The No-cloning Theorem and its Implications in Quantum Cryptography

Jose Manuel Torres Lopez, Kapitza Society, Spring 2022

April 19, 2022

Abstract

For the last thirty years, the interest on quantum information science has been growing enormously within the physics community. The main reason behind this trend is that quantum systems show promise to simulate computations that are inaccessible within the classical realm, by taking advantage of properties that are fundamentally quantum in nature, such as quantum entanglement. An important example of such applications is quantum cryptography, where quantum theory is applied to devise safe protocols for the safe transmission of information. This is often feasible thanks to the fact that, generally speaking, measuring a quantum system unavoidably alters its original state. More concretely, the no-cloning theorem states that it is impossible to measure information that distinguishes between two non-orthogonal quantum states without altering them. This is useful for quantum communications because it implies that an eavesdropper cannot read a message without disturbing it, and there exist procedures to check that an original state has not

who is trying to send a message to her accomplice Bob, making sure that the information will not be intercepted and read by an adversary eavesdropper, called Eve. This discussion will follow the presentation of EPR quantum key distribution found in [2].

Now, suppose that Alice and Bob share a supply of qubits that are entangled in pairs, in such a way that all pairs are in the state $j^{+}i = \frac{1}{\sqrt{2}}$

$$(\ {}^{(A)}_{3}\ {}^{(B)}_{3})|+\rangle = (\ {}^{(A)}_{3}\ {}^{(B)}_{3})\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$= \frac{1}{\sqrt{2}}(\ {}^{(A)}_{3}|0\rangle\ {}^{(B)}_{3}|0\rangle + \ {}^{(A)}_{3}|1\rangle\ {}^{(B)}_{3}|1\rangle)$$

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

There are different variations of the quantum key distribution procedure presented above. For instance, instead of using an ensemble of entangled pairs that was previously created and distributed, Alice can prepare the $|\Psi^+\rangle$ ensemble herself, measure a single qubit from each pair, and then send the other half of each pair to Bob. This is equivalent to preparing and sending, for each pair, one of the four states

$$|\uparrow_z\rangle, |\downarrow_z\rangle, |\uparrow_x\rangle, |\downarrow_x\rangle$$

chosen at random with equal probability 1/4. This variation is called the BB84 quantum key distribution protocol, and it is fundamentally equivalent to the entanglement-based scheme.

Finally, we comment on an important fact about the robustness of quantum cryptography against errors due to channel imperfections. It can be shown that, if the channel error rate is low enough, the $|\uparrow_z\rangle, |\downarrow_z\rangle$ th/4.

As a particular case, we see that the BB84 quantum key distribution protocol is safe against eavesdropping as a consequence of the no-cloning theorem, given that the four states $|\uparrow_z^+\rangle, |\downarrow_z^-\rangle, |\uparrow_x^+\rangle, |\downarrow_x^-\rangle$ being sent are not all mutually orthogonal, and their generation is random so that there is no way for the eavesdroppers to know which state is being sent.

On the other hand, if the only states being used in the protocol where $|\uparrow_x^+\rangle, |\downarrow_x^-\rangle$ or $|\uparrow_z^+\rangle, |\downarrow_z^-\rangle$ (in general, sets of mutually orthogonal states), there are of course corresponding choices of measurements that will identify one of the two states inside the pair without altering the state. This of course happens for the measurement of an operator that has the two possible outcomes (i.e. the two possible states being transmitted) as eigenstates. For instance, $|\uparrow_x^+\rangle, |\downarrow_x^-\rangle$ can be perfectly distinguished without alteration if we measure σ_x on them (and similarly for $|\uparrow_z^+\rangle, |\downarrow_z^-\rangle$ and σ_z), which of course implies that they can be copied perfectly without disturbing them. In fact, the notions of distinguishing between arbitrary states and copying them are equivalent. The direction just used is obvious. For the other direction, suppose that we are free to make copies of a quantum state, say, a qubit $|\psi\rangle$. Then, we can create an ensemble of identical $|\psi\rangle$s large enough to measure non-commuting observables such as $\sigma_x, \sigma_y, \sigma_z$ as many times as needed to determine their mean values. In the limit of infinite measurements of each σ_i, which is achievable thanks to our assumed ability to copy $|\psi\rangle$ infinitely many times, the mean values measure approach the spin components $\langle\psi|\sigma_i|\psi\rangle$ to a perfect accuracy. But this components together determine the qubit state $|\psi\rangle$ exactly. Therefore, the fact that nonorthogonal states cannot be distinguished implies also that it is not possible to arbitrarily copy quantum states, and the two concepts are thus equivalent.

Of course, it was reasonable to expect the fact that the no-cloning theorem does not prohibit the copy of orthogonal quantum states. Indeed, it is perfectly feasible to copy arbitrary bits in the context of classical information, and sets of orthogonal quantum states can be interpreted as classical bits of information. In other words, a qubit that is restricted to stay in $\{|0\rangle, |1\rangle\}$ (with no linear combinations of the two allowed) is just a classical bit with two possible values, and as such it can be copied in principle. In fact, this is illustrated by the following unitary tranformation:

$$\begin{aligned} U : |0\rangle_A|0\rangle_E &\to |0\rangle_A|0\rangle_E \\ |1\rangle_A|0\rangle_E &\to |1\rangle_A|1\rangle_E ; \end{aligned} \tag{8}$$

which copies the first bit onto the second slot. But, of course, U does not act in the same way for other input qubits (that is, for states that are in a superposition of $|0\rangle$ and $|1\rangle$). This remark concludes our introduction to the no-cloning theorem and, by extension, to its central role in quantum cryptography.

References

[1] Rivest, Ronald L (1990). Cryptography, In J. Van Leeuwen (ed.). Handbook of Theoretical Computer Science. Vol. 1. Elsevier.

[2] Preskill, John (2001). Lecture Notes for Ph219/CS219: Quantum Information and Computation, Chapter 4 , California Institute of Technology.