Introduction to Quantum Computing

Sugata Gangopadhyay

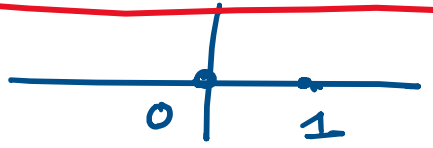
Department of Computer Science and Engineering

Indian Institute of Technology Roorkee

Qubits (Quantum (Bits) → binary digit 0, 1

- A quantum bit or a qubit is a fundamental unit of quantum information processing just as a bit is a fundamental unit of classical information processing.

- A single qubit state is represented by a pair of complex numbers $\begin{pmatrix} a \\ b \end{pmatrix}$ where $|a|^2 + |b|^2 = 1$.



- So a single qubit can exist in an infinite number of states whereas a bit can exist in either in 0 state or 1 state.

Bits

Quantum Bits Qubits

1. I should be able to set a bit to the 0 or 1, as I please. WRITE ✓
2. I should be able to read what I have written.
3. I should be able to store whatever I have written for ever(!) no matter how many times I read it

Our reading capability is extremely limited! ✗

✗

A single qubit is a quantum mechanical system that is completely specified by a pair of complex number $\begin{pmatrix} a \\ b \end{pmatrix}$, called its state vector.

Satisfy the equation $|a|^2 + |b|^2 = 1$

$a = \alpha_1 + i\alpha_2$, $\alpha_1, \alpha_2 \in \mathbb{R}$. $i^2 = -1$.

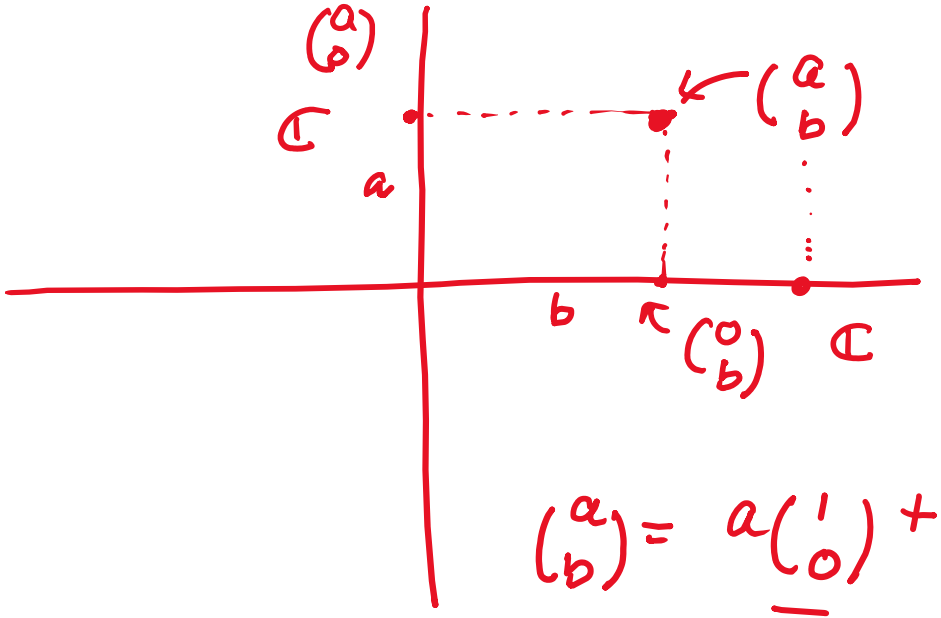
$|a|^2 = \alpha_1^2 + \alpha_2^2$ $\quad b = \beta_1 + i\beta_2$. $|b|^2 = \beta_1^2 + \beta_2^2$.

$\bar{a} = \alpha_1 - i\alpha_2$. $\quad a.\bar{a} = (\alpha_1 + i\alpha_2)(\alpha_1 - i\alpha_2)$

$= \alpha_1^2 - i\alpha_1\alpha_2 + i\alpha_2\alpha_1 - i^2\alpha_2^2 = \alpha_1^2 + \alpha_2^2$.

The State Space under consideration is $\mathbb{C} \times \mathbb{C}$ $\{0,1\}$

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



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

$\left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$

Basis

Writing conventions

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

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

- It is customary to write $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

Ket 0

Ket 1

- Then, a single qubit state is

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

- We must not forget that

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

A single qubit state

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

ket psi

$a, b \in \mathbb{C}$

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

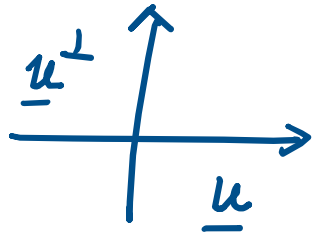
$a = x + iy$

$\bar{a} = x - iy$

$|a|^2 = a\bar{a} = (x+iy)(x-iy)$

$= x^2 - ixy - iyx + y^2 = x^2 + y^2$

Reading ≡ measuring



$\langle \underline{u} | \underline{u} \rangle = 1$

$\langle \underline{u}^\perp | \underline{u}^\perp \rangle = 1$

$\langle u | u^\perp \rangle = \langle u^\perp | u \rangle = 0.$

Either $|\underline{u}\rangle$ — $|\langle \underline{u} | \psi \rangle|^2$

$|\underline{u}^\perp\rangle$ — $|\langle \underline{u}^\perp | \psi \rangle|^2$

We can transform a quantum state.

We can transform a quantum state using a unitary transformation.

U → dagger

$$U = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \qquad U^\dagger = \begin{pmatrix} \bar{a}_{11} & \bar{a}_{21} \\ \bar{a}_{12} & \bar{a}_{22} \end{pmatrix} \qquad U^{-1} = U^\dagger.$$

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$I = |0\rangle\langle 0| + |1\rangle\langle 1| \qquad X = |1\rangle\langle 0| + |0\rangle\langle 1| \qquad Y = -|1\rangle\langle 0| + |0\rangle\langle 1| \qquad Z = |0\rangle\langle 0| - |1\rangle\langle 1|$$

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

Recalling complex numbers

- A complex number is written as $z = x + \mathbf{i}\, y$ where x, y are real numbers, and $\mathbf{i}^2 = -1$.

- The conjugate of z is $\bar{z} = x - \mathbf{i}y$.

- The modulus of a complex number is $|z|$ where

$$|z|^2 = z\bar{z} = x^2 + y^2$$

A single-bit system

- A single-bit system can exist in one of the two states: 0 and 1. Such a system can be visualized as

- In a classical computer it is possible to set a bit to the 0 or 1 state. It is also possible to read (measure) that state, and reading from a bit does not change its state.
- On a quantum computer it is possible to create a single-qubit state, but it is not possible to measure it without changing the state.

Quantum bits – Qubits

- Quantum bits – Qubits :

  A qubit is the fundamental unit of quantum information just as a bit is the fundamental unit of classical information.

  - A bit can exist in two states: 0 and 1.

  - A qubit is a vector having two complex components.

    Consider the vector space $\mathbb{C}^2 = \mathbb{C} \times \mathbb{C} = \left\{ \begin{pmatrix} a \\ b \end{pmatrix} : a, b \in \mathbb{C} \right\}$.

    A vector of the form $\begin{pmatrix} a \\ b \end{pmatrix}$ defines a state of a qubit if and only if

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

$\mathbb{C}^2 = \mathbb{C} \times \mathbb{C} = \left\{ \begin{pmatrix} a \\ b \end{pmatrix} : a, b \in \mathbb{C} \right\}$. $c \in \mathbb{C}$ $c\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} ca \\ cb \end{pmatrix}$

Basis of $\mathbb{C}^2$

• Linear dependence and independence.

- The set of vectors $\left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$ is said to be a basis is $\mathbb{C}^2$ since any element in $\mathbb{C}^2$ can be written uniquely as a linear combination

$$\begin{pmatrix} a \\ b \end{pmatrix} = a \begin{pmatrix} 1 \\ 0 \end{pmatrix} + b \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

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

$\Rightarrow a = 0, b = 0$

- Any set of vectors with this property is said to be a basis of $\mathbb{C}^2$.

  For example: $\left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\}$, $\left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ \mathbf{i} \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -\mathbf{i} \end{pmatrix} \right\}$

  where $\mathbf{i}^2 = -1$.

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

$$\mathcal{B}_1 = \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\} = \{|0\rangle, |1\rangle\}$$

$$\mathcal{B}_2 = \left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\} = \{|+\rangle, |-\rangle\}$$

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

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

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

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

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

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

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

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

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

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

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

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

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

Inner Product

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

$$|\phi\rangle = \begin{pmatrix} c \\ d \end{pmatrix} = c|0\rangle + d|1\rangle.$$

The inner product of $|\psi\rangle$ and $|\phi\rangle$

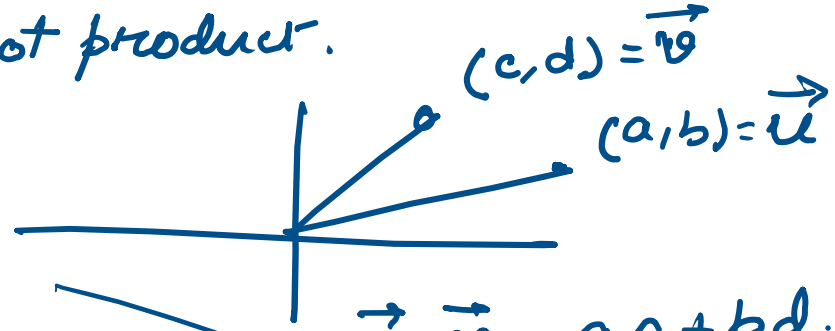
$$\langle\psi|\phi\rangle = \bar{a}c + \bar{b}d.$$

$$\langle\psi|\psi\rangle = \bar{a}a + \bar{b}b$$

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

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

Dot product.



$$\vec{u}\cdot\vec{v} = ac + bd.$$

$$\vec{u}\cdot\vec{u} = a^2 + b^2$$

Norm

$$\|\psi\| = \sqrt{\langle\psi|\psi\rangle}$$

$$= \sqrt{|a|^2 + |b|^2} = 1$$

Dirac's bra/ket notation.

$|\psi\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$ ket ψ

$|\phi\rangle = \begin{pmatrix} c \\ d \end{pmatrix}$ ket ϕ

$\langle\psi| = (\bar{a}\ \bar{b})$ bra ψ

$\langle\psi|\phi\rangle = (\bar{a}\ \bar{b}) \begin{pmatrix} c \\ d \end{pmatrix}$

$= \bar{a}c + \bar{b}d$

braket ψ, ϕ $= \langle\psi|\phi\rangle$

Inner product on $\mathbb{C}^2$

$|\psi\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$, $|\phi\rangle = \begin{pmatrix} c \\ d \end{pmatrix}$

- Inner product of two vectors $\begin{pmatrix} a \\ b \end{pmatrix}, \begin{pmatrix} c \\ d \end{pmatrix} \in \mathbb{C}^2$ is

$$\begin{pmatrix} a \\ b \end{pmatrix}^\dagger \begin{pmatrix} c \\ d \end{pmatrix} = (\bar{a} \quad \bar{b}) \begin{pmatrix} c \\ d \end{pmatrix} = \bar{a}c + \bar{b}d.$$

$|\psi\rangle$ and $|\phi\rangle$ will be said to be orthogonal vectors.

- Two vector are said to be orthogonal if

$$\begin{pmatrix} a \\ b \end{pmatrix}^\dagger \begin{pmatrix} c \\ d \end{pmatrix} = (\bar{a} \quad \bar{b}) \begin{pmatrix} c \\ d \end{pmatrix} = \bar{a}c + \bar{b}d = 0.$$

$\langle\psi|\phi\rangle$ $= \bar{a}c + \bar{b}d = 0$

Orthonormal basis of $\mathbb{C}^2$

Such a basis is called an orthonormal basis.

- Suppose $\left\{\begin{pmatrix} a \\ b \end{pmatrix}, \begin{pmatrix} c \\ d \end{pmatrix}\right\}$ is a basis such that

$|\psi\rangle \quad |\phi\rangle$

$$\begin{pmatrix} a \\ b \end{pmatrix}^\dagger \begin{pmatrix} c \\ d \end{pmatrix} = (\bar{a} \quad \bar{b}) \begin{pmatrix} c \\ d \end{pmatrix} = \bar{a}c + \bar{b}d = 0$$

and

$$\langle\psi|\psi\rangle = \begin{pmatrix} a \\ b \end{pmatrix}^\dagger \begin{pmatrix} a \\ b \end{pmatrix} = (\bar{a} \quad \bar{b}) \begin{pmatrix} a \\ b \end{pmatrix} = \bar{a}a + \bar{b}b = |a|^2 + |b|^2 = 1$$ ✓

$$\langle\phi|\phi\rangle = \begin{pmatrix} c \\ d \end{pmatrix}^\dagger \begin{pmatrix} c \\ d \end{pmatrix} = (\bar{c} \quad \bar{d}) \begin{pmatrix} c \\ d \end{pmatrix} = \bar{c}c + \bar{d}d = |c|^2 + |d|^2 = 1$$ ✓

$\langle\psi|\phi\rangle = \langle\phi|\psi\rangle = 0.$

Orthonormal basis of $\mathbb{C}^2$

- Computational basis: $\mathcal{B} = \left\{\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}\right\}$:

$$\begin{pmatrix}1\\0\end{pmatrix}^{\dagger}\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}\bar{1} & \bar{0}\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} = \bar{1}0 + \bar{0}1 = 0$$

$$\begin{pmatrix}1\\0\end{pmatrix}^{\dagger}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}\bar{1} & \bar{0}\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \bar{1}1 + \bar{0}0 = 1$$

$$\begin{pmatrix}0\\1\end{pmatrix}^{\dagger}\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}\bar{0} & \bar{1}\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} = \bar{0}0 + \bar{1}1 = 1$$

Orthonormal basis of $\mathbb{C}^2$: Examples

- Hadamard basis: $\mathcal{H} = \left\{\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}, \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}\right\}$.
- Nega-Hadamard basis: $\mathcal{N} = \left\{\frac{1}{\sqrt{2}}\begin{pmatrix}1\\\mathbf{i}\end{pmatrix}, \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-\mathbf{i}\end{pmatrix}\right\}$.
- Verify that $\mathcal{H}$ and $\mathcal{N}$ are orthonormal bases.

