CS6846 – Quantum Algorithms and Cryptography

Computation and No-Cloning

Instructor: Shweta Agrawal, IIT Madras
Email: shweta@cse.iitm.ac.in

What Operations can we do on Quantum States?

Phase Shifts: Changing material in double slit experiment might change phase of diffraction pattern. Represented by multiplying one of the amplitudes by $e^{i\theta}$, where θ is the angle by which the pattern is shifted

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

What Operations can we do on Quantum States?

Phase Shifts: Changing material in double slit experiment might change phase of diffraction pattern. Represented by multiplying one of the amplitudes by $e^{i\theta}$, where θ is the angle by which the pattern is shifted

$$\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right) \longrightarrow \left(\frac{|0\rangle+e^{i\theta}|1\rangle}{\sqrt{2}}\right).$$

Represent using matrix:

$$\underbrace{\begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix}}_{\text{operator}} \underbrace{\begin{bmatrix} \alpha \\ \beta \end{bmatrix}}_{\text{state}} = \begin{bmatrix} \alpha \\ e^{i\theta}\beta \end{bmatrix}.$$

Examples: If $\theta = \pi$, $e^{i\theta} = -1$.

$$\alpha|0\rangle + \beta|1\rangle \rightarrow \alpha|0\rangle - \beta|1\rangle$$

If $\theta = \frac{\pi}{2}$, $e^{i\theta} = i$

$$\alpha|0\rangle + \beta|1\rangle \rightarrow \alpha|0\rangle + i\beta|1\rangle.$$

What Operations can we do on Quantum States?

Bit Flips: $|0\rangle \longrightarrow |1\rangle$ and $|1\rangle \longrightarrow |0\rangle$.

What Operations can we do on Quantum States?

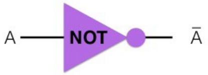
Bit Flips: $|0\rangle \longrightarrow |1\rangle$ and $|1\rangle \longrightarrow |0\rangle$.

Matrix Representation:

matrix for NOT

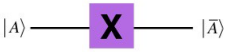
$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix}$$

Pauli X Matrix – computational NOT gate



A	Ā
0	1
1	0

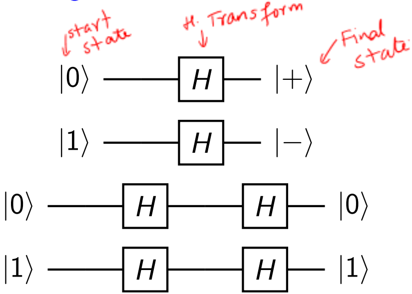
PAULI X GATE



$\|A\rangle$	$\|\bar{A}\rangle$
0	1
1	0

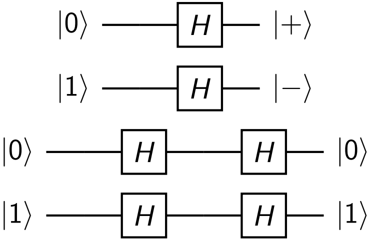
What Operations can we do on Quantum States?

Hadamard Transform: changes Standard to Hadamard Basis



What Operations can we do on Quantum States?

Hadamard Transform: changes Standard to Hadamard Basis

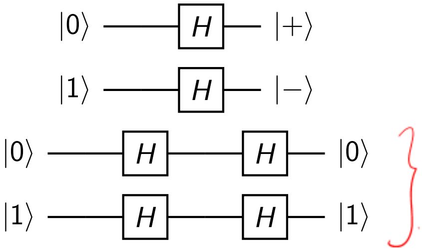


Matrix Representation: $\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$ $\underbrace{\begin{bmatrix}1\\0\end{bmatrix}}_{|0\rangle} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

$|+\rangle$

What Operations can we do on Quantum States?

Hadamard Transform: changes Standard to Hadamard Basis



Matrix Representation: $\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1 \\ 1 & -1\end{bmatrix}$

What happens when we multiply two Hadamard matrices?

Identity.

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

What Operations can we do on Quantum States?

