Introduction to quantum information and quantum cryptography: Lecture 4

WANTED

DEAD **&** ALIVE

Schrödinger's cat

$$\frac{1}{\sqrt{2}}(|\mathrm{DEAD}\rangle + |\mathrm{ALIVE}\rangle)$$

Some simple applications of entanglement

Dense coding

Using this method, Bob can send Alice (or vice versa) two bits of classical information by transmitting only one qubit. This protocol is based – what a surprise – on quantum entanglement.

In the beginning, Alice and Bob share an entangled pair of qubits whose state is one of the four Bell states:

$$|\Phi_-\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|01\rangle_{AB} - |10\rangle_{AB}\right), \tag{1}$$

where indeces A and B refer to the name of the person who has the given member of the pair.

Dense coding

As we know, the four Bell states form an orthonormal basis in the four dimensional Hilbert space, and they have the following shapes:

$$|\Phi_{\pm}\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle \pm |10\rangle\right)$$

$$|\Psi_{\pm}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle \pm |11\rangle\right).$$

Dense coding

Suppose Alice performs one of the four preconcerted unitary operations on the qubit she has. The four possible operataions are enumerated below:

- she applies operator $\hat{I}$ on her qubit: or in other words, she does nothing
- she applies operator σ_x
- she applies operator σ_y
- she applies operator σ_z

Dense coding

Let us recall the shapes of the three Puali matrices and the unit operator, then try to find out their effect on Alice's single qubit, finally calculate the resulted two-particle states. So, the shape of the three Pauli matrices and the unit operator can be seen below:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}; \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}; \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix};$$

$$\hat{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Dense coding

Now, let us see their effect on a single quantum bit whose state can be either $|0\rangle$ or $|1\rangle$:

$$\sigma_x|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$$

$$\sigma_x|1\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle.$$

Dense coding

The other four results can be derived similarly:

$$\sigma_y|0\rangle = i|1\rangle$$

$$\sigma_y|1\rangle = -i|0\rangle$$

$$\sigma_z|0\rangle = |0\rangle$$

$$\sigma_z|1\rangle = -|1\rangle$$

Dense coding

Finally, we are interested in the two-particle states resulted by the four different operations of Alice. Let us see how will the initial entangled state in equation (1) be altered by Alice's operations. In case she works with operator $\hat{I}$, it is evident the state remains the same:

$$|\Phi_-\rangle = \frac{1}{\sqrt{2}}\big(|01\rangle - |10\rangle\big),$$

where indeces A and B are omitted now.

Dense coding

If he apply σ_x on her qubit the resulted entangled state is

$$\frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right).$$

In case of applying σ_y, they get the following two-particle state:

$$-i\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right).$$

Dense coding

Finally, in case of applying operator σ_z on Alice's single qubit, the common state of the two entangled qubits they share will be changed into the following state:

$$-\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle).$$

Dense coding

Let us realize the four two-particle states which can be resulted by Alice's operation are actually the elements of the orthonormal Bell basis.

The only difference between Bell states (which form the Bell basis) and the state we can obtain is two scalar factors $(-i, -1)$.

Hence any of Alice's operations results a state which is one of the elements of a four dimensional, orthogonal basis.

Dense coding

Knowing this very important fact, we can turn to the second step of the protocol:

After performing her operation, Alice sends her qubit to Bob, hence from the moment he gets Alice's qubit, Bob has the whole system, hence setting four othogonal detectors – correspondently the four possible states – he can find out the resulted state and the corresponsive operation.

Dense coding

There is a crucial point here which has to be realized, namely:

Bob's measurement selects one of the *four* possibilities which means *two bits* of classical information, though Alice sent *one* piece of *quantum bit*..... and this is the reason for the name of this protocol, namely: *dense* coding.

Quantum teleportation

Quantum teleportation

In this protocol, Alice has a qubit denoted by A_1 in a state

$$|\Psi\rangle_{A_1} = \alpha|0\rangle + \beta|1\rangle,$$

and she would like to transfer this state onto Bob's quantum bit denoted by B. It is worth notify that Alice does not even need to know anything about the state of her qubit.