Dirac's bra/ket notation

- A vector $\begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{C}^2$ is written as $|\psi\rangle$ read as *"ket psi"*.

- The vector $\begin{pmatrix} a \\ b \end{pmatrix}^\dagger = (\bar{a} \quad \bar{b})$ is written as $\langle\psi|$.

- Inner product of two vectors $|\phi\rangle = \begin{pmatrix} c \\ d \end{pmatrix}$, and $|\psi\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$ is

  $\langle\psi|\phi\rangle = \begin{pmatrix} a \\ b \end{pmatrix}^\dagger \begin{pmatrix} c \\ d \end{pmatrix} = (\bar{a} \quad \bar{b}) \begin{pmatrix} c \\ d \end{pmatrix} = \bar{a}c + \bar{b}d.$

  The order in the which $|\phi\rangle$ and $|\psi\rangle$ appear matters. This is the inner product of $|\phi\rangle$ and $|\psi\rangle$ and not $|\psi\rangle$ and $|\phi\rangle$.

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

$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $\quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ $\quad |\psi\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$ $\quad |a|^2 + |b|^2 = 1.$

$|\psi\rangle$, $|\phi\rangle$ $\quad |\psi\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$

$\langle\psi| = \begin{pmatrix} a \\ b \end{pmatrix}^\dagger = (\bar{a}, \bar{b})$

$\langle\psi|\phi\rangle = \begin{pmatrix} a \\ b \end{pmatrix}^\dagger \begin{pmatrix} c \\ d \end{pmatrix} = (\bar{a} \ \bar{b}) \begin{pmatrix} c \\ d \end{pmatrix} = \bar{a}c + \bar{b}d$

↑

braket ψ ϕ

Computational, Hadamard and Nega-Hadamard Bases in Dirac's notation

- Computational basis: $|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}, |1\rangle = \begin{pmatrix}0\\1\end{pmatrix}.$

- Hadamard basis: $|+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} = \frac{|0\rangle+|1\rangle}{\sqrt{2}}, |-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix} = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$

- Nega-Hadamard basis:

  $|\mathbf{i}\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\\mathbf{i}\end{pmatrix} = \frac{|0\rangle+\mathbf{i}|1\rangle}{\sqrt{2}}, |-\mathbf{i}\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-\mathbf{i}\end{pmatrix} = \frac{|0\rangle-\mathbf{i}|1\rangle}{\sqrt{2}}$

- Verify that all the above bases are orthonormal.

|0⟩ |1⟩ bit qubit 0 → |0⟩ 1 → |1⟩

Superposition of states

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

A single qubit can exist in any one of the state

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

a=1 b=0 a=0 b=1

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

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

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

$a \neq 0, \quad b \neq 0$

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

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

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

- However, the representation of $|\psi\rangle$ with respect to the basis $\mathcal{H} = \{|+\rangle, |-\rangle\}$ is $|\psi\rangle = |+\rangle$.

Hadamard Basis

- 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:

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

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

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

Global phase versus relative phase

$e^{i\theta}|\psi\rangle = e^{i\theta}a|0\rangle + e^{i\theta}b|1\rangle$ $\quad |e^{i\theta}a|^2 + |e^{i\theta}b|^2 = |e^{i\theta}|^2|a|^2 + |e^{i\theta}|^2|b|^2 = (a^2+b^2) = 1$

- 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.

$|\psi\rangle = a|0\rangle + b|1\rangle$ $\quad \frac{a}{b} = e^{i\varphi}\frac{|a|}{|b|}$.

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

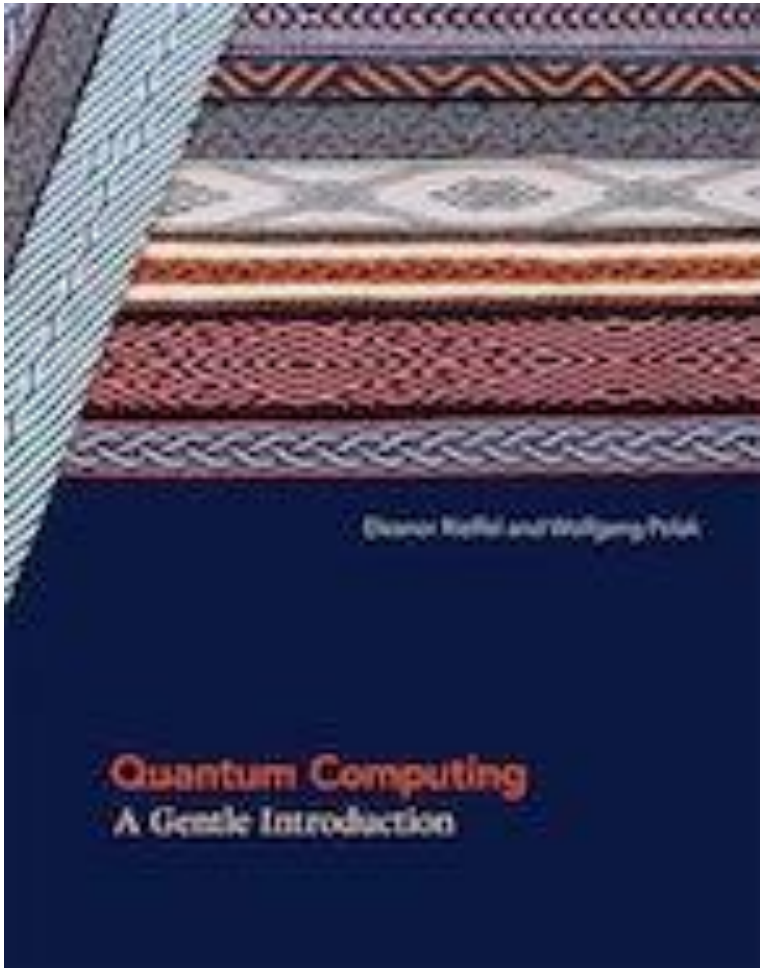
- Consider: $\frac{1}{\sqrt{2}}(\,|0\rangle + |1\rangle)$ and $\frac{1}{\sqrt{2}}(-|0\rangle + \mathbf{i}|1\rangle)$

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

  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.



2nd day. First week

Quantum Computing
A Gentle Introduction
By Eleanor G. Rieffel and Wolfgang H. Polak

Quantum Inf. & Computing
Nielsen & Chuang.

- **Qubit**
- State of a qubit. $|\psi\rangle = a|0\rangle + b|1\rangle$

ket psi ket zero ket one.

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

- Suppose $|\psi\rangle = a|0\rangle + b|1\rangle$, $|\phi\rangle = c|0\rangle + d|1\rangle$. are two single qubit states. Then their inner product

$\langle\psi|\phi\rangle = \bar{a}c + \bar{b}d$. $\|\psi\| = \sqrt{\langle\psi|\psi\rangle} = \sqrt{|a|^2 + |b|^2} = 1$

- Basis, dimension.
- Orthogonality and Orthonormality.

Suppose V is a vector space over $\mathbb{C}$. $V = \mathbb{C} \times \mathbb{C}$

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

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

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

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

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

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

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

is an orthonormal basis of $\mathbb{C} \times \mathbb{C}$

$|+\rangle = \dfrac{|0\rangle + |1\rangle}{\sqrt{2}}$ $\qquad |-\rangle = \dfrac{|0\rangle - |1\rangle}{\sqrt{2}}$

$\{|+\rangle, |-\rangle\}$

Measurements

- I have a qubit in the state. $|\psi\rangle = a|0\rangle + b|1\rangle$.

- We need a measurement device to measure.
- Any measurement process is related to an orthonormal basis in the quantum state space.

- $\{|0\rangle, |1\rangle\}$ —— M
- If we measure the qubit $|\psi\rangle$ with M, the outcome of the measurement is either $|0\rangle$ or $|1\rangle$

$|\psi\rangle = a|0\rangle + b|1\rangle$ measurement $M \{|0\rangle, |1\rangle\}$

outcome of M is either $|0\rangle$ or $|1\rangle$

outcome of a measurement is not deterministic.

The probability of obtaining $|0\rangle$ as the measurement M result is

$$|\langle 0|\psi\rangle|^2 = |\langle 0|(a|0\rangle + b|1\rangle)|^2$$

$$= |a\langle 0|0\rangle + b\langle 0|1\rangle|^2 = |a \cdot 1|^2 = |a|^2$$

The probability of obtaining $|1\rangle$ as the measurement M result is

$$|\langle 1|\psi\rangle|^2 = |\langle 1|(a|0\rangle + b|1\rangle)|^2 = |a\langle 1|0\rangle + b\langle 1|1\rangle|^2 = |b|^2.$$

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

Suppose that we have measured the quantum state

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

using the measurement M having the basis $\{|0\rangle, |1\rangle\}$

If the result of the measurement is $|0\rangle$, then the quantum state $|\psi\rangle$ has already changed to $|0\rangle$.

If the result of the measurement is $|1\rangle$, the the quantum state $|\psi\rangle$ has already changed to $|1\rangle$.

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

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

Inner Product

An ***inner product*** $\langle v_2|v_1\rangle$, or ***dot product***, on a complex vector space V is a complex function defined on pairs of vectors $|v_1\rangle$ and $|v_2\rangle$, satisfying

- $\langle v|v\rangle$ is non-negative real,
- $\langle v_2|v_1\rangle = \overline{\langle v_1|v_2\rangle}$, and
- $(a\langle v_2| + b\langle v_3|)|v_1\rangle = a\langle v_2|v_1\rangle + b\langle v_3|v_1\rangle$
- where $\bar{z}$ is the complex conjugate $\bar{z} = a - \imath b$ of $z = a + \imath b$.

Orthogonality of vector

- Two vectors $|v_1\rangle$ and $|v_2\rangle$ are said to be ***orthogonal*** if $\langle v_1|v_2\rangle = 0$.
- A set of vectors is orthogonal if all of its members are orthogonal to each other.
- The ***length***, or norm, of a vector $|v\rangle$ is $||v\rangle| = \sqrt{\langle v|v\rangle}$.
- Since all vectors representing quantum states are of unit length, $\langle x|x\rangle = 1$ for any state vector $|x\rangle$.

Orthonormal bases

- A set of vectors is said to be ***orthonormal*** if all of its elements are of length one, and orthogonal to each other: a set of vectors $B = \{|\beta_1\rangle, |\beta_2\rangle, \dots, |\beta_n\rangle\}$ is orthonormal if $\langle\beta_i|\beta_j\rangle = \delta_{ij}$ for all i, j, where
- $\delta_{ij} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherewise.} \end{cases}$
- A basis of a vector space consisting of orthonormal vectors is said to be an ***orthonormal basis***.

For the $\boldsymbol{n}$-dimensional space over $\mathbb{C}$

- In general, a vector $|v\rangle$ in an n dimensional space is a column vector $v = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}$. The conjugate transpose of ket is called ***bra*** and is written as $\langle v|$.

- The matrix corresponding to $\langle v|$ is $v^\dagger = (\bar{a}_1, \dots, \bar{a}_n)$.

The Inner Product

- If $|a\rangle = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}$ and $|b\rangle = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$, the inner product

$$\langle a|b\rangle = \langle a\|b\rangle = (\bar{a}_1 \quad \bar{a}_2 \quad \cdots \quad \bar{a}_n)\begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = \sum_{i=1}^{n} \bar{a}_i b_i$$

Single-Qubit Measurement

- Any device that measures a two-state quantum system must have two preferred states whose representative vectors, $\{|u\rangle, |u^{\perp}\rangle\}$, form an orthogonal basis for the associated vector space. Suppose that we intend to measure a single qubit state $|\psi\rangle$ which is represented as

$$|\psi\rangle = a|u\rangle + b|u^{\perp}\rangle.$$

- After measurement, the state $|\psi\rangle$ gets transformed into one of the measuring devices associated basis states, namely $|u\rangle$ or $|u^{\perp}\rangle$. The probability that $|\psi\rangle$ is transformed to $|u\rangle$ is $|a|^2$ and the probability that it is transformed to $|u^{\perp}\rangle$ is $|b|^2$. This behavior of measurement is an axiom of quantum mechanics.

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

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

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

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

We can transform the quantum state vectors by unitary linear transformations.

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

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

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

$= \begin{pmatrix}a\\b\end{pmatrix}_{2\times 1}$

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

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

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

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

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

dagger

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

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

$X|\psi\rangle = b|0\rangle + a|1\rangle$ where $|\psi\rangle = a|0\rangle + b|1\rangle$.

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

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

So in a way X works exactly as the NOT gate.

