Lab: Quantum Postulates & Formal Proof of the No-Cloning Theorem

Lab Objectives

1. Understand the four postulates of quantum mechanics and their mathematical representations.
2. Derive and prove the No-Cloning Theorem formally.
3. Explore the implications of the theorem for quantum cryptography.
4. Simulate a failed cloning attempt using a simple quantum circuit.

I. Theoretical Background

Postulates of Quantum Mechanics

Postulate 1: State Space

The state of an isolated quantum system is described by a unit vector in a complex Hilbert space.

Postulate 2: Evolution

The evolution of a closed quantum system is described by a unitary transformation:
$|\psi(t_2)\rangle = U(t_1, t_2)|\psi(t_1)\rangle$

Postulate 3: Measurement

Quantum measurements are described by a collection $\{M_m\}$ of measurement operators satisfying $\sum_m M_m^\dagger M_m = I$.
Probability: $p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle$
State after measurement: $|\psi'\rangle = M_m|\psi\rangle/\sqrt{p(m)}$

Postulate 4: Composite Systems

The state space of a composite system is the tensor product of the component state spaces.

II. Formal Proof of the No-Cloning Theorem

Theorem Statement

There exists no unitary operator U and fixed initial state |s⟩ such that for any arbitrary state |ψ⟩:
$U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle$

Proof by Contradiction

Step 1: Assume cloning is possible
Assume $\exists$ U and $|s\rangle$ such that:

1. $U(|\psi\rangle\otimes|s\rangle) = |\psi\rangle\otimes|\psi\rangle$ for all $|\psi\rangle$
2. $U(|\varphi\rangle\otimes|s\rangle) = |\varphi\rangle\otimes|\varphi\rangle$ for all $|\varphi\rangle$

Step 2: Consider the inner product

Take the inner product of both equations:

$\langle\psi|\langle s|U^\dagger U|\varphi\rangle|s\rangle = (\langle\psi|\langle\psi|)(|\varphi\rangle|\varphi\rangle)$

Since U is unitary ($U^\dagger U = I$):

$\langle\psi|\varphi\rangle\langle s|s\rangle = \langle\psi|\varphi\rangle\langle\psi|\varphi\rangle$

Step 3: Simplify

Since $\langle s|s\rangle = 1$ (normalized state):

$\langle\psi|\varphi\rangle = (\langle\psi|\varphi\rangle)^2$

Step 4: Solve the equation

Let $x = \langle\psi|\varphi\rangle$. Then:

$x = x^2 \Rightarrow x(1 - x) = 0 \Rightarrow x = 0$ or $x = 1$

Step 5: Interpret the result

This means either:

- $\langle\psi|\varphi\rangle = 0$ (states are orthogonal)
- $\langle\psi|\varphi\rangle = 1$ (states are identical)

Conclusion: A universal cloning device can only clone states that are either identical or orthogonal. It cannot clone arbitrary unknown quantum states.

III. Experimental Simulation

Part A: Attempting to Clone a Qubit

We'll attempt to create a "cloning" circuit and show it fails for arbitrary states.

Circuit Design:

Initial state: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, with $|\alpha|^2 + |\beta|^2 = 1$
Ancilla: $|0\rangle$

Goal: Create $(\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle)$

Code Lab is located in Repo https://github.com/learningdungeon/qamp-2025

Part B: Mathematical Verification

Exercise: Prove that the following "cloning" circuit fails:

```
|ψ⟩ --[U]--[CNOT]--------
       |      |

|0⟩ --[H]--[CNOT]--[measure]
```

Where U prepares $|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\varphi}\sin(\theta/2)|1\rangle$

Steps:

1. Write the initial state: $|\psi\rangle \otimes |0\rangle$
2. Apply the gates step by step
3. Show the final state is NOT $|\psi\rangle \otimes |\psi\rangle$ for arbitrary θ, φ
4. For which specific states does it work?

IV. Implications for Quantum Cryptography

Exercise: BB84 Protocol Security

Explain how the No-Cloning Theorem ensures the security of the BB84 quantum key distribution protocol.

Questions:

1. Why can't an eavesdropper copy qubits without detection?
2. How does the theorem relate to the uncertainty principle in BB84?
3. What happens if Eve tries to measure and resend qubits?

V. Lab Report Requirements

1. Theoretical Section
   - Summarize the four postulates in your own words
   - Reproduce the No-Cloning Theorem proof with detailed explanations
   - Explain why the proof fails for orthogonal states
2. Experimental Section
   - Include your simulation results
   - Plot fidelity vs. state parameter θ
   - Show that fidelity = 1 only for $\theta = 0, \pi$ ($|0\rangle$ and $|1\rangle$)
3. Analysis
   - Why does the CNOT-based circuit seem to "clone" $|0\rangle$ and $|1\rangle$?
   - Calculate the output state for $|+\rangle = (|0\rangle+|1\rangle)/\sqrt{2}$

    - What is the actual output state for arbitrary input?

4. Applications
    - Explain how the No-Cloning Theorem enables:
        - Quantum key distribution
        - Quantum money
        - Certified deletion of quantum information

VI. Extension: Approximate Cloning

Research Question: While exact cloning is impossible, approximate cloning (Buzek-Hillery cloning machine) exists. Investigate:

1. What is the optimal cloning fidelity?
2. How does the fidelity depend on the number of clones?
3. Implement the Buzek-Hillery cloning circuit and compare with our naive attempt.

Assessment Rubric

Criteria	Excellent (4)	Good (3)	Satisfactory (2)	Needs Improvement (1)
Proof Understanding	Complete, clear derivation with insights	Correct proof with minor gaps	Basic understanding with errors	Major errors or omissions

Simulation Implementation	Clean code, multiple test cases, good analysis	Working code with basic analysis	Code runs but incomplete analysis	Code doesn't run or major errors
Analysis & Interpretation	Deep insights connecting theory and results	Clear explanation of results	Basic description of results	Minimal or incorrect analysis
Lab Report	Professional, complete, well-organized	Complete with minor issues	Missing some sections or unclear	Incomplete or poorly organized

References

1. Nielsen, M. A., & Chuang, I. L. (2010). *Quantum Computation and Quantum Information*. Cambridge University Press.
2. Wootters, W. K., & Zurek, W. H. (1982). A single quantum cannot be cloned. *Nature*, 299(5886), 802-803.
3. Dieks, D. (1982). Communication by EPR devices. *Physics Letters A*, 92(6), 271-272.

Total Lab Time: 3-4 hours

Note: This lab combines theoretical quantum mechanics with practical simulation. The key insight is that while quantum mechanics allows many counterintuitive phenomena, it fundamentally restricts copying of information, which becomes a feature for security applications.