No-Cloning Theorem

Quantum Foundations · Module 7 — Quantum Information

Node 7.2

Position in Knowledge Graph

System: Quantum Foundations **Structural Domain:** Quantum Information **Node:** 7.2

The no-cloning theorem — Wootters–Zurek and Dieks, independently in 1982 — says that there is no physical process that can take an arbitrary unknown quantum state as input and produce two identical copies of it as output. Unlike classical bits, which can be freely copied, quantum states are "use-once" resources in a precise structural sense: whatever the state is, the only way to make a second instance of it is to already know it classically (in which case one can prepare the second copy directly).

No-cloning is the structural reason quantum key distribution is secure, the reason quantum error correction must work differently from classical repetition codes, and the reason there is no quantum amplifier that faithfully preserves a single-photon state. It is also one of the cleanest illustrations that quantum mechanics is not just "classical mechanics with extra ingredients" — it is a fundamentally different theory of information whose constraints are inherited directly from the linearity of unitary dynamics.

Formal Statement

The theorem

Theorem (Wootters–Zurek, Dieks 1982). There is no unitary operator U acting on $\mathcal{H} \otimes \mathcal{H}$ and no fixed "blank" state $|0\rangle \in \mathcal{H}$ such that, for every $|\psi\rangle \in \mathcal{H}$,

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

Proof

Suppose such a U exists. Apply it to two arbitrary states $|\psi\rangle$ and $|\phi\rangle$:

$$U(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle,$$
$$U(|\phi\rangle \otimes |0\rangle) = |\phi\rangle \otimes |\phi\rangle.$$

Unitary operators preserve inner products. Taking the inner product of the left-hand sides:

$$\langle\psi| \otimes \langle 0|\, U^\dagger U\, |\phi\rangle \otimes |0\rangle = \langle\psi|\phi\rangle\langle 0|0\rangle = \langle\psi|\phi\rangle.$$

And of the right-hand sides:

$$\big(\langle\psi| \otimes \langle\psi|\big)\big(|\phi\rangle \otimes |\phi\rangle\big) = \langle\psi|\phi\rangle^2.$$

Therefore $\langle\psi|\phi\rangle = \langle\psi|\phi\rangle^2$, which means $\langle\psi|\phi\rangle \in \{0, 1\}$. But $|\psi\rangle$ and $|\phi\rangle$ were arbitrary, and generic pairs of states have inner products strictly between 0 and 1. Contradiction. ■

Corollaries and refinements

- **No approximate universal cloning at perfect fidelity.** Even if one relaxes to imperfect cloning, the best achievable fidelity for universal cloners is bounded below 1 (Buzek–Hillery bound: $F = 5/6$ for optimal $1 \to 2$ qubit cloning).
- **No deletion.** A complementary theorem (Pati–Braunstein 2000): there is no unitary that takes $|\psi\rangle \otimes |\psi\rangle \to |\psi\rangle \otimes |0\rangle$ for arbitrary $|\psi\rangle$. Quantum information cannot be unconditionally deleted either.
- **Orthogonal states can be copied.** The theorem does not forbid cloning a known basis: if one knows $|\psi\rangle \in \{|0\rangle, |1\rangle\}$, a CNOT gate clones it perfectly. The theorem forbids a *single* unitary that clones *every* state.

Intuition

The intuitive story is that to clone a state, one would need to learn enough about it to reproduce it, and learning a quantum state means measuring it — which in general disturbs or destroys the state. But this intuition is only suggestive; the theorem is stronger. It says that no unitary can produce a clone, even if no classical information is extracted. The ban is on the *shape* of the required transformation, not on the information-theoretic resources of the cloner.

The cleanest way to see why is through linearity. Suppose a unitary cloner U exists. Then for any superposition $\alpha|\psi\rangle + \beta|\phi\rangle$, linearity forces

$$U\big((\alpha|\psi\rangle + \beta|\phi\rangle) \otimes |0\rangle\big) = \alpha\,|\psi\rangle|\psi\rangle + \beta\,|\phi\rangle|\phi\rangle.$$

But "two copies of the superposition" would require

$$(\alpha|\psi\rangle + \beta|\phi\rangle) \otimes (\alpha|\psi\rangle + \beta|\phi\rangle) = \alpha^2|\psi\rangle|\psi\rangle + \alpha\beta(|\psi\rangle|\phi\rangle + |\phi\rangle|\psi\rangle) + \beta^2|\phi\rangle|\phi\rangle.$$

These are manifestly different unless the cross-terms vanish, which happens only if $\alpha\beta = 0$ or the states are orthogonal. Cloning is incompatible with quantum superposition because it is a nonlinear operation on the state, and quantum dynamics is linear.