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

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

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

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

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

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

$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = a\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + b\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + c\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + d\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$

$= a|0\rangle\langle 0| + b|0\rangle\langle 1| + c|1\rangle\langle 0| + d|1\rangle\langle 1|$

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

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

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

$$= |0\rangle\langle 1| + |1\rangle\langle 0|$$

From the outer product formalism we have seen that-

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

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

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

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

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

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

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

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

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

$|0\rangle$ q

c 1/

Two qubit states

- Consider two qubits

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

and

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

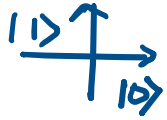
If these two qubits exist side by side, then we have a two-qubit state

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

From single qubits to two qubits

$|\phi_1\rangle = a|0\rangle + b|1\rangle$, $|\phi_2\rangle = c|0\rangle + d|1\rangle$

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



The possible measurement results are:

$\|0\rangle\|0\rangle$	$\|0\rangle\|1\rangle$	$\|1\rangle\|0\rangle$	$\|1\rangle\|1\rangle$
$\|a\|^2 \times \|c\|^2$	$\|ad\|^2$	$\|bc\|^2$	$\|bd\|^2$
$= \|ac\|^2$			

$|\Phi_1\rangle = a|0\rangle + b|1\rangle \qquad |\Phi_2\rangle = c|0\rangle + d|1\rangle$

Kronecker product

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

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

$\begin{pmatrix}\alpha\\ \beta\end{pmatrix} \otimes \begin{pmatrix}\gamma\\ \delta\end{pmatrix} = \begin{pmatrix}\alpha\begin{pmatrix}\gamma\\ \delta\end{pmatrix}\\ \beta\begin{pmatrix}\gamma\\ \delta\end{pmatrix}\end{pmatrix} = \begin{pmatrix}\alpha\gamma\\ \alpha\delta\\ \beta\gamma\\ \beta\delta\end{pmatrix}.$

$\begin{pmatrix}1\\0\end{pmatrix}\otimes\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\\0\\0\\0\end{pmatrix} \qquad \begin{pmatrix}1\\0\end{pmatrix}\otimes\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}1\begin{pmatrix}0\\1\end{pmatrix}\\ 0\begin{pmatrix}0\\1\end{pmatrix}\end{pmatrix} = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}$

$\begin{pmatrix}0\\1\end{pmatrix}\otimes\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0\\0\\1\\0\end{pmatrix} \qquad \begin{pmatrix}0\\1\end{pmatrix}\otimes\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}$

$= ac\begin{pmatrix}1\\0\\0\\0\end{pmatrix} + ad\begin{pmatrix}0\\1\\0\\0\end{pmatrix} + bc\begin{pmatrix}0\\0\\1\\0\end{pmatrix} + bd\begin{pmatrix}0\\0\\0\\1\end{pmatrix}$

$= \begin{pmatrix}ac\\ad\\bc\\bd\end{pmatrix}$

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

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

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

- 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 = $|bd|^2$

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

$\left[\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right] \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix}$

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

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

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

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

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

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

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

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

$= 1 \times 1 = 1$

Two-qubit states

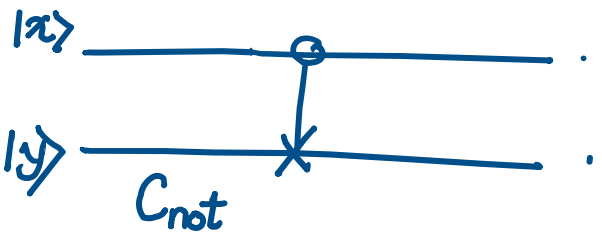
- $|\Psi\rangle = a_{00}|0\rangle \otimes |0\rangle + a_{01}|0\rangle \otimes |1\rangle + a_{10}|1\rangle \otimes |0\rangle + a_{11}|1\rangle \otimes |1\rangle$

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

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.

So far, we have seen quantum gates that operates over a single qubit. Now, we describe a unitary transformation that operates over a pair of qubits.



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

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

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

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

$\|0\rangle \otimes \|0\rangle$	$\|0\rangle \otimes \|1\rangle$	$\|1\rangle \otimes \|0\rangle$	$\|1\rangle \otimes \|1\rangle$
$\|00\rangle$	$\|01\rangle$	$\|10\rangle$	$\|11\rangle$
$\|0\rangle\|0\rangle$	$\|0\rangle\|1\rangle$	$\|1\rangle\|0\rangle$	$\|1\rangle\|1\rangle$

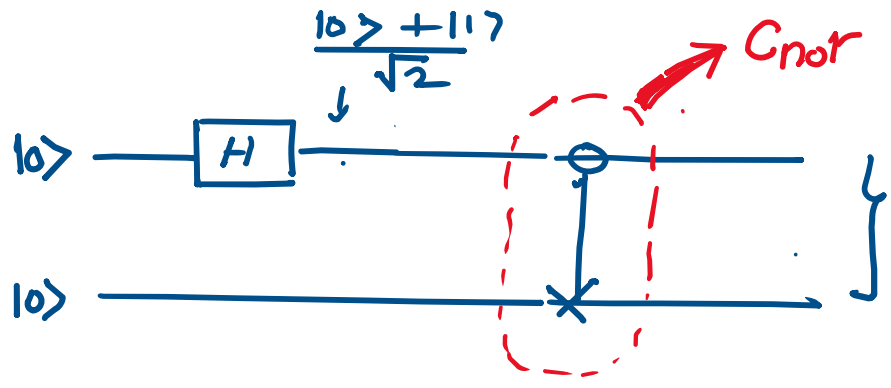
$C_{not}(|00\rangle) = |00\rangle + 0|01\rangle + 0|10\rangle + 0|11\rangle$

$C_{not}(|01\rangle) = 0|00\rangle + |01\rangle + 0|10\rangle + 0|11\rangle$

$C_{not}(|10\rangle) = 0|00\rangle + 0|01\rangle + 0|10\rangle + |11\rangle$

$C_{not}(|11\rangle) = 0|00\rangle + 0|01\rangle + |10\rangle + 0|11\rangle$

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



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

$|1\rangle$ $|1\rangle$

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

An entangled state

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

$= \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|10\rangle$

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

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

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

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

$a \neq 0, b \neq 0, c \neq 0, d \neq 0$

A CONTRADICTION.

Entangled states

- Consider the state

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

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

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

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

- $ac = \frac{1}{\sqrt{2}},\ ad = 0, bc = 0, bd = \frac{1}{\sqrt{2}}$
- $ad = 0 \Rightarrow a = 0\ or\ d = 0$. 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 Versions of Classical Computation

- Form reversible classical computations to quantum computations
  - Reversible quantum versions of simple classical gates
- Reversible implementations of classical gates
  - A naïve reversible implementation
  - A general construction
- A language for quadratic implementation
  - The basics
  - Functions

Quantum version of classical computation.

NOT XOR AND

x	$\bar{x}$
0	1
1	0

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

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

$$= |0\rangle\langle 1|0\rangle + |1\rangle\langle 0|0\rangle$$

$$= 0 \cdot |0\rangle + 1 \cdot |1\rangle$$

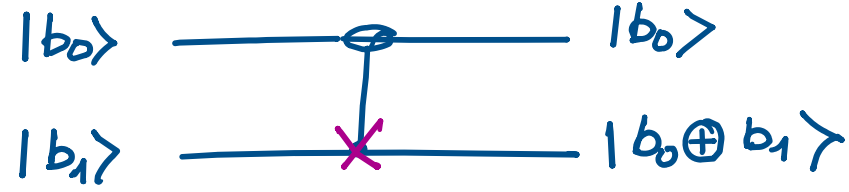
$$= |1\rangle$$

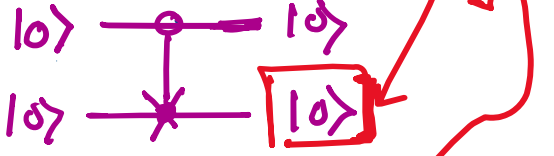
$$X|1\rangle = |0\rangle$$

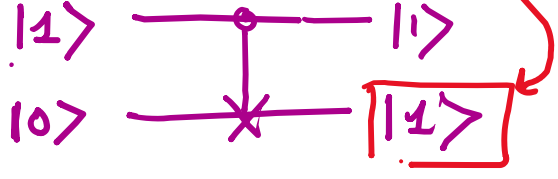
XOR

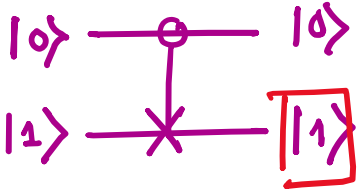
A reversible implementation of XOR quantum

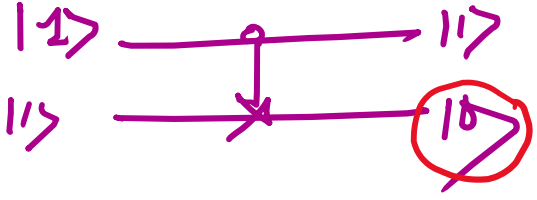
b_0	b_1	$b_0 \oplus b_1$
0	0	0
0	1	1
1	0	1
1	1	0











$\otimes \longrightarrow$ Tensor product

$\oplus \longrightarrow$ XOR

Quantum Versions of Classical Computation

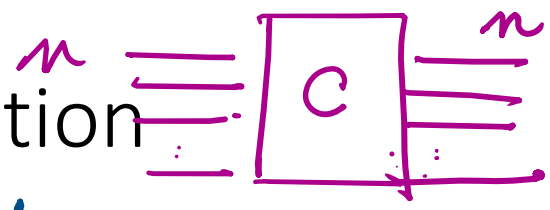
- Some example programs for arithmetic operations
  - Efficient implementation of AND
  - Efficient implementation of multiply controlled single-qubit transformations
  - In-place Addition
  - Modular Addition
  - Modular Multiplication
  - Modular Exponentiation

Quantum Versions of Classical Computation

- Any system of quantum transforms effects a unitary transformation U on the quantum system.
- A transformation U means the inverse transformation $U^{-1} = U^{\dagger}$ where $U^{\dagger}$ is the conjugate transpose of the transformation U.
- Suppose $|\psi\rangle$ is the initial quantum state. The transformed state is $U|\psi\rangle$.
- The initial quantum state $|\psi\rangle$ can be obtained from $U|\psi\rangle$ by applying the transformation $U^{\dagger}$

$$U^{\dagger}(U|\psi\rangle) = \left(U^{\dagger}U\right)|\psi\rangle$$

$x \longmapsto \pi(x)$



Classical reversible computation

π is a permutation.

$\mathbb{Z}_N = \{0, 1, 2, \cdots, N-1\}$

- Any classical reversible computation with n input and n output is a permutation of $N = 2^n$ bit strings. Let us denote such a permutation by π.
- It is a mapping from $\mathbb{Z}_N$ to $\mathbb{Z}_N$. $= \mathbb{Z}_4 = \{00, 01, 10, 11\}$ $= \{0, 1, 2, 3\}$ $= \{q_0, q_1, q_2, q_3\}$
- The corresponding quantum transformation is

$$U_\pi : \sum_{x=0}^{N-1} a_x |x\rangle \mapsto \sum_{x=0}^{N-1} a_x |\pi(x)\rangle$$

- The transformation π is unitary since it simply reorders standard basis elements.

$|0\rangle \mapsto |0\rangle$
$|1\rangle \mapsto |01\rangle$
$|2\rangle \mapsto |10\rangle$
$|3\rangle \mapsto |11\rangle$

00 0 $\pi(0)$
01 1 $\pi(1)$
10 2 $\pi(2)$
11 3 $\pi(3)$

Classical irreversible computations

- Any classical computation on n input and m output bits defines a function

$$\begin{bmatrix} f: \mathbb{Z}_N \to \mathbb{Z}_M \\ x \mapsto f(x) \end{bmatrix}$$

where $N = 2^n$ and $M = 2^m$.

- Such a function can be extended to a reversible function with $n + m$ bit input and output, $\pi_f: \mathbb{Z}_L \to \mathbb{Z}_L$ where $L = 2^{n+m}$ defined by

$$(x, y) \mapsto \big(x, y \oplus f(x)\big)$$

- The unitary transformation corresponding to π_f is U_f.

$\pi_f : (x, y) \longmapsto (x, y \oplus f(x))$

$f : \{0,1\}^n \to \{0,1\}^n$

$(x', y') \longmapsto (x', y' \oplus f(x'))$

$(x, y) = (x', y')$

$(x, y \oplus f(x)) = (x', y' \oplus f(x'))$

$x = x' \Rightarrow f(x) = f(x')$

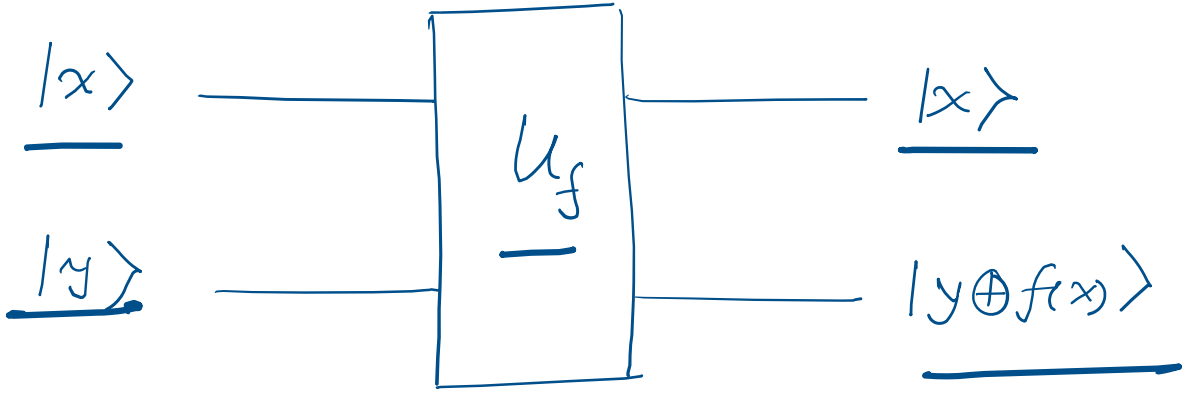
$y \oplus f(x) = y' \oplus f(x')$

$= y' \oplus f(x)$

$\Rightarrow \underline{y = y'}$

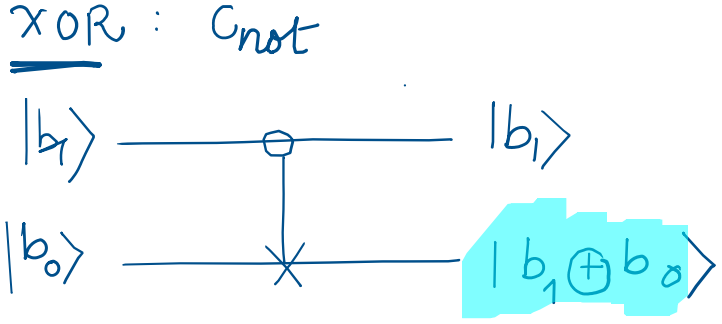
A graphical representation of U_f

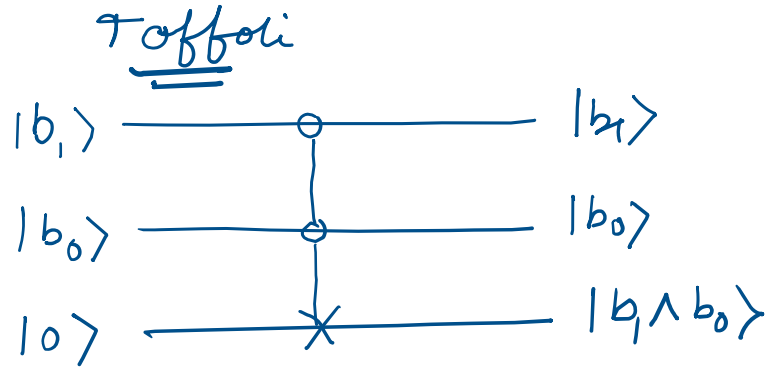
- $U_f: |x, y\rangle \mapsto |x, y \oplus f(x)\rangle$