Quantum teleportation

The question is what she can do to reach her goal. As a first idea one can suggest Alice to measure the state of her qubit and to transmit the resulted classical information to Bob.

Unfortunately this strategy would not work, because - as we know - the obtained information is not enough to reconstruct an arbitrary, unknown state (as we know this is caused by the effect of the measurement on the state vector).

Quantum teleportation

In the method of quantum teleportation, Alice and Bob share an entangled pair, A_2, B in one of the Bell states:

$$|\Phi_-\rangle_{A_2B} = \frac{1}{\sqrt{2}}\left(|01\rangle_{A_2B} - |10\rangle_{A_2B}\right).$$

Quantum teleportation

The whole state of their three qubits, the one whose state is to be teleported, and the entangled pair can be expressed as a tensor product:

$$|\Psi\rangle_{A_1}|\Phi_-\rangle_{A_2B} = \frac{1}{\sqrt{2}}\left(\alpha|0\rangle_{A_1} + \beta|1\rangle_{A_1}\right)\left(|01\rangle_{A_2B} - |10\rangle_{A_2B}\right) =$$

$$= \frac{1}{\sqrt{2}}\left(\alpha|00\rangle_{A_1A_2}|1\rangle_B - \alpha|01\rangle_{A_1A_2}|0\rangle_B + \beta|10\rangle_{A_1A_2}|1\rangle_B\right.$$

$$\left. -\beta|11\rangle_{A_1A_2}|0\rangle_B\right)$$

Quantum teleportation

Instead of using a product basis, let us rewrite this expression into another shape via the elements of the Bell basis spanned by the four basis vectors below:

$$|\Phi_{\pm}\rangle = \frac{1}{\sqrt{2}}\big(|01\rangle \pm |10\rangle\big)$$

$$|\Psi_{\pm}\rangle = \frac{1}{\sqrt{2}}\big(|00\rangle \pm |11\rangle\big).$$

Quantum teleportation

From these elements, it directly follows that

$$\sqrt{2}|\Phi_{\pm}\rangle = |01\rangle \pm |10\rangle$$

$$\sqrt{2}|\Psi_{\pm}\rangle = |00\rangle \pm |11\rangle.$$

Quantum teleportation

Using these equations, after a trivial calculation we obtain that

$$\frac{1}{\sqrt{2}}\left(|\Phi_+\rangle + |\Phi_-\rangle\right) = |01\rangle$$

$$\frac{1}{\sqrt{2}}\left(|\Phi_+\rangle - |\Phi_-\rangle\right) = |10\rangle$$

$$\frac{1}{\sqrt{2}}\left(|\Psi_+\rangle + |\Psi_-\rangle\right) = |00\rangle$$

$$\frac{1}{\sqrt{2}}\left(|\Psi_+\rangle - |\Psi_-\rangle\right) = |11\rangle.$$

Quantum teleportation

If we use these results, we can continue rewriting the initial expression of the whole state, namely

$$|\Psi\rangle_{A_1}|\Phi_-\rangle_{A_2B} = \frac{1}{2}\Big[\alpha\big(|\Psi_+\rangle + |\Psi_-\rangle\big)|1\rangle_B - \alpha\big(|\Phi_+\rangle + |\Phi_-\rangle\big)|0\rangle_B +$$

$$\beta\big(|\Phi_+\rangle - |\Phi_-\rangle\big)|1\rangle_B - \beta\big(|\Psi_+\rangle - |\Psi_-\rangle\big)|0\rangle_B\Big] =$$

$$\frac{1}{2}\Big[|\Psi_+\rangle_{A_1A_2}\big(\alpha|1\rangle_B - \beta|0\rangle_B\big) + |\Psi_-\rangle_{A_1A_2}\big(\alpha|1\rangle_B + \beta|0\rangle_B\big) +$$

$$|\Phi_+\rangle_{A_1A_2}\big(-\alpha|0\rangle_B + \beta|1\rangle_B\big) + |\Phi_-\rangle_{A_1A_2}\big(-\alpha|0\rangle_B - \beta|1\rangle_B\big)\Big]$$

Quantum teleportation

The key element of this process can be seen in the last two rows. What is it all about?

