QUANTUM CRYPTOGRAPHY

LECTURE -3

Outline :

- Multi - Qubit Quantum States
- Inner and outer products
- Examples of Quantum Gates
- Entanglement
-

LAST CLASS : 2 qubit quantum states "pure"

Today : An n-qubit quantum state is a vector $\mathbb{C}^{2^n}$.

Helps to identify a basis for $\mathbb{C}^{2^n}$.

express all possible n-qubit quantum states as a linear combination of the basis states.

$|0\rangle \equiv \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $|1\rangle \equiv \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ are a basis of $\mathbb{C}^2$

$|00\rangle = |0\rangle \otimes |0\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$ $|01\rangle = |0\rangle \otimes |1\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$ $|10\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$ $|11\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$

are a basis for $\mathbb{C}^{2^2}$.

Basis vectors for n-qubit system will be :

$|00\ldots0\rangle, |00\ldots01\rangle, |0\ldots010\rangle \ldots\ldots\ldots |11\ldots1\rangle$

(2^n vectors). $|1\rangle\otimes|1\rangle\otimes|1\rangle\ldots$

$$|\psi\rangle = \alpha_{00\ldots0}|00\ldots0\rangle + \alpha_{00\ldots01}|00\ldots01\rangle + \ldots\ldots$$

$$= \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$$

Example : $|\psi\rangle = \sum_{x \in \{0,1\}^n} \frac{|x\rangle}{2^{n/2}}$

Inner and Outer Products

$$\langle \psi | \phi \rangle = (|\psi\rangle, |\phi\rangle)$$

where $|\psi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$ and $|\phi\rangle = \sum_x \beta_x |x\rangle$

$|\psi\rangle$ "ket" $= \begin{bmatrix} \alpha_{0\ldots0} \\ \alpha_{00\ldots1} \\ \vdots \\ \alpha_{11\ldots1} \end{bmatrix}$

$\langle \psi |$ "bra" $= \begin{bmatrix} \alpha^*_{00\ldots0} & \alpha^*_{0\ldots1} & \cdots & \alpha^*_{111\ldots1} \end{bmatrix}$

$|\phi\rangle = \begin{bmatrix} \beta_{00\ldots0} \\ \beta_{00\ldots1} \\ \\ \beta_{11\ldots1} \end{bmatrix}$

$\langle \psi | \phi \rangle =$ product of row vector $\langle \psi |$ column vector $|\phi\rangle$

$$= \begin{bmatrix} \alpha^*_{000\ldots0} & \alpha^*_{00\ldots1} & \cdots & \alpha^*_{11\ldots1} \end{bmatrix} \begin{bmatrix} \beta_{00\ldots0} \\ \\ \\ \beta_{1\ldots1} \end{bmatrix}$$

$$= \sum_x \alpha^*_x \beta_x$$

(scalar)

If for any $|\psi\rangle, |\phi\rangle$, $\langle \psi | \phi \rangle = 0$ then $\langle \psi | \phi \rangle$ are orthogonal.

For any (pure) quantum state, $\langle \psi | \psi \rangle = 1$.

For any $|\psi\rangle, |\phi\rangle$,

$$|\langle \psi | \phi \rangle|^2 \leq \underbrace{\langle \psi | \psi \rangle}_{=1} \cdot \underbrace{\langle \phi | \phi \rangle}_{=1} \leq 1.$$

Outer Product

$|\phi\rangle\langle\psi| = |\phi\rangle \otimes \langle\psi|$

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

$|\psi\rangle$ = "ket" $= \begin{bmatrix}\alpha_{0\ldots0}\\ \alpha_{00\ldots1}\\ \vdots\\ \alpha_{11\ldots1}\end{bmatrix} = \begin{bmatrix}\beta_{00\ldots0}\\ \\ \\ \beta_{11\ldots1}\end{bmatrix} \otimes \begin{bmatrix}\alpha^*_{00\ldots0} & \cdots & \alpha^*_{11\ldots1}\end{bmatrix}$

$|\phi\rangle = \begin{bmatrix}\beta_{00\ldots0}\\ \beta_{00\ldots1}\\ \\ \beta_{11\ldots1}\end{bmatrix} = \begin{bmatrix}\beta_{00\ldots0}\alpha^*_{00\ldots0} & \beta_{00\ldots0}\alpha^*_{00\ldots1} & \cdots\\ \beta_{00\ldots1}\alpha^*_{00\ldots0} & & \\ \vdots & & \ddots\end{bmatrix}$

$= \sum_{x,y \in \{0,1\}^n} \beta_x \alpha_y^* |x\rangle\langle y|$

Sum of diagonal entries $= tr(|\phi\rangle \otimes \langle\psi|)$

$tr(AB) = tr(BA)$

$tr(A+B) = tr(A) + tr(B)$

$tr(zA) = z\,tr(A)$

$= \beta_{0\ldots0}\alpha^*_{0\ldots0} + \beta_{0\ldots1}\alpha^*_{00\ldots1} + \cdots$

$= \sum_x \beta_x \alpha_x^* = \sum_x \alpha_x^* \beta_x = \langle\psi|\phi\rangle$

Quantum Circuits.