Reversible and quantum versions of simple classical gates

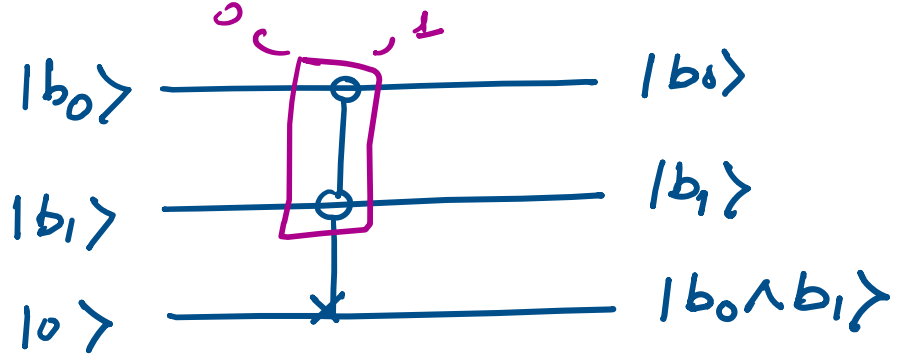
- NOT: $X = |0\rangle\langle 1| + |1\rangle\langle 0|$
- XOR: The controlled not gate, $C_{not} = \Lambda_1 X$
- AND: The three-bit controlled-controlled-not gate, or Toffoli gate $T = \Lambda_2 X$





$b_1 \oplus b_0$

Quantum version Classical AND gate

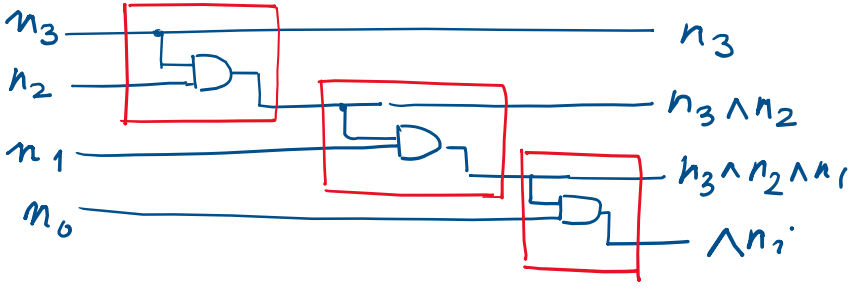


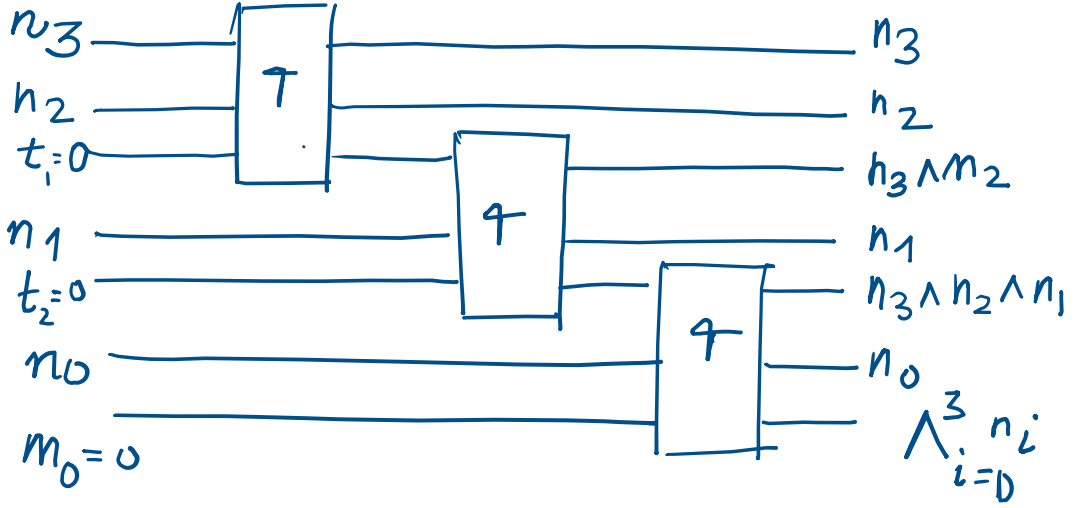
$$f(b_0, b_1) = b_0 \wedge b_1$$

$$|y\rangle \longrightarrow |y \oplus f(b_0, b_1)\rangle$$

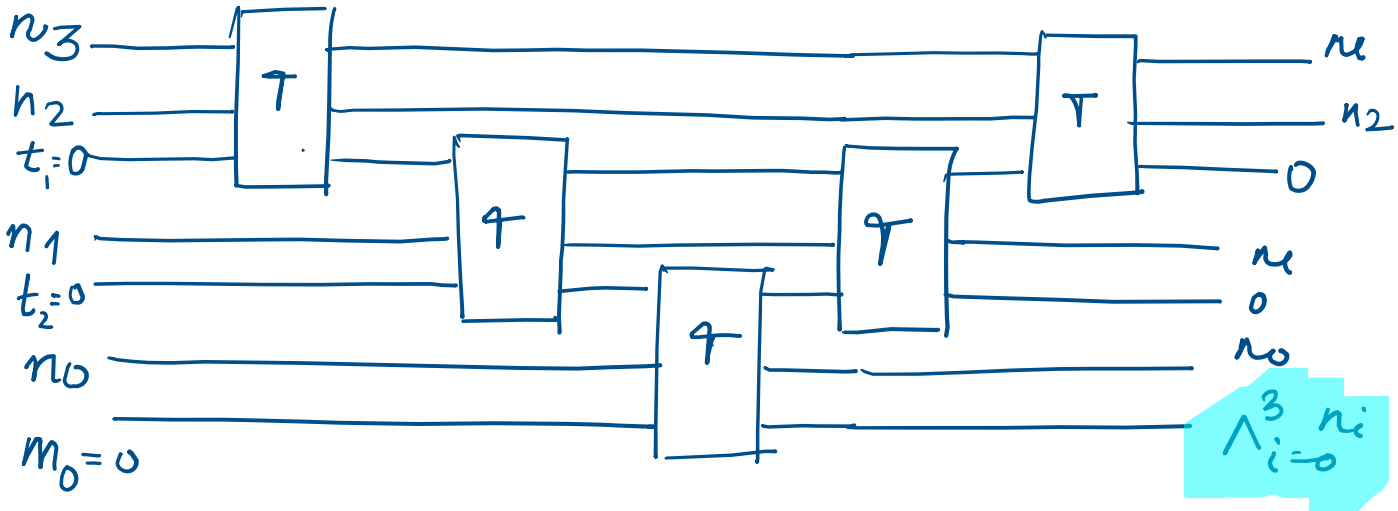
y	b_0	b_1	$b_0 \wedge b_1$
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	1
1	0	1	1
1	1	0	1
1	1	1	0

Reversible implementation.





Reversible classical circuit for four-bit conjunction.



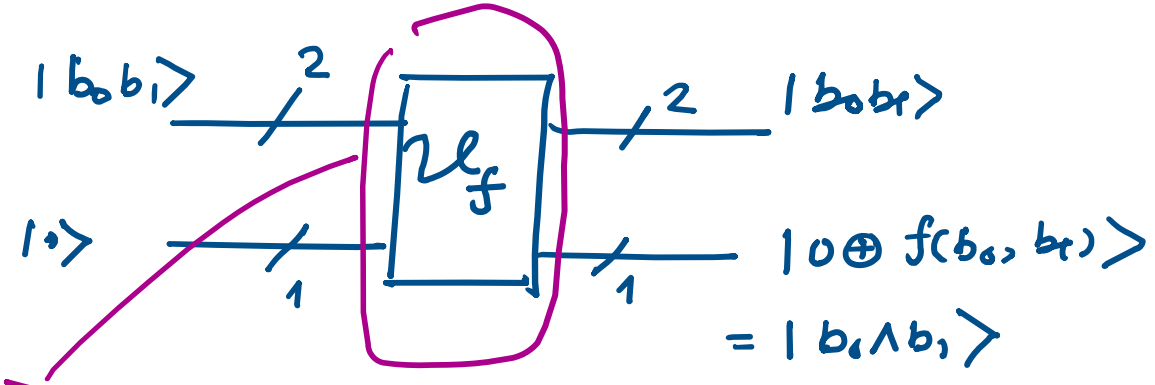
Reversible circuit that reclaims temporary bits.

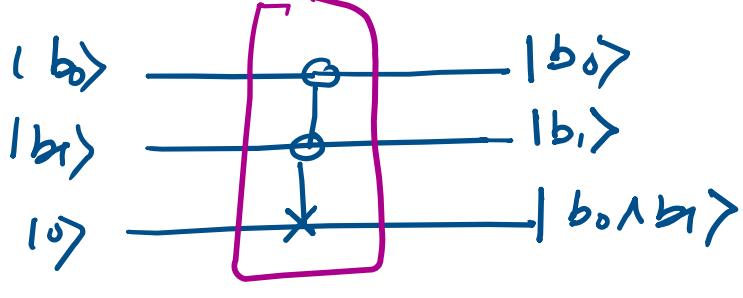
$n_0 \wedge n_1 \wedge n_2 \wedge n_3$

Quantum Implementation of Boolean functions

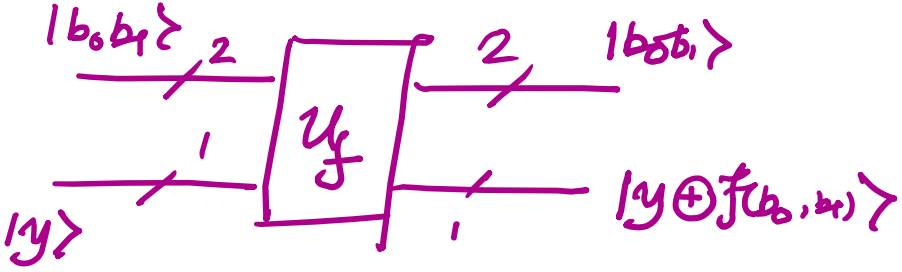
b_0	b_1	$b_0 \wedge b_1$
0	0	0
0	1	0
1	0	0
1	1	1

$f(b_0, b_1) = b_0 \wedge b_1$





Toffoli gate



Quantum implementation of a 2-variable Boolean function

- Let $f: \{0,1\}^2 \to \{0,1\}$ be a 2-variable Boolean function

- The quantum implementation of f is

$$U_f: |x\rangle|y\rangle \to |x\rangle|y \oplus f(x)\rangle$$

- $x = x_1 x_0$ where $x_1, x_0 \in \{0,1\}$ and $y \in \{0,1\}$

x_0	x_1	$f(x_0, x_1)$
0	0	$f(00)$
0	1	$f(01)$
1	0	$f(10)$
1	1	$f(11)$

Quantum implementation of a function

$x_0 x_1$

- $U_f : |x\rangle|y\rangle \mapsto |x\rangle|y \oplus f(x)\rangle$
- The effect of U_f on the computational basis is

$|000\rangle \longmapsto |000\rangle$ $|001\rangle \longleftrightarrow |001\rangle$
$|010\rangle \longleftrightarrow |011\rangle$ $|011\rangle \longmapsto |010\rangle$
$|100\rangle \longleftrightarrow |101\rangle$ $|101\rangle \longmapsto |100\rangle$
$|110\rangle \longleftrightarrow |110\rangle$ $|111\rangle \longmapsto |111\rangle$

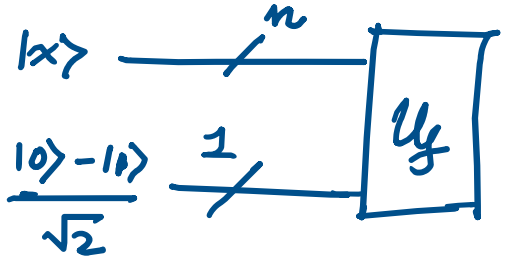
x_0	x_1	$f(x_0, x_1)$
0	0	0
0	1	1
1	0	1
1	1	0

$|00\rangle|0\rangle \mapsto |00\rangle|0 \oplus f(00)\rangle = |00\rangle|0 \oplus 0\rangle = |000\rangle$
$|01\rangle|0\rangle \mapsto |01\rangle|0 \oplus f(01)\rangle = |01\rangle|0 \oplus f(01)\rangle = |011\rangle$
$|10\rangle|0\rangle \mapsto |10\rangle|0 \oplus f(10)\rangle = |10\rangle|0 \oplus f(10)\rangle = |101\rangle$
$|11\rangle|0\rangle \mapsto |11\rangle|0 \oplus f(11)\rangle = |11\rangle|0 \oplus f(11)\rangle = |110\rangle$
$|00\rangle|1\rangle \mapsto |00\rangle|1 \oplus f(00)\rangle = |00\rangle|1 \oplus f(00)\rangle = |001\rangle$
$|01\rangle|1\rangle \mapsto |01\rangle|1 \oplus f(01)\rangle = |01\rangle|1 \oplus 1\rangle = |010\rangle$
$|10\rangle|1\rangle \mapsto |10\rangle|1 \oplus f(10)\rangle = |10\rangle|1 \oplus 1\rangle = |100\rangle$
$|11\rangle|1\rangle \mapsto |11\rangle|1 \oplus f(11)\rangle = |11\rangle|1 \oplus 0\rangle = |111\rangle$

$(\mathbb{C}^2)^{\otimes 3}$

Quantum implementation of a function

- $U_f: |x\rangle|y\rangle \mapsto |x\rangle|y \oplus f(x)\rangle$ *(The bit oracle implementation)*
- Suppose $|y\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$