We can see Alice has two quantum bits, A_1 and A_2. What if she makes a Bell measurement on the system of these two qubits (which is the subsystem of the whole threepartite qubit system)?

Quantum teleportation

Let us remember, in case of a Bell measurement on a bipartite system like Alice has, one of the four Bell states will be resulted.

As we can see in the last two rows, after making her measurement, the (eigen)state of Alice's subsystem can be one of the well known Bell states.

Quantum teleportation

Nevertheless, what is more, let us focus on the state of Bob's qubit after Alice's measurement, say, what if the resulted state of Alice's qubits is $|\Phi_+\rangle_{A_1A_2}$?

As we can see, in this case the state of Bob's qubit will be $-\alpha|0\rangle_B + \beta|1\rangle_B$, because the whole threepartite system will get to the state $|\Phi_+\rangle_{A_1A_2}\big(-\alpha|0\rangle_B + \beta|1\rangle_B\big)$ by Alice's measurement.

Quantum teleportation

Why is it so important? To answer this question we need to realize the fact that if Bob knew Alice's result ($|\Phi_+\rangle_{A_1A_2}$), he would know what to do to get the state Alice wanted to teleport to him.

Four instance, in the discussed case, he would make a unitary transformation on his qubit state. The question is what kind of transformation should be done by Bob?

The answer is nearly trivial: the respective operator of the transformation is $-\sigma_z$.

Quantum teleportation

Let us try to find out if it is true or not: the matrix which represents $-\sigma_z$ is

$$-\sigma_z = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Once again: in case Alice's measurement results the state $|\Phi_+\rangle_{A_1A_2}$, Bob's qubit will be in $-\alpha|0\rangle_B + \beta|1\rangle_B$.

Quantum teleportation

Let us see the effect of $-\sigma_z$ on this state:

$$-\sigma_z(-\alpha|0\rangle_B + \beta|1\rangle_B) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -\alpha \\ \beta \end{pmatrix} =$$

$$= \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha|0\rangle_B + \beta|1\rangle,$$

which means the state of Bob's qubit after making the transformation is exactly the same like the state which was wanted to teleport by Alice.

All she had to do was to send the result of her Bell measurement to Bob.

Quantum teleportation

This is almost exactly the case when any of the three other possible outcomes is resulted by Alice's measurment. The only difference is the kind of the transformation which has to be applied by Bob on his quantum bit to get the state to be teleported. These "result – transformation" pairs are scheduled in the table below:

result of Alice's Bell measurement	$\|\Phi_+\rangle$	$\|\Phi_-\rangle$	$\|\Psi_+\rangle$	$\|\Psi_-\rangle$
Bob's transformation	$-\sigma_z$	$-\hat{I}$ (or $\hat{I}$)	$-\sigma_x\sigma_z$	σ_x

Quantum teleportation

Let us summarize the discussed process of quantum teleportation. In the beginning the two parties share an entangled state consisting of two qubits.

On Alice's side there is another qubit whose state is wanted to teleport (or in other words to transfer onto Bob's qubit) by Alice.

Quantum teleportation

To reach her goal, Alice makes a Bell measurement on her two qubits and then she messages her result to Bob via a classical channel.

Knowing Alice's result, Bob knows what kind of transformation has to be applied on his quantum bit to transfer / teleport the state of qubit A_1 onto his quantum bit.

Quantum teleportation

There is a very important fact which we have to realize:

This protocol is *not* copying / cloning, because the quantum bit – A_1 – which was in the teleported state initially, will be in a totally different state after applying the protocol.

Quantum teleportation

And another interesting remark:

In case we do not know the state to be cloned, we can not clone it (if we know the state, we can prepare it and there is no need to clone), on the other hand, we can teleport any of the states, even if we do not know anything about it.

