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.

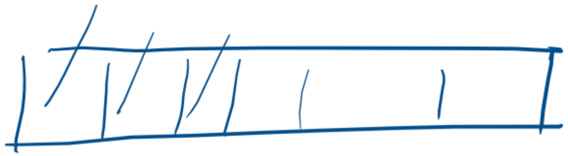
✓ Superposition – quantum state → qubits

✓ Entanglement – of $\boxed{\text{qubit}}$

$\boxed{\text{bits}}$

A single bit is a system that can exist in two states.

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



64

What can we do with bits?

x Read
x Write
x Store → without and error for a long 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

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

ket zero

$\mathbb{C}$

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

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

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

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

$\mathbb{C}$

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

ket one

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

$|\psi\rangle$

ket psi.

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

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

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 combination 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

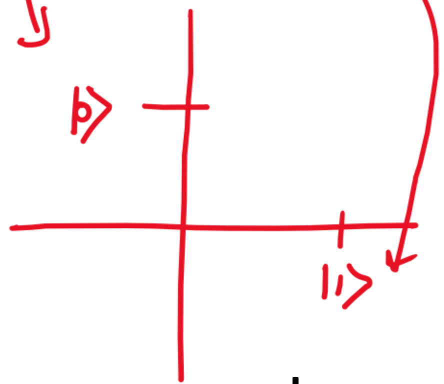
~~Storing a qubit~~ ✗

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

0, 1



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

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

when $a \neq 0$, $b \neq 0$, Then $|\psi\rangle$ 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.

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

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

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

$$|\psi\rangle = c\,|+\rangle + d\,|-\rangle$$

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

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

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

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

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

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

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

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.

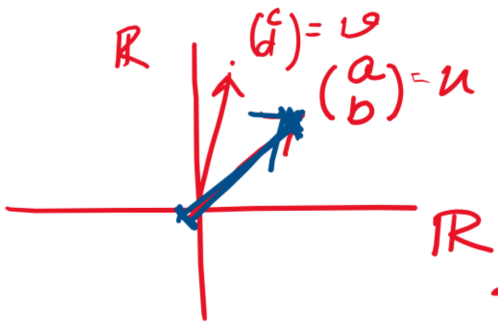
Examples of qubits differing by relative phases

- 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 → Inner product.

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

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

$1+i$

$-1-i$

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

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

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

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

$a_i \in \mathbb{C}$

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

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

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

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

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

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

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

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

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

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

ket a

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

bra a

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

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

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

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

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

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

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

bra 'a' ket 'b'

bra(c)ket a, b

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

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

$$a_i = x + iy$$

$$\bar{a}_i = x - iy \qquad i^2 = -1$$

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

$$= \underline{x^2 + y^2} = |a_i|^2$$

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 measurement corresponds to an orthonormal basis.

  ↓ of a quantum state ↓ single qubit state

  ↓ of the state space ↓ 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 $|\langle 1|\psi\rangle|^2$.

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

$$|\Psi\rangle\langle\Phi| = \binom{a}{b}\binom{c}{d}^{\dagger} = \binom{a}{b}\begin{pmatrix}\bar{c} & \bar{d}\end{pmatrix}$$

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

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

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

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

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

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

Two qubit states

- 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

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

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

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

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

- $\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |0\rangle \otimes |1\rangle = |0\rangle|1\rangle = |01\rangle$

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

- $\begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |1\rangle \otimes |0\rangle = |1\rangle|0\rangle = |10\rangle$

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

- $\begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle \otimes |1\rangle = |1\rangle|1\rangle = |11\rangle$

Two-qubit states

- $$\begin{aligned}|\Phi\rangle|\Psi\rangle &= ac|0\rangle \otimes |0\rangle + ad|0\rangle \otimes |1\rangle + bc|1\rangle \otimes |0\rangle + bd|1\rangle \otimes |1\rangle \\ &= ac\ |00\rangle + ad\ |01\rangle + bc\ |01\rangle + bd\ |11\rangle\end{aligned}$$