Arbitrary Transforms

$$|0\rangle \longrightarrow U_{00}|0\rangle + U_{01}|1\rangle$$
$$|1\rangle \longrightarrow U_{10}|0\rangle + U_{11}|1\rangle$$

$U = \begin{bmatrix} U_{00} & U_{10} \\ U_{01} & U_{11} \end{bmatrix}$. , $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.

Now For any $|\psi\rangle$, $U|\psi\rangle$ is a valid qubit.

$U|\psi\rangle = \begin{bmatrix} U_{00}\alpha + U_{10}\beta \\ U_{01}\alpha + U_{11}\beta \end{bmatrix} = \phi$.

For being valid $|\phi\rangle^{\dagger}|\phi\rangle = 1$. , $(U|\psi\rangle)^{\dagger}(U|\psi\rangle) = 1$.

$\Rightarrow |\psi\rangle^{\dagger} \underbrace{U^{\dagger}U}_{M.} |\psi\rangle = 1$. , $\underbrace{(\alpha^* \ \beta^*) \begin{pmatrix} M_{00} & M_{10} \\ M_{01} & M_{11} \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix}}_{I.} = 1$.

We know that : $|\alpha|^2 + |\beta|^2 = 1$

Special Matrices

- Unitary: A matrix U which satisfies $U^\dagger U = \mathbb{I}$ is called a **unitary** matrix. Note that

$$U^\dagger U = \mathbb{I} \iff U^\dagger = U^{-1}$$

Special Matrices

- Unitary: A matrix U which satisfies $U^\dagger U = \mathbb{I}$ is called a **unitary** matrix. Note that

$$U^\dagger U = \mathbb{I} \iff U^\dagger = U^{-1}$$

- Hermitian: A matrix U is called **Hermitian** if $U = U^\dagger$.

Exercise: If U is unitary matrix then it preserves norm.

$$\|U\phi\|^2 = \langle U\phi | U\phi \rangle$$
$$= \langle \phi | \underbrace{U^\dagger U}_{I} \phi \rangle \quad \text{By linear algebra}$$
$$= \|\phi\|^2$$

(Any unitary matrix constitutes a valid operation on a qubit.)

Multiple Qubits: Partial Measurement

Let $|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$.

Multiple Qubits: Partial Measurement

Let $|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$.

Can perform partial measurement: measure only one of the two.

Multiple Qubits: Partial Measurement

Let $|\psi\rangle = \underline{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle} + \left(\alpha_{10}\cancel{|10\rangle} + \alpha_{11}\cancel{|11\rangle}\right)$.

Can perform partial measurement: measure only one of the two. What is probability of first qubit being $|0\rangle$? $|\alpha_{00}|^2 + |\alpha_{01}|^2$.

What remains?

Drop terms where first qubit is 1 and renormalize.

$\downarrow$

Post-measurement state: $|\Psi'\rangle = \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}$

Multiple Qubits: Entanglement

Consider the state

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

Entangled state

If measure first qubit → w.p. $\frac{1}{2}$, get 0

→ w.p. $\frac{1}{2}$ get 1.

Multiple Qubits: Entanglement

Consider the state

$$\left[|\text{EPR}\rangle = \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle \big) \right] = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Cannot be written as a tensor product of two qubits: why?

Assume otherwise.

$$|\psi_1\rangle \otimes |\psi_2\rangle = \begin{pmatrix} \alpha_1\alpha_2 \\ \alpha_1\beta_2 \\ \beta_1\alpha_2 \\ \beta_1\beta_2 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

contradiction

REPRESENT EPR as $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ Rank 2.

Entanglement

A system of two qubits $|\phi\rangle$ is entangled when it cannot be written as the tensor product of two qubits $|\phi_0\rangle$ and $|\phi_1\rangle$.

Multiple Qubits: Entanglement

Suppose we measure the first qubit. What do we get?

w.p. $\frac{1}{2} \rightarrow |0\rangle$

w.p. $\frac{1}{2} \rightarrow |1\rangle$.