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

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

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

$f(x)=0$

$f(x)=1$

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

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

Quantum implementation of a function

- $U_f|x\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}} \xrightarrow{U_f} \frac{1}{\sqrt{2}}|x\rangle|f(x)\rangle - \frac{1}{\sqrt{2}}|x\rangle|1 \oplus f(x)\rangle$
- Suppose $f(x) = 0$
- $U_f|x\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}} \xrightarrow{U_f} \frac{1}{\sqrt{2}}|x\rangle|0\rangle - \frac{1}{\sqrt{2}}|x\rangle|1\rangle = |x\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}}$
- Suppose $f(x) = 1$
- $U_f|x\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}} \xrightarrow{U_f} \frac{1}{\sqrt{2}}|x\rangle|1\rangle - \frac{1}{\sqrt{2}}|x\rangle|0\rangle = |x\rangle\frac{|1\rangle-|0\rangle}{\sqrt{2}}$

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

The quantum implementation

- $f(x) = 0: \; U_f|x\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}} \overset{U_f}{\rightarrow} \frac{1}{\sqrt{2}}|x\rangle|0\rangle - \frac{1}{\sqrt{2}}|x\rangle|1\rangle = |x\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}}$
- $f(x) = 1 \; : U_f|x\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}} \overset{U_f}{\rightarrow} \frac{1}{\sqrt{2}}|x\rangle|1\rangle - \frac{1}{\sqrt{2}}|x\rangle|0\rangle = (-1)|x\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}}$
- Therefore *(The phase oracle implementation)*

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

- Or, simply $U_f|x\rangle \overset{U_f}{\rightarrow} (-1)^{f(x)}|x\rangle$

$|y\rangle$

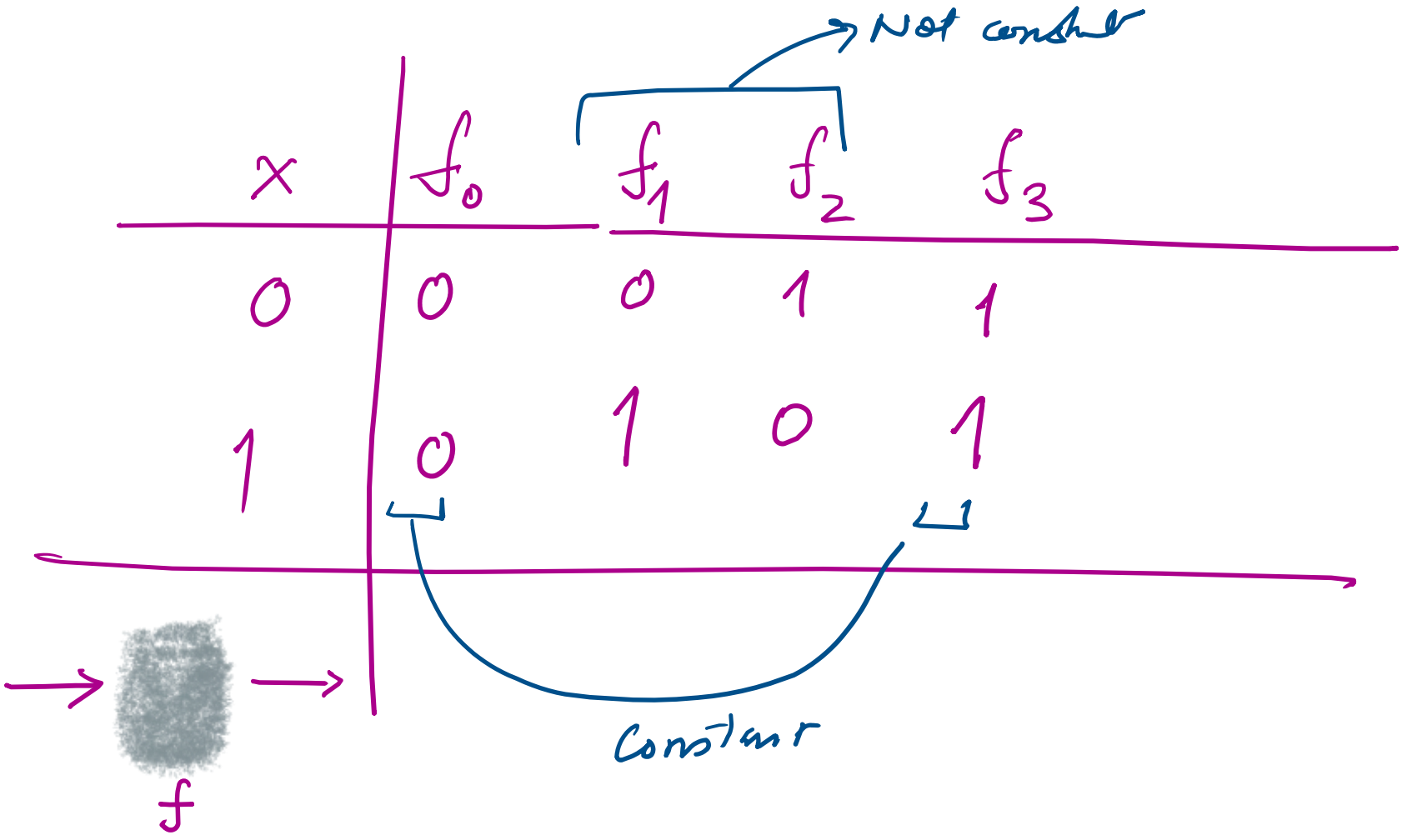
How to construct superposition states using Dirac's notaton

- The Hadamard transform H in the bra-ket form
  - $H = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|)$
- Consider the computational basis state
  - $|0\rangle$
  - $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|)|0\rangle$

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

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

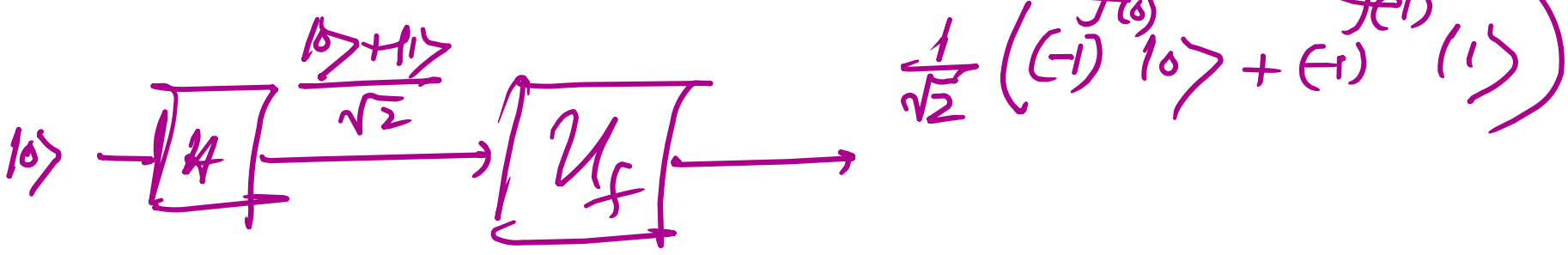
$$= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

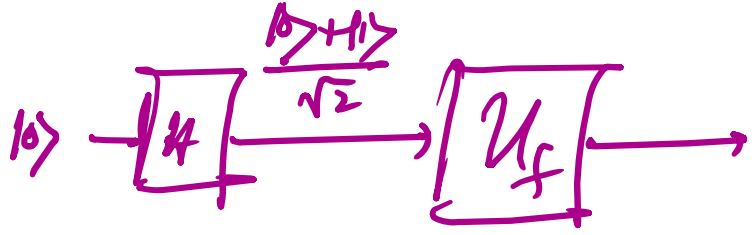

Not constant
x
f_0
f_1
f_2
f_3
0
0
0
1
1
1
0
1
0
1
Constant
f

$$|x\rangle \xrightarrow{U_f} (-1)^{f(x)}|x\rangle \qquad x \in \{0,1\}$$

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

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



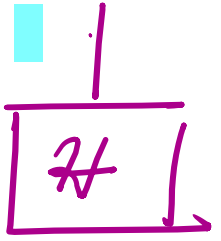


$$\frac{1}{\sqrt{2}}\left((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\right)$$

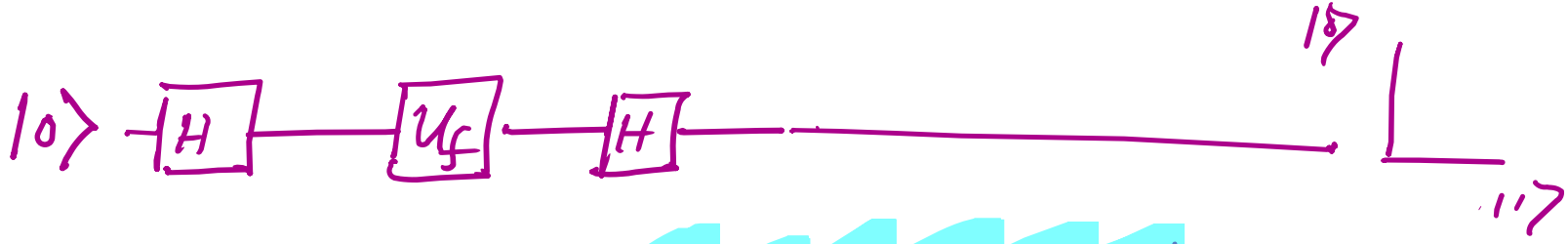
$$\frac{1}{\sqrt{2}}(-1)^{f(0)} H|0\rangle + \frac{1}{\sqrt{2}}(-1)^{f(1)} H|1\rangle)$$

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

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



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



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

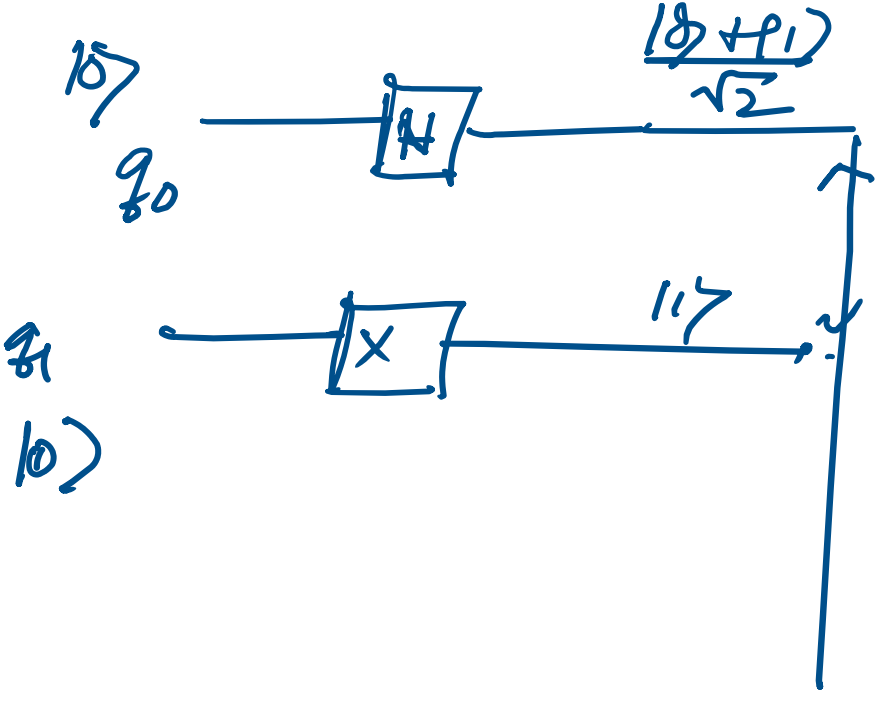
Suppose f is not constant.

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

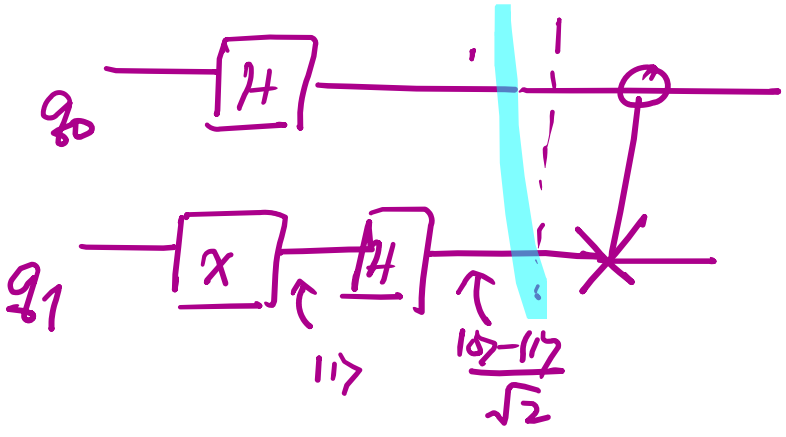
$$\| \quad 0$$

Suppose f is constant

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



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



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

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

$$= \frac{1}{2}\left[|00\rangle - |01\rangle + |10\rangle - |11\rangle\right]$$

Cnot

$$\frac{1}{2}\left[|00\rangle - |01\rangle + |11\rangle - |10\rangle\right]$$

Two-qubit superposition states

- $H \otimes H(|0\rangle \otimes |0\rangle) = H|0\rangle \otimes H|0\rangle$

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

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

Quantum parallelism

- Consider the two-qubit superposition state

$$|\psi\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

- Apply U_f on it

$$U_f|\psi\rangle = \frac{1}{2}\Big(U_f(|00\rangle) + U_f(|01\rangle) + U_f(|10\rangle) + U_f(|11\rangle)\Big)$$

$$= \frac{1}{2}\Big((-1)^{f(00)}|00\rangle + (-1)^{f(01)}|01\rangle + (-1)^{f(10)}|10\rangle + (-1)^{f(11)}|11\rangle\Big)$$

Quantum parallelism

- Consider the two-qubit superposition state

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

- Apply U_f on it

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

One small step

- $U_f|\psi\rangle = \frac{1}{\sqrt{2}}\Big(U_f(|0\rangle) + U_f(|1\rangle)\Big) = \frac{1}{\sqrt{2}}\Big((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\Big)$
- Apply H on the above state

