The No-Cloning Theorem

Mikko Lahola

February 27th, 2008

- In the Bennett-Brassard key distribution protocol Alice and Bob can generate a shared secret key through the usage of quantum signals from Alice to Bob.
- This should foil an eavesdropper Eve's plans on getting hold of information about the key through measuring the signals since:
- a) Eve can only be sure of getting a correct bit of the signal if she guesses the base correctly and cannot determine if the guess has been correct or not
- b) the measuring can modify the signal and cause Alice and Bob to detect the presence of Eve

- But what if Eve would not make any measurements at all but instead tried to make a personal copy of each photon as it passes?
- If she would be able to do this then she could wait until - per protocol - Alice would publicly transfer information about the used basis and with the correct basis decode the secret key bits from the copy.
- In this presentation we will see that full copying of a quantum object while preserving the original copy is in the general sense theoretically impossible.

- Definition: Let $|s\rangle = \begin{pmatrix} s_1 \\ s_2 \end{pmatrix}$ and $|m\rangle = \begin{pmatrix} m_1 \\ m_2 \end{pmatrix}$ be a pair of two-dimensional complex vectors. The inner product between $|s\rangle$ and $|m\rangle$ is denoted $\langle s|m\rangle$ and is defined to be the complex number $\overline{s_1}m_1 + \overline{s_2}m_2$

- Definition: Let M be an operator. The adjoint of M, denoted M^*, is the complex conjugate of the transpose of M.
- Definition: Let U be an operator. We say that U is unitary iff $U^*U = I$, where I is the identity matrix.
- The third rule from the basic quantum mechanical rules for arbitrary polarizations of a photon: Every allowed reversible physical transformation on the polarization of a photon is represented by a 2 x 2 unitary matrix U, and every such U represents an allowed transformation.

- Definition: Let $|v\rangle = \sum_i v_i |b^{(i)}\rangle$ be an element of H_N and $|w\rangle = \sum_j w_j |c^{(j)}\rangle$ be an element of H_M. The tensor product of $|v\rangle$ with $|w\rangle$ is denoted $|v\rangle \otimes |w\rangle$ and is defined to be the vector $\sum_{ij} v_i w_j |b^{(i)} c^{(j)}\rangle$ in $H_N \otimes H_M$.
- The composite system rule: Let H_N and H_M, of dimensions N and M respectively, be the state spaces of two quantum variables A and B. Then the allowed states of the combined system consisting of both A and B are represented by the normalized vectors in $H_N \otimes H_M$. The combined system follows all the rules of quantum mechanics for a variable with NM dimensions.

- If we have access to information in a classical sense we can make "copies" of the information without any theoretical limits. The claim of the No-Cloning Theorem is that in the case of quantum information perfect copying is impossible unless the information is "essentially classical".
- To prove the theorem we formalize the idea of cloning quantum information mathematically.

- Consider a quantum object that could be in any of a number of states $|s_1\rangle, |s_2\rangle, ..., |s_m\rangle$.
- We would like to copy the state of the object faithfully if the state resides in the set of some specific states $|s_i\rangle$ (as opposed to copying arbitrary states).
- Assume that we are given a similar quantum object in a known state $|0\rangle$ to which we would like to copy the state of the previous object.
- This is possible iff there exists an unitary transformation U with the following effect: $U(|s_i\rangle \otimes |0\rangle) = |s_i\rangle \otimes |s_i\rangle$ for each of the possible states $|s_i\rangle$.

- Lemma 1: Unitary transformations preserve inner products. To put it in another way, if $|v\rangle$ and $|w\rangle$ are two vectors and $|y\rangle = U|v\rangle$ and $|z\rangle = U|w\rangle$ then $\langle v|w\rangle = \langle y|z\rangle$.
- Lemma 2: Inner product of two tensor product states is an ordinary product of two separate inner products in the following way: $(\langle a| \otimes \langle b|)(|c\rangle \otimes |d\rangle) = \langle a|c\rangle\langle b|d\rangle$, where $|a\rangle$ and $|c\rangle$ are two possible quantum states of some object A and $|b\rangle$ and $|d\rangle$ are two possible quantum states of some object B.

- Starting from
  $U(|s_i\rangle \otimes |0\rangle) = |s_i\rangle \otimes |s_i\rangle$
  we set
  $|v\rangle = |s_i\rangle \otimes |0\rangle$,
  $|w\rangle = |s_j\rangle \otimes |0\rangle$
  and apply Lemma 1 to get
  $(\langle s_i| \otimes \langle 0|)(|s_j\rangle \otimes |0\rangle) = (\langle s_i| \otimes \langle s_i|)(|s_j\rangle \otimes |s_j\rangle)$.
- Applying Lemma 2 to each side separately gives
  $\langle s_i|s_j\rangle\langle 0|0\rangle = \langle s_i|s_j\rangle\langle s_i|s_j\rangle$.
- Therefore $\langle s_i|s_j\rangle$ must be either 1 or 0.

- The inner product being 1 would mean that the states s_i and s_j are identical and being 0 it would mean that the states are orthogonal.
- Therefore a quantum state chosen from a given set of states can be cloned perfectly only if the states in the set are mutually orthogonal.
- This however would remove the ambiguity in the relation among quantum states and therefore make the information being cloned essentially classical.
- The ambiguity is used in e.g. Bennett-Brassard where the four states $|\updownarrow\rangle$, $|\leftrightarrow\rangle$, $(|\updownarrow\rangle + |\leftrightarrow\rangle)/\sqrt{2}$ and $(|\updownarrow\rangle - |\leftrightarrow\rangle)/\sqrt{2}$ are not all mutually orthogonal.

- Although perfect cloning of quantum information is impossible one of the best known eavesdropping strategies against the Bennett-Brassard scheme uses some of the ideas discussed earlier and is called "partial cloning".
- The idea is that the eavesdropper Eve prepares a photon of her own in a right-hand circular polarization state and together with Alice's photon the composite system is allowed a certain interaction that can be viewed as an unitary transformation.
- Eve stores her own photon after the interaction and Alice's photon is allowed to continue its travel to Bob without any further disturbances.

- Eve's stored photon will not generally be an exact clone of Alice's photon and the interaction causes disturbance to Alice's photon which might be caught later on during the protocol.
- Still, the Renyi information per probability of causing an error ratio turns out to be better than with the strategy involving measurement of the received photon and a resend of a prepared copy of it to the real receiver ("measure-resend" strategy).

- Cloning quantum information perfectly turned out to be theoretically impossible.
- It is however possible to devise an interaction where the eavesdropper is able to make an approximate clone of a photon while causing some disturbance to the original signal.
- It is also possible to clone quantum information (for an example to some distance) if we don't require that the original copy should survive the process ("faxing with destruction"). The technique is called quantum teleportation.