Introduction to quantum information and quantum cryptography: Lecture 3

WANTED

DEAD & ALIVE

Schrödinger's cat

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

Quantum cloning

Quantum cloning

First of all, we have to make the meaning of word *quantum cloning* clear:

Let us suppose we would like to build a machine which is able to create a perfect replica of an arbitrary system being in an unknown quantum state. A tool like that seems to be neceassary for certain information processing tasks. Error correction, for instance, could be done using procedures making use of several perfect copies of the original system carrying the information. Such a creation of one or more exact replicas of physical systems in arbitrary (and unknown) quantum states is termed as quantum cloning. The reason for the name, as we shall see, is that the “cloned” system cannot be in fact distinguished from the original one.

Quantum cloning

It is natural to ask if the laws of quantum mechanics allow us to build such a machine. To put it formally, we consider e.g. a quantum bit in the state. $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$. In addition we need an ancillary sytem which will be the replica. Its initial state can be arbitrary, say $|0\rangle$ w.l.o.g. The desired operation is then

$$|\Psi\rangle|0\rangle \to |\Psi\rangle|\Psi\rangle. \qquad (1)$$

Quantum cloning

Let us first assume that an arbitrary state, say $|\Psi_1\rangle$ can be simply cloned by a unitary operator U:

$$U|\Psi_1\rangle|0\rangle = |\Psi_1\rangle|\Psi_1\rangle. \tag{2}$$

If our machine works as we expected, we can continue cloning with another state $|\Psi_2\rangle$. The state of the target qubit is the same before. In this case we get the following states:

$$U|\Psi_2\rangle|0\rangle = |\Psi_2\rangle|\Psi_2\rangle. \tag{3}$$

Quantum cloning

Due to the unitarity, inner product of the left sides of equations 2 and 3 has to equal the inner product between the right sides of these equations. Hence we obtain the equation below:

$$\langle 0|\langle \Psi_1|U^\dagger U|\Psi_2\rangle|0\rangle = \langle \Psi_1|\Psi_2\rangle^2.$$

After simplifying, we get the following form:

$$\langle \Psi_1|\Psi_2\rangle = \langle \Psi_1|\Psi_2\rangle^2. \tag{4}$$

From equation (4), it directly follows that

$$\langle \Psi_1|\Psi_2\rangle = \begin{cases} 0 \\ 1 \end{cases}. \tag{5}$$

Quantum cloning

As we can see in equation (5), our basic assumption (namely: quantum cloning is a unitary map) leads us results which can be true if and only if we have a total knowledge of the states to be cloned. Obviously, if we knew everyting about these states, we would be able to create them without using any device to clone.

More generally it can be shown that the cloning map in equation (1) is not completely positive, so it is not physical. And this holds not only for quantum bits, but also for any kind of quantum systems. This is the *no cloning theorem* of quantum mechanics first pointed out by Zurek[a].

[a] W. K. Wooters and W. H. Zurek, A single quantum cannot be cloned, Nature **299**, 802 (1982)

Quantum cloning

While thus far we have argued that cloning would be a useful operation in information processing, it is easy to see that the fact of its impossibility has also positive implications from practical point of view. For instance it is a basic ingredient of quantum cryptography.

Quantum cloning

If quantum cloning – in the sense of creating perfect replicas of an unknown state – were a possible map, this protocol would be breakable, because – as we saw it last time – an eavesdropper, after the cloining of the quantum system transmitted between the parties, could make measurements on the clones of the qubits sent by Alice to Bob and the quantum key distribution were not secure anymore.

Conclusion

As we saw, there are two things which makes quantum cryptography unbreakable. On one hand, if Eve makes measurements on the quantum bits she caught, her presence will become visible for the parties of the secret communication.

On the other hand, she can even try to make perfect replicas of the transmitted quantum bits to circumvent the protocol, but quantum cloning is forbidden by the fundamental laws of quantum mechanics, hence she does not have any possibility to break the safety of quantum cryptography.

Conclusion

Nevertheless, as usual, a real life situation is never as simple as the presented one. For example, quantum channels are not ideal channels, but more or less they are noisy.