On input an n-qubit quantum state $|\psi\rangle$ and m qubits all initialized to $|0\rangle$.

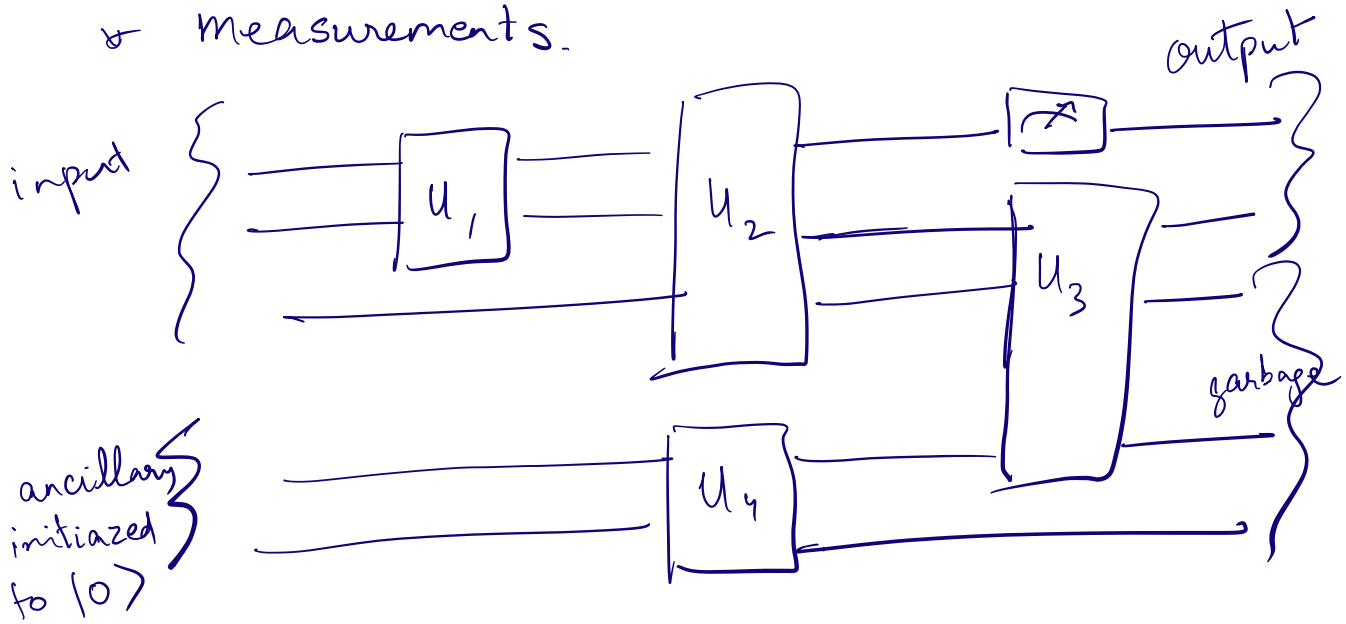
"ancila" qubits / extra workspace

the circuit results in an $(n+m)$ qubit state.

of which some are "output" qubits, others are "garbage".

Two types of gates:

* Unitaries
* measurements.



EXAMPLES OF UNITARIES

Subsection 1: Single-Qubit Gates.

Hadamard Gate H : $\begin{bmatrix}1\\0\end{bmatrix} \rightarrow \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix} \equiv \frac{|0\rangle + |1\rangle}{\sqrt{2}}$

H : $\begin{bmatrix}0\\1\end{bmatrix} \rightarrow \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix} \equiv \frac{|0\rangle - |1\rangle}{\sqrt{2}}$

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

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

Hadamard gate $\xrightarrow{\text{matrix}}$ $\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$

Pauli Gates X, Y, Z

X-gate "exchange amplitudes on $|0\rangle$ and $|1\rangle$"

$X(|0\rangle) \rightarrow |1\rangle, \quad X(|1\rangle) \rightarrow |0\rangle.$

$X(\alpha|0\rangle + \beta|1\rangle) \rightarrow \alpha X(|0\rangle) + \beta X(|1\rangle)$

$= \beta|0\rangle + \alpha|1\rangle.$

$\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$ is the corresponding matrix

Both Hermitian and unitary.

