \end{pmatrix} + b\begin{pmatrix} 0 \\ 1 \end{pmatrix} = a|0\rangle + b|1\rangle}$$

$|0\rangle$, $|1\rangle$, and $|\psi\rangle = a|0\rangle + b|1\rangle$ when $a \neq 0$, $b \neq 0$, Then

where $|a|^2 + |b|^2 = 1$.

$|\psi\rangle$ is called a SUPERPOSITION of the states $|0\rangle$ and $|1\rangle$

- If $a \neq 0$ and $b \neq 0$ the qubit is said to be in the superposition of two states $|0\rangle$ and $|1\rangle$.

$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ $|\psi\rangle = a|0\rangle + b|1\rangle$

The pair $\{|0\rangle, |1\rangle\}$ is called a basis of the single-qubit state space.

This is a very important basis, so much so that it has special name. It is called the COMPUTATIONAL BASIS.

Hadamard Basis

We have a qubit state $|\psi\rangle$ written in the computational basis.

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

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

$$|\psi\rangle = a|0\rangle + b|1\rangle$$

$$|\psi\rangle = c\,\underbrace{|+\rangle} + d\,\underbrace{|-\rangle}$$

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

$$= \frac{c+d}{\sqrt{2}}|0\rangle + \frac{c-d}{\sqrt{2}}|1\rangle = a|0\rangle + b|1\rangle$$

$$\frac{c+d}{\sqrt{2}} = a, \quad \frac{c-d}{\sqrt{2}} = b$$

$$c+d = a\sqrt{2} \qquad c-d = b\sqrt{2}$$

$$2c = (a+b)\sqrt{2} \qquad 2d = (a-b)\sqrt{2}$$

$$c = \frac{a+b}{\sqrt{2}} \qquad d = \frac{a-b}{\sqrt{2}}$$

$$|\psi\rangle = \frac{a+b}{\sqrt{2}}|+\rangle + \frac{a-b}{\sqrt{2}}|-\rangle$$

Suppose there is a quantum state $|\psi\rangle$ which is in superposition with respect to the computational basis.

Is it in superposition with all other basis?

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

With respect to the Hadamard basis $|\psi\rangle$ is just $|+\rangle$. So it is not in superposition.

Once a superposition, always a superposition?

NO

- $|\psi\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ is a superposition of two states $|0\rangle$, and $|1\rangle$.
- We say that $|\psi\rangle$ is in superposition with respect to the basis $\{|0\rangle, |1\rangle\}$.
- However, the representation of $|\psi\rangle$ with respect to the basis $\mathcal{H} = \{|+\rangle, |-\rangle\}$ is $|\psi\rangle = |+\rangle$.
- Therefore, $|\psi\rangle$ is not in superposition with respect to the basis $\mathcal{H}$.

Changing a Qubit representation from computational to Hadamard basis

- $|\psi\rangle = a|0\rangle + b|1\rangle$ is a single-qubit state written in computational basis.
- The Hadamard basis vectors in terms of computational basis vectors are:

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \qquad |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

- Solving for $|0\rangle$ and $|1\rangle$ yields:

$$|0\rangle = \frac{|+\rangle + |-\rangle}{\sqrt{2}}, \qquad |1\rangle = \frac{|+\rangle - |-\rangle}{\sqrt{2}}.$$

- $|\psi\rangle = a\left(\frac{|+\rangle+|-\rangle}{\sqrt{2}}\right) + b\left(\frac{|+\rangle-|-\rangle}{\sqrt{2}}\right) = \frac{a+b}{\sqrt{2}}\ |+\rangle + \frac{a-b}{\sqrt{2}}\ |-\rangle.$

Global phase versus relative phase

- Two single-qubit states $|\psi\rangle = a|0\rangle + b|1\rangle$ and $|\phi\rangle = c|0\rangle + d|1\rangle$ are said to differ by the global phase θ if

$$|\psi\rangle = a|0\rangle + b|1\rangle = e^{\mathbf{i}\theta}(c|0\rangle + d|1\rangle) = e^{\mathbf{i}\theta}\,|\phi\rangle.$$

- If two quantum states differ by a global phase, they are considered to be same. We write $|\psi\rangle \sim |\phi\rangle$.

- The relative phase of a single-qubit state $|\psi\rangle = a|0\rangle + b|1\rangle$ is a number φ which satisfies the equation

$$\frac{a}{b} = e^{\mathbf{i}\varphi}\,\frac{|a|}{|b|}.$$

- Two quantum states with different relative phases are not the same quantum state.

Examples of qubits differing by a global phase

- Consider: $\frac{1}{\sqrt{2}}\left(|0\rangle + e^{\frac{\mathbf{i}\pi}{4}}|1\rangle\right)$ and $\frac{1}{\sqrt{2}}\left(e^{-\frac{\mathbf{i}\pi}{4}}|0\rangle + |1\rangle\right)$

- The qubit state $\frac{1}{\sqrt{2}}\left(e^{-\frac{\mathbf{i}\pi}{4}}|0\rangle + |1\rangle\right) = \frac{e^{-\frac{\mathbf{i}\pi}{4}}}{\sqrt{2}}\left(|0\rangle + e^{\frac{\mathbf{i}\pi}{4}}|1\rangle\right)$

- Therefore, these two quantum states are the same.

Examples of qubits differing by relative phases

- Consider: $\frac{1}{\sqrt{2}}(\,|0\rangle + |1\rangle)$ and $\frac{1}{\sqrt{2}}(-|0\rangle + \mathbf{i}|1\rangle)$

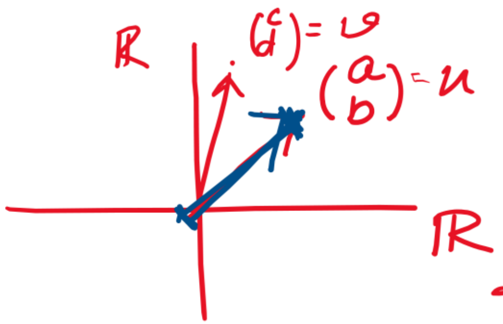
- Let $$a|0\rangle + b|1\rangle = \frac{1}{\sqrt{2}}(\,|0\rangle + |1\rangle)$$

  and $$a'|0\rangle + b'|1\rangle = \frac{1}{\sqrt{2}}(-|0\rangle + \mathbf{i}|1\rangle).$$

  $\frac{a}{b} = \frac{1}{\sqrt{2}}\frac{\sqrt{2}}{1} = e^{0\mathbf{i}}\frac{|a|}{|b|}$, and $\frac{a'}{b'} = -\frac{1}{\sqrt{2}}\frac{\sqrt{2}}{\mathbf{i}} = -\frac{1}{\mathbf{i}} = \mathbf{i} = e^{\frac{\pi\mathbf{i}}{2}}\frac{|a'|}{|b'|}$.

  By definition the relative phase of the first qubit is 0 and the relative phase of the second qubit is $\frac{\pi}{2}$. Since they have different relative phases they are different quantum states.

Complex Inner Product



$u \cdot v$
$= ac + bc$.

$\begin{pmatrix} a \\ b \end{pmatrix}^T \begin{pmatrix} c \\ d \end{pmatrix} = (a \; b) \begin{pmatrix} c \\ d \end{pmatrix}$
$= ac + bd$.

- Let V be an n-dimensional $\mathbb{C}$-vector space.
- Let $|a\rangle = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}$ and $|b\rangle = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$
- $\langle a|b\rangle = (\bar{a}_1, \bar{a}_2, \dots, \bar{a}_n) \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = \sum_{i\in[n]} \bar{a}_i b_i$

$\mathbb{R}^n = \left\{ \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \vec{a} : a_i \in \mathbb{R} \right\}$

$\bar{a}, \bar{b} \in \mathbb{R}^n$

$\bar{a} \cdot \bar{b} = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}^T \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$

$= (a_1 \cdots a_n) \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$

$= a_1 b_1 + \cdots + a_n b_n$

$\underline{ac + bd = 0}$

$\|u\|^2 = u \cdot u = a^2 + b^2$

$\|u\| = \sqrt{a^2 + b^2}$

Dot product in Complex vector space $\rightarrow$ Inner product.

$$\mathbb{C}^n = \left\{ \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} : a_i \in \mathbb{C} \right\}$$

$$\bar{a} = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$$

$$\bar{b} = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$$

$$\bar{a} \cdot b = (a_1 \cdots a_n) \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$$

$$= a_1 b_1 + \cdots + a_n b_n .$$

$1+i$

$-1-i$

$$\bar{a} \cdot \bar{a} = \sum_{i=1}^{n} a_i^2$$

$a_i \in \mathbb{C}$

$a_i^2 \in \mathbb{C}$

$\bar{a} \cdot \bar{a}$

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

$$x^{\dagger} = (\bar{x}_1, \bar{x}_2, \dots, \bar{x}_n)$$

$$\mathbb{C}^n = \left\{ x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} : x_i \in \mathbb{C} \right\}$$

$$\boxed{\begin{aligned} a &= a_0 + i a_1 \\ \bar{a} &= a_0 - i a_1 \end{aligned}}$$

$$\langle x, y \rangle = x^{\dagger} y = (\bar{x}_1, \dots, \bar{x}_n) \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

$$= \bar{x}_1 y_1 + \cdots + \bar{x}_n y_n .$$

$$\langle x, x \rangle = (\bar{x}_1 \cdots, \bar{x}_n) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \bar{x}_1 x_1 + \cdots + \bar{x}_n x_n =$$

$$= |x_1|^2 + \cdots + |x_n|^2 .$$

ket a

$$|a\rangle = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$$

bra a

$$\langle a| = (\bar{a}_1 \cdots\cdots \bar{a}_n)$$

$$= \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}^{+}$$

$$\underbrace{\langle a| \ |b\rangle}$$

$$\downarrow \langle a|b\rangle$$

$$\underbrace{\langle a|b\rangle}$$

$$= (\bar{a}_1, \bar{a}_2, \cdots, \bar{a}_n) \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$$

$$= \bar{a}_1 \cdot b_1 + \cdots + \bar{a}_n b_n = \sum_{i=1}^{n} \bar{a}_i b_i$$

bra 'a' ket 'b'

$$\underbrace{\qquad}$$

bra(c)ket a, b

$$\langle a|a\rangle = (\bar{a}_1, \dots, \bar{a}_n)\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \sum_{i=1}^{n} \bar{a}_i a_i$$

$$= \sum_{i=1}^{n} |a_i|^2$$

$$a_i = x + iy \qquad i^2 = -1$$

$$\bar{a}_i = x - iy$$

$$\bar{a}_i \cdot a_i = (x+iy)(x-iy) = x^2 - \cancel{ixy} + \cancel{ixy} - i^2 y^2$$

$$= x^2 + y^2 = |a_i|^2.$$

Measuring a qubit

Measurement of a Single-Qubit System

How do we "read" a qubit state??

- Any measurement of a quantum system is associated to an orthonormal basis of its state space.
- Two orthonormal bases of $\mathbb{C}^2$ are

× Orthonormal Basis

$$\mathcal{B} = \{|0\rangle, |1\rangle\}$$
$$\mathcal{H} = \{|+\rangle, |-\rangle\} = \left\{\frac{|0\rangle + |1\rangle}{\sqrt{2}}, \frac{|0\rangle - |1\rangle}{\sqrt{2}}\right\}$$

- $\mathcal{B}_1$ is said to be the computational basis, $\mathcal{B}_2$ is said to be the Hadamard basis of $\mathbb{C}^2$.

- Any measurent corresponds to an orthonormal basis.