In addition to this, although, to make perfect replicas of a quantum system which is in an unknown quantum state is an impossible quantum map – as we saw – , imperfect clones can be done by a device called *quantum cloner*[a].

[a] This device and some related things will be shortly presented in a future chapter.

Conclusion

In case the effect introduced by the cloning process is smaller than the noise caused by the channel, an eavesdropper can pass undetected. Naturally (and fortunately) there are strategies to eliminate this problem, but the discussion of these methods points beyond the frame of our short course.

Quantum entanglement

Quantum entanglement

From this slide, we begin to learn about *quantum entanglement*. The reason for this is that there are a lot of quantum protocols which can not be understood without knowing this phenomenon.

Besides being a very interesting topic, without quantum entanglement, several quantum protocols (e. g. quantum teleportation, dense coding, E91 quantum key distribution protocol, some of the quantum error correction processes, etc.) were not possible.

Quantum entanglement

Let us get acquinted with the phenomenon of quantum entanglement and outline its aspects which are relevant for our course. We say that the quantum state $|\Psi\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$ of a bipartite system is *separable* if it is a product of states of each subsystem:

$$|\Psi\rangle = |\Psi_1\rangle\,|\Psi_2\rangle\,, \quad |\Psi_1\rangle \in \mathcal{H}_1,\ |\Psi_2\rangle \in \mathcal{H}_2. \tag{6}$$

If a state is not separable, it is *entangled*.

Quantum entanglement

The definition can be obviously extended to multipartite systems. And as we shall see later, the entanglement of multipartite systems bears a rich structure.

Quantum entanglement

If a pure state $|\Psi\rangle$ is separable, then all the subsystems are in a pure state. Thus their density operators are projectors. E.g. for

$$\varrho^{(1)} = \mathrm{Tr}_2 \, |\Psi\rangle \langle\Psi| \tag{7}$$

we have

$$\left(\varrho^{(1)}\right)^2 = \varrho. \tag{8}$$

As $\mathrm{Tr}\,\varrho = 1$, it implies that

$$\mathrm{Tr}\left(\varrho^{(1)}\right)^2 = 1. \tag{9}$$

This holds for all the subsystems if and only if the state is separable.

Quantum entanglement

Considering a bipartite system this leads to a possibility of quantifying entanlgement: the “more mixed” a subsystem is, the more entangled the state is. The mixedness of the state is commonly measured by the von Neumann entropy of the density operator

$$H(\varrho) = -\operatorname{Tr}(\varrho \log_2 \varrho), \tag{10}$$

which bears a sound information theoretic interpretation.

Quantum entanglement

In a d-dimensional system its maximum value is $\log_2 d$, attained by the state

$$\varrho_{CM} = \frac{1}{d}\hat{I}. \tag{11}$$

This is termed as the completely mixed state.

It is the only state which produces a uniform distribution of measurement results when measured in any possible basis. For reasons not detailed here the partial traces of a pure bipartite state have the same von Neumann entropy. Hence it is reasonable to say that the *entanglement* of the state is quantified by

$$E\left(|\Psi\rangle\right) = H\left(\mathrm{Tr}_2 |\Psi\rangle\langle\Psi|\right) \tag{12}$$

Quantum entanglement

For practical reasons it is worth mentioning that a mathematically simpler quantity can also be used to quantify the mixedness of the state, and thus entanglement, albeit without an operational or direct information theoretic meaning.

Its construction stems from the fact that Eq. (9) holds if the state is pure. As the diagonal elements of the density matrix describe a probability distributions, for mixed states we have

$$\mathrm{Tr}\,\varrho^2 < 1. \tag{13}$$

Quantum entanglement

Hence, the trace of the square of the density matrix is related to the purity of the state in a way. It can be shown that its minimum value is $1/d$ attained by the completely mixed state only.

For quantum bits (i.e. $d = 2$ we can thus construct a quantity with in the $[0, 1]$ range (just like the von Neuman entropy):

$$H_{\text{lin}}(\varrho) = 2\left(\frac{1}{2} - \varrho^2\right). \tag{14}$$

This is termed as the *linear entropy* of the state.

It can be easily verified that the von Neumann entropy is a monotone function of the linear entropy, and so that of its square root. Hence, entanglement can be described also in terms of concurrence

$$C\left(|\Psi\rangle\right) = \sqrt{H_{\mathrm{lin}}\left(\mathrm{Tr}_2\, |\Psi\rangle\,\langle\Psi|\right)}. \tag{15}$$

The entanglement in Eq. (12) is its monotone function in the same range, it can be evaluated with less effort, but does not admit an operational interpretation.

Mixed state entanglement

Mixed state entanglement

If a multipartite system is in a mixed state, its entanglement properties are far more complex. As for the definition, a mixed state is said to be a separable one, if it can be constructed as a convex combination of separable pure states or – in other words – it has a form like

$$\varrho = \sum_i p_i |\Psi_i\rangle\langle\Psi_i| \tag{16}$$

in which every $|\Psi_i\rangle$ is separable. Unseparaple mixed states are called entangled.

Mixed state entanglement

In many cases it is hard even to decide if a state is separable or entangled at all: obviously in this case the subsystems of a separable state may well be mixed.

Consider the complete mixture of two qubits as an example. It is obviously separable (the density operator being proportional the equal-weight convex combination of the projectos of an arbitrary orthonormal basis, including any product-state basis). Both subsystems are in a completely mixed state though.

Mixed state entanglement

Also, while pure-state entaglement is fully characterized by the quantity in Eq. (12), for mixed states there are several similar quantities which coincide for pure states but they have different operational meanings otherwise.

One of them is *entanglement of formation* defined as follows:

$$E(\varrho) = \inf_{\substack{(p_k,\ |\psi_k\rangle \text{ separable}) \\ \sum_k p_k |\psi_k\rangle\langle\psi_k| = \varrho}} \sum_k p_k E(|\psi_k\rangle), \tag{17}$$

that is, the infimum of the average of the entaglements of all the constituent pure states over all of its pure-state decompositions. As we deal with finite dimensional states, the infimum can be understood as minimum.

Mixed state entanglement

A similar quantity can be defined via concurrence:

$$C(\varrho) = \inf_{\substack{(p_k,\ |\psi_k\rangle \text{ separable}) \\ \sum_k p_k |\psi_k\rangle\langle\psi_k| = \varrho}} \sum_k p_k C(|\psi_k\rangle), \tag{18}$$

It can be shown that entanglement of formation is its monotone function, and in the special case of two qubits it can be calculated analytically. This is the celebrated Wootters formula which is very broadly used in the literature, including our work. Hence we describe it in what follows. For the detailed derivations we refer to the original papers.

The Wootters formula

The Wootters formula

In order to calculate the concurrence of a two-qubit state ϱ, first we define the Wootters tilde operation:

$$\tilde{\varrho} = (\sigma_y \otimes \sigma_y)\varrho^*(\sigma_y \otimes \sigma_y), \tag{19}$$

where $*$ means the complex conjugation (or, otherwise speaking, the transpose) of the density matrix in a product state basis, whereas σ_y is the second Pauli-operator.

The Wootters formula

Next the spectrum of the Hermitian operator has to be determined

$$\sqrt{\sqrt{\varrho}\tilde{\varrho}\sqrt{\varrho}}. \tag{20}$$

Its eigenvalues λ are in fact the square roots of the eigenvaluses of the (non-Hermitian) operator

$$\varrho\tilde{\varrho}. \tag{21}$$

Let us put the eigenvalues $\lambda_1, \lambda_2, \lambda_3, \lambda_4$ to decreasing order. The concurrence then reads

$$C(\varrho) = max\{0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4\} \tag{22}$$

We shall employ this latter formula when calculating concurrence in some future lessons.

Entanglement of multi-qubit systems

Entanglement of multi-qubit systems

It may be an interesting question how can be featured the entanglement of two chosen quantum bits in a system consisting of N quantum bits, if the whole system is in a pure state. As an illustration, let us consider the following specific example: we have three quantum bits in a state which is called Greenberger-Horne-Zeilinger (GHZ) state:

$$|\Psi_{\mathrm{GHZ}}\rangle_{123} = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle). \quad (23)$$

Entanglement of multi-qubit systems

In this case, the state of the first two quantum bits is described by the density operator

$$\varrho_{12} = \frac{1}{2}(|00\rangle\langle 00| + |11\rangle\langle 11|). \tag{24}$$

This state is obviously entangled. In fact, all the subsystems are in a completely mixed state.

Entanglement of multi-qubit systems

When considering any of the two qubits (e.g. the first two, any of them can be choosen for symmetry reasons), however, using the formula in (22), for this density operator, we get $C(\varrho_{12}) = 0$. This means that state (24) is a separable state or, in other words, the first two quantum bits are not entangled with each other as a pair.

Entanglement of multi-qubit systems

It means that in the present entangled state there is no qubit-pair entanglement whatsoever.

Indeed, after carrying out a measurement on the third quantum bit in the basis $|0\rangle$, $|1\rangle$, the state of the first two quantum bits will be either $|00\rangle$ or $|11\rangle$ with equal probability. This means that the bipartite state can be constructed as a convex combination of separable pure states.

Entanglement of multi-qubit systems

So the entanglement of the first two quantum bits can be juggled away by achieving measurement on the third one. Due to the symmetry of the state, this holds true of the case of any pair of quantum bits in this state.

In the GHZ state (23), the state of any quantum bit pair can be separated. The whole system is an entagled state, after all!

Entanglement of multi-qubit systems

State (23) is not separable. This can be seen, if we choose one of the three quantum bits, its state, according to (11), is a maximally mixed state, that is, the chosen quantum bit is maximally entangled with the subsystem of the other two quantum bits.

Hence, the entanglement present in this state is *genuine threepartite*.

Interestingly, it can be converted to maximal bipartite entanglement though. Carrying out a properly chosen measurement on one of the quantum bits, we can make the state of the system of other two quantum bits maximally entangled.

Indeed, if the eigenvectors of the measurement are now $\frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$, we get the maximally entangled states $\frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$ with equal probability.

Both states are maximally entangled bipartite states. If we are aware of the measurement result, we know which state we have obtained, so we can use it, e.g. for teleportation[a]. In this system, its tripartite entanglement can be completly converted into a bipartite entanglement.

[a] more on this later

Monogamy of entanglement

Monogamy of entanglement

Note that a maximally entangled state of two quantum bits is necessarily a pure state. Hence the two quantum bits cannot be entangled with any other system.

This means that (unlike classical correlations) quantum entanglement has a property which is called *monogamy*: pairwise entanglement of two subsystems limits the entanglement with the other subsystems.

Monogamy of entanglement

As for a quantitative description of monogamy, we introduce another quantity which we will use in our work. This is the *tangle* denoted by τ, which is the linear entropy in Eq. (14) of a given subsystem, which, for qubits can also expressed as

$$\tau_k = 4\mathrm{det}\varrho(k).$$

This is the so-called one-tangle, characterizing the entanglement between the given qubit and the rest of the total system which is in a pure state.

Monogamy of entanglement

In case we have two qubits in a pure state, the tangle relating to one of them equals the square of the concurrence. Let us consider a system consisting of many qubits and suppose the system is in a pure state. Checking concurrences of the qubit pairs in the system, we get that Coffmann-Kundu-Wootters (CKW) inequalities[a] are satisfied:

$$\tau_k \geq \sum_{l \neq k} C_{k,l}^2 \tag{25}$$

[a] V. Coffman, J. Kundu, and W. K. Wootters, Phys. Rev. **61**, 052306 (2000)

Monogamy of entanglement

This formula can be interpreted in the following way: the entanglement measured in tangle between the k-th qubit and the rest of the total system gives an upper bound for the concurrence calculated between the k-th qubit and another arbitrary qubit in the system. If these inequalities are saturated, the bipartite entanglement is maximal.

The CKW inequalities had been originally formulated as a conjecture, but they were later proven. Their saturation reflects that the bipartite entanglement is in a way maximal in the system.

Bell inequalities

Bell inequalities

Since entangled states can have stronger correlations than any of the classical correlations can be, they are a valuable resource in quantum communication. Before getting on the protocols based on the phenomenon of quantum entanglement, let us get to know Bell's inequalities to understand what nonclassical correlations mean.

As we know, in quantum mechanics, an observable physical quantity does not have value until we measure it. However, there were (and are) theories according to which – unlike in quantum mechanics – , observables have values, even we have not carried on a measurement on them.

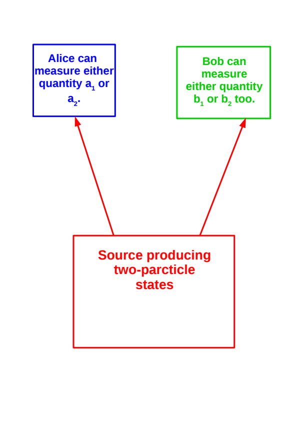
Bell inequalities

Since they depend on some "hidden variables", we do not know their actual values, because we do not know anything about these hidden variables. Bell's inequalities show that in case of very general conditions, hidden variable theories (more precisely: *local* hidden variables theories) yield predictions which conflict with quantum mechanics and – what is more – these can be experimentally tested.

Spoiler: experimetal tests support quantum mechanics and reject the locality of our world. In essence – as we shall see – Bell's inequalities make a philosophical debate testable experimentally. And this was / is the biggest merit of Bell and his inequalities.

Bell inequalities

In case of Bell's inequalities, we can see two observers (see the figure below), namely: Alice and Bob (who else?). Between them, there is a source producing two-particle states. One of these particles is sent to Alice and the other one to Bob.



Bell inequalities

On her particle, Alice can measure one of two quantities, a_1 and a_2. The resulted values of these observable quantities can be either 1 or -1. Similarly, Bob can measure either b_1 or b_2 , and the measured values can equal either 1 or -1, too. The essence of this idea is to execute this gedankenexperiment many times, and use the results to calculate the quantities $\langle a_i b_j \rangle$.

First of all, let us see how a hidden-variable theory would describe this case.

The source produces regulation sets which go with the particles. For instance, one of these regulation set can say, in case Alice measures a_1, she will get 1, and measuring a_2 , she gets -1, furthermore if Bob measures b_1 he will get -1, and in case of measuring a_2 he gets -1. We do not know which regulation set will be produced by the source, hence the regulation set is our hidden variable.

Bell inequalities

This kind of a hidden-variable theory are called *local* theory, because the regulations to Alice's particle do not depend on Bob's decision on the quantity to be measured. That is, the regulation set does not say anything like, measuring a_1, Alice will obtain 1 if Bob measures b_1 and she gets -1 if Bob measures b_2. We will consider local theories only.

Bell inequalities

In a situation like this, a hidden variable can be the state of the source. If we know the source is in some state m, results of the measurments can be prognosticated. Obviously there are 16 possibilities:

value of m	a_1	a_2	b_1	b_2
1	-1	-1	-1	-1
2	-1	-1	-1	1
3	-1	-1	1	-1
4	-1	-1	1	1
.	.	.	.	.
.	.	.	.	.
.	.	.	.	.
16	1	1	1	1

Bell inequalities

Supposing we do not have access to the source, we assume $P(m)$ is a distribution function of the states of the source, or equivalently, a certain number foursome (a_1, a_2, b_1, b_2) can appear with a given probability. This means there is a $P(a_1, a_2, b_1, b_2)$ distribution function. From this it follows that the expectation value $\langle a_1 b_1 \rangle$ can be calculated as

$$\langle a_1 b_1 \rangle = \sum_{a_1=1}^{-1} \sum_{a_2=1}^{-1} \sum_{b_1=1}^{-1} \sum_{b_2=1}^{-1} a_1 b_2 P(a_1, a_2, b_1, b_2).$$

Bell inequalities

There can be possible 4 pieces of correlation functions like this, namely: $\langle a_1 b_1 \rangle$, $\langle a_1 b_2 \rangle$, $\langle a_2 b_1 \rangle$, $\langle a_2 b_2 \rangle$. According to calculations (not detailed here), the following expression yields the biggest value which can be reached by this kind of (classical) correlations:

$$S = \langle a_1 b_1 \rangle + \langle a_1 b_2 \rangle + \langle a_2 b_1 \rangle - \langle a_2 b_2 \rangle =$$

$$= \sum_{a_1=1}^{-1} \sum_{a_2=1}^{-1} \sum_{b_1=1}^{-1} \sum_{b_2=1}^{-1} \left[a_1(b_1 + b_2) + a_2(b_1 - b_2) \right] P(a_1,\, a_2,\, b_1,\, b_2).$$

Bell inequalities

Let us call the expression in brakets multiplying the probability distribution X. As it can be seen

$$X = \begin{cases} a_1(b_1 + b_2), & \text{if} \quad b_1 = b_2 \\ a_2(b_1 - b_2), & \text{if} \quad b_1 \neq b_2. \end{cases}$$

In both cases $|X| = 2$, hence

$$|S| \leq 2 \sum_{a_1=1}^{-1} \sum_{a_2=1}^{-1} \sum_{b_1=1}^{-1} \sum_{b_2=1}^{-1} P(a_1, a_2, b_1, b_2) = 2.$$

Bell inequalities

Expression $|S| \leq 2$ is Bell's inequality. Naturally, similar inequalities can be derived simply by interchanging a_1 and a_2 , b_1 and b_2, or both.

Now, supposing we are measuring the spins of two half-spin particles, we describe the same experiment using the apparatus of quantum mechanics. (a_1 and a_2 (just like b_1 and b_2) can be considered as measurements of the spin (or polarization of a photon) along two different directions.)

Having a quantum source, let us suppose that

$$a_1 = \sigma_{x_a} \quad a_2 = \sigma_{y_a}$$

$$b_1 = \sigma_{x_b} \quad b_2 = \sigma_{y_b},$$

and that the source emits particles in a state which is a maximally entangled pure (bipartite) state (multiplied with a phase factor), or in other words, one of the four Bell states:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + e^{i\frac{\pi}{4}}|11\rangle\right),$$

where

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

$$\sigma_x|1\rangle = |0\rangle \quad \sigma_y|1\rangle = -i|0\rangle.$$

Bell inequalities

In this case

$$\langle a_1 b_1 \rangle = \langle \Psi | \sigma_{x_a} \otimes \sigma_{x_b} | \Psi \rangle =$$

$$= \frac{1}{2} \left[\left(\langle 00| + e^{-i\frac{\pi}{4}} \langle 11| \right) \sigma_{x_a} \otimes \sigma_{x_b} \left(|00\rangle + e^{i\frac{\pi}{4}} |11\rangle \right) \right] =$$

$$= \frac{1}{2} \left(\langle 00| + e^{-i\frac{\pi}{4}} \langle 11| \right) \left(|11\rangle + e^{i\frac{\pi}{4}} |00\rangle \right) = \frac{1}{2} \left(e^{i\frac{\pi}{4}} + e^{-i\frac{\pi}{4}} \right) =$$

$$= \frac{1}{2} 2 \cos \frac{\pi}{4} = \frac{1}{2} 2 \frac{\sqrt{2}}{2} = \frac{\sqrt{2}}{2}.$$

Bell inequalities

Since

$$\langle a_1 b_1 \rangle = \langle a_1 b_2 \rangle = \langle a_2 b_1 \rangle = \frac{\sqrt{2}}{2}$$

and

$$\langle a_2 b_2 \rangle = -\frac{\sqrt{2}}{2},$$

it directly follows that

$$S = \langle a_1 b_1 \rangle + \langle a_1 b_2 \rangle + \langle a_2 b_1 \rangle - \langle a_2 b_2 \rangle = 4\frac{\sqrt{2}}{2} = 2\sqrt{2} \geq 2,$$

that is quantum mechanics violates Bell's inequality.

This fact has three consequences:

- Quantum mechanics – that is our world – can not be described by a local, hidden variable theory. From this, it follows that our world is nonlocal(!).

- In the local hidden variable theory, correlations came from a joint probability distribution function.

- Quantum mechanics can create stronger correlations than classical systems can.