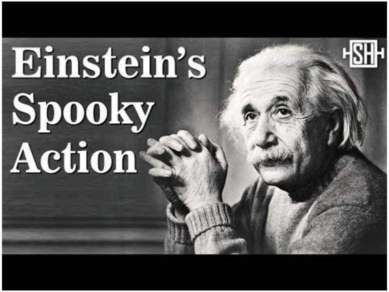
Now, suppose we measure the second qubit – what do we get?

Same as when I measured the first qubit.

Multiple Qubits: Entanglement

Spooky Action at a Distance!

Measuring the first tells us something about the second, no matter how far apart the qubits are – no speed-of-light delay!



No Cloning

(Weakened) No Cloning

There does not exist any unitary transformation U such that for all $|\Psi\rangle$, we have that

$$U\left(|\Psi\rangle \otimes |0\rangle\right) \rightarrow |\Psi\rangle \otimes |\Psi\rangle$$

Suppose that there does exist such U.

$$U(|0\rangle \otimes |0\rangle) = |00\rangle$$

$$U(|1\rangle \otimes |0\rangle) = |11\rangle$$

By linearity $U\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |0\rangle\right) = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$ Not Equal.

Consider LHS : $U(|+\rangle \otimes |0\rangle) = |+\rangle|+\rangle$

$$\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \neq \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$ contradiction.

No Cloning: Blessing or Curse?

Implications to eavesdropping attacks?

No Cloning: Blessing or Curse?

Implications to digital money?

So far..

- How to represent quantum information – single and multi-bit.

So far..

- How to represent quantum information – single and multi-bit.
- How to measure a quantum system – single and multi-bit.

So far..

- How to represent quantum information – single and multi-bit.
- How to measure a quantum system – single and multi-bit.
- How to compute on a qubit – single. How?

So far..

- How to represent quantum information – single and multi-bit.
- How to measure a quantum system – single and multi-bit.
- How to compute on a qubit – single. How?

What about computing on multiple bits?

So far..

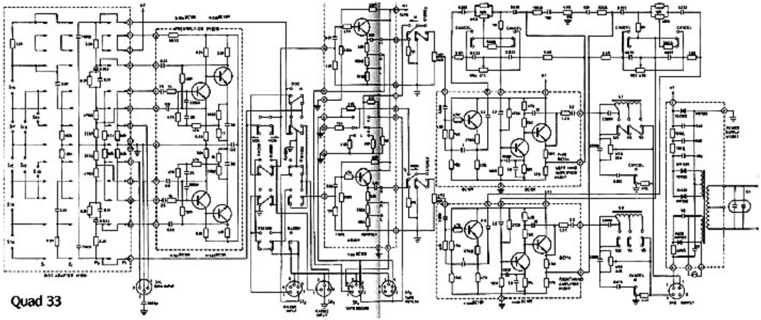
- How to represent quantum information – single and multi-bit.
- How to measure a quantum system – single and multi-bit.
- How to compute on a qubit – single. How?

What about computing on multiple bits?
Even classical computers can do that!

So far..

- How to represent quantum information – single and multi-bit.
- How to measure a quantum system – single and multi-bit.
- How to compute on a qubit – single. How?

What about computing on multiple bits?
Even classical computers can do that!



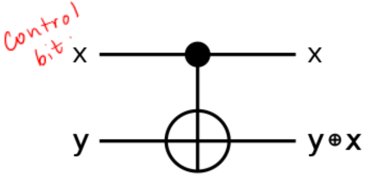
How to perform classical computation?

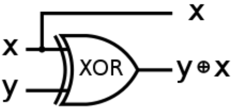
Let's start with some simple multi-bit operations....

How to perform classical computation?

Let's start with some simple multi-bit operations....

