

Entanglement and information

Lately we've spent a lot of time examining properties of entangled states such as

$$|\Psi_{ab}\rangle = \frac{1}{\sqrt{2}}(|0_a 1_b\rangle - |1_a 0_b\rangle).$$

We have learned that they exhibit quantum correlations that are basis-independent, and that they can be used to demonstrate violations of Bell Inequalities. Today we will consider the deceptively simple question of whether states like $|\Psi_{ab}\rangle$ can in any sense be used to *transmit* information from system A to system B .

Technically the answer is no. However, we know of a small but growing number of ways in which entangled states can greatly facilitate the *sharing* or *transmission* of information. In recent years this has become a very active field of theoretical research, and some experiments are even starting to be done.

Let's start by trying to construct an analogy between communication and the "basis-independence" of quantum correlations. Say we have two two-level systems, A and B . We prepare the initial joint state to be

$$|\Psi_{ab}\rangle = \frac{1}{\sqrt{2}}(|0_a 1_b\rangle - |1_a 0_b\rangle),$$

then send system A to our friend Alice and B to our friend Bob. Let's say that Alice and Bob are located far apart from each other, and that Bob decides to make a measurement on the system we have sent him. If Bob performs the measurement specified by

$$\mathbf{P}_0^b = |0_b\rangle\langle 0_b|, \quad \mathbf{P}_1^b = |1_b\rangle\langle 1_b|,$$

then the possible post-measurement states of the joint system are given by

$$\begin{aligned} 0 : |\Psi_{ab}\rangle &\mapsto \frac{\mathbf{1}^a \otimes \mathbf{P}_0^b |\Psi_{ab}\rangle}{\sqrt{\langle \Psi_{ab} | \mathbf{1}^a \otimes \mathbf{P}_0^b | \Psi_{ab} \rangle}} = |1_a 0_b\rangle, \\ 1 : |\Psi_{ab}\rangle &\mapsto \frac{\mathbf{1}^a \otimes \mathbf{P}_1^b |\Psi_{ab}\rangle}{\sqrt{\langle \Psi_{ab} | \mathbf{1}^a \otimes \mathbf{P}_1^b | \Psi_{ab} \rangle}} = |0_a 1_b\rangle. \end{aligned}$$

Hence, if Alice decides to perform the corresponding measurement

$$\mathbf{P}_0^a = |0_a\rangle\langle 0_a|, \quad \mathbf{P}_1^a = |1_a\rangle\langle 1_a|,$$

on her system, her results is guaranteed to be perfectly (anti)correlated with Bob's.

However, given the same initial preparation $|\Psi_{ab}\rangle$, what if Bob decides to perform the alternative measurement

$$\begin{aligned}\mathbf{P}_x^b &= |x_b\rangle\langle x_b|, & \mathbf{P}_x^b &= |y_b\rangle\langle y_b|, \\ |x_b\rangle &= \frac{1}{\sqrt{2}}(|0_b\rangle + |1_b\rangle), \\ |y_b\rangle &= \frac{1}{\sqrt{2}}(|0_b\rangle - |1_b\rangle),\end{aligned}$$

instead? Noting that

$$\begin{aligned}|\Psi_{ab}\rangle &= \frac{1}{\sqrt{2}}(|0_a 1_b\rangle - |1_a 0_b\rangle) \\ &= \frac{1}{\sqrt{2}}\left(\frac{1}{2}(|x_a\rangle + |y_a\rangle)(|x_b\rangle - |y_b\rangle) - \frac{1}{2}(|x_a\rangle - |y_a\rangle)(|x_b\rangle + |y_b\rangle)\right) \\ &= \frac{1}{2\sqrt{2}}\begin{pmatrix} |x_a x_b\rangle - |x_a y_b\rangle + |y_a x_b\rangle - |y_a y_b\rangle \\ -|x_a x_b\rangle - |x_a y_b\rangle + |y_a x_b\rangle + |y_a y_b\rangle \end{pmatrix} \\ &= \frac{-1}{\sqrt{2}}(|x_a y_b\rangle - |y_a x_b\rangle),\end{aligned}$$

the two possible post-measurement joint states will be given by

$$\begin{aligned}x : |\Psi_{ab}\rangle &\mapsto \frac{\mathbf{1}^a \otimes \mathbf{P}_x^b |\Psi_{ab}\rangle}{\sqrt{\langle \Psi_{ab} | \mathbf{1}^a \otimes \mathbf{P}_x^b | \Psi_{ab} \rangle}} = |y_a x_b\rangle, \\ y : |\Psi_{ab}\rangle &\mapsto \frac{\mathbf{1}^a \otimes \mathbf{P}_y^b |\Psi_{ab}\rangle}{\sqrt{\langle \Psi_{ab} | \mathbf{1}^a \otimes \mathbf{P}_y^b | \Psi_{ab} \rangle}} = |x_a y_b\rangle.\end{aligned}$$