E91 quantum key distribution protocol

E91 quantum key distribution protocol

In 1991 Artur Ekert suggested a protocol based on shared entanglement instead of sending particles via a quantum channel (as we saw it in the case of BB84 protocol).

Let us suppose a source sending entangled quantum bit pairs to Alice and Bob. One member of each qubit pair is sent to Alice and the other one is sent to Bob.

E91 quantum key distribution protocol

Each qubit pair is in a singlet state which is the same in both X basis and Y basis. We already know the elements of X basis, namely: $\{|+\rangle; |-\rangle\}$.

Nevertheless, also the basis vectors of Y were mentioned in a subsection (titled *The quantum theory of the half spin: two component spinors and Pauli matrices*) of the textbook on the quantum mechanical background of this subject, where we wrote the eigenvectors of σ_y Pauli matrix.

E91 quantum key distribution protocol

These eigenvectors, $|\pm\rangle_y = \frac{1}{\sqrt{2}}(|0\rangle \pm i|1\rangle)$, where

$$|+\rangle_y = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ i\end{pmatrix} \quad \text{and} \quad |-\rangle_y = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ -i\end{pmatrix},$$

span the Y basis.

As we said, the singlet state of the qubit pairs has equivalent expressions on both X and Y basis:

$$\frac{1}{\sqrt{2}}\left(|+\rangle_A|-\rangle_B - |-\rangle_A|+\rangle_B\right) = \frac{1}{\sqrt{2}}\left(|+\rangle_{y_A}|-\rangle_{y_B} - |-\rangle_{y_A}|+\rangle_{y_B}\right).$$

E91 quantum key distribution protocol

This is true, because on X basis, it has the following shape:

$$\frac{1}{\sqrt{2}}(|+\rangle|-\rangle - |-\rangle|+\rangle) = \frac{1}{\sqrt{2}}\left(\begin{pmatrix} 1 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ -1 \end{pmatrix} - \begin{pmatrix} 1 \\ -1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right) =$$

$$= \frac{1}{\sqrt{2}}\left(\begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix} - \begin{pmatrix} 1 \\ 1 \\ -1 \\ -1 \end{pmatrix} \right) = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ -2 \\ 2 \\ 0 \end{pmatrix}.$$

E91 quantum key distribution protocol

And then on Y basis, its form is the expression below:

$$\frac{1}{\sqrt{2}}(|+\rangle_y|-\rangle_y - |-\rangle_y|+\rangle_y) = \frac{1}{\sqrt{2}}\left(\begin{pmatrix} 1 \\ i \end{pmatrix} \begin{pmatrix} 1 \\ -i \end{pmatrix} - \begin{pmatrix} 1 \\ -i \end{pmatrix} \begin{pmatrix} 1 \\ i \end{pmatrix} \right) =$$

$$= \frac{1}{\sqrt{2}}\left(\begin{pmatrix} 1 \\ -i \\ i \\ 1 \end{pmatrix} - \begin{pmatrix} 1 \\ i \\ -i \\ 1 \end{pmatrix} \right) = i\frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ -2 \\ 2 \\ 0 \end{pmatrix}.$$

We can see the singlet state is the same in both bases (as we know a state and itself multiplied by i are the same states).

E91 quantum key distribution protocol

The point of the protocol is that Alice and Bob autonomously choose a measurement basis from between X and Y randomly and make a measurement in the selected bases.

After this, they communicate each other the basis they chose (but not the result).

In case they chose the same basis, the results of their measurements are perfectly anti-correlated.

E91 quantum key distribution protocol

Hence the presence of an eavesdropper can be detected in exactly the way as we saw in the case of BB84 protocol: they need to check a part of the (raw) key.

Nevertheless, there is an important difference, namely: they can use their measurement results obtained in the cases when they chose different bases, hence they can test if a Bell inequality is violated or not.

In case Eve had taken over the source and were sending particles in definite states to Alice and Bob, for instance a $|+\rangle$ to Alice and a $|-\rangle$ to Bob, then the Bell inequality would not be violated, and Alice and Bob would detect her.