Control NOT gate: Flips the "data" bit if "control" bit is set to 1.





input		output	
x	y	x	y+x
$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$
$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$
$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$

unchanged.

flipped.

input		output	
x	y	x	y+x
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

CNOT Gate

Consider a general quantum state: control bit

0

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

What is CNOT $|\psi\rangle$? $= \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|11\rangle + \alpha_{11}|10\rangle$

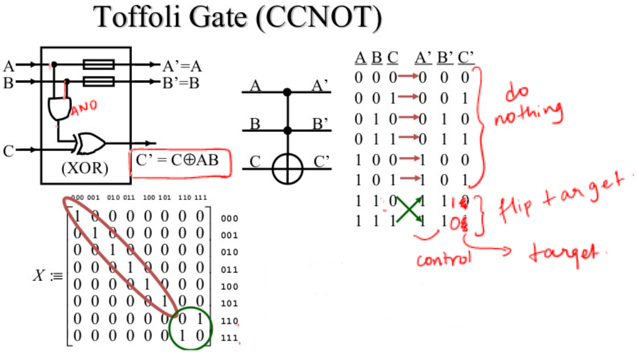
$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{pmatrix} = \begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{11} \\ \alpha_{10} \end{pmatrix}$$

Represent in matrix form:

$$\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

CCNOT or Toffoli Gate

What about three qubit gates?



Target flipped if both control bits are set to 1. Which gate is this?

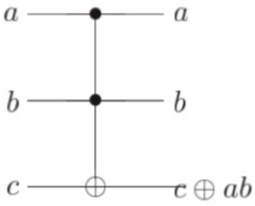
CCNOT or Toffoli Gate

Claim: Toffoli is an implementation of the AND gate

CCNOT or Toffoli Gate

Claim: Toffoli is an implementation of the AND gate

Inputs			Outputs		
a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1 ✓
1	1	1	1	1	0



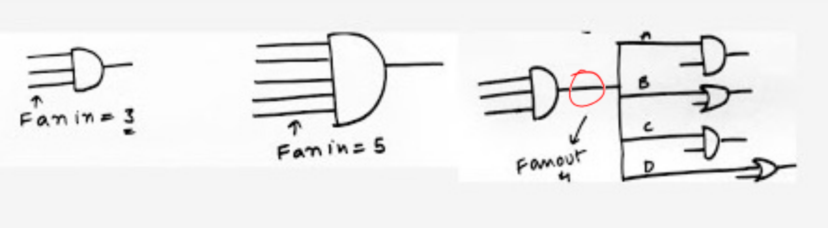
0 AND gate

How to simulate NAND?

$c = 1.$

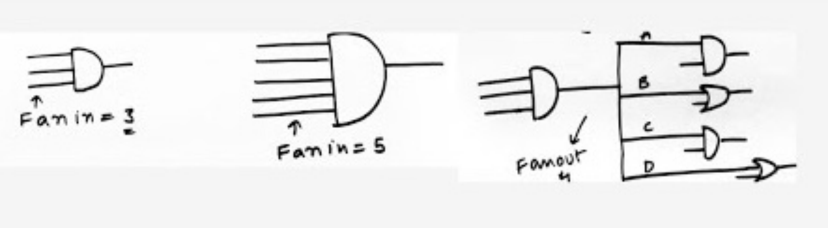
CCNOT or Toffoli Gate

Recall the definition of fanin and fanout



CCNOT or Toffoli Gate

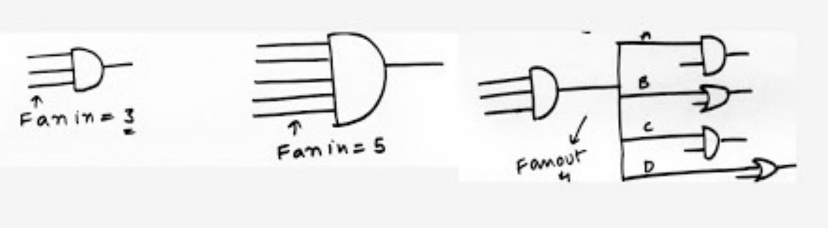
Recall the definition of fanin and fanout



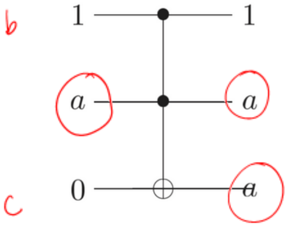
Claim: Toffoli gate can be used to simulate fanout

CCNOT or Toffoli Gate

Recall the definition of fanin and fanout



Claim: Toffoli gate can be used to simulate fanout



$c \oplus ab = a\underset{1}{\underset{\uparrow}{b}}$ when $c=0$

$= a.$