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

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

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

The second small step

- $HU_f|\psi\rangle = \frac{1}{\sqrt{2}}\left((-1)^{f(0)}H|0\rangle + (-1)^{f(1)}H|1\rangle\right)$

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

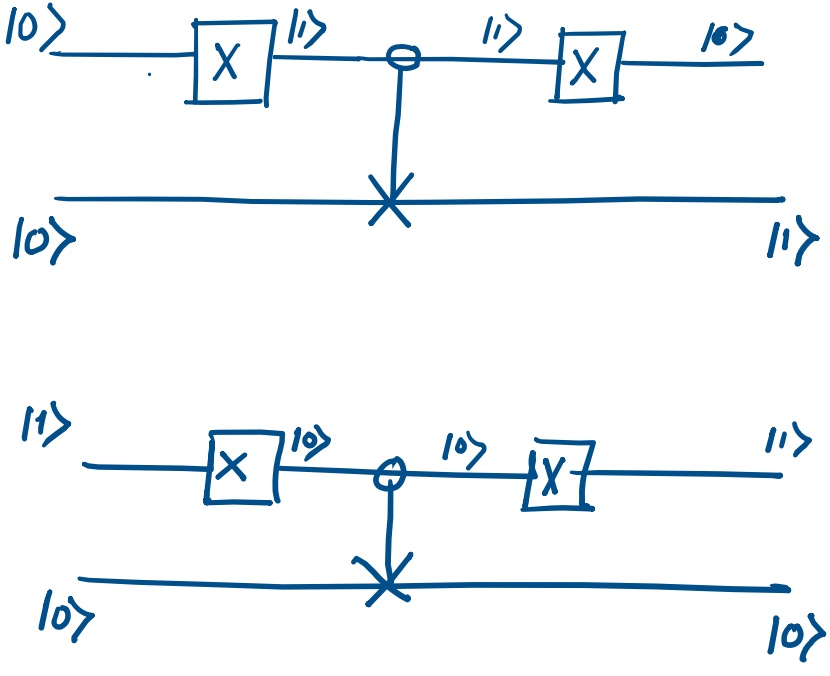
- If $f(0) = f(1)$, the measurement of $HU_f|\psi\rangle$ yields $\pm|0\rangle$
- If $f(0) \neq f(1)$, the measurement of $HU_f|\psi\rangle$ yields $\pm|1\rangle$

The decision step

- If $f(0) = f(1)$, the measurement of $HU_f|\psi\rangle$ yields $\pm|0\rangle$
- If $f(0) \neq f(1)$, the measurement of $HU_f|\psi\rangle$ yields $\pm|1\rangle$

- Therefore, based on a single measurement we can decide whether the function f is constant or not constant.
- There is no known classical algorithm that can achieve this feet.

Implementation of Boolean functions



The quantum circuit corresponding to the Boolean function

x	f
0	1
1	0

Quantum Algorithms
computing with superpositions

Introduction to quantum algorithms

- Computing with superpositions
  - The Walsh-Hadamard transformation
  - Quantum parallelism
- Notion of complexity
  - Query complexity
  - Communication complexity

Introduction to quantum algorithms

- A few simple quantum algorithms
  - Deutsch’s problem
  - Deutsch-Jozsa problem
  - Bernstein-Vazirani problem
  - Simon’s problem

- Distributed computation

Computing with superpositions

- We have seen that when a quantum computer performs classical computation, it uses computational basis states.

- True quantum algorithms typically employ quantum states that are superpositions of computational basis states.

- That is why we say that quantum algorithms perform ***computing with superpositions.***

How to construct superposition states

- The Hadamard transformation H
  - Matrix form: $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
  - $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ is the matrix corresponding to the state $|0\rangle$.
  - $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \frac{1}{\sqrt{2}}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$

How to construct superposition states using Dirac's notaton

- The Hadamard transform H in the bra-ket form
  - $H = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|)$
- Consider the computational basis state
  - $|0\rangle$
  - $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|)|0\rangle$

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

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

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

Two-qubit superposition states

- Let $|u\rangle$ and $|v\rangle$ be two single-qubit states. Construct the two-qubit state $|u\rangle \otimes |v\rangle$. It is also written as $|u\rangle|v\rangle$

- We can transform each of these qubit states by the Hadamard transformation independently. The resulting transformation is denoted by $H \otimes H$.

- $H \otimes H(|u\rangle \otimes |v\rangle) = H|u\rangle \otimes H|v\rangle$

Two-qubit superposition states

- $H \otimes H(|0\rangle \otimes |0\rangle) = H|0\rangle \otimes H|0\rangle$

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

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

Quantum implementation of a function

- Let $f: \{0,1\}^2 \rightarrow \{0,1\}$ be a 2-variable Boolean function

- The quantum implementation of f is

$$U_f: |x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle$$

- $x = x_1 x_0$ where $x_1, x_0 \in \{0,1\}$ and $y \in \{0,1\}$

Quantum implementation of a function

- $U_f : |x\rangle|y\rangle \mapsto |x\rangle|y \oplus f(x)\rangle$
- The effect of U_f on the computational basis is

$$
\begin{aligned}
|00\rangle|0\rangle &\mapsto |00\rangle|0 \oplus f(00)\rangle \\
|01\rangle|0\rangle &\mapsto |01\rangle|0 \oplus f(01)\rangle \\
|10\rangle|0\rangle &\mapsto |10\rangle|0 \oplus f(10)\rangle \\
|11\rangle|0\rangle &\mapsto |11\rangle|0 \oplus f(11)\rangle \\
|00\rangle|1\rangle &\mapsto |00\rangle|1 \oplus f(00)\rangle \\
|01\rangle|1\rangle &\mapsto |01\rangle|1 \oplus f(01)\rangle \\
|10\rangle|1\rangle &\mapsto |10\rangle|1 \oplus f(10)\rangle \\
|11\rangle|1\rangle &\mapsto |11\rangle|1 \oplus f(11)\rangle
\end{aligned}
$$

Quantum implementation of a function

- $U_f : |x\rangle|y\rangle \mapsto |x\rangle|y \oplus f(x)\rangle$
- Suppose $|y\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$
- $|x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}|x\rangle|0\rangle - \frac{1}{\sqrt{2}}|x\rangle|1\rangle$

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

Quantum implementation of a function

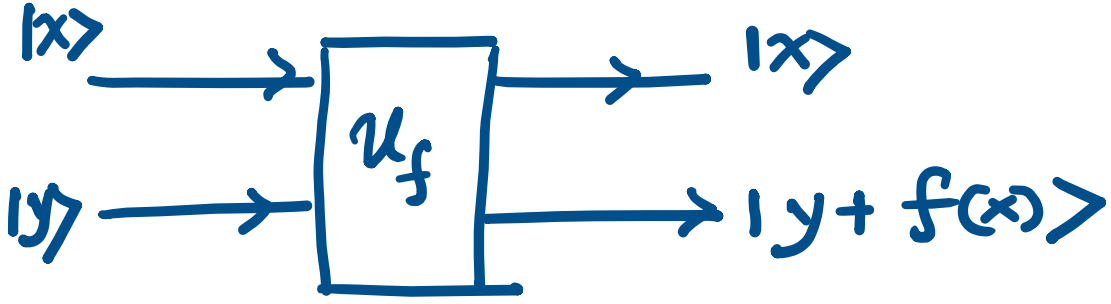
- $U_f|x\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}} \overset{U_f}{\rightarrow} \frac{1}{\sqrt{2}}|x\rangle|f(x)\rangle - \frac{1}{\sqrt{2}}|x\rangle|1 \oplus f(x)\rangle$
- Suppose $f(x) = 0$
- $U_f|x\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}} \overset{U_f}{\rightarrow} \frac{1}{\sqrt{2}}|x\rangle|0\rangle - \frac{1}{\sqrt{2}}|x\rangle|1\rangle = |x\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}}$
- Suppose $f(x) = 1$
- $U_f|x\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}} \overset{U_f}{\rightarrow} \frac{1}{\sqrt{2}}|x\rangle|1\rangle - \frac{1}{\sqrt{2}}|x\rangle|0\rangle = |x\rangle\frac{|1\rangle-|0\rangle}{\sqrt{2}}$

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

Creating an equal superposition

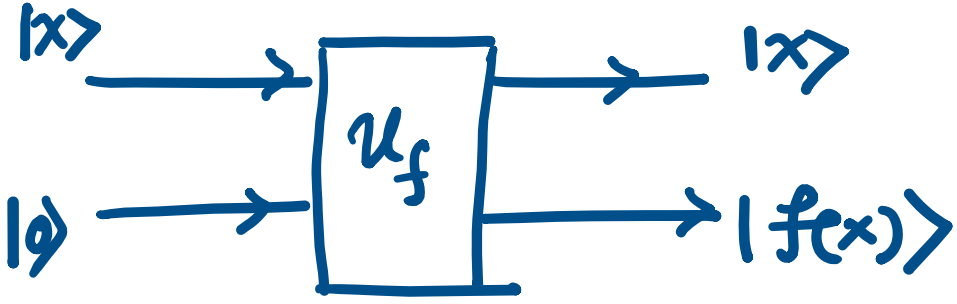
Boolean functions

- 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:

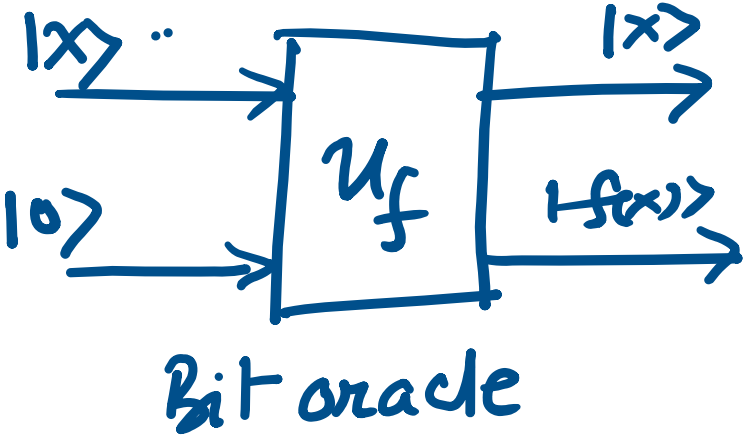


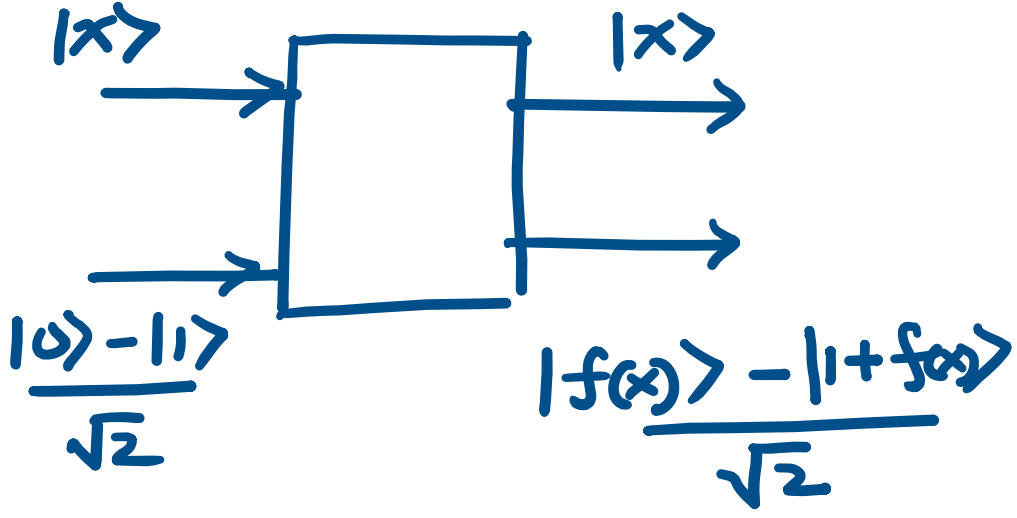
Boolean functions

- 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





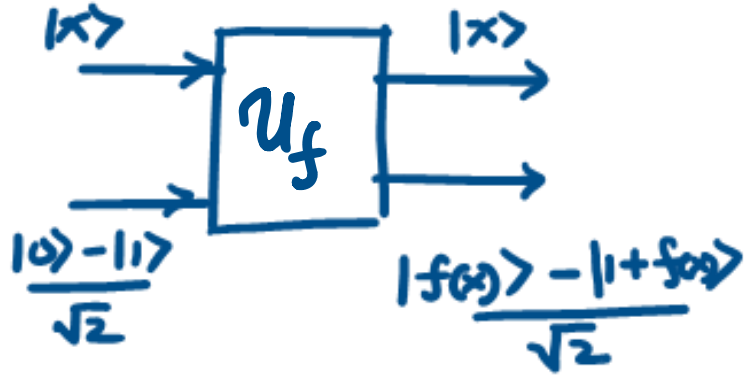
Bit oracle to phase oracle

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

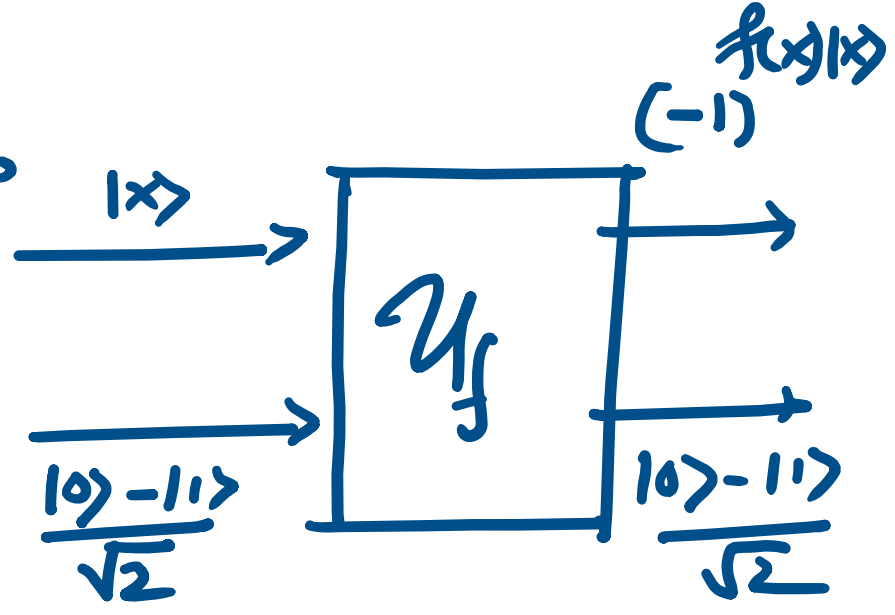
$$= (-1)^{f(x)} \frac{(|0\rangle - |1\rangle)}{\sqrt{2}}$$