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

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

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

$= 1\ \times 1 = 1$

Two-qubit states

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

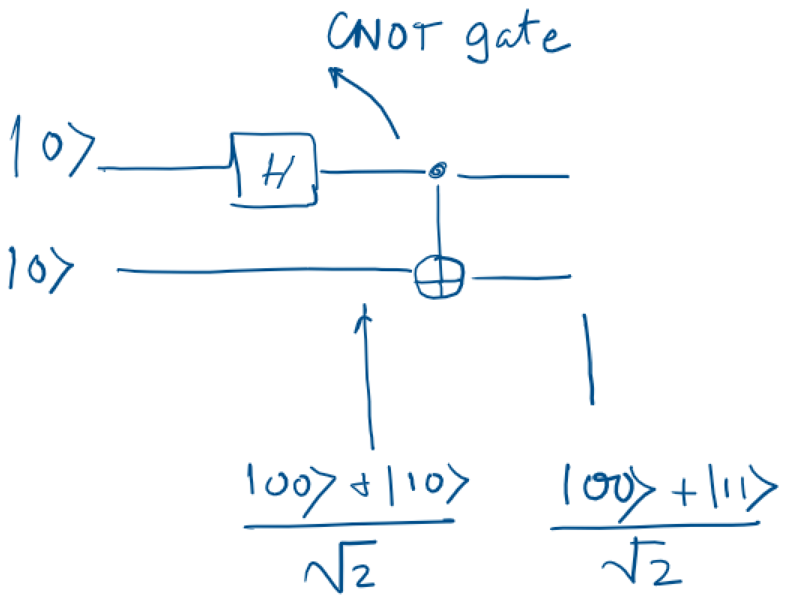
  $$= a_{00}\,|00\rangle + a_{01}\,|01\rangle + a_{10}\,|01\rangle + a_{11}\,|11\rangle$$

  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

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

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

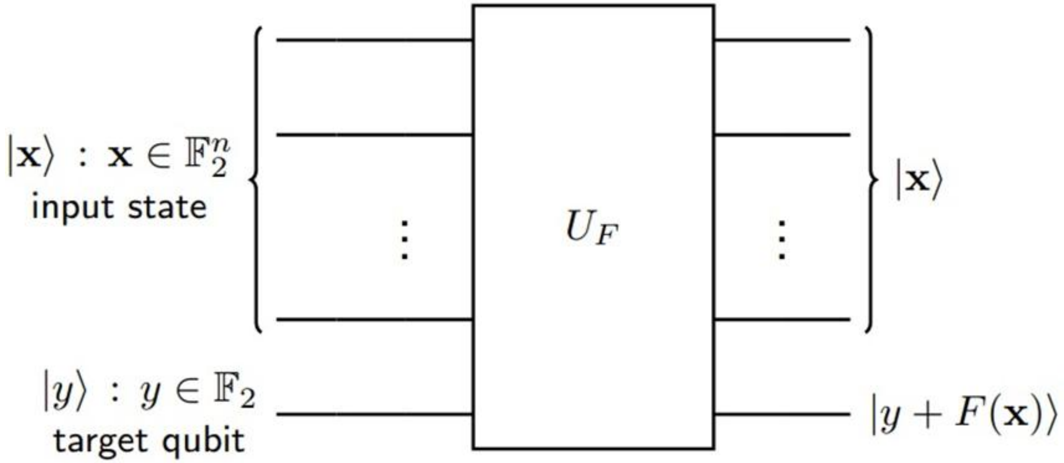
$$|\Psi\rangle = a_0|000\rangle + a_1|001\rangle + a_2|010\rangle + a_3|011\rangle$$
$$+a_4|100\rangle + a_5|101\rangle + a_6|110\rangle + a_7|111\rangle$$

