CS 506 : Intro to Quantum Computing

Scribe: Gaurav Chintakunta

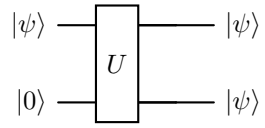
Date: 9/17/2025

1 No-Cloning Theorem recap

The no-cloning theorem states that it is impossible to create an identical copy of an arbitrary, unknown quantum state.

1.1 Why we use $|0\rangle$ as junk input

Let's consider an input state $|\psi\rangle$ and a junk input $|0\rangle$. We need $|0\rangle$ because Quantum circuits are reversible and unitary which means number of inputs should be equal to number of outputs.

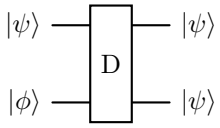


The operation of a cloning unitary U would be:

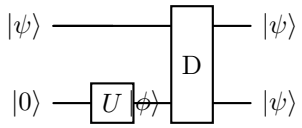
$$U(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle$$

This is possible only when the initial states are orthogonal, i.e., $\langle\psi|0\rangle = 0$.

Suppose we have a cloning device, a circuit D.



And we can also have circuit D as:



We apply Unitary Transformation on $|0\rangle$ to get $|\phi\rangle$. Hence if D is possible, then D' is also possible. If we take the contrapositive, if D' is not possible then D is not possible as well.

1.2 Proof that you cannot clone a quantum state

Let us take a circuit C,

$$C(|0\rangle \otimes |0\rangle) \rightarrow |0\rangle \otimes |0\rangle$$
$$C(|0\rangle \otimes |1\rangle) \rightarrow |1\rangle \otimes |1\rangle$$

Now, let a general state be $|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$. Applying the cloning operator C:
If the cloning were truly successful, the desired output would be:

$$\begin{aligned} C|0\rangle (\alpha_0 |0\rangle + \alpha_1 |1\rangle) &= (\alpha_0 |0\rangle + \alpha_1 |1\rangle) \otimes (\alpha_0 |0\rangle + \alpha_1 |1\rangle) \\ &= \alpha_0^2 |00\rangle + \alpha_0\alpha_1 |01\rangle + \alpha_1\alpha_0 |10\rangle + \alpha_1^2 |11\rangle \quad \text{— (1)} \end{aligned}$$

Using the linearity of quantum mechanics, we obtain:

$$\begin{aligned} C|0\rangle (\alpha_0 |0\rangle + \alpha_1 |1\rangle) &= C|0\rangle (\alpha_0 \otimes |0\rangle) + C|0\rangle (\alpha_1 \otimes |1\rangle) \\ &= \alpha_0(|0\rangle \otimes |0\rangle) + \alpha_1(|1\rangle \otimes |1\rangle) \quad \text{— (2)} \end{aligned}$$

However, Comparing expressions (1) and (2), they are not the same unless $\alpha_0 = 0$, $\alpha_1 = 1$ or $\alpha_0 = 1$, $\alpha_1 = 0$. Therefore, a general quantum state cannot be cloned. This theorem was proposed by Wootters and Zurek in 1982.

2 Quantum Gates

There are 4 well-known quantum gates called Pauli gates, named after Wolfgang Pauli, who is a pioneer in Quantum mechanics.

- **I Gate (Identity)**

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

  $I|0\rangle = |0\rangle$, $I|1\rangle = |1\rangle$, $I^2 = I$

- **X Gate (NOT)**

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

  $X|0\rangle = |1\rangle$, $X|1\rangle = |0\rangle$, $X^2 = I$

- **Y Gate**

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

  $Y|0\rangle = i|1\rangle$, $Y|1\rangle = -i|0\rangle$, $Y^2 = I$

- **Z Gate**

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

  $Z|0\rangle = |0\rangle$, $Z|1\rangle = -|1\rangle$, $Z^2 = I$

The X, Y, and Z gates are rotation gates.

3 Rotation Gates

3.1 Matrix Exponential

Suppose A is a square matrix such that $A^2 = I$. Here, x is a scalar and A is a matrix. We can find the value of e^{iAx} using the Taylor expansion.

$$\begin{aligned} e^{iAx} &= I + \frac{iAx}{1!} + \frac{(iAx)^2}{2!} + \frac{(iAx)^3}{3!} + \frac{(iAx)^4}{4!} + \dots \\ &= I + iA\frac{x}{1!} - I\frac{x^2}{2!} - iA\frac{x^3}{3!} + I\frac{x^4}{4!} + \dots \\ &= I\left(1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \dots\right) + iA\left(x - \frac{x^3}{3!} + \frac{x^5}{5!} - \dots\right) \\ &= I\cos(x) + iA\sin(x) \end{aligned}$$

3.2 Rotation Gates (R_x, R_y, R_z)

The rotation gates are defined as:

$$R_k(\theta) = e^{-i\frac{\theta}{2}\sigma_k} = \cos(\frac{\theta}{2})I - i\sin(\frac{\theta}{2})\sigma_k \quad \text{where } k \in \{x, y, z\}$$

and σ_k are the Pauli matrices (X, Y, Z).