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

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



So



Deutsch Algorithm

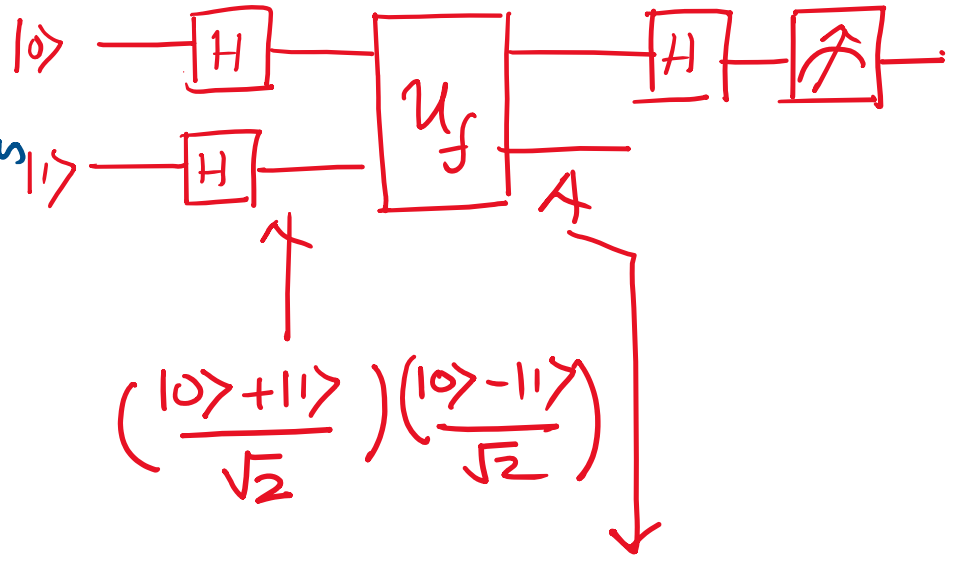
Consider Boolean functions in 1-variable. There are 4 such functions namely

x	f_0
0	0
1	0

x	f_1
0	0
1	1

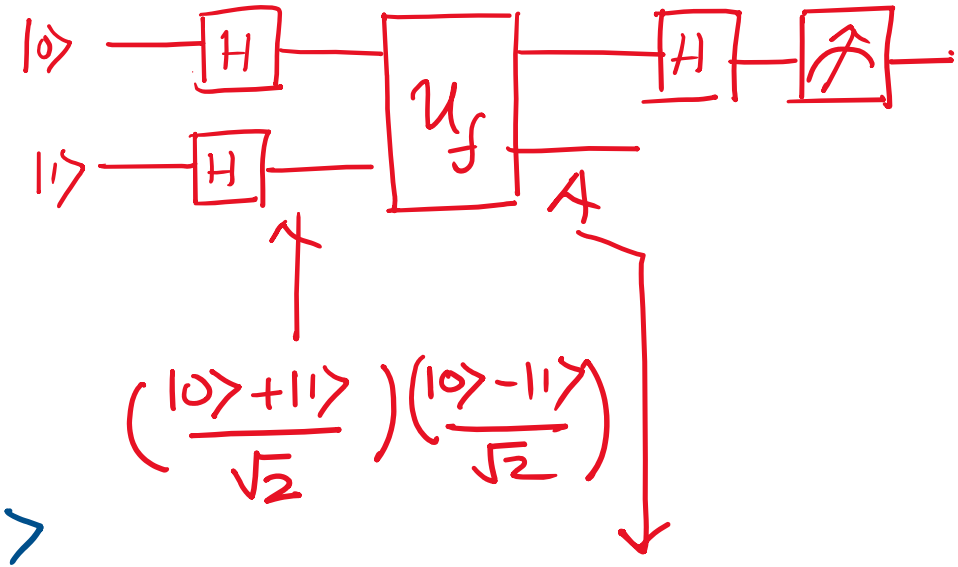
x	f_2
0	1
1	0

x	f_3
0	1
1	1



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

Deutsch Algorithm



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

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

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

So, the combined state is

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

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

Deutsch Algorithm

After the transformation the quantum state is

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

Let us measure the first qubit.

If $f = f_0$ or f_3 we will observe $|0\rangle$

If $f = f_1$ or f_2 we will observe $|1\rangle$.

Deutsch Algorithm

- So, with a single query on a quantum computer we can decide whether f is constant or non-constant.

- We know of no classical algorithm that can achieve this.

Deutsch Algorithm ⟶ Deutsch-Jozsa Algorithm.

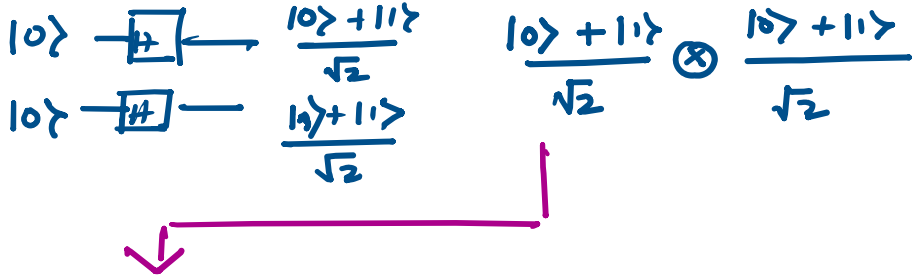
Deutsch-Jozsa Problem

* Prepare an n-qubit state with equal superposition

* Convert U_f to the phase oracle model.

$$|x\rangle|y\rangle \xmapsto{U_f} |x\rangle|y \oplus f(x)\rangle$$

$$|x\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) \xmapsto{U_f} (-1)^{f(x)}|x\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$



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

By definición

$$(H\otimes H)(|0\rangle\otimes|0\rangle) = H|0\rangle\otimes H|0\rangle$$

$$(H\otimes I)(|0\rangle\otimes|0\rangle) = H|0\rangle\otimes I|0\rangle$$

$$= H|0\rangle\otimes|0\rangle$$

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

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

$$= \frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle + |11\rangle\right)$$

($|00\rangle \to 0_2$, $|01\rangle \to 1_2$, $|10\rangle \to 2_2$, $|11\rangle \to 3_2$)

$$= \frac{1}{2}(|0\rangle + |1\rangle + |2\rangle + |3\rangle)$$

$$= \frac{1}{2}\sum_{i=0}^{2^2-1}|i\rangle$$

From 2 to n qubits

$$\underbrace{|0\rangle \otimes |0\rangle \otimes \cdots \otimes |0\rangle}_{n} = \underbrace{|0 \cdots 0\rangle}_{n} = |0_n\rangle$$

$$H^{\otimes n}|0_n\rangle = \overset{n}{H|0\rangle \otimes H|0\rangle \otimes \cdots \otimes H|0\rangle}$$

$$= \left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\cdots\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right) \quad n \text{ terms.}$$

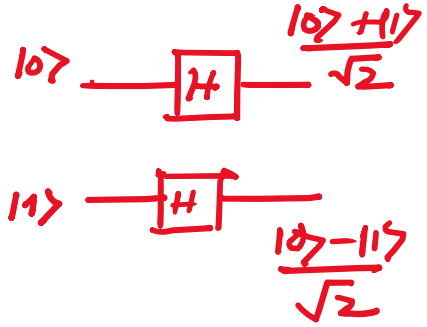
$$= \frac{1}{(\sqrt{2})^n}(|0\rangle+|1\rangle)(|0\rangle+|1\rangle)\cdots(|0\rangle+|1\rangle)$$

$$= 2^{-n/2} \sum_{i=0}^{2^n-1} |i\rangle$$

$(H \otimes H)(|0\rangle \otimes |0\rangle)$

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

$(H \otimes H)(|0\rangle \otimes |1\rangle) \rightarrow |01\rangle$



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

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

$= \frac{1}{2}\left((-1)^{(0,1)\cdot(0,0)}|00\rangle + (-1)^{(0,1)(0,1)}|01\rangle + (-1)^{(0,1)(1,0)}|10\rangle + (-1)^{(1,1)\cdot(1,1)}|11\rangle\right)$

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

Deutsch-Jozsa Algorithm

$\mathbb{Z}_{2^n}$ → The set of all integers modulo 2^n. $\{0, 1, 2, \ldots, 2^n - 1\}$

- David Deutsch and Richard Jozsa $\{\underbrace{00\ldots0}_{n}, \underbrace{00\ldots1}_{n}, \underbrace{00\ldots10}_{n} \ldots \underbrace{11\ldots1}_{n}\}$
- Deutsch-Jozsa Problem:

  A function f is balanced if an equal number of input values to the function return 0 and 1. — $\{0,1\}$

- *Given a function $f : \mathbb{Z}_{2^n} \to \mathbb{Z}_2$ that is known to be either constant or balanced, and a quantum oracle $U_f : |x\rangle|y\rangle \mapsto |x\rangle|y \oplus f(x)\rangle$ for f, determine whether the function f is constant or balanced.*

  n-variable functions that are constant

  n-variable balanced functions.

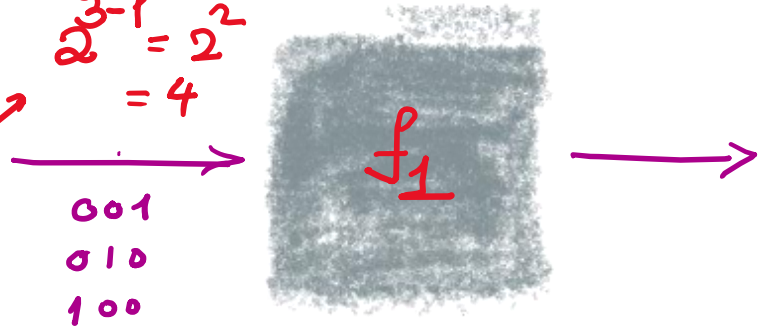
x_0	x_1	x_2	f_0	f_1	f_1'
0	0	0	1	0	1
0	0	1	1	1	1
0	1	0	1	1	1
0	1	1	1	0	1
1	0	0	1	1	0
1	0	1	1	0	0
1	1	0	1	0	0
1	1	1	1	1	0

f_0 is a constant function

f_1 is a balance function.

$$Q = 2^{n-1} + 1$$

$2^{3-1} = 2^2 = 4$



001
010
100
111
001

$f_0(000) = 1$

$f_1(000) = 0$

Multiple qubit superposition states

- If $x = x_{n-1}x_{n-2}\cdots x_2x_1x_0$ where $x_i \in \{0, 1\}$. This is a computational basis vector.

- The effect of applying the Hadamard transform H on each qubit of $|x\rangle$ is

$$H^{\otimes n}|x\rangle = H \otimes H \otimes \cdots \otimes H(|x_{n-1}x_{n-2}\cdots x_2x_1x_0\rangle)$$
$$= H|x_{n-1}\rangle \otimes H|x_{n-2}\rangle \otimes \cdots \otimes H|x_1\rangle \otimes H|x_0\rangle$$

Creating equal superposition

- $H^{\otimes n}|0_n\rangle = H \otimes H \otimes \cdots \otimes H(|000\cdots 0\rangle)$

$$= H|0\rangle \otimes H|0\rangle \otimes \cdots \otimes H|0\rangle \otimes H|0\rangle$$

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

$$= \frac{1}{2^{\frac{n}{2}}} \sum_{x_{n-1},\ldots,x_1,x_0 \in \{0,1\}} |x_{n-1}x_{n-2}\cdots x_1 x_0\rangle$$

Creating equal superposition

- $H^{\otimes n}|0_2\rangle = H \otimes H(|00\rangle) = H|0\rangle \otimes H|0\rangle$

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

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

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

Creating equal superpositions

- $H^{\otimes n}|0_3\rangle = H \otimes H(|000\rangle) = H|0\rangle \otimes H|0\rangle \otimes H|0\rangle$

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

$$= \frac{1}{2^{\frac{3}{2}}}(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)$$

$$= \frac{1}{2^{\frac{3}{2}}}(|0\rangle|0\rangle|0\rangle + |0\rangle|0\rangle|1\rangle + |0\rangle|1\rangle|0\rangle + |0\rangle|1\rangle|1\rangle + |1\rangle|0\rangle|0\rangle + |1\rangle|0\rangle|1\rangle + |1\rangle|1\rangle|0\rangle + |1\rangle|1\rangle|1\rangle)$$

Creating equal superposition

- $H^{\otimes n}|01\rangle = H \otimes H(|01\rangle) = H|0\rangle \otimes H|1\rangle$

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

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

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

$$= \frac{1}{2}\left((-1)^{(0,1)\cdot(0,0)}|0\rangle|0\rangle + (-1)^{(0,1)\cdot(0,1)}|0\rangle|1\rangle + (-1)^{(0,1)\cdot(1,0)}|1\rangle|0\rangle + (-1)^{(0,1)\cdot(1,1)}|1\rangle|1\rangle\right)$$

Creating equal superposition

- $H^{\otimes n}|01\rangle = H \otimes H(|01\rangle) = H|0\rangle \otimes H|1\rangle$

$$= \frac{1}{2}\Big((-1)^{(0,1)\cdot(0,0)}|0\rangle|0\rangle + (-1)^{(0,1)\cdot(0,1)}|0\rangle|1\rangle + (-1)^{(0,1)\cdot(1,0)}|1\rangle|0\rangle$$

$$+ (-1)^{(0,1)\cdot(1,1)}|1\rangle|1\rangle\Big)$$

$$H \otimes H\,|1_n\rangle = \frac{1}{2}\big((-1)^{1\cdot 0}|0\rangle + (-1)^{1\cdot 1}|1\rangle + (-1)^{1\cdot 2}|2\rangle + (-1)^{1\cdot 3}|3\rangle\big)$$