The philosophical upshot: classical information is "free" — it can be copied, broadcast, and distributed — because classical states are distinguishable pointers to definite facts. Quantum information is "private" — a state cannot be broadcast to multiple recipients without destroying its coherence — because quantum states are not pointers but the actual objects of physical interest, and linearity forbids the operation that would distribute them.

Structural Role

- **Cryptography foundation.** No-cloning is the structural reason BB84 and other QKD protocols are secure. An eavesdropper cannot tap a quantum channel without disturbing the states — and any disturbance is detectable by the legitimate users. Section 9.3 of Nielsen–Chuang develops this chain of reasoning in full.
- **Constraint on error correction.** Classical error correction uses repetition codes: to protect a bit, make three copies and majority-vote. Quantum error correction cannot use this directly because making copies is forbidden. Instead, quantum codes like the Shor code and Steane code distribute information *across* qubits via entanglement, in a way that does not require cloning.
- **No quantum signal amplification.** A classical amplifier boosts a weak signal by creating many high-energy copies. A quantum amplifier cannot do this for a single-photon state — any attempt to amplify introduces noise (this is the basis of the quantum limits on amplifier noise in nonlinear optics, and forms one pillar of the theory of quantum channels).

- **Contrast with classical channels.** A broadcast channel in classical information theory distributes one input to multiple receivers. The quantum analogue (the "quantum broadcast channel") is fundamentally different: one cannot split a quantum state into two independent copies, only into an entangled pair whose marginals have reduced purity.
- **Foundational significance.** No-cloning is one of a family of no-go theorems (no-cloning, no-deleting, no-broadcasting, no-hiding) that together characterize quantum information as a resource distinct from classical information. Each is proved by similar linearity arguments.

Mathematical Development

Proof via inner product preservation

The proof above uses the fact that unitary operators preserve inner products. This is the cleanest proof of no-cloning and generalizes easily. Any linear operator V satisfying $V|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle$ and $V|\phi\rangle|0\rangle = |\phi\rangle|\phi\rangle$ for two non-orthogonal states is inconsistent, regardless of unitarity. Unitarity is sufficient but not strictly necessary; linearity is the essential property.

Proof via linearity of superposition

For states $|\psi\rangle$ and $|\phi\rangle$ that can be cloned, linearity forces the superposition to map as

$$U\big((\alpha|\psi\rangle + \beta|\phi\rangle) \otimes |0\rangle\big) = \alpha|\psi\rangle|\psi\rangle + \beta|\phi\rangle|\phi\rangle,$$

which is an entangled state, not a product state of the form $(\alpha|\psi\rangle + \beta|\phi\rangle) \otimes (\alpha|\psi\rangle + \beta|\phi\rangle)$. So even if U could clone each of $|\psi\rangle$ and $|\phi\rangle$ individually, it cannot clone any proper superposition of them.

Approximate cloning: the Bužek–Hillery bound

Suppose one relaxes the requirement and asks for a "universal quantum cloner" that produces two output states, each approximately equal to the input, with maximum average fidelity over input states. Bužek and Hillery showed that for a qubit $1 \to 2$ universal cloner, the maximum achievable fidelity is

$$F = \frac{5}{6} \approx 0.833.$$

The optimal cloner produces entangled outputs whose reduced density matrices have this fidelity with the input. For d-dimensional systems, the bound is

$$F_{d,1\to 2} = \frac{1}{2} + \frac{1}{d+1}.$$

This converges to $1/2$ as $d \to \infty$ — high-dimensional states cannot even be copied to better-than-guessing fidelity.

State-dependent cloning

If one is willing to clone only a specific (known) pair of states rather than all states, better fidelity is possible. For two non-orthogonal states $|\psi_0\rangle, |\psi_1\rangle$ with inner product $\langle\psi_0|\psi_1\rangle = s$, the optimal state-dependent cloner has fidelity

$$F = \frac{1}{2}\left(1 + \sqrt{\frac{1-s^2}{1-s^2+s^2/2}}\right).$$

As $s \to 0$ (orthogonal states), $F \to 1$ — orthogonal states can be perfectly cloned. As $s \to 1$ (nearly identical states), $F \to 1/2$ — the cloner is no better than random guessing.

Broadcast generalization

No-broadcasting theorem (Barnum–Caves–Fuchs–Jozsa–Schumacher 1996): for mixed states, "broadcasting" — finding a joint state ρ_{AB} whose marginals are both equal to the input ρ — is impossible unless the input is classical (commuting with itself on some basis). This generalizes no-cloning from pure to mixed states.