- **X-Rotation:**

$$R_x(\theta) = \cos(\frac{\theta}{2})I - i\sin(\frac{\theta}{2})X = \cos(\frac{\theta}{2})\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} - i\sin(\frac{\theta}{2})\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} = \begin{pmatrix}\cos(\frac{\theta}{2}) & -i\sin(\frac{\theta}{2})\\ -i\sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2})\end{pmatrix}$$

- **Y-Rotation:**

$$R_y(\theta) = \cos(\frac{\theta}{2})I - i\sin(\frac{\theta}{2})Y = \cos(\frac{\theta}{2})\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} - i\sin(\frac{\theta}{2})\begin{pmatrix}0 & -i\\ i & 0\end{pmatrix} = \begin{pmatrix}\cos(\frac{\theta}{2}) & -\sin(\frac{\theta}{2})\\ \sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2})\end{pmatrix}$$

- **Z-Rotation:**

$$R_z(\theta) = \cos(\frac{\theta}{2})I - i\sin(\frac{\theta}{2})Z = \cos(\frac{\theta}{2})\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} - i\sin(\frac{\theta}{2})\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix} = \begin{pmatrix}\cos(\frac{\theta}{2}) - i\sin(\frac{\theta}{2}) & 0\\ 0 & \cos(\frac{\theta}{2}) + i\sin(\frac{\theta}{2})\end{pmatrix}$$

$$\mathrm{R}_z(\theta) = \begin{pmatrix}e^{-i\theta/2} & 0\\ 0 & e^{i\theta/2}\end{pmatrix}$$

3.3 General Form of a Qubit and R_z Application

The general form of a qubit is:

$$|\psi\rangle = \cos(\frac{\sigma}{2})|0\rangle + e^{i\phi}\sin(\frac{\sigma}{2})|1\rangle \quad \text{— (1)}$$

Applying $R_z(\theta)$ to $|\psi\rangle$:

$$R_z(\theta)|\psi\rangle = \begin{pmatrix}e^{-i\theta/2} & 0\\ 0 & e^{i\theta/2}\end{pmatrix}\begin{pmatrix}\cos(\frac{\sigma}{2})\\ e^{i\phi}\sin(\frac{\sigma}{2})\end{pmatrix} = \begin{pmatrix}e^{-i\theta/2}\cos(\frac{\sigma}{2})\\ e^{i\theta/2}e^{i\phi}\sin(\frac{\sigma}{2})\end{pmatrix}$$

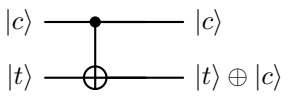
Which can be written as:

$$\begin{aligned} R_z(\theta)|\psi\rangle &= e^{-i\theta/2}\cos(\frac{\sigma}{2})|0\rangle + e^{i\theta/2}e^{i\phi}\sin(\frac{\sigma}{2})|1\rangle \\ &= e^{-i\theta/2}\left(\cos(\frac{\sigma}{2})|0\rangle + e^{i(\phi+\theta)}\sin(\frac{\sigma}{2})|1\rangle\right) \quad \text{— (2)} \end{aligned}$$

The term $e^{-i\theta/2}$ is a global phase, so we can neglect it when considering the physical state. Comparing (1) and (2), the angle ϕ is changed by $\phi + \theta$.

4 Multi-Qubit Gates

4.1 Controlled-NOT Gate (CNOT)



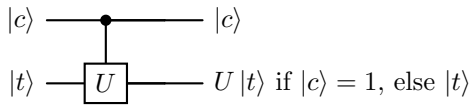
The CNOT gate acts on two qubits, a control ($|c\rangle$) and a target ($|t\rangle$). If $|c\rangle = 0$, the output for $|t\rangle$ is $|t\rangle$. If $|c\rangle = 1$, the output for $|t\rangle$ is NOT($|t\rangle$)

The C-NOT gate acts as:

$$\text{C-NOT}\,|0\rangle\,|t\rangle = |0\rangle\,|t\rangle$$
$$\text{C-NOT}\,|1\rangle\,|t\rangle = |1\rangle\,NOT(|t\rangle)$$

4.2 Controlled-U Gate (C-U)

Let U be an arbitrary unitary matrix. This is a 2-qubit gate.



The C-U gate acts as:

$$\text{C-U}\,|0\rangle\,|t\rangle = |0\rangle\,|t\rangle$$
$$\text{C-U}\,|1\rangle\,|t\rangle = |1\rangle\,U(|t\rangle)$$

The matrix for CU in Dirac notation is:

$$\text{CU} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U$$

4.3 Verification of Controlled-U Gate (C-U)

Let us try to verify the C-U gate.
If the inputs are $|0\rangle$ and $|t\rangle$, the expected output is $|0\rangle|t\rangle$.

$$\begin{aligned}\text{C-U}\,|0\rangle\,|t\rangle &= (|0\rangle\langle 0| \otimes I)\,|0\rangle\,|t\rangle + (|1\rangle\langle 1| \otimes U)\,|0\rangle\,|t\rangle \\ &= |0\rangle\langle 0|0\rangle \otimes I\,|t\rangle + |1\rangle\langle 1|0\rangle \otimes U\,|t\rangle \\ &= |0\rangle\,|t\rangle\end{aligned}$$

5 Other Single-Qubit Gates

- **Hadamard Gate (H)**

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

Action on the basis states:

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

- **Another 1-qubit gate: $\pi/8$ phase gate**

$$R = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

$$R = e^{i\pi/8} \begin{pmatrix} e^{-i\pi/8} & 0 \\ 0 & e^{i\pi/8} \end{pmatrix}$$

Action on the basis states:

$$R\,|0\rangle = |0\rangle$$
$$R\,|1\rangle = e^{i\pi/4}\,|1\rangle$$

6 Quantum Superdense Coding

Introduction:

Alice	**Channel**	**Bob**
Wants to send bits to Bob {00, 01, 10, 11}	$\longrightarrow$	

In quantum superdense coding, we are able to reduce the communication cost by 50%.
Let us take a scenario where Alice wants to send two classical bits (e.g., 00, 01, 10, or 11) to Bob. This method allows her to achieve this by sending only one qubit and Bob can figure out what the other qubit is based on the qubit sent by Alice, thereby reducing the communication cost by 50%.