  $\downarrow$ of a quantum state $\downarrow$ single qubit state

  $\downarrow$ of the state space $\downarrow$ single qubit state

-

$$|\psi\rangle = a|0\rangle + b|1\rangle$$

$\mathbb{C}^2$ $\{|0\rangle, |1\rangle\}$ — $\mathcal{B}_0$

$\{|+\rangle, |-\rangle\} = \mathcal{H}$

If I measure $|\psi\rangle$ by the measurement basis $\{|0\rangle, |1\rangle\}$

the measurement outcome is

$|0\rangle$ with probability $|\langle 0|\psi\rangle|^2$ and

$|1\rangle$ with probability $|\langle 1|\psi\rangle|^2$.

Racap

Qubit → a qubit is the fundamental unit of quantum informatn. just as a bit is the fundamental unit of classical infmtn.

$\begin{pmatrix} a \\ b \end{pmatrix}$, $a, b \in \mathbb{C}$. $|a|^2 + |b|^2 = 1$ ✓ $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

$|\psi\rangle = a|0\rangle + b|1\rangle$

$\mathbb{C} \times \mathbb{C} = \mathbb{C}^2$ → Basis of $\mathbb{C}^2$. $\{|0\rangle, |1\rangle\}$, $\{|+\rangle, |-\rangle\}$ ✓

Orthonormality A basis $\{|\psi_1\rangle, |\psi_2\rangle\}$ is said to be orthonormal if

$\langle\psi_1|\psi_1\rangle = 1$, $\langle\psi_2|\psi_2\rangle = 1$

$\langle\psi_1|\psi_2\rangle = 0$, $\langle\psi_2|\psi_1\rangle = 0$

1. Computational basis $\{|0\rangle, |1\rangle\}$ $\longrightarrow$ orthonormal

$$\langle 0|0\rangle = (1\ 0)\begin{pmatrix}1\\0\end{pmatrix} = 1 \qquad \langle 1|1\rangle = (0\ 1)\begin{pmatrix}0\\1\end{pmatrix} = 1$$

$$|0\rangle = \begin{pmatrix}1\\0\end{pmatrix} \qquad \langle 0|1\rangle = (1\ 0)\begin{pmatrix}0\\1\end{pmatrix} = 0+0 = 0$$

$$\langle 0| = (1\ 0)$$

2. Hadamard basis $|+\rangle = \dfrac{|0\rangle + |1\rangle}{\sqrt{2}}$ $\quad |-\rangle = \dfrac{|0\rangle - |1\rangle}{\sqrt{2}}$

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

$$= \frac{1}{2}\left(\langle 0|0\rangle + \langle 0|1\rangle + \langle 1|0\rangle + \langle 1|1\rangle\right) = \frac{\langle 0|0\rangle + \langle 1|1\rangle}{2}$$

$$= \frac{2}{2} = 1$$

Similarly $\langle -|-\rangle = 1$

$$\langle + | - \rangle = \frac{\langle 0| + \langle 1|}{\sqrt{2}} \times \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{1}{2}\left(\langle 0| + \langle 1|\right)\left(|0\rangle - |1\rangle\right)$$

$$= \frac{1}{2}\left(\langle 0|0\rangle - \underbrace{\langle 0|1\rangle}_{0} + \underbrace{\langle 1|0\rangle}_{0} - \langle 1|1\rangle \right)$$

$$= \frac{1}{2}\left(\langle 0|0\rangle - \langle 1|1\rangle \right) = \frac{1}{2}(1-1) = 0$$

$$\langle - | + \rangle = 0$$

We have proved that the Hadamard basis $\{|+\rangle, |-\rangle\}$ is also an orthonormal basis.

Measurement

Any measurement process/device corresponds to a (specific) orthonormal basis.

Suppose $\{|\psi_1\rangle, |\psi_2\rangle\}$ be an orthonormal basis corresponding to the measurement M.

If we measure the quantum state $|\psi\rangle$ by M, the output is

$|\psi_1\rangle$ with probability $|\langle\psi_1|\psi\rangle|^2$ and

$|\psi_2\rangle$ with probability $|\langle\psi_2|\psi\rangle|^2$.

Single qubit measurement

- A single-qubit measurement, M is associated to an orthonormal basis

$$\{|\Phi_1\rangle, |\Phi_2\rangle\}$$

- Measuring $|\Psi\rangle = a|0\rangle + b|1\rangle$ by M outputs either $|\Phi_1\rangle$ or $|\Phi_2\rangle$.
- The probability of outcome $|\Phi_1\rangle$ is $|\langle\Phi_1|\Psi\rangle|^2$
- The probability of outcome $|\Phi_2\rangle$ is $|\langle\Phi_2|\Psi\rangle|^2$

Example 1

- Consider the single-qubit state $|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + \mathbf{i}|1\rangle)$ and the measurement basis $\{|0\rangle, |1\rangle\}$.

- The measurement outcome is $|0\rangle$ with probability
$$|\langle 0|\Psi\rangle|^2 = \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}$$

- The measurement outcome is $|1\rangle$ with probability
$$|\langle 1|\Psi\rangle|^2 = \left|\mathbf{i}\,\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}$$

Calculations

- $\langle 0|\Psi\rangle = \langle 0|\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}\mathbf{i}|1\rangle\right) = \frac{1}{\sqrt{2}}\langle 0|0\rangle + \frac{1}{\sqrt{2}}\mathbf{i}\langle 0|1\rangle = \frac{1}{\sqrt{2}}.$

- $\langle 0|\Psi\rangle = \langle 1|\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}\mathbf{i}|1\rangle\right) = \frac{1}{\sqrt{2}}\langle 1|0\rangle + \frac{1}{\sqrt{2}}\mathbf{i}\langle 1|1\rangle = \frac{1}{\sqrt{2}}\mathbf{i}.$

Example 2

- Consider the single-qubit state $|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + \mathbf{i}|1\rangle)$ and the measurement basis $\{|+\rangle, |-\rangle\}$.

- The measurement outcome is $|+\rangle$ with probability
$$|\langle + | \Psi\rangle|^2 = \left|\frac{1}{2}(1+\mathbf{i})\right|^2 = \frac{1}{2}.$$

- The measurement outcome is $|-\rangle$ with probability
$$|\langle - | \Psi\rangle|^2 = \left|\frac{1}{2}(1-\mathbf{i})\right|^2 = \frac{1}{2}.$$

Calculations

- $\langle +|\Psi\rangle = \left(\frac{1}{\sqrt{2}}(\langle 0| + \langle 1|)\right)\left(\frac{1}{\sqrt{2}}(|0\rangle + \mathbf{i}|1\rangle)\right) = \frac{1}{2}(1 + \mathbf{i})$.
- $\langle -|\Psi\rangle = \left(\frac{1}{\sqrt{2}}(\langle 0| - \langle 1|)\right)\left(\frac{1}{\sqrt{2}}(|0\rangle + \mathbf{i}|1\rangle)\right) = \frac{1}{2}(1 - \mathbf{i})$.
- $|\langle +|\Psi\rangle|^2 = \left|\frac{1}{2}(1 + \mathbf{i})\right|^2 = \frac{1}{2}$.
- $|\langle -|\Psi\rangle|^2 = \left|\frac{1}{2}(1 - \mathbf{i})\right|^2 = \frac{1}{2}$.

Outer product

- Let $|\psi\rangle$ and $|\Phi\rangle$ be two vector.
- $|\psi\rangle = a|0\rangle + b|1\rangle$ and $|\Phi\rangle = c|0\rangle + d|1\rangle$.

- The outer product of $|\psi\rangle$ and $|\Phi\rangle$ is

$$|\Psi\rangle\langle\Phi| = \binom{a}{b}\binom{c}{d}^{\dagger} = \binom{a}{b}(\bar{c} \quad \bar{d})$$

$$= \begin{pmatrix} a\bar{c} & a\bar{d} \\ b\bar{c} & b\bar{d} \end{pmatrix}$$

Transforming single qubit state

$$|\psi\rangle = a|0\rangle + b|1\rangle$$

$$\downarrow$$

$$\begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{C}^2$$

$$|a|^2 + |b|^2 = 1$$

probability amplitude

$$\begin{pmatrix} a \\ b \end{pmatrix} \longrightarrow \begin{pmatrix} b \\ a \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} b \\ a \end{pmatrix} \checkmark$$

Can I write this entire process (transformation) using the bra-ket notation?

$$|0\rangle\langle 0| = \underset{2\times 1}{\begin{pmatrix} 1 \\ 0 \end{pmatrix}} \begin{pmatrix} 1 & 0 \end{pmatrix}_{1\times 2} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}_{2\times 2}$$

$$|0\rangle\langle 1| = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}_{2\times 2}$$

$$|1\rangle\langle 0| = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}_{2\times 2}$$

$$|1\rangle\langle 1| = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}_{2\times 2}$$

$|0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ $|0\rangle\langle 1| = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ $|1\rangle\langle 0| = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ $|1\rangle\langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$.

$$\begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix} = a_{00}|0\rangle\langle 0| + a_{01}|0\rangle\langle 1| + a_{10}|1\rangle\langle 0| + a_{11}|1\rangle\langle 1|$$

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = |0\rangle\langle 1| + |1\rangle\langle 0|$$

$|\psi\rangle = a|0\rangle + b|1\rangle$

$|a|^2 + |b|^2 = 1$

$$X|\psi\rangle = (|0\rangle\langle 1| + |1\rangle\langle 0|)(a|0\rangle + b|1\rangle)$$

$$= a|0\rangle\underbrace{\langle 1|0\rangle}_{0} + b|0\rangle\underbrace{\langle 1|1\rangle}_{1} + a|1\rangle\underbrace{\langle 0|0\rangle}_{1} + b|1\rangle\underbrace{\langle 0|1\rangle}_{0}$$

$$= b|0\rangle + a|1\rangle$$

$$\boxed{\begin{aligned} X|0\rangle &= |1\rangle \\ X|1\rangle &= |0\rangle \end{aligned}}$$

NOT

$$\begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix} = a_{00}|0\rangle\langle 0| + a_{01}|0\rangle\langle 1| + a_{10}|1\rangle\langle 0| + a_{11}|1\rangle\langle 1|$$

Only unitary transformations can be implemented on a quantum computer.

$$\begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix}^{-1} = \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix}^{\dagger}$$

conjugate transpose.

$$H|1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|\right)|1\rangle$$

$$= \frac{1}{\sqrt{2}}\left(|0\rangle\underbrace{\langle 0|1\rangle}_{0} + |0\rangle\underbrace{\langle 1|1\rangle}_{1} + |1\rangle\underbrace{\langle 0|1\rangle}_{0} - |1\rangle\underbrace{\langle 1|1\rangle}_{1}\right)$$

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

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

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

Quantum state transformations

- Quantum computers have the capability of transforming one quantum state to another by applying unitary transformations on the former.

- A linear transformation T is said to be unitary if

$$T\,T^{\dagger} = I$$

where I is the identity operator.

The Pauli Transformations

- I : $|0\rangle\langle 0| + |1\rangle\langle 1| = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \end{pmatrix}$
$$= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

- X : $|1\rangle\langle 0| + |0\rangle\langle 1| = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \end{pmatrix}$
$$= \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

The Pauli Transformations

$Y|0\rangle = |1\rangle$
$Y|1\rangle = -|0\rangle$

- $Y: \; -|1\rangle\langle 0| + |0\rangle\langle 1| = -\begin{pmatrix} 0 \\ 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \end{pmatrix}$
$$= -\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

- $Z: \; |0\rangle\langle 0| - |1\rangle\langle 1| = \begin{pmatrix} 1 \\ 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \end{pmatrix} - \begin{pmatrix} 0 \\ 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \end{pmatrix}$
$$= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$Z|0\rangle = |0\rangle$
$Z|1\rangle = -|1\rangle$

Action of the Pauli Transformations

- I = identity transformation
- X = negation, it is similar to the classical not operation
- Z = changing the relative phase of a superposition in the standard basis.
- $Y = ZX$.