Worked Example

Cannot clone $|0\rangle$ and $|+\rangle$

Suppose a hypothetical cloner exists with $U(|0\rangle \otimes |0\rangle) = |0\rangle|0\rangle$ and $U(|+\rangle \otimes |0\rangle) = |+\rangle|+\rangle$. Write out $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$:

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

For this to equal $|+\rangle|+\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$, we would need

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}U(|1\rangle|0\rangle) = \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle.$$

But the left-hand side has amplitude $1/\sqrt{2}$ on $|00\rangle$, and the right-hand side has amplitude $1/2$. Contradiction. No such U exists.

Equivalently, via the inner product argument: $\langle 0|+\rangle = 1/\sqrt{2}$, so cloning would require $1/\sqrt{2} = (1/\sqrt{2})^2 = 1/2$, which is false. The theorem applies in a concrete, verifiable way.

BB84 eavesdropping detection

In BB84, Alice sends qubits to Bob in randomly chosen bases $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$. Eve, the eavesdropper, wants to learn the bit and forward a copy to Bob. If Eve could clone, she could copy each qubit, measure her copy, and send Bob an identical copy. No-cloning forbids this.

Eve's only option is to measure each qubit in some basis of her choice and send Bob a freshly prepared state. If Eve measures in the wrong basis (because she doesn't know which basis Alice used), she randomizes the state. Alice and Bob can detect this by comparing a random subset of their bits after the transmission: if the error rate is above the expected noise level, Eve is detected.

The structural chain is: no-cloning → Eve must disturb → disturbance is detectable → QKD is secure (modulo noise model assumptions). This is the cleanest application of no-cloning in a practical protocol.

Quantum money

Wiesner (1970) proposed "quantum money": bills encoded as specific quantum states such that the bank can verify authenticity (by measuring in the right basis) but counterfeiters cannot duplicate the states (no-cloning). The concept predates no-cloning's formal statement and motivated the theorem. Modern quantum money schemes build on this idea but require additional cryptographic assumptions beyond just no-cloning.

Cross-Links

- **Module 2.4 (Unitary evolution):** The proof relies essentially on the linearity of unitary dynamics. No-cloning is a direct consequence of this linearity.
- **Module 7.1 (Qubits):** Qubits are the natural setting for the cleanest version of the theorem and for BB84-style applications.
- **Module 7.3 (Quantum channels):** The no-broadcasting theorem generalizes no-cloning to mixed states and channels.
- **Module 7.6 (Teleportation):** Teleportation moves a quantum state from Alice to Bob *without* violating no-cloning: the original is destroyed in the process. This is the no-cloning-compatible way to transmit quantum information.
- **VQA:** One cannot "checkpoint" an intermediate quantum state in a variational circuit for diagnostic purposes. The circuit must be re-run from the initial state each time.
- **Quantum error correction:** Must use entanglement rather than repetition.

Structural Compression

Invariant: There is no unitary U that maps $|\psi\rangle|0\rangle \to |\psi\rangle|\psi\rangle$ for all $|\psi\rangle$ in a Hilbert space of dimension ≥ 2. Quantum states cannot be copied, only transported (teleportation) or distributed via entanglement.

Mechanism: Unitarity preserves inner products, and the cloning relation forces $\langle\psi|\phi\rangle = \langle\psi|\phi\rangle^2$, which has no solutions for non-trivial superpositions. Equivalently, cloning is a nonlinear operation on the state, incompatible with linear quantum dynamics.

Cross-System Echo: Classical Shannon information is freely copiable — a bit stream can be duplicated and distributed arbitrarily. Quantum information is not, and this gap is the structural source of both quantum cryptography's security and quantum error correction's nontrivial form.

Exercises

1. Prove the no-cloning theorem using the inner-product argument for two distinct non-orthogonal states.
2. Prove the no-cloning theorem using the linearity-of-superposition argument. Where in the calculation does the contradiction appear?
3. Show that orthogonal states can be cloned by exhibiting the unitary (hint: CNOT clones computational-basis states).
4. Compute the Bužek–Hillery fidelity bound 5/6 for $1 \to 2$ qubit cloning explicitly by constructing the optimal cloner.
5. Describe how BB84 uses no-cloning to detect eavesdropping. What assumption about the noise model is required for the protocol to be secure?
6. State the no-deletion theorem and sketch its proof. Why is it a complementary result to no-cloning?
7. Argue, structurally, why no-cloning is a consequence of linearity and not of some deeper "measurement disturbance" principle. What would happen if quantum dynamics were nonlinear?

Quantum Foundations · Module 7 — Quantum Information · Node 7.2
Concepts: unitary-evolution, linear-operators
Prerequisites: 7.1, 2.4
Enables: 7.6

hbar.university — own.your.cognition