Note: No-Cloning Theorem

Author: Hao Chung *last revised: September 23, 2019*

Conceptually, the no-cloning theorem states that given an unknown quantum state, we cannot always have an identical copy of the state. Ideally, we want to have a "cloning machine" that takes an arbitrary quantum state $|\psi\rangle$ in a system A as input, and outputs an identical state in another system B while leaving $|\psi\rangle$ intact.

Theorem 1 (no-cloning theorem)**.** *For any Hilbert space H, there is no unitary operator U on $H \otimes H$ such that for all normalized $|\psi\rangle_A \in H$ and $|e\rangle_B \in H$ satisfies*

$$U(|\psi\rangle_A \otimes |e\rangle_B) = |\psi\rangle_A \otimes |\psi\rangle_B .$$

Proof. Suppose we have an unitary operator U that works for two particular states $|\psi\rangle$ and $|\phi\rangle$ such that

$$U(|\psi\rangle_A \otimes |e\rangle_B) = |\psi\rangle_A \otimes |\psi\rangle_B .$$

and

$$U(|\phi\rangle_A \otimes |e\rangle_B) = |\phi\rangle_A \otimes |\phi\rangle_B .$$

Because U is unitary, we have

$$\langle\psi|_A \otimes \langle e|_B \, |\phi\rangle_A \otimes |e\rangle_B = \langle\psi|_A \otimes \langle e|_B \, U^\dagger U \, |\phi\rangle_A \otimes |e\rangle_B = e^{i\theta} \, \langle\psi|_A \otimes \langle\psi|_B \, |\phi\rangle_A \otimes |\phi\rangle_B = e^{i\theta} \, \langle\psi|\phi\rangle^2 ,$$

where $e^{i\theta}$ is the phase generated by unitary operators. However, $|e\rangle_B$ is normalized, so $\langle\psi|_A \otimes \langle e|_B \, |\phi\rangle_A \otimes |e\rangle_B = \langle\psi|\phi\rangle$. Thus, we have

$$|\,\langle\psi|\phi\rangle\,| = |\,\langle\psi|\phi\rangle\,|^2,$$

which implies $|\,\langle\psi|\phi\rangle\,| = 0$ or 1. Thus, we can only clone the states which are mutually orthogonal (see Example 2), but cannot have a universal cloning machine for arbitrary quantum states. □

Alternative proof of Theorem 1. Assume that we have an universal cloning machine U such that for an arbitrary state $|\psi\rangle$,

$$U(|\psi\rangle_A \otimes |e\rangle_B) = |\psi\rangle_A \otimes |\psi\rangle_B .$$

Choose $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, we have

$$U\left(\frac{1}{\sqrt{2}}(|0\rangle_A + |1\rangle_A) \otimes |e\rangle_B\right) = \frac{1}{\sqrt{2}}(|0\rangle_A + |1\rangle_A) \otimes \frac{1}{\sqrt{2}}(|0\rangle_B + |1\rangle_B). \tag{1}$$

However, by the linearity of U, we have

$$U\left(\frac{1}{\sqrt{2}}(|0\rangle_A + |1\rangle_A) \otimes |e\rangle_B\right) = \frac{1}{\sqrt{2}}U(|0\rangle_A \otimes |e\rangle_B) + \frac{1}{\sqrt{2}}U(|1\rangle_A \otimes |e\rangle_B) = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B) + \frac{1}{\sqrt{2}}(|1\rangle_A \otimes |1\rangle_B). \tag{2}$$

However, Equation (1) is not equal to Equation (2), which leads to a contradiction. □

Example 2 (cloning machine for orthogonal states)**.** If we know $|\psi\rangle$ is one of the basis vectors $\{|b_i\rangle\}_i$, it is possible to clone $|\psi\rangle$. For example, CNOT gate is the cloning machine of the computational basis $\{|0\rangle, |1\rangle\}$, because

$$CNOT(|0\rangle \otimes |0\rangle) = |0\rangle \otimes |0\rangle \text{ and } CNOT(|1\rangle \otimes |0\rangle) = |1\rangle \otimes |1\rangle .$$

However, if we want to clone the state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, which is not in $\{|0\rangle, |1\rangle\}$, we get

$$CNOT\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle\right) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle),$$

which is not $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ as we want. This is the contradiction between Equation (1) and Equation (2).