The Hadamard Transformation

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

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

$X|0\rangle = |1\rangle$. $X|1\rangle = |0\rangle$

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

$= \frac{1}{\sqrt{2}}\Big(|0\rangle \underbrace{\langle 0|0\rangle}_{1} + |1\rangle\underbrace{\langle 0|0\rangle}_{1} + |0\rangle\underbrace{\langle 1|0\rangle}_{0} - |1\rangle\underbrace{\langle 1|0\rangle}_{0}\Big)$

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

Qubit Quantum binary digit $\longleftrightarrow$ Bit Binary digit

$\begin{pmatrix} a \\ b \end{pmatrix}$ $\quad |a|^2 + |b|^2 = 1$

$0 \quad 1$

$|\psi\rangle = a|0\rangle + b|1\rangle$

$\boxed{q_1}$ — Write

Store

Read

Bra|ket $\quad |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

What is a Basis?

What is an orthonormal basis?

inner product

complex inner product

Measurement $\longleftrightarrow$ Each measurement (process) is associated to an orthonormal basis.

Measure and using the measurement result we can get (some) idea of quantum state

$|\psi\rangle = a|0\rangle + b|1\rangle.$ $\quad a, b \in \mathbb{C}$ $\quad \boxed{|a|^2 + |b|^2 = 1}$

$= \underbrace{r_1 e^{i\theta_1}}|0\rangle + r_2 e^{i\theta_2}|1\rangle$

$a = a_0 + i a_1 = r_1 e^{i\theta_1}$

$= r_1(\cos\theta_1 + i \sin\theta_1)$

$= r_1 \cos\theta_1 + i r_1 \sin\theta_1$

$|a|^2 + |b|^2$

$= r_1^2 \underbrace{|e^{i\theta_1}|}^2 + r_2^2 \underbrace{|e^{i\theta_2}|}^2$

$= \underline{r_1^2 + r_2^2} = 1$

$b = b_0 + i b_1 = r_2 \cos\theta_2 + i r_2 \sin\theta_2$

$= r_2 e^{i\theta_2}$

$$|\psi\rangle = r_1 e^{i\theta_1}|0\rangle + r_2 e^{i\theta_2}|1\rangle$$

$r_1^2 + r_2^2 = 1$

r_1 and r_2 are real numbers

$$= e^{i\theta_1}\underline{\left(r_1|0\rangle + r_2 e^{i(\theta_2-\theta_1)}|1\rangle\right)}$$

$\theta_2 - \theta_1 = \theta$

uniquely identified the quantum state vector

$$|\psi\rangle = e^{i\theta_1}\left(\underline{r_1|0\rangle + r_2 e^{i\theta}|1\rangle}\right)$$

$\underline{r_1, r_2, \theta}$

$\underline{r_1^2 + r_2^2 = 1}$

$$|\psi\rangle = r_1|0\rangle + r_2 e^{i\theta}|1\rangle$$

$$\boxed{= \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}} e^{i\theta}|1\rangle}$$

$0 < \theta < 2\pi$

$\boxed{010 \ldots 01} \rightarrow \underline{(0, 2\pi)}$

$X = |0\rangle\langle 1| + |1\rangle\langle 0| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ $Y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

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

ERiettel W. Polak

$$H|0\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + |1\rangle \right).$$

2x2   2x1   2x1

$$H|0\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1| \right) |0\rangle$$

$$= \frac{1}{\sqrt{2}} \left(|0\rangle \underbrace{\langle 0|0\rangle}_{1} + |0\rangle \underbrace{\langle 1|0\rangle}_{0} + |1\rangle \underbrace{\langle 0|0\rangle}_{1} - |1\rangle \underbrace{\langle 1|0\rangle}_{0} \right)$$

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

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

$$= |-\rangle .$$

Two qubit states

$|\Phi_1\rangle = a|0\rangle + b|1\rangle$ $\quad |a|^2 + |b|^2 = 1$

$|\Phi_2\rangle = c|0\rangle + d|1\rangle$ $\quad |c|^2 + |d|^2 = 1$

- Consider two qubits

$$|\Phi_1\rangle = a\,|0\rangle + b\,|1\rangle$$

and

$$|\Phi_2\rangle = c\,|0\rangle + d\,|1\rangle$$

If these two qubits exist side by side, then we have a two-qubit state

$$(|\Phi_1\rangle, |\Phi_2\rangle) = (a\,|0\rangle + b\,|1\rangle, \quad c\,|0\rangle + d\,|1\rangle)$$

$$|\Phi_1\rangle = a|0\rangle + b|1\rangle$$

$$|\Phi_2\rangle = c|0\rangle + d|1\rangle$$

$$(|\Phi_1\rangle, |\Phi_2\rangle)$$

$$= (a|0\rangle + b|1\rangle, \; c|0\rangle + d|1\rangle)$$

$$\{|0\rangle, |1\rangle\} \qquad \{|0\rangle, |1\rangle\}$$

$$|0\rangle|0\rangle, \quad |0\rangle|1\rangle, \quad |1\rangle|0\rangle, \quad |1\rangle|1\rangle$$

$$|a|^2|c|^2 \qquad |a|^2|d|^2 \qquad |b|^2|c|^2 \qquad |b|^2|d|^2$$

$$= |ac|^2 \qquad = |ad|^2 \qquad = |bc|^2 \qquad = |bd|^2$$

$$|ac|^2 + |ad|^2 + |bc|^2 + |bd|^2$$

$$= |a|^2(|c|^2 + |d|^2) + |b|^2(|c|^2 + |d|^2)$$

$$= |a|^2 + |b|^2 = 1$$

$$|0\rangle|0\rangle \qquad |0\rangle|1\rangle \qquad |1\rangle|0\rangle \qquad |1\rangle|1\rangle$$

$$|\psi\rangle$$

$$= ac|0\rangle|0\rangle + ad|0\rangle|1\rangle$$

$$+ bc|1\rangle|0\rangle + bd|1\rangle|1\rangle$$

$$\begin{pmatrix} a \\ b \end{pmatrix} \quad \begin{pmatrix} c \\ d \end{pmatrix} \qquad \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix}$$

Kronecker product

$$\begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} a\begin{pmatrix} c \\ d \end{pmatrix} \\ b\begin{pmatrix} c \\ d \end{pmatrix} \end{pmatrix} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix}$$

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

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

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

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

$$|0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad |0\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad |1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad |1\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

$$|\psi\rangle = (a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle)$$

$$= \begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix}$$

$$= \begin{pmatrix} a\begin{pmatrix} c \\ d \end{pmatrix} \\ b\begin{pmatrix} c \\ d \end{pmatrix} \end{pmatrix} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix} = ac\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + ad\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + bc\begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + bd\begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

$$= ac\,|0\rangle \otimes |0\rangle + ad\,|0\rangle \otimes |1\rangle + bc\,|1\rangle \otimes |0\rangle + bd\,|1\rangle \otimes |1\rangle$$

$$= ac\,|0\rangle|0\rangle + ad\,|0\rangle|1\rangle + bc\,|1\rangle|0\rangle + bd\,|1\rangle|1\rangle$$

$$= ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle$$

$|00\rangle = |0\rangle \otimes |0\rangle$ $\quad |01\rangle = |0\rangle \otimes |1\rangle$ $\quad |10\rangle = |1\rangle \otimes |0\rangle.$ $\quad |11\rangle = |1\rangle \otimes |1\rangle$

$$|\psi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle$$

$$|a_{00}|^2 + |a_{01}|^2 + |a_{10}|^2 + |a_{11}|^2 = 1$$

Yes

No

$$|\psi\rangle = (a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle)$$

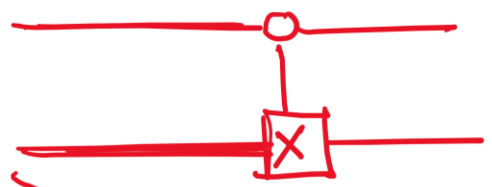
How to construct a two qubit state which cannot be written as a Kronecker product (tensor product) of $\underbrace{\text{two single qubit states}}$?

Single-qubit transformations (Gate) X, Y, Z, H.

Two-qubit gate

Controlled not gate $\to X$

$|0\rangle, |1\rangle$



$|0\rangle, |1\rangle$

$$X(a|0\rangle + b|1\rangle)$$
$$= aX|0\rangle + bX|1\rangle = a|1\rangle + b|0\rangle$$

$|\psi\rangle$ — $\boxed{T}$ — $T|\psi\rangle$

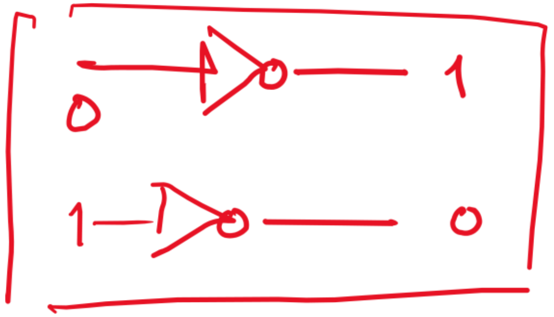
$|\psi\rangle$ — $\boxed{X}$ — $X|\psi\rangle$

$$|\psi\rangle = a|0\rangle + b|1\rangle$$

$a|0\rangle + b|1\rangle$ — $\boxed{X}$ — $b|0\rangle + a|1\rangle$

$\parallel$ $\qquad$ $\qquad$ $X|\psi\rangle$

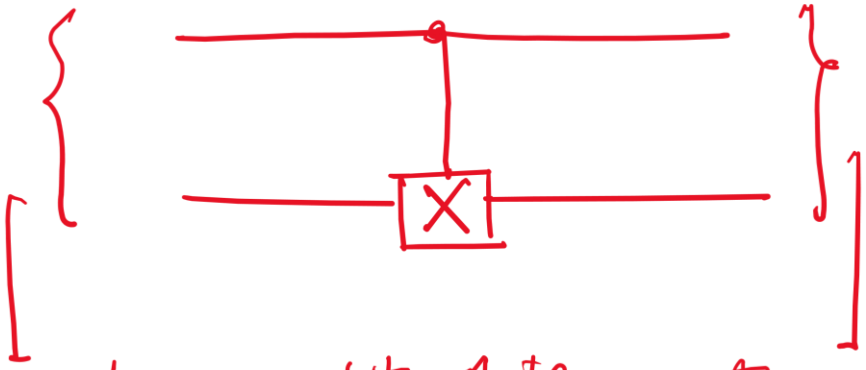
$|\psi\rangle$



$|0\rangle$ — $\boxed{X}$ — $|1\rangle$

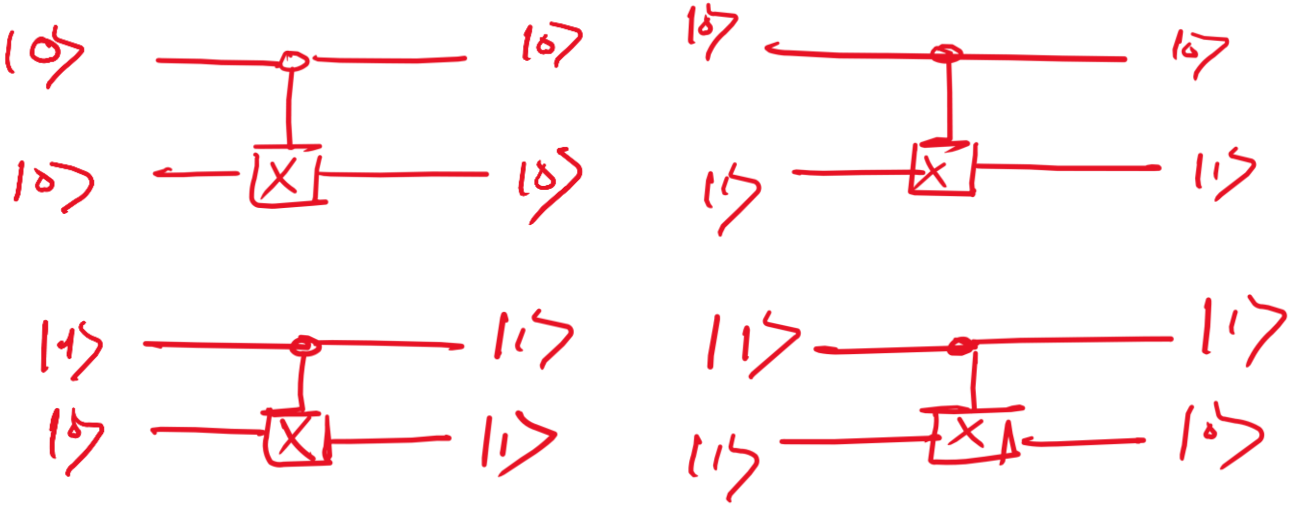
$|1\rangle$ — $\boxed{X}$ — $|0\rangle$

Controlled not gate (X)