Deutsch-Jozsa Algorithm

- $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} (-1)^{f(i)} \, |i\rangle$
- $|\phi\rangle = \frac{1}{N} \sum_{i=0}^{N-1} \left((-1)^{f(i)} \sum_{j=0}^{N-1} (-1)^{i \cdot j} \, |j\rangle \right)$

$$= \frac{1}{N} \sum_{j=0}^{N-1} \left(\sum_{i=0}^{N-1} (-1)^{f(i)+i \cdot j} \right) |j\rangle$$

- For $j = 0$, we have

$$\sum_{i=0}^{N-1} (-1)^{f(i)+i \cdot 0} = \sum_{i=0}^{N-1} (-1)^{f(i)} = \begin{cases} 0 \; if \; f \; is \; balance \\ 2^n = N \quad if \; f \; is \; constant \end{cases}$$

Creating equal superpositions

- $H^{\otimes n}|2_3\rangle = H \otimes H(|010\rangle) = H|0\rangle \otimes H|1\rangle \otimes H|0\rangle$

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

$$= \frac{1}{2^{\frac{3}{2}}}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)(|0\rangle + |1\rangle)$$

$$= \frac{1}{2^{\frac{3}{2}}}(|0\rangle|0\rangle|0\rangle + |0\rangle|0\rangle|1\rangle - |0\rangle|1\rangle|0\rangle - |0\rangle|1\rangle|1\rangle + |1\rangle|0\rangle|0\rangle + |1\rangle|0\rangle|1\rangle - |1\rangle|1\rangle|0\rangle - |1\rangle|1\rangle|1\rangle)$$

$$= \frac{1}{2^{\frac{3}{2}}}\left((-1)^{2\cdot 0}|0\rangle + (-1)^{2\cdot 1}|1\rangle + (-1)^{2\cdot 2}|2\rangle + (-1)^{2\cdot 3}|3\rangle + (-1)^{2\cdot 4}|4\rangle + (-1)^{2\cdot 5}|5\rangle + (-1)^{2\cdot 6}|6\rangle + (-1)^{2\cdot 7}|7\rangle\right)$$

$H^{\otimes n}|i\rangle = 2^{-n/2}\sum_{j=0}^{2^n-1}(-1)^{i\cdot j}|j\rangle$

$0 \le i \le 2^n - 1$

$010 \longmapsto 2$

$$H^{\otimes n}|i\rangle = 2^{-n/2} \sum_{j=0}^{2^n-1} (-1)^{i \cdot j} |j\rangle$$

$0 \le i < 2^n - 1$

0

$$H^{\otimes n}|0\rangle = 2^{-n/2} \sum_{i=0}^{2^n-1} |i\rangle$$

$$U_f(H^{\otimes n}|0\rangle) = U_f\left(2^{-n/2} \sum_{i=0}^{2^n-1} |i\rangle\right) = 2^{-n/2} \sum_{i=0}^{2^n-1} U_f|i\rangle$$

$$= 2^{-n/2} \sum_{i=0}^{2^n-1} (-1)^{f(i)} |i\rangle$$

$$U_f(H^{\otimes n}|0\rangle) = 2^{-n/2} \sum_{i=0}^{2^n-1} (-1)^{f(i)} |i\rangle$$

$$U_f\left(H^{\otimes n}|0\rangle\right) = 2^{-n/2}\sum_{i=0}^{2^n-1}(-1)^{f(i)}|i\rangle$$

$$H^{\otimes n}\left(U_f\left(H^{\otimes n}|0\rangle\right)\right) = H^{\otimes n}\left(2^{-n/2}\sum_{i=0}^{2^n-1}(-1)^{f(i)}|i\rangle\right)$$

$$= 2^{-n/2}\sum_{i=0}^{2^n-1}(-1)^{f(i)}H^{\otimes n}|i\rangle = 2^{-n/2}\sum_{i=0}^{2^n-1}(-1)^{f(i)}\cdot 2^{-n/2}\sum_{j=0}^{2^n-1}(-1)^{i\cdot j}|j\rangle$$

$$= 2^{-n}\sum_{i=0}^{2^n-1}(-1)^{f(i)}\sum_{j=0}^{2^n-1}(-1)^{i\cdot j}|j\rangle = 2^{-n}\sum_{j=0}^{2^n-1}\left(\sum_{i=0}^{2^n-1}(-1)^{f(i)+i\cdot j}\right)|j\rangle$$

$$H^{\otimes n}\left(U_f\left(H^{\otimes n}|0\rangle\right)\right)$$

$$= 2^{-n} \sum_{j=0}^{2^n-1} \left(\sum_{i=0}^{2^n-1} (-1)^{f(i)+i\cdot j} \right) |j\rangle$$

$$\sum_{i=0}^{2^n-1} (-1)^{f(i)}$$

- 0 if f is balanced
- 2^n
- 1 if f is constant.

$|0\ldots0\rangle$ (n)

The function f is either balanced or constant

Shor’s Algorithm

Peter Shor 1994

- Peter Shor, in 1994, proposed a bounded probability polynomial time integer factorization algorithm.
- Suppose that the input integer is M.
- The number of bits required to store M is $m = \lceil \log M \rceil$.
- The best known classical algorithm to solve is problem uses the number field sieve.
- The complexity of the number field sieve algorithm is $O\left(\exp\left(m^{1/3}\right)\right)$.

Classical reduction to period finding

- The *order* of an integer a modulo M is the smallest integer $r > 0$ such that $a^r = 1 \bmod M$.
- If no such integer exists then the order is said to be infinite.
- Two integers are said to be relatively prime if they share no common factor.
- If a and M are relatively prime then a has a finite order modulo M.

Classical reduction to period finding

- Define a function $f: \mathbb{Z} \to \mathbb{Z}$ by $f(k) = a^k \bmod M$.
- We know that $a^r = 1 \bmod M$.
- $f(k+r) = a^{k+r} \bmod M = a^k \times a^r \bmod M = a^k \bmod M$.
- f has a period r
- Let r be a positive even integer
- $\left(a^{r/2} + 1\right)\left(a^{r/2} - 1\right) = 0 \bmod M$
- Both $a^{r/2} + 1$ and $a^{r/2} - 1$ are likely to have a proper common factor with M.

A randomized classical algorithm

- Randomly choose an integer a and determine the period r of

$$f(k) = a^k \bmod M$$

- If r is even, use the Euclidean algorithm to compute efficiently the greatest common divisor of $a^{r/2} + 1$ and M
- Repeat if necessary

The classical Fourier Transform

- Discrete Fourier transform

$$A: [0, \dots, N-1] \to \mathbb{C}$$

  defined by

$$A(x) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} a(k) \exp\left(2\pi\iota \frac{kx}{N}\right)$$

- The discrete Fourier transform is a linear transformation taking $\big(a(0), \dots, a(N-1)\big)^T$ to $\big(A(0), \dots, A(N-1)\big)^T$

The classical Fourier transformation

- $F: \big(a(0), \dots, a(N-1)\big)^T \rightarrow \big(A(0), \dots, A(N-1)\big)^T$
- $F = (F_{xk})_{N \times N}$ where $F_{xk} = \exp\left(2\pi\iota \frac{kx}{N}\right)$
- The values $A(0), A(1), \dots, A(N-1)$ are called the Fourier coefficients of a.

Fast Fourier Transform

- The fast Fourier transform is an efficient implementation of the discrete Fourier transform
- Let $N = 2^n$
- Let $\omega_{(n)} = \exp\left(\frac{2\pi\iota}{N}\right)$ be the Nth root of unity
- The matrix $F^{(n)}$ corresponding to the Fourier transform is

$$F^{(n)} = \left(\omega_{(n)}^{ij}\right)_{N\times N}$$

Fast Fourier transform

- The fast Fourier transform is an efficient implementation of the discrete Fourier transform.
- $F^{(k)}$ is the $2^k \times 2^k$ matrix for the 2^k-dimensional Fourier transform
- $I^{(k)}$ is the $2^k \times 2^k$ identity matrix.
- $D^{(k)}$ is the $2^k \times 2^k$ diagonal matrix with elements $\omega_{(k+1)}^{0}, \omega_{(k+1)}^{1}, \cdots, \omega_{(k+1)}^{2^k-1}$

Fast Fourier transform

- $R^{(k)}$ is the permutation defined by

$$R_{ij}^{(k)} = \begin{cases} 1 & \text{if } 2i = j \\ 1 \text{ if } 2\left(i - 2^k\right) + 1 = j \\ 0 & \text{otherwise} \end{cases}$$

Fast Fourier transform

- $U_F^{(k+1)} = \frac{1}{\sqrt{2}} \begin{pmatrix} I^{(k)} & D^{(k)} \\ I^{(k)} & -D^{(k)} \end{pmatrix} \begin{pmatrix} U_F^{(k)} & 0 \\ 0 & U_F^{(k)} \end{pmatrix} R^{(k+1)}$

- Where $U_F^{(1)}: |0\rangle \mapsto \frac{1}{\sqrt{2}} \sum_{x=0}^{1} e^{0} |x\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)$

$$|1\rangle \mapsto \frac{1}{\sqrt{2}} \sum_{x=0}^{1} e^{\pi \imath x} |x\rangle = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$$

The permutation matrix $R^{(k)}$

$$R_{ij}^{(k)} = \begin{cases} 1 \text{ if } & 2i = j \\ 1 \text{ if } & 2i - 2^k + 1 = j \\ 0 & \text{otherwise} \end{cases}$$

i	$2i$	$2i - 4 + 1$
0	0	-3
1	2	-1
2	4	1
3	6	3

$$R^{(2)} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

The recursive decomposition of $U_F^{(k+1)}$

- $U_F^{(k+1)} = \frac{1}{\sqrt{2}} \begin{pmatrix} I^{(k)} & D^{(k)} \\ I^{(k)} & -D^{(k)} \end{pmatrix} \begin{pmatrix} U_F^{(k)} & 0 \\ 0 & U_F^{(k)} \end{pmatrix} R^{(k+1)}$
- $R^{(k+1)} = \sum_{i=0}^{2^k-1} |i\rangle\langle 2i| + \left|i + 2^k\right\rangle\langle 2i+1|$
- $R^{(2)} = |0\rangle\langle 0| + |2\rangle\langle 1| + |1\rangle\langle 2| + |3\rangle\langle 3|$
- This permutation can be implemented using $k-1$ swap operations.

The recursive decomposition of $U_F^{(k+1)}$

- The transformation

$$\begin{pmatrix} U_F^{(k)} & 0 \\ 0 & U_F^{(k)} \end{pmatrix} = I \otimes U_F^{(k)}$$

- The above transformation can be implemented by recursively applying the quantum Fourier transform to qubits 0 through k.

Implementing $D^{(k)}$

- $D^{(k)}$ is the $2^k \times 2^k$ diagonal matrix with elements
$$\omega_{(k+1)}^{0}, \dots, \omega_{(k+1)}^{2^k-1}$$
- $D^{(k-1)}$ is the $2^{k-1} \times 2^{k-1}$ diagonal matrix with elements
$$\omega_{(k)}^{0}, \dots, \omega_{(k)}^{2^{k+1}-1}$$
- Claim:
$$D^{(k)} = D^{(k-1)} \otimes \begin{pmatrix} 1 & 0 \\ 0 & \omega_{(k+1)} \end{pmatrix}$$
- $D^{(k)}$ can be implemented using k single-qubit gates.

Implementing $\frac{1}{\sqrt{2}}\begin{pmatrix} I^{(k)} & D^{(k)} \\ I^{(k)} & -D^{(k)} \end{pmatrix}$

- $\frac{1}{\sqrt{2}}\begin{pmatrix} I^{(k)} & D^{(k)} \\ I^{(k)} & -D^{(k)} \end{pmatrix} = (H|0\rangle\langle 0|) \otimes I^{(k)} + (H|1\rangle\langle 1|) \otimes D^{(k)}$

$$= \left(H \otimes I^{(k)}\right)\left(|0\rangle\langle 0| \otimes I^{(k)} + |1\rangle\langle 1| \otimes D^{(k)}\right)$$

- This controlled version of $D^{(k)}$ can be implemented as a sequence of k two-qubit controlled gates that apply each of the single-qubit operations making up $D^{(k)}$ to bit i controlled by bit k.

Shor's Algorithms: the quantum core

- $f(x) = a^x \bmod M$ can be computed efficiently classically
- $U_f: |x\rangle|0\rangle \mapsto |x\rangle|f(x)\rangle$ has an efficient implementation
- Use quantum parallelism to obtain: $2^{-n/2} \sum_{x=0}^{2^n-1} |x\rangle\,|f(x)\rangle$
- Measuring the second register randomly returns a value u for $f(x)$ and the state becomes $C \sum_x g(x)|x\rangle|u\rangle$ where

$$g(x) = \begin{cases} 1 \text{ if } f(x) = u \\ 0 \text{ if } f(x) \neq u \end{cases}$$

Shor's Algorithms: the quantum core

- Applying the quantum Fourier transform to the first register

$$U_F\left(C\sum_x g(x)|x\rangle\right) = C'\sum_x G(C)|c\rangle$$

where

$$G(c) = \sum_x g(x)e^{\frac{2\pi\imath cx}{2^n}}$$

Shor's Algorithms: the quantum core

- $G(c) = \sum_{x=0}^{2^n-1} g(x)\, e^{\frac{2\pi \imath c x}{2^n}}$
- Suppose $g(x) = e^{-2\pi \imath \frac{ux}{2^n}}$ is a periodic function
- $G(c) = \sum_{x=0}^{2^n-1} e^{-\frac{2\pi \imath u x}{2^n}}\, e^{\frac{2\pi \imath c x}{2^n}} = \sum_{x=0}^{2^n-1} e^{\frac{2\pi \imath\,(c-u)x}{2^n}}$
- $G(c) = \begin{cases} 1 \text{ if } u = c \\ 0 \text{ if } u \neq c \end{cases}$
- $U_F(C \sum_x g(x)|x\rangle) = C' \sum_x G(C)|c\rangle$
- The measurement value gives u, hence $r \approx 2^n/u$.