$U = U^\dagger$ $\quad U^\dagger U = I$

Z-Gate

"phase flip gate".

$$Z(|0\rangle) \to |0\rangle \qquad Z(|1\rangle) \to -|1\rangle.$$

$$Z(\alpha|0\rangle + \beta|1\rangle) \to \alpha|0\rangle - \beta|1\rangle.$$

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \leftarrow \text{matrix representation.}$$

Y-Gate

$$Y(|0\rangle) \to i|1\rangle, \quad Y(|1\rangle) \to -i|0\rangle.$$

$$Y(\alpha|0\rangle + \beta|1\rangle) = \alpha i|1\rangle - \beta i|0\rangle$$
$$= -\beta i|0\rangle + \alpha i|1\rangle.$$

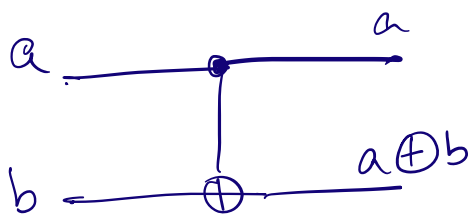
$$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \leftarrow \text{matrix representation}$$

X, Y, Z are unitary (i.e. $U^\dagger U = I$)
Hermitian (i.e. $U = U^\dagger$)
which implies that $X^2 = Y^2 = Z^2 = I$

Subsection 2 : 2-Qubit Gates

CNOT Gate

Input	Output
$\|00\rangle$	$\|00\rangle$
$\|01\rangle$	$\|01\rangle$
$\|10\rangle$	$\|11\rangle$
$\|11\rangle$	$\|10\rangle$



$$CNOT\left(|a\ b\rangle\right) = |a\ \ a\oplus b\rangle.$$

$a, b \in \{0,1\}$

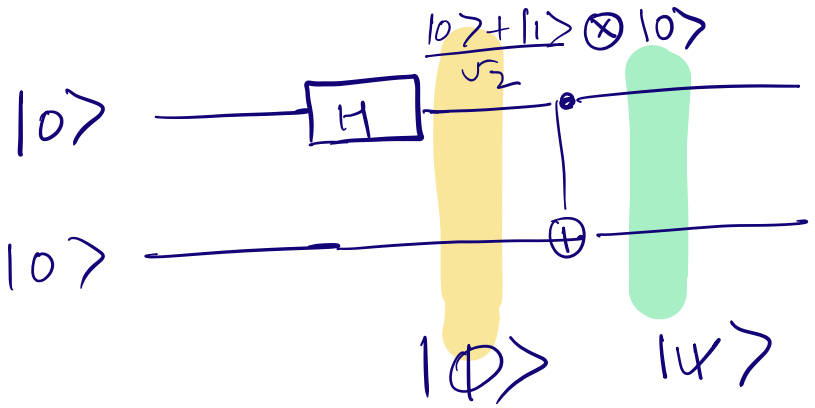
$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

$$CNOT\left(|\psi\rangle\right) = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|11\rangle + \alpha_{11}|10\rangle$$

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

H.W. Prove that

$$CCNOT\left(|\psi\rangle\right) = \sum_{x \in \{000,001,010,011,100,101\}} \alpha_x |x\rangle + \alpha_{111}|110\rangle + \alpha_{110}|111\rangle$$



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

$$|\Psi\rangle = \text{CNOT}(|\Phi\rangle) = \frac{1}{\sqrt{2}}\left(\text{CNOT}(|00\rangle) + \text{CNOT}\,|10\rangle\right)$$

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

Can you write $|\Psi\rangle$ as $|\phi_0\rangle \otimes |\phi_1\rangle$?

$$\frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\0\\1\end{bmatrix}\begin{matrix}00\\01\\10\\11\end{matrix} = \begin{bmatrix}\alpha_0\\\beta_0\end{bmatrix} \otimes \begin{bmatrix}\alpha_1\\\beta_1\end{bmatrix}$$

$$= \begin{bmatrix}\alpha_0\alpha_1\\\alpha_0\beta_1\\\beta_0\alpha_1\\\beta_0\beta_1\end{bmatrix}$$

$\Rightarrow \alpha_0\alpha_1 = \beta_0\beta_1 = \frac{1}{\sqrt{2}}$ and $\alpha_0\beta_1 = \beta_0\alpha_1 = 0$.

$\Rightarrow \alpha_0 = 0$ or $\beta_1 = 0$

$\Rightarrow \alpha_0\alpha_1 = 0$ or $\beta_0\beta_1 = 0$

ENTANGLEMENT

A 2-qubit state $|\psi\rangle$ is entangled if it cannot be expressed as a tensor product of two 1-qubit states.

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

EPR pair (Einstein-Podolsky-Rosen)

measure the first qubit in the computational basis.

outcome

"0" w.p. $\left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$. Residual state: $|00\rangle$

"1" w.p. $\left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$ Residual state: $|11\rangle$

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

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

Can you clone an arbitrary quantum state?

Is there a unitary U s.t. $\forall |\psi\rangle$,

$$U(|\psi\rangle|0\rangle) \rightarrow |\psi\rangle \otimes |\psi\rangle$$

[Weakening of "no cloning" theorem].

No.

Proof. Suppose such a U existed.

$$U|0\rangle|0\rangle \rightarrow |00\rangle$$

$$U|1\rangle|0\rangle \rightarrow |11\rangle$$

$$U\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}|0\rangle\right) \rightarrow \frac{U|00\rangle + U|10\rangle}{\sqrt{2}} = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

But $U\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes |0\rangle\right)$ should have been $\frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle+|1\rangle}{\sqrt{2}}$