a two-qubit state

a two qubit state



The computational basis of the two-qubit state space

$$\mathcal{B} = \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$$

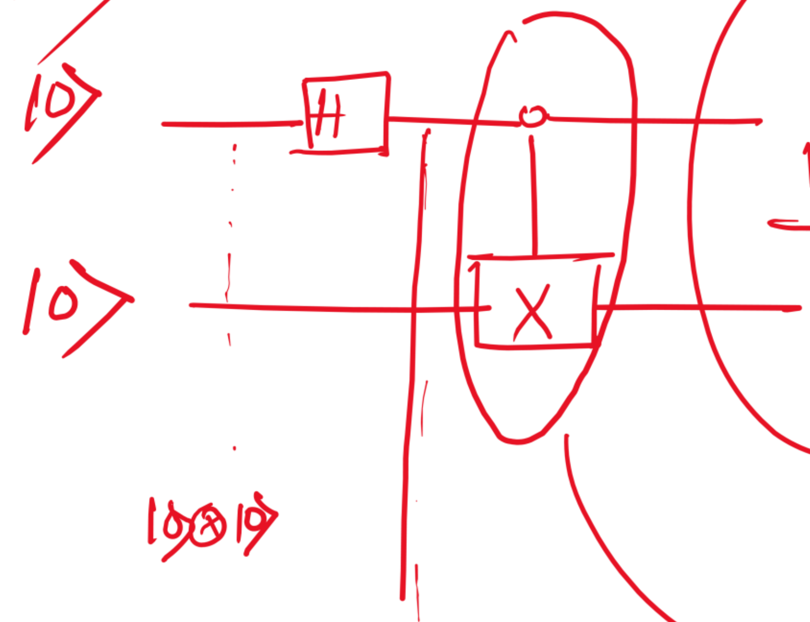
$$= \{|0\rangle\otimes|0\rangle, |0\rangle|1\rangle, |1\rangle\otimes|0\rangle, |1\rangle\otimes|1\rangle\}$$

Cnot:

$$|00\rangle \mapsto |00\rangle$$
$$|01\rangle \mapsto |01\rangle$$
$$|10\rangle \mapsto |11\rangle$$
$$|11\rangle \mapsto |10\rangle$$

$$C_{not} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$|00\rangle$



$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

Entangled state

$|0\rangle \otimes |0\rangle \longrightarrow |0\rangle \otimes |0\rangle = |00\rangle$

$|1\rangle \otimes |0\rangle \longrightarrow |1\rangle \otimes |1\rangle = |11\rangle$

$|0\rangle \otimes |0\rangle$

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

Cnot

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

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

Cnot

$$\frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle$$

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

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} = (a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle)$$

$$= ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle$$

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle = ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle$$

$ac = \frac{1}{\sqrt{2}}$ $\quad$ $ad = 0$ $\quad$ $bc = 0$ $\quad$ $bd = \frac{1}{\sqrt{2}}$

$a = 0$ or $d = 0$

but $a \neq 0$

$d = 0$

$0 = \frac{1}{\sqrt{2}}$

$$|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

$|0\rangle$

880

200

1080

$$00 \longmapsto 0$$
$$01 \longmapsto 1$$
$$10 \longmapsto 2$$
$$11 \longmapsto 3$$

* Multiple-qubit states

- Single-qubit states
- Two-qubit states
- Multi-qubit states ......

$$\{|0\rangle\otimes|0\rangle,\ |0\rangle\otimes|1\rangle,\ |1\rangle\otimes|0\rangle,\ |1\rangle\otimes|1\rangle\}$$

$$= \{|0\rangle|0\rangle, |0\rangle|1\rangle, |1\rangle|0\rangle, |1\rangle|1\rangle\} = \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$$

$$= \{|0\rangle_2, |1\rangle_2, |2\rangle_2, |3\rangle_2\}$$

3-qubit system $n=3$ $\quad 0, -2^3-1$ $\quad 0 - 7$

State space has the basis

$$\{|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle\}$$

$$= \{|0\rangle, |1\rangle, |2\rangle, |3\rangle, |4\rangle, |5\rangle, |6\rangle, |7\rangle\}$$

$$(a|0\rangle + b|1\rangle)\otimes(c|0\rangle + d|1\rangle)\otimes(e|0\rangle + f|1\rangle)$$

$$= \underbrace{\begin{pmatrix}a\\b\end{pmatrix}\otimes\begin{pmatrix}c\\d\end{pmatrix}}\otimes\begin{pmatrix}e\\f\end{pmatrix}$$

$$= \begin{pmatrix}ac\\ad\\bc\\bd\end{pmatrix}\otimes\begin{pmatrix}e\\f\end{pmatrix} = \underbrace{\begin{pmatrix}ace\\acf\\ade\\adf\\bce\\bcf\\bde\\bdf\end{pmatrix}}_{8\times 1} = ace|000\rangle + acf|001\rangle$$
$$+ ade|010\rangle + adf|011\rangle$$
$$+ bce|100\rangle + bcf|101\rangle$$
$$+ bde|110\rangle + bdf|111\rangle \checkmark$$

n-qubit state

$$|0\rangle_n = |\underbrace{0 \cdots 0}\rangle$$

$$|1\rangle_n = |0 0 \overset{n}{\cdots} 1\rangle$$

An n-qubit quantum state $|\psi\rangle$ has form

$$|\psi\rangle = a_0|0\rangle + a_1|1\rangle + a_2|2\rangle + \cdots + a_{2^n-1}|2^n-1\rangle$$

$$= \sum_{i=0}^{2^n-1} a_i |i\rangle \qquad a_i \in \mathbb{C}$$

$$\sum_{i=0}^{2^n-1} |a_i|^2 = 1 \qquad |a_0|^2 + |a_1|^2 + |a_2|^2 + \cdots + |a_{2^n-1}|^2 = 1$$

* The quantum gates are linear transformation ✓

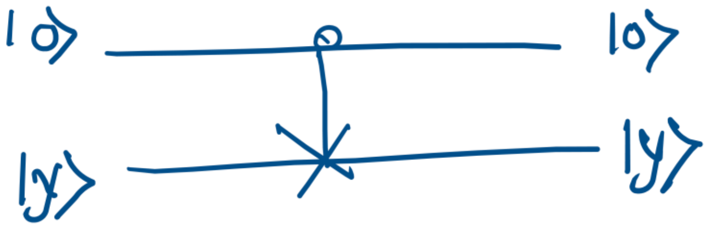
Cnot gate

$|00\rangle \longmapsto |00\rangle$

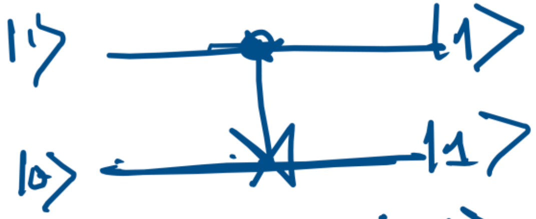
$|01\rangle \longmapsto |01\rangle$

$|10\rangle \longmapsto |11\rangle$

$|11\rangle \longmapsto |10\rangle$

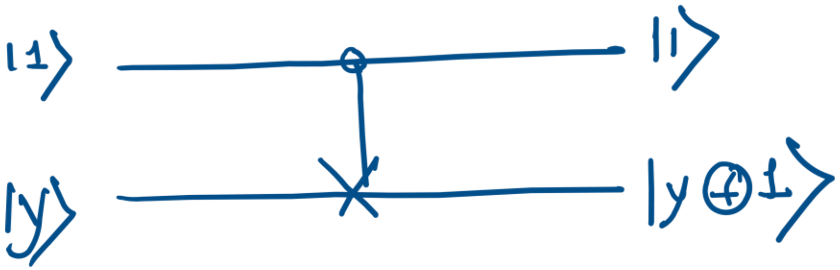


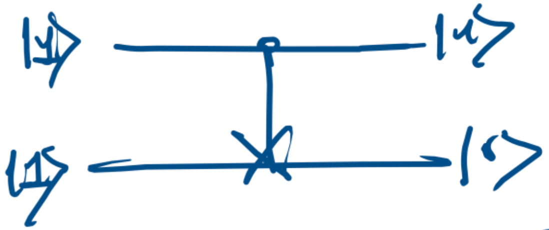
Cnot



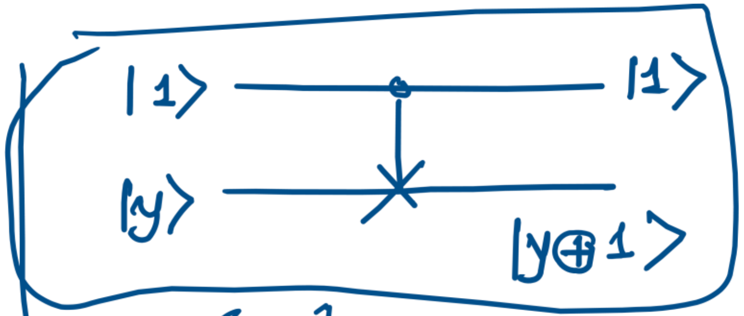
$|10\rangle \longmapsto |11\rangle$

$y \in \{0,1\}$





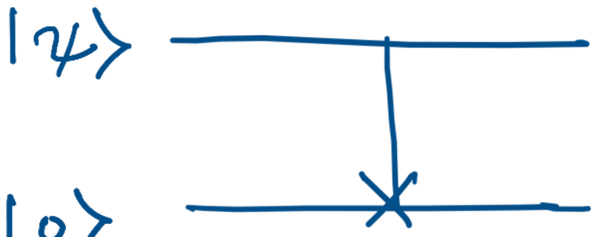
$|11\rangle \longmapsto |10\rangle$



$y \in \{0,1\}$

$\oplus$	0	1
0	0	1
1	1	0

$$|\psi\rangle = \underline{a|0\rangle + b|1\rangle}$$



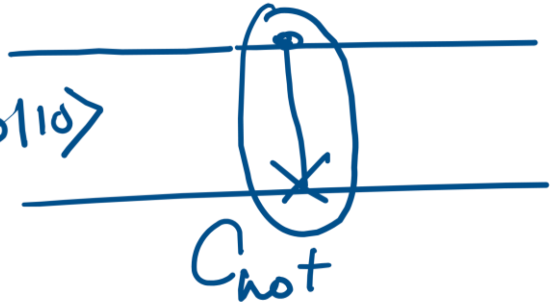
$$|\psi\rangle \otimes |0\rangle$$

$$= (a|0\rangle + b|1\rangle) \otimes |0\rangle$$

$$= a|0\rangle \otimes |0\rangle + b|1\rangle \otimes |0\rangle$$

$$= \underline{a|00\rangle + b|10\rangle}$$

$$a|00\rangle + b|10\rangle$$

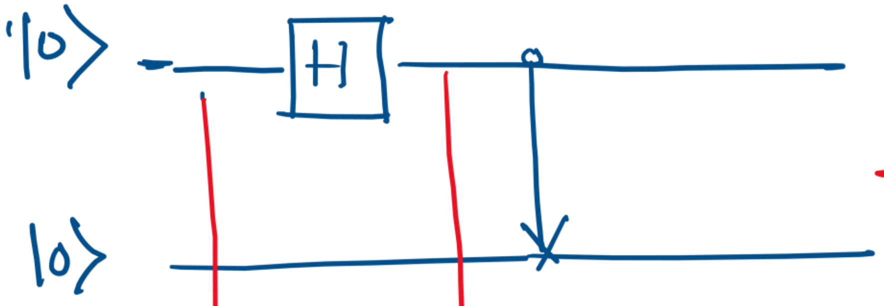


$$C_{not}(a|00\rangle + b|10\rangle)$$

$$= a\,\boxed{C_{not}|00\rangle} + b\,\boxed{C_{not}|10\rangle}$$

$$= \underline{a|00\rangle + b|11\rangle}$$

$|0\rangle \otimes |0\rangle = \underline{|00\rangle}$



$$\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

Entangled state
(a Bell state)