where

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

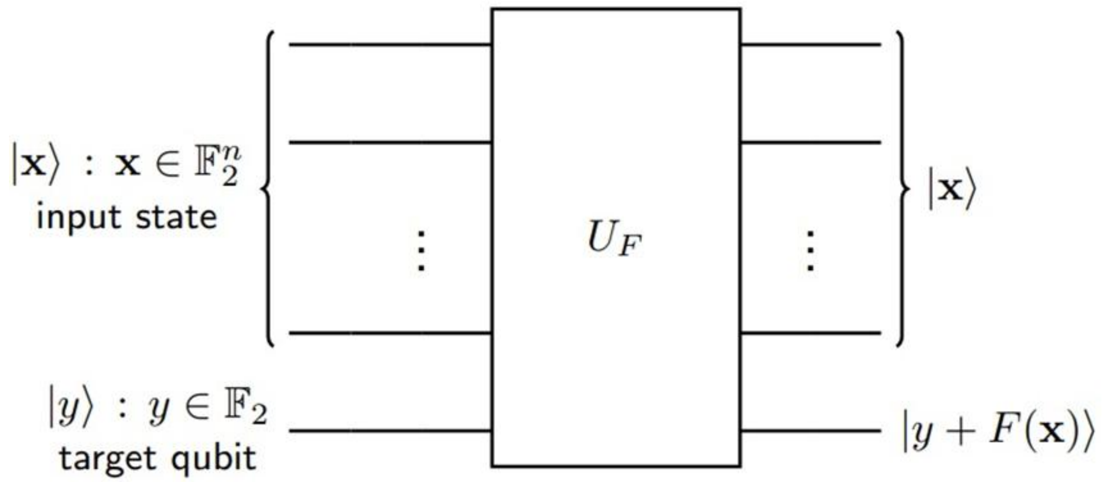
Quantum implementation of Boolean functions

- 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 $i \in [n]$)

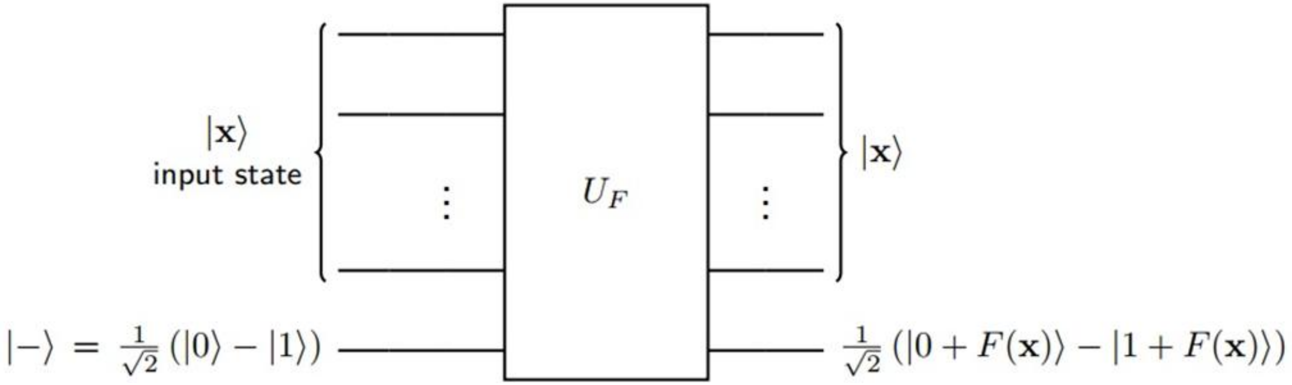


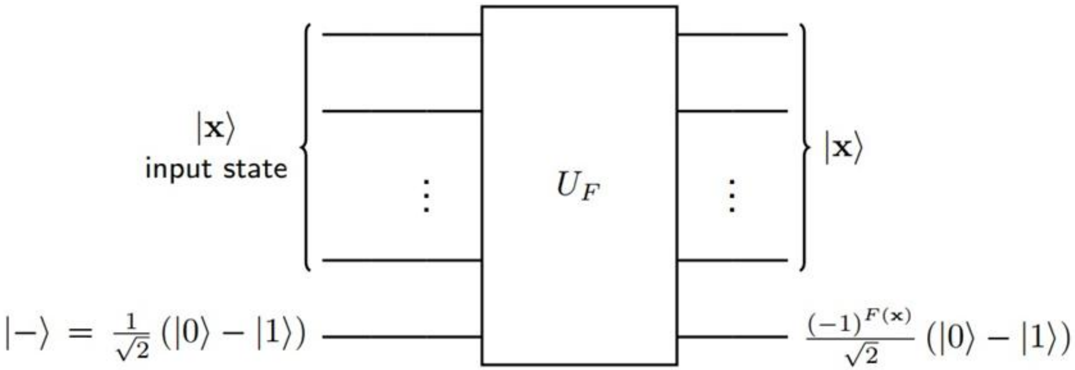
Quantum implementation of Boolean functions