Hence, **immediately after** Bob decides to perform the alternative measurement on system B , Alice's system knows to be correlated with Bob's result in the x, y basis instead of the $0, 1$ basis! For example,

$$\begin{aligned}\langle y_a x_b | \mathbf{P}_x^a \otimes \mathbf{1}^b | y_a x_b \rangle &= 0, \\ \langle y_a x_b | \mathbf{P}_y^a \otimes \mathbf{1}^b | y_a x_b \rangle &= 1, \\ \langle y_a x_b | \mathbf{P}_0^a \otimes \mathbf{1}^b | y_a x_b \rangle &= \langle y_a x_b | \mathbf{P}_1^a \otimes \mathbf{1}^b | y_a x_b \rangle = \frac{1}{2}.\end{aligned}$$

Does this imply that some sort of communication, or transfer of information is taking place between A and B regarding Bob's choice of measurement basis? Does it mean that Bob might some how be able to communicate with Alice superluminally (instantaneously) by making use of this effect?

Well the answer to the second question is definitely NO!!

The reason for this is that whichever basis Bob chooses to measure, he still has absolutely no control over the result. So even though we know for sure that Alice's measurement result will be perfectly correlated with Bob's if and only if she uses the same measurement basis, the result she gets in any one measurement is still just a random binary variable – just like Bob's! We can see this by noting that

$$\tilde{\rho}_A = \frac{1}{2}\mathbf{1}^a, \quad \tilde{\rho}_B = \frac{1}{2}\mathbf{1}^b,$$

and

$$\text{Tr}\left[\frac{1}{2}\mathbf{1}\mathbf{P}_q\right] = \frac{1}{2}$$

for *any* rank-one projector \mathbf{P}_q .

Regardless of what Bob does in terms of choosing measurement basis during a sequence of preparations and measurements, Alice just gets a string of random bits that have no correlation whatsoever with Bob's **choices** of measurement bases. Alice's bits may be correlated with Bob's bits, but Bob's bits are totally random and no messages can be exchanged by this procedure.

And what about the first question, of whether the basis-independence of quantum correlations might imply that some sort of transfer of information is taking place between A and B regarding Bob's choice of measurement basis? Even though it is impossible for Alice and Bob to utilize this effect for instantaneous communication, some people like to think that some sort of abstract "information" is indeed flying from B to A (or vice versa) in these sorts of scenarios. Given what **we** know about the interpretation of quantum states, however, it seems clear that no such magic need be invoked! The quantum collapse of the joint state vector immediately following Bob's measurement is simply a formal reflection of the fact that

$$|\Psi_{ab}\rangle = \frac{1}{\sqrt{2}}(|0_a 1_b\rangle - |1_a 0_b\rangle)$$

means that A and B are prepared in such a way that Alice's and Bob's measurement results will be perfectly anticorrelated if and only if they choose the same (but arbitrary) basis.

Nevertheless, it does seem like one might be able to draw something "useful" from this loose analogy between communication and quantum correlations. For example, say Alice and Bob have some way of obtaining multiple pairs of systems prepared in the entangled joint state

$$|\Psi_{ab}\rangle = \frac{1}{\sqrt{2}}(|0_a 1_b\rangle - |1_a 0_b\rangle).$$

If they agree beforehand on a fixed basis such as $\{|0\rangle, |1\rangle\}$, they can use the string of measurement results to establish a shared *cryptographic key*.

Recall that Alice and Bob can send private messages over a public communication channel by encoding via one-time pad. If Alice's "plaintext" message is given as a sequence of 0's and 1's (binary representation of ASCII codes, for example) then she can simply XOR this string with a random binary string of equal length (the cryptographic key) to produce an encoded "cryptotext." This cryptotext can then be broadcast over public channels, and can only be decoded by someone who knows the cryptographic key. Decoding can be performed simply by XORing the cryptotext again with the key, so if Bob (and only Bob) knows the key it is easy for Alice to send him secret messages.