$\boxed{(H\otimes I)\,|00\rangle}$ $\qquad \frac{1}{\sqrt{2}}\left(|00\rangle + |10\rangle\right)$

$$H|0\rangle \otimes |0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)\otimes |0\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |10\rangle\right)$$

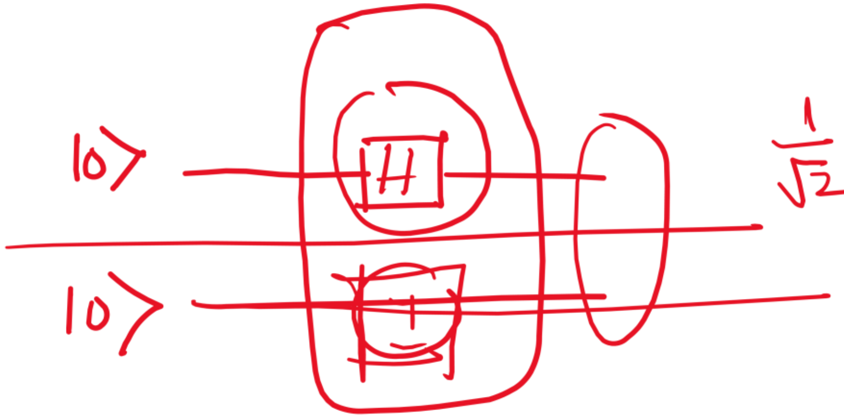
$H \otimes I$

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

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

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

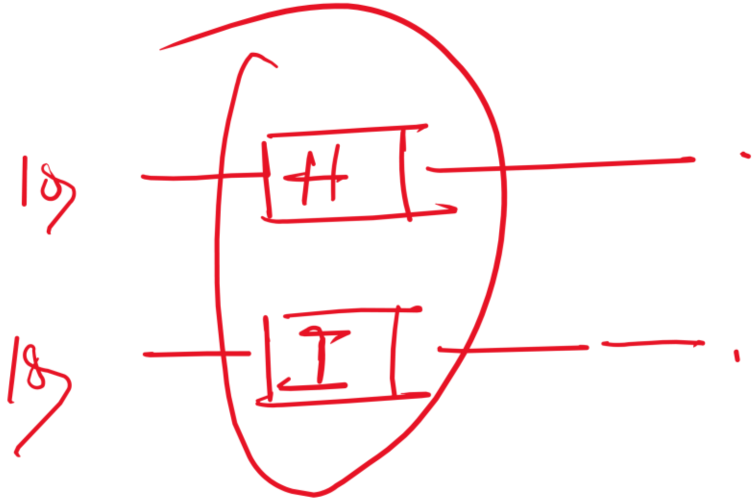
$$= \frac{1}{\sqrt{2}}\begin{pmatrix}1\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} & 1\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\\ 1\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} & -1\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 0 & 1 & 0\\ 0 & 1 & 0 & 1\\ 1 & 0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



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

$|0\rangle$

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



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

$|0\rangle|0\rangle \longmapsto \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|10\rangle$

$|0\rangle|1\rangle \longmapsto \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|1\rangle = \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|11\rangle$

$|1\rangle|0\rangle \longrightarrow \frac{1}{2}(|0\rangle - |1\rangle)|0\rangle = \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|10\rangle$

$|1\rangle|1\rangle \longrightarrow \frac{1}{2}(|0\rangle - |1\rangle)|1\rangle \quad \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|11\rangle$

$x_i \in \{0,1\}$

$$\begin{array}{ccccccc} |x_1\rangle & \otimes & |x_2\rangle & \otimes \cdots \otimes & |x_n\rangle \\ \downarrow T_1 & & \downarrow T_2 & & \downarrow T_n \end{array}$$

$$\downarrow$$

$$T_1|x_1\rangle \otimes T_2|x_2\rangle \otimes \cdots \otimes T_n|x_n\rangle$$

$$\|$$

$$\underline{(T_1 \otimes T_2 \otimes \cdots \otimes T_n)}\, |x_1\rangle \otimes \cdots |x_n\rangle$$

$$= (T_1 \otimes T_2 \otimes \cdots \otimes T_n)\, |x_1 \cdots x_n\rangle$$

- We would like to see a quantum algorithm

1970s. 1980s

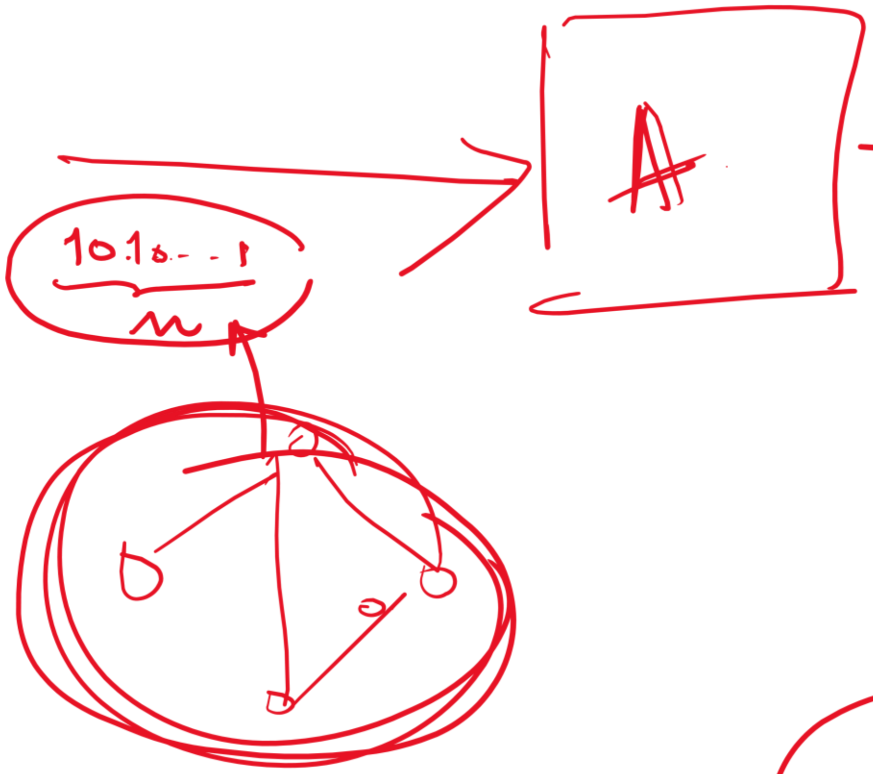
Boolean function.

An n-variable Boolean function is a function from the set $\{0,1\}^n = \{x_1 \cdots x_n : x_i \in \{0,1\}\}$ all binary string of length n

to $\{0,1\}$. Let $f : \{0,1\}^n \to \{0,1\}$ be a Boolean function

Whether a graph is "Hamiltonian" or not?

$$A : \{0,1\}^* \longrightarrow \{0,1\}$$



$\longrightarrow$ 0/1

1 means that the input graph is Hamiltonian.

0 means that the input graph is not Hamiltonian

$$A : \{0,1\}^n \longrightarrow \{0,1\}$$

1-variable Boolean function.

x	f_0	f_1	f_2	f_3
0	0	0	1	1
1	0	1	0	1

$\{0,1\}^n \rightarrow \{0,1\}$

How to represent a Boolean function on a quantum computer?

$000\ldots0 \quad f(\cdot) \qquad 00\ldots01 \quad f(\cdot\cdot) \qquad \ldots \qquad 11\ldots1$

$|00\ldots0\rangle \qquad |00\ldots01\rangle \qquad \ldots \qquad |11\ldots1\rangle$

$|0\rangle_n \qquad |1\rangle_n \qquad \ldots \qquad |2^n-1\rangle_n$

$0 \longmapsto |0\rangle$

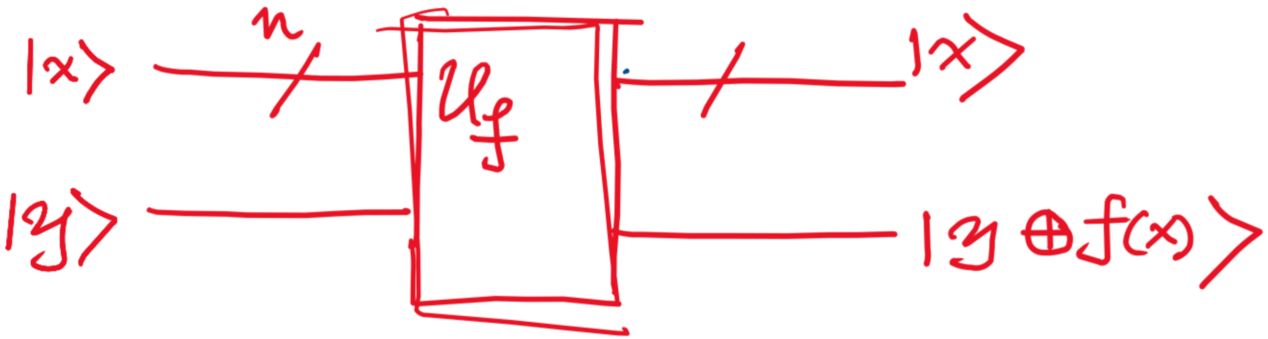
$1 \longmapsto |1\rangle$

→ Quantum Implementations of Boolean function.