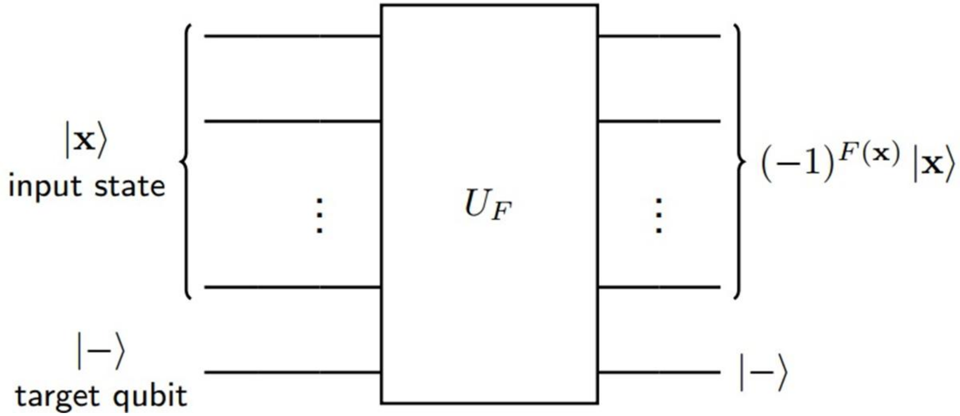
- A Boolean function in n variables is a mapping from $\{0,1\}^n$ to $\{0,1\}$.
- Suppose f is an n-variable Boolean function.
- On a quantum computer f is implemented as a transformation $\mathcal{U}_f$ as follows:



Bit Oracle to Phase Oracle

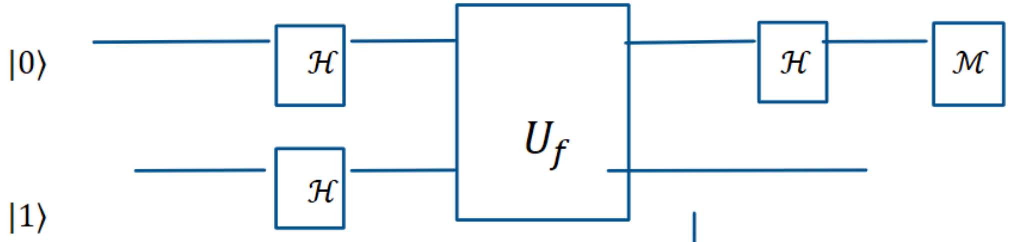






Deutsch Algorithm

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



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

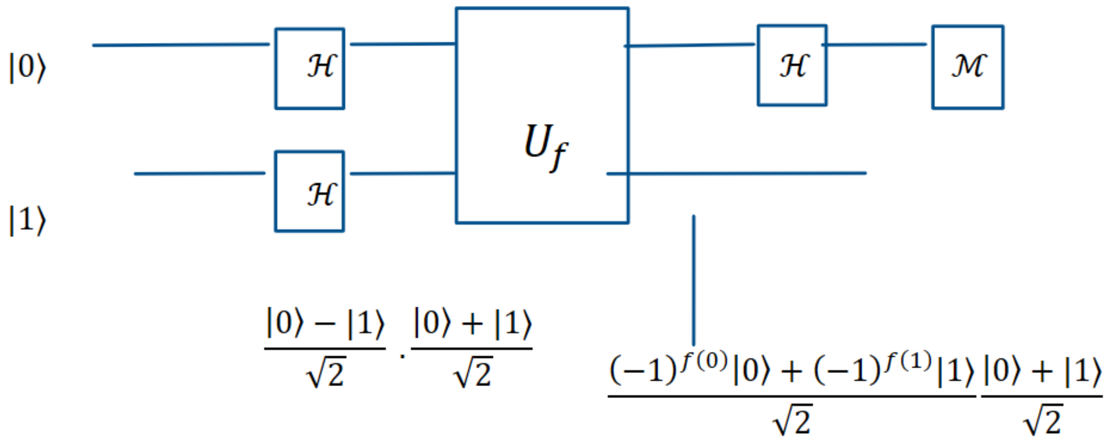
$$\frac{(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle}{\sqrt{2}} \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

Deutsch Algorithm

- After the final Hadamard transformation we have

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

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



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!?