Even if Alice and Bob are far apart, they can use quantum correlations to establish a cryptographic key. Alice, for instance, can produce pairs of entangled two-level systems in her lab and send only the B part to Bob through a public quantum channel. If the initial A, B

joint state is the singlet state discussed above and both Alice and Bob make measurements in the $\{|0\rangle, |1\rangle\}$ basis, Bob need only take the NOT of his sequence of measurement results to share a cryptographic key with Alice.

Recall, however, that a public quantum channel is by definition one that an eavesdropper could perform measurements on. In the current scenario, this means that an eavesdropper Eve could perform measurements on system B while it is en route from Alice's lab to Bob's lab. How can Alice and Bob be sure that Eve doesn't end up knowing their cryptokey as well!?

In 1991 Artur Ekert published a very clever paper ("Quantum cryptography based on Bell's theorem," Phys. Rev. Lett. **67**, 661) in which he argues that Alice and Bob can detect eavesdroppers by using a subset of their entangled quantum systems to test a Bell Inequality!

Let's say that rather than agreeing on just one measurement basis, Alice uses two bases A, A' and Bob uses two bases B, B' as in our discussion of Bell Inequalities. Alice and Bob each switches bases randomly and independently from one round to the next. After a large number of measurements have taken place, Alice and Bob can reveal (over a public classical channel) which bases they used in each round of measurements. In the subset of cases where they chose the same basis, they know their results should be anticorrelated, so they can use most of them (without broadcasting them) to generate cryptokey. But Alice and Bob should set some of these same-basis results aside to compute a correlation function $\langle AB \rangle$, and likewise compute correlation functions $\langle A'B \rangle$, $\langle AB' \rangle$, $\langle A'B' \rangle$, and

$$|\langle g \rangle| = |\langle AB \rangle + \langle A'B \rangle + \langle AB' \rangle - \langle A'B' \rangle|.$$

If all is well, they should find $|\langle g \rangle| > 2$, in violation of Bell's Inequality (as we discussed in the previous lecture).

But what about Eve? Let's say that Eve tries to tap into Alice and Bob's procedure by intercepting the B systems and performing standard measurements on them. Following Eve's measurement, we know that the A and B systems will be left in a factorizable state! Eve has to then send something on to Bob (or else he'll surely know that something is up), and even if she sends the post-measurement B there will be no entanglement left between Alice and Bob. And without entanglement, there are no violations of Bell Inequalities, implying that Alice and Bob will find $|\langle g \rangle| \leq 2$ in their eavesdropper-detection protocol.

If Eve is allowed to make generalized measurements, the proof of security is **much** more complicated. However, the latest word on the street is that the Ekert protocol can be generalized to make it unconditionally secure (see H. K. Lo and H. F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances," Science **283**, 2050 (1999)).

Quantum-state teleportation

Theory: C. H. Bennett *et al*, “Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels,” Phys. Rev. Lett. **70**, 1895 (1993).

Experiments: A. Furusawa *et al*, “Unconditional quantum teleportation,” Science **282**, 706 (1998); D. Bouwmeester *et al*, “Experimental quantum teleportation,” Nature **390**, 575 (1997); D. Boschi *et al*, “Experimental realization of teleporting an unknown pure quantum state via dual classical and Einstein-Podolsky-Rosen channels,” Phys. Rev. Lett. **80**, 1121 (1998).

Say Alice has a two-level quantum system A prepared in initial state

$$|\varphi_a\rangle = a_0|0_a\rangle + a_1|1_a\rangle.$$

She would like Bob to have a two-level quantum system B prepared in the “identical” state

$$|\varphi_b\rangle = a_0|0_b\rangle + a_1|1_b\rangle.$$

However, let’s say she cannot directly send system A to Bob, nor can she communicate the coefficients a_0, a_1 with sufficient precision for their liking. In fact, let’s imagine that Alice does not even *know* these coefficients explicitly – the initial state of system A could have been prepared by a third person Charlie, who has now asked her to send it somehow to Bob (without telling her the coefficients).

The secret of quantum-state teleportation is that Alice and Bob need to have a shared quantum resource: **entanglement**. Let’s say that the last time Alice and Bob got together, they prepared a pair of two-level quantum systems B, C in the entangled joint state

$$|\Psi_{bc}^-\rangle = \frac{1}{\sqrt{2}}(|0_b1_c\rangle - |1_b0_c\rangle).$$

A state of this form is often called a “singlet.” Alice keeps system C with her, and Bob takes B away with him. Recall that B eventually needs to end up in the state $|\varphi_b\rangle$, whose coefficients are known only to Charlie.