✓ Bit-oracle implementation

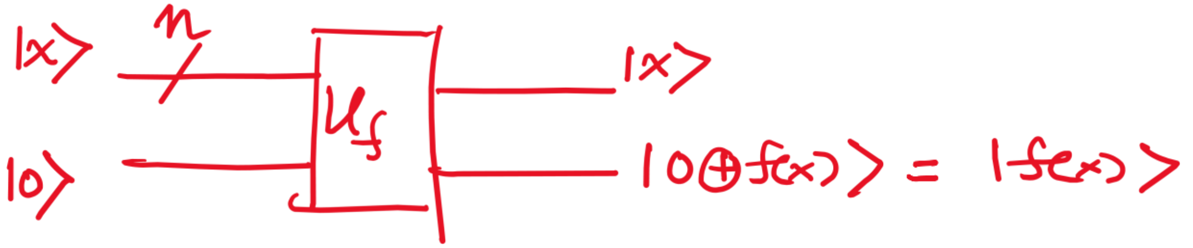
$|x\rangle = |x_1 \ldots x_n\rangle \quad x_i \in \{0,1\}$

$|y\rangle \in \{|0\rangle, |1\rangle\}$

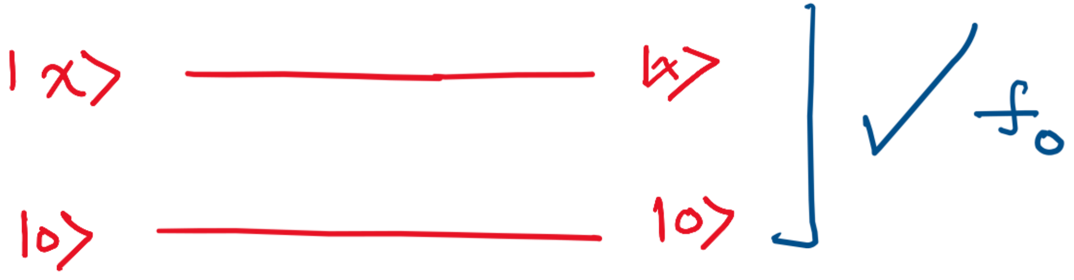


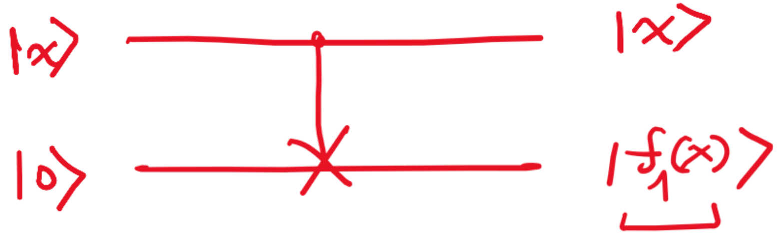
⟼ This transformation is a unitary transformation.

How to implement a single variable Boolean function on a Quantum Computer?



x	f_0 ✓	f_1 ✓	f_2	f_3
0	0	0	1	1
1	0	1	0	1

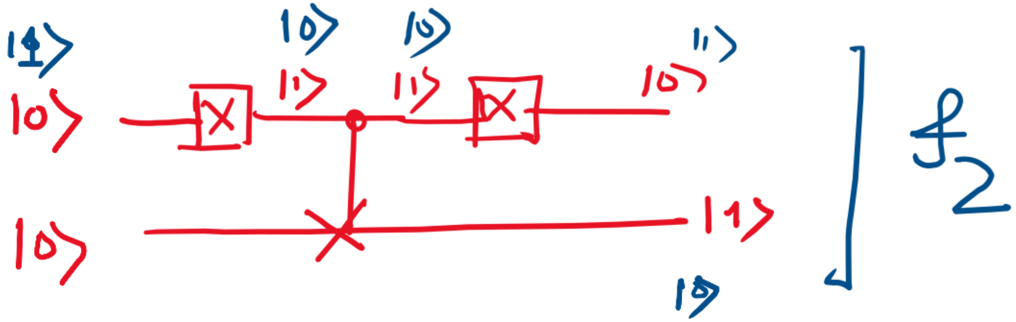


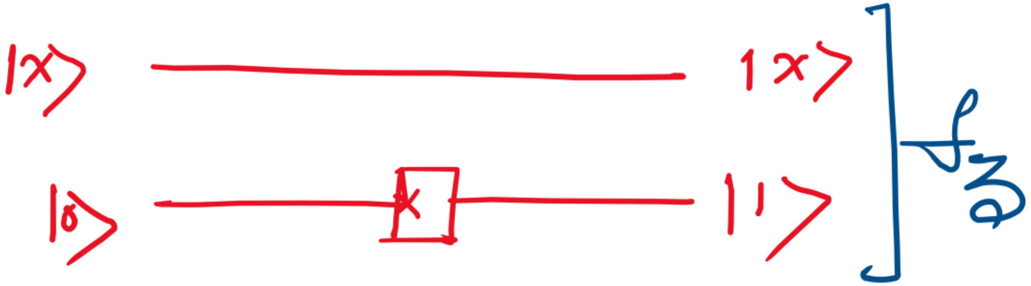


$|0\rangle|0\rangle \longleftrightarrow |0\rangle|0\rangle$

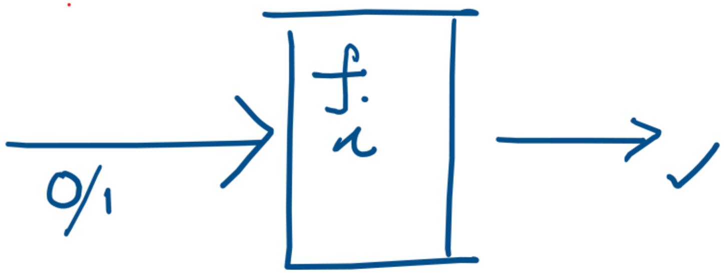
$|1\rangle|0\rangle \longleftrightarrow |1\rangle|1\rangle$

f_2





* Now the question is whether the unknown function is constant or not constant?



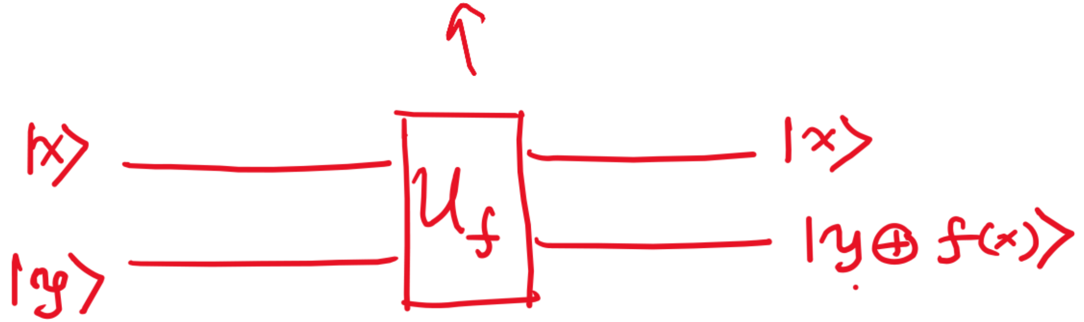
$i = 0, 1, 2, 3$

x	f_0	f_1	f_2	f_3
0	0	0	1	1
1	0	1	0	1

Suppose we assume an Oracle Access to the functions f_i.

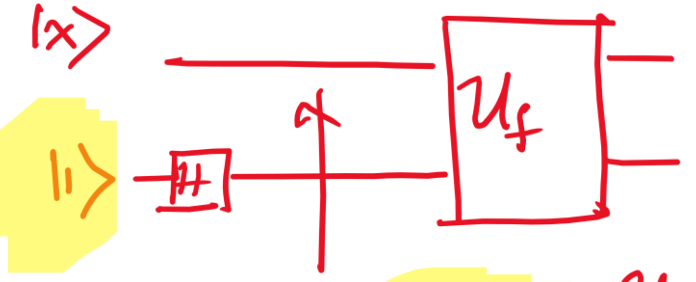
- If I have to know the functional value of f_i (i not known but fixed) I have to ask the value at 0 and at 1

I do not know 'i'.



$y = 0 \quad y = 1$

$f \in \{f_0, f_1, f_2, f_3\}$



$$|x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \xrightarrow{U_f} |x\rangle \otimes \frac{1}{\sqrt{2}}\left(|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle\right)$$

$$= |x\rangle \otimes (-1)^{f(x)} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

$$= \underline{(-1)^{f(x)} |x\rangle} \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$\left(|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle\right)$$

$f(x) = 0$ or $f(x) = 1$

If $f(x) = 0$

$$\underline{|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle}$$

$$= |0\rangle - |1\rangle$$

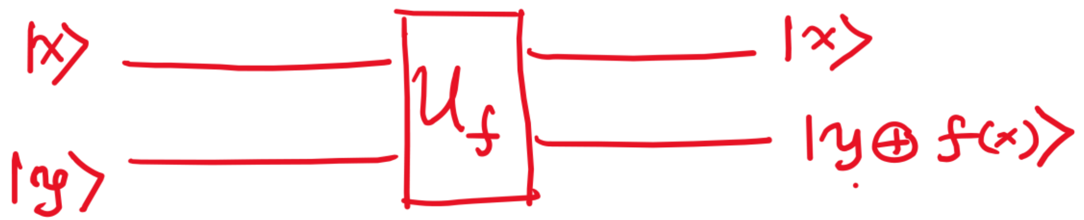
$$= (-1)^{f(x)}(|0\rangle - |1\rangle)$$

If $f(x) = 1$

$$|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle$$

$$= |1\rangle - |1 \oplus 1\rangle = |1\rangle - |0\rangle$$

$$= (-1)^{f(x)}(|0\rangle - |1\rangle)$$

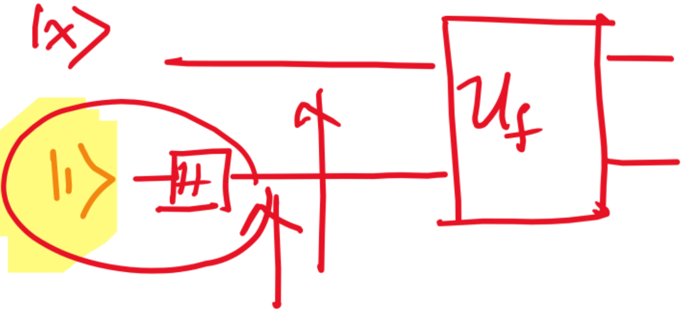


$y = 0 \qquad y = 1$

Phase oracle representation

$$|x\rangle|-\rangle \xrightarrow{U_f} (-1)^{f(x)}|x\rangle|-\rangle$$

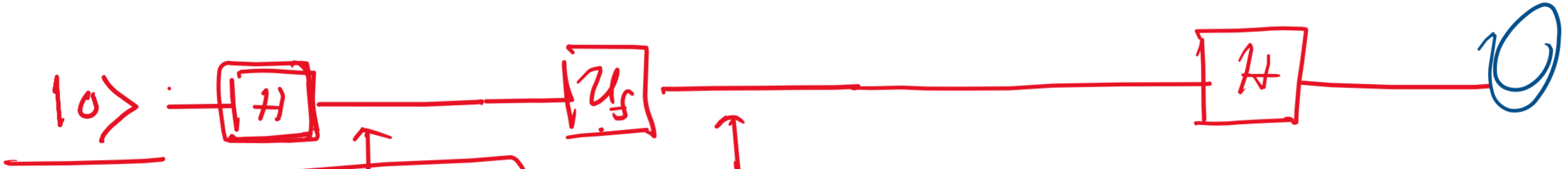
$$|x\rangle \xmapsto{U_f} (-1)^{f(x)}|x\rangle$$



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

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

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



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

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

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

$$\Big\downarrow H$$

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

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

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

$$\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \xrightarrow{U_f} 0 \xrightarrow{H}$$

Output: $\underbrace{\frac{1}{2}\left[\underbrace{(-1)^{f(0)} + (-1)^{f(1)}}\right]|0\rangle + \frac{1}{2}\left[\underbrace{(-1)^{f(0)} - (-1)^{f(1)}}\right]|1\rangle}$ $\begin{cases} |0\rangle \\ |1\rangle \end{cases}$

f is either constant $f(0) = 0,\ f(1) = 0$, $f(0) = 1,\ f(1) = 1$

Deutsch Algorithm

Two qubit states: All measurements are with respect to $\{|0\rangle, |1\rangle\}$

$$(|\Phi_1\rangle, |\Phi_2\rangle) = (a\,|0\rangle + b\,|1\rangle, \quad c\,|0\rangle + d\,|1\rangle)$$

- If we measure $|\Phi_1\rangle$ and $|\Phi_2\rangle$ the outcomes are

$$|0\rangle|0\rangle, |0\rangle|1\rangle, |1\rangle|0\rangle, |1\rangle|1\rangle$$

or

$$|00\rangle, |01\rangle, |10\rangle, |11\rangle$$

Two qubit states: All measurements are with respect to $\{|0\rangle, |1\rangle\}$

$$(|\Phi_1\rangle, |\Phi_1\rangle) = (a\,|0\rangle + b\,|1\rangle, \quad c\,|0\rangle + d\,|1\rangle)$$

- Probability of observing $|0\rangle\,|0\rangle$ is = $|ac|^2$
- Probability of observing $|0\rangle\,|1\rangle$ is = $|ad|^2$
- Probability of observing $|1\rangle\,|0\rangle$ is = $|bc|^2$
- Probability of observing $|1\rangle\,|1\rangle$ is = $|bd|^2$

Two qubit states:
All measurements are with respect to $\{|0\rangle, |1\rangle\}$

$(|\Phi_1\rangle, |\Phi_1\rangle) = (a|0\rangle + b|1\rangle, c|0\rangle + d|1\rangle)$

- Probability of observing $|0\rangle\ |0\rangle$ is $=\ |ac|^2$
- Probability of observing $|0\rangle\ |1\rangle$ is $=\ |ad|^2$
- Probability of observing $|1\rangle\ |0\rangle$ is $=\ |bc|^2$
- Probability of observing $|1\rangle\ |1\rangle$ is $=\ |bd|^2$

- $\binom{a}{b} \otimes \binom{c}{d} = \begin{pmatrix} a\binom{c}{d} \\ b\binom{c}{d} \end{pmatrix} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix}$
- $\binom{1}{0} \otimes \binom{1}{0} = \begin{pmatrix} 1\binom{1}{0} \\ 0\binom{1}{0} \end{pmatrix} = \begin{pmatrix} 1 \times 1 \\ 1 \times 0 \\ 0 \times 1 \\ 0 \times 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$
- $\binom{1}{0} \otimes \binom{1}{0} = |0\rangle \otimes |0\rangle = |0\rangle|0\rangle = |00\rangle$

Two qubit states:
All measurements are with respect to $\{|0\rangle, |1\rangle\}$

- $\binom{a}{b} \otimes \binom{c}{d} = \begin{pmatrix} a\binom{c}{d} \\ b\binom{c}{d} \end{pmatrix} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix} = |\Phi\rangle \otimes |\Psi\rangle$

- $\binom{1}{0} \otimes \binom{0}{1} = \begin{pmatrix} 1\binom{0}{1} \\ 0\binom{0}{1} \end{pmatrix} = \begin{pmatrix} 1 \times 0 \\ 1 \times 1 \\ 0 \times 0 \\ 0 \times 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$

- $\binom{1}{0} \otimes \binom{0}{1} = |0\rangle \otimes |1\rangle = |0\rangle|1\rangle = |01\rangle$

- $\binom{0}{1} \otimes \binom{1}{0} = \begin{pmatrix} 0\binom{1}{0} \\ 1\binom{1}{0} \end{pmatrix} = \begin{pmatrix} 0 \times 1 \\ 0 \times 0 \\ 1 \times 1 \\ 1 \times 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$

- $\binom{0}{1} \otimes \binom{1}{0} = |1\rangle \otimes |0\rangle = |1\rangle|0\rangle = |10\rangle$

- $\binom{0}{1} \otimes \binom{0}{1} = \begin{pmatrix} 0\binom{0}{1} \\ 1\binom{0}{1} \end{pmatrix} = \begin{pmatrix} 0 \times 0 \\ 0 \times 1 \\ 1 \times 0 \\ 1 \times 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$

- $\binom{0}{1} \otimes \binom{0}{1} = |1\rangle \otimes |1\rangle = |1\rangle|1\rangle = |11\rangle$

Two-qubit states

- $|\Phi\rangle|\Psi\rangle = ac|0\rangle \otimes |0\rangle + ad|0\rangle \otimes |1\rangle + bc|1\rangle \otimes |0\rangle + bd|1\rangle \otimes |1\rangle$
  $= ac\ |00\rangle + ad\ |01\rangle + bc\ |01\rangle + bd\ |11\rangle$

- $|ac|^2 + |ad|^2 + |bc|^2 + |bd|^2$

$= |a|^2|c|^2 + |a|^2|d|^2 + |b|^2|c|^2 + |b|^2|d|^2$

$= |a|^2(|c|^2 + |d|^2) + |b|^2(|c|^2 + |d|^2) = (|a|^2 + |b|^2)(|c|^2 + |d|^2)$

$= 1\ \times 1 = 1$

Two-qubit states

- $|\Psi\rangle = a_{00}|0\rangle \otimes |0\rangle + a_{01}|0\rangle \otimes |1\rangle + a_{10}|1\rangle \otimes |0\rangle + a_{11}|1\rangle \otimes |1\rangle$

  $= a_{00}\,|00\rangle + a_{01}\,|01\rangle + a_{10}\,|01\rangle + a_{11}\,|11\rangle$

  where $|a_{00}|^2 + |a_{01}|^2 + |a_{10}|^2 + |a_{11}|^2 = 1$

- Any vector of the above type is a two-qubit state.
- All such vector are not (tensor) products of single-qubit states.

Entangled states

- Consider the state

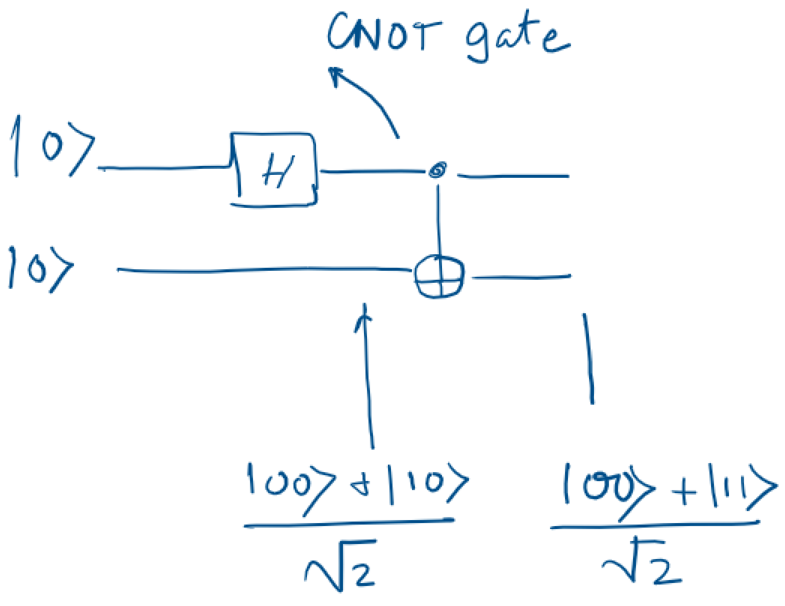
$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$(a|0\rangle + b|1\rangle)\,(c|0\rangle + d|1\rangle)$$

$$= ac|0\rangle \otimes |0\rangle + ad|0\rangle \otimes |1\rangle + bc|1\rangle \otimes |0\rangle + bd|1\rangle \otimes |1$$

$$= ac\;|00\rangle + ad\;|01\rangle + bc\;|01\rangle + bd\;|11\rangle$$

- $ac = \frac{1}{\sqrt{2}},\;\; ad = 0, bc = 0, bd = \frac{1}{\sqrt{2}}$
- $ad = 0 \Rightarrow a = 0\; or\; d = 0$. Both options lead to a contradiction.
- Therefore, the quantum state $|\Phi^+\rangle$ cannot be written as a tensor product of two single-qubit states.



Multiple qubit states

- An n-qubit state is

$$|\Psi\rangle = a_0|\mathbf{0}\rangle + a_1|\mathbf{1}\rangle + a_2|\mathbf{2}\rangle + \cdots + a_{2^n-1}|\boldsymbol{2^n-1}\rangle$$

where $|a_0|^2 + |a_1|^2 + \cdots + |a_{2^n-1}|^2 = 1$.

- For any number, m, between $0 \leq m \leq 2^n - 1$, its binary representation is denoted by $\mathbf{m}$.

Multiple qubit states

- An n-qubit state is

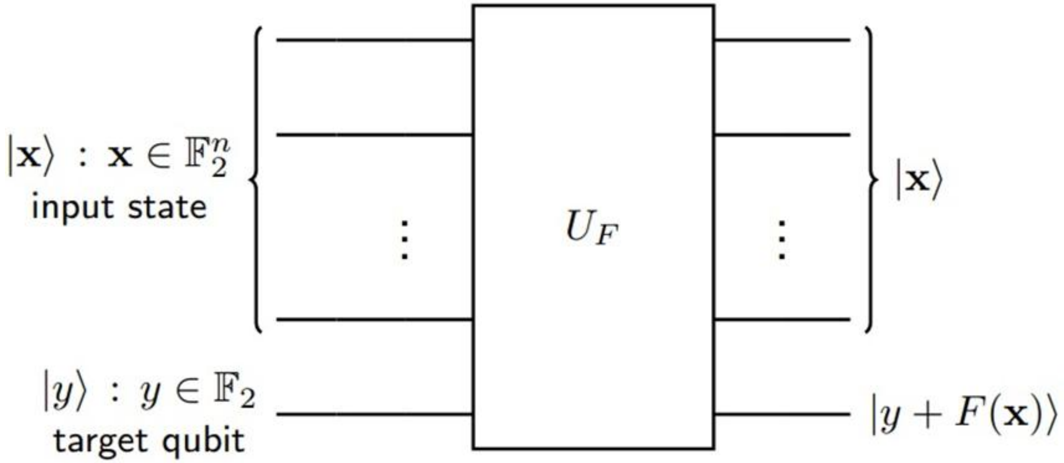
$$
\begin{aligned}
|\Psi\rangle = a_0|000\rangle + a_1|001\rangle + a_2|010\rangle + a_3|011\rangle \\
+a_4|100\rangle + a_5|101\rangle + a_6|110\rangle + a_7|111\rangle
\end{aligned}
$$

where

$$|a_0|^2 + |a_1|^2 + |a_2|^2 + |a_3|^2 + |a_4|^2 + |a_5|^2 + |a_6|^2 + |a_7|^2 = 1.$$

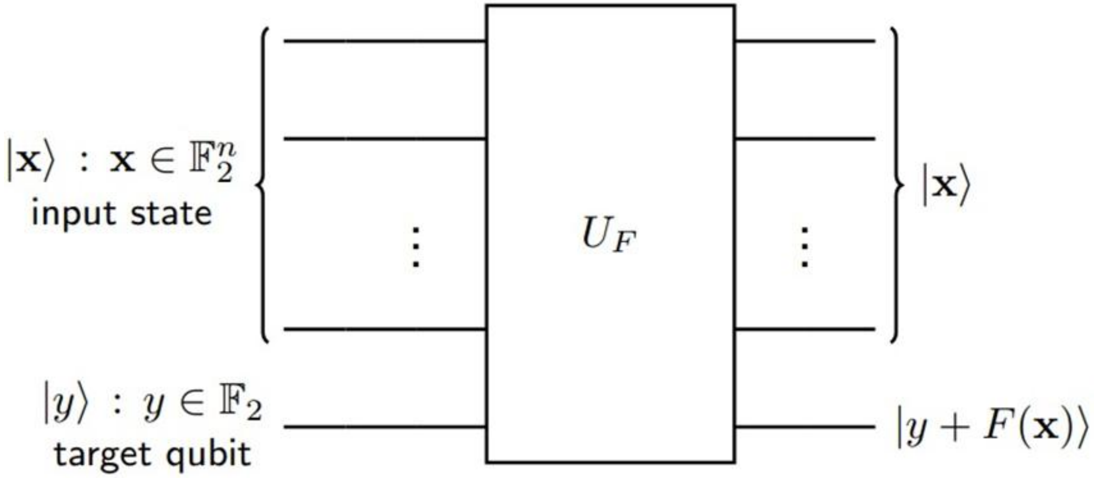
Quantum implementation of Boolean functions

- A Boolean function in n variables is a mapping from $\{0,1\}^n$ to $\{0,1\}$.
- Suppose f is an n-variable Boolean function.
- On a quantum computer f is implemented as a transformation $\mathcal{U}_f$ as follows: ($x_i, y \in \{0,1\}$ for all $i \in [n]$)

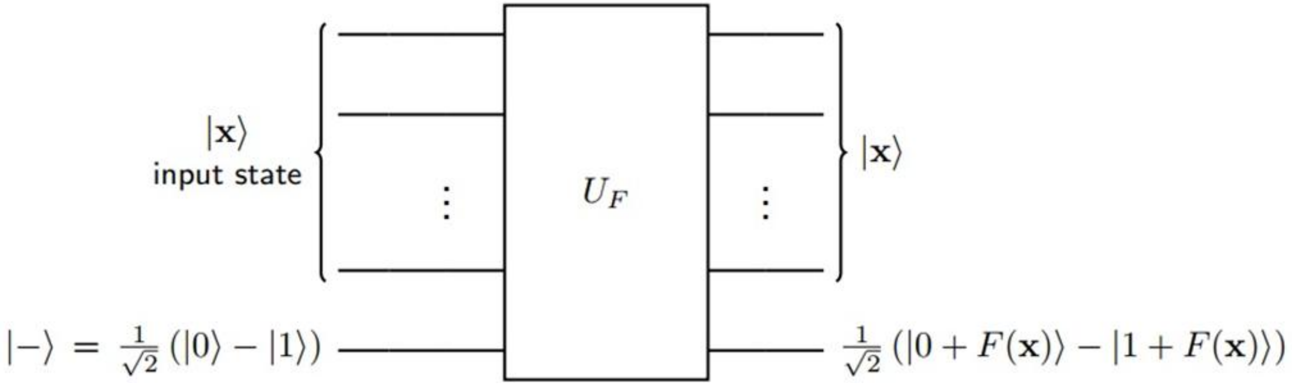


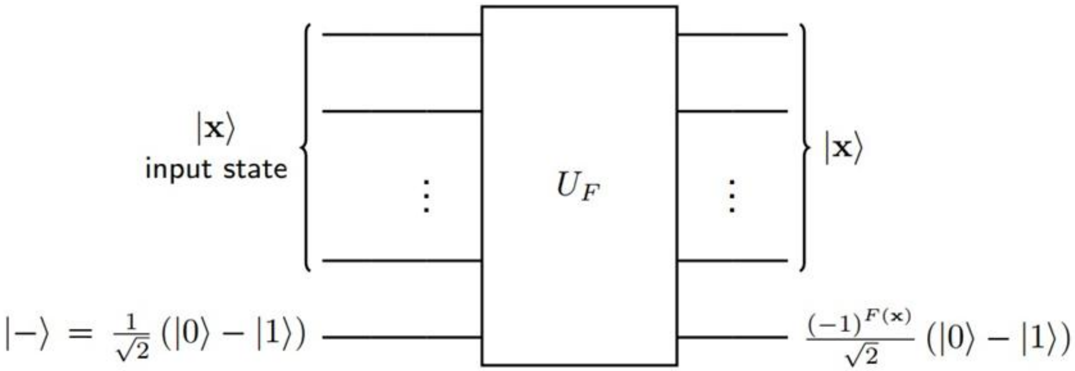
Quantum implementation of Boolean functions

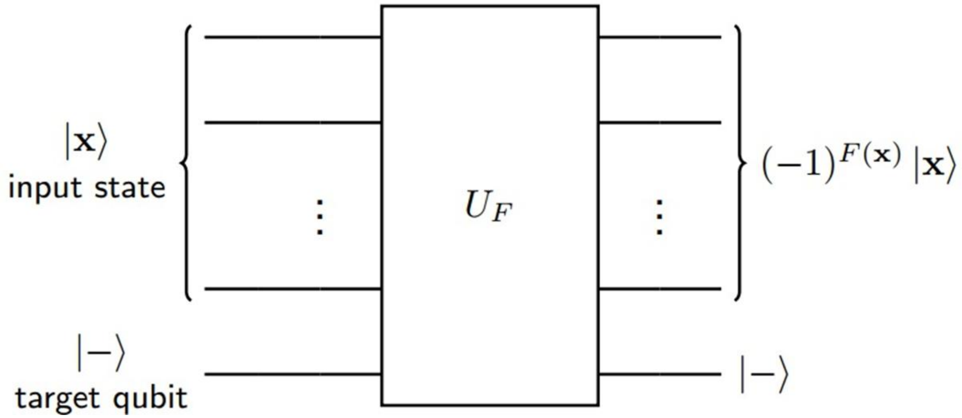
- A Boolean function in n variables is a mapping from $\{0,1\}^n$ to $\{0, 1\}$.
- Suppose f is an n-variable Boolean function.
- On a quantum computer f is implemented as a transformation $\mathcal{U}_f$ as follows:



Bit Oracle to Phase Oracle

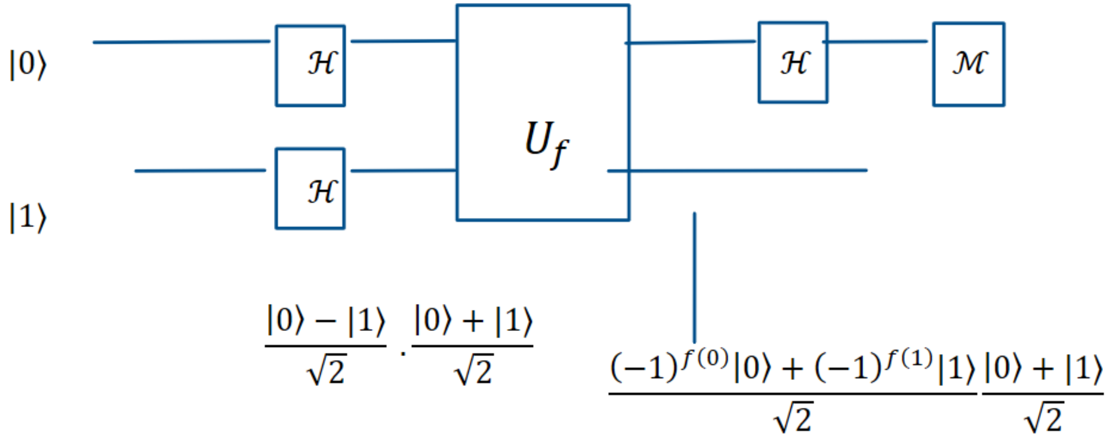






Deutsch Algorithm

- Consider 1-variable Boolean functions
  - $f_0(0) = 0, f_0(1) = 0$
  - $f_1(0) = 0, f_1(1) = 1$
  - $f_2(0) = 1, f_2(1) = 0$
  - $f_3(0) = 1, f_3(1) = 1$

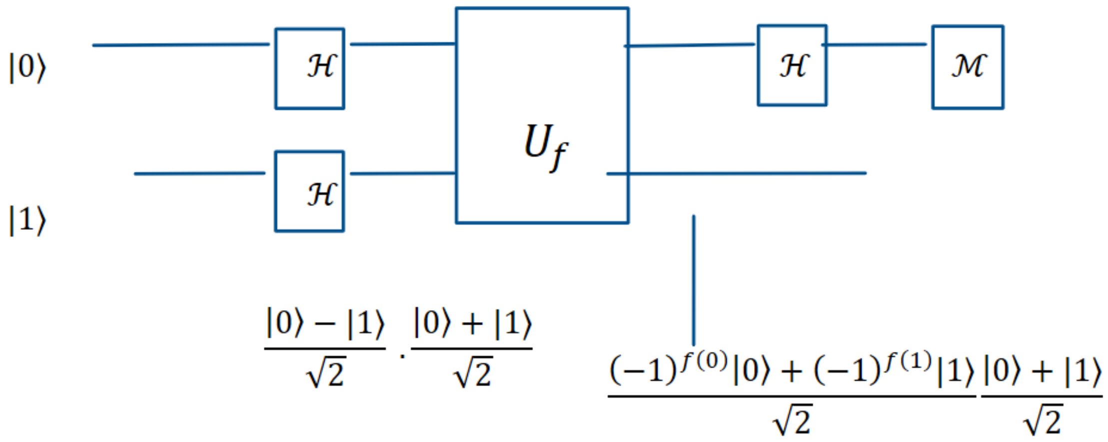


Deutsch Algorithm

- After the final Hadamard transformation we have

$$(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle \rightarrow (-1)^{f(0)} \frac{|0\rangle+|1\rangle}{\sqrt{2}} + (-1)^{f(1)} \frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

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



Deutsch-Jozsa Algorithm

- Let $\mathbf{x} = x_1 \cdots x_n \in \{0,1\}^n$
- $|x_i\rangle \xrightarrow{H} \frac{|0\rangle + (-1)^{x_i}|1\rangle}{\sqrt{2}}$
- $|\mathbf{x}\rangle \xrightarrow{H^{\otimes n}} 2^{-n/2} \sum_{\mathbf{y} \in \{0,1\}^n} (-1)^{\mathbf{x} \cdot \mathbf{y}} |\mathbf{y}\rangle$
- $|\mathbf{0}_n\rangle \xrightarrow{H^{\otimes n}} 2^{-n/2} \sum_{\mathbf{x} \in \{0,1\}^n} |\mathbf{x}\rangle \xrightarrow{U_f} 2^{-n/2} \sum_{\mathbf{x} \in \{0,1\}^n} (-1)^{f(\mathbf{x})} |\mathbf{x}\rangle$
- $2^{-n/2} \sum_{\mathbf{x} \in \{0,1\}^n} (-1)^{f(\mathbf{x})} |\mathbf{x}\rangle \xrightarrow{H^{\otimes n}} 2^{-n} \sum_{\mathbf{x} \in \{0,1\}^n} \sum_{\mathbf{y} \in \{0,1\}^n} (-1)^{f(\mathbf{x}) + \mathbf{x} \cdot \mathbf{y}} |\mathbf{y}\rangle$

Deutsch-Jozsa Algorithm

- $|\psi\rangle = 2^{-n} \sum_{\mathbf{x}\in\{0,1\}^n} \sum_{\mathbf{y}\in\{0,1\}^n} (-1)^{f(\mathbf{x})+\mathbf{x}\cdot\mathbf{y}} |\mathbf{y}\rangle$
  $= \sum_{\mathbf{y}\in\{0,1\}^n} \left(2^{-n} \sum_{\mathbf{x}\in\{0,1\}^n} (-1)^{f(\mathbf{x})+\mathbf{x}\cdot\mathbf{y}}\right) |\mathbf{y}\rangle$

- Suppose we measure $|\psi\rangle$ using the computational basis.
- The state $|\mathbf{0}_n\rangle$ appears with probability $2^{-n}\left|\sum_{\mathbf{x}\in\{0,1\}^n} (-1)^{f(\mathbf{x})}\right|^2$.
  - If f is balanced $2^{-n}\left|\sum_{\mathbf{x}\in\{0,1\}^n} (-1)^{f(\mathbf{x})}\right|^2 = 0$. So $|\mathbf{0}_n\rangle$ will never appear.
  - If f is a constant $2^{-n}\left|\sum_{\mathbf{x}\in\{0,1\}^n} (-1)^{f(\mathbf{x})}\right|^2 = 1$. So $|\mathbf{0}_n\rangle$ will always be the result of the measurement.

Thank You

Questions Please!?