When Charlie finally gives Alice system A (prepared in the “unknown” state $|\varphi_a\rangle$), there are three two-level systems in the picture: $H_A \otimes H_B \otimes H_C$. The initial state of this three-part system is simply

$$|\varphi_a\rangle \otimes |\Psi_{bc}^-\rangle.$$

In order to accomplish quantum-state teleportation, Alice performs the following procedure:

1. Alice brings A together with C , and performs a joint measurement in the “Bell basis”

$$\begin{aligned}
|\Psi_{ac}^-\rangle &= \frac{1}{\sqrt{2}}(|0_a 1_c\rangle - |1_a 0_c\rangle), \\
|\Psi_{ac}^+\rangle &= \frac{1}{\sqrt{2}}(|0_a 1_c\rangle + |1_a 0_c\rangle), \\
|\Phi_{ac}^-\rangle &= \frac{1}{\sqrt{2}}(|0_a 0_c\rangle - |1_a 1_c\rangle), \\
|\Phi_{ac}^+\rangle &= \frac{1}{\sqrt{2}}(|0_a 0_c\rangle + |1_a 1_c\rangle).
\end{aligned}$$

Note that this is a complete basis for $H_A \otimes H_C$, and that these are all entangled states. The outcome probabilities can be computed explicitly by rewriting the three-part state of A, B, C in terms of the Bell states on A, C :

$$\begin{aligned}
|\varphi_a\rangle|\Psi_{bc}^-\rangle &= \frac{1}{\sqrt{2}}(a_0|0_a\rangle + a_1|1_a\rangle) \otimes (|0_b 1_c\rangle - |1_b 0_c\rangle) \\
&= \frac{1}{\sqrt{2}}(a_0|0_a 0_b 1_c\rangle - a_0|0_a 1_b 0_c\rangle + a_1|1_a 0_b 1_c\rangle - a_1|1_a 1_b 0_c\rangle) \\
&= \frac{1}{2} \begin{pmatrix} a_0|0_b\rangle(|\Psi_{ac}^+\rangle + |\Psi_{ac}^-\rangle) - a_0|1_b\rangle(|\Phi_{ac}^+\rangle + |\Phi_{ac}^-\rangle) \\ +a_1|0_b\rangle(|\Phi_{ac}^+\rangle - |\Phi_{ac}^-\rangle) - a_1|1_b\rangle(|\Psi_{ac}^+\rangle - |\Psi_{ac}^-\rangle) \end{pmatrix} \\
&= \frac{1}{2} \begin{pmatrix} |\Psi_{ac}^+\rangle(a_0|0_b\rangle - a_1|1_b\rangle) + |\Psi_{ac}^-\rangle(a_0|0_b\rangle + a_1|1_b\rangle) \\ +|\Phi_{ac}^+\rangle(a_1|0_b\rangle - a_0|1_b\rangle) + |\Phi_{ac}^-\rangle(-a_1|0_b\rangle - a_0|1_b\rangle) \end{pmatrix}.
\end{aligned}$$

Since $|a_0|^2 + |a_1|^2 = 1$, we see that all four outcomes have probability $\frac{1}{4}$. Also, we can easily read off the post-measurement states for system B :

$$\begin{aligned}
\Psi^+ : \quad a_0|0_b\rangle - a_1|1_b\rangle &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} |\varphi_b\rangle, \\
\Psi^- : \quad a_0|0_b\rangle + a_1|1_b\rangle &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} |\varphi_b\rangle, \\
\Phi^+ : \quad a_1|0_b\rangle - a_0|1_b\rangle &= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} |\varphi_b\rangle, \\
\Phi^- : \quad -a_1|0_b\rangle - a_0|1_b\rangle &= \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} |\varphi_b\rangle.
\end{aligned}$$

Note that each of the four transformation operators are unitary, and therefore **invertible**.

2. Alice broadcasts a number from 1..4 corresponding to the result she actually obtained. Note that this is just two bits of classical information, versus an infinite number of bits that would be needed to transmit two complex coefficients (a_0, a_1) with arbitrary precision.

3. When Bob learns the result, he knows which of the four post-measurement states B has been left in! To recover $|\varphi_b\rangle$ exactly, he need only apply the appropriate inverse

transformation.

So when Alice and Bob implement this quantum-state teleportation protocol, they can be certain that Bob will end up with system B left in the state

$$|\varphi_b\rangle = a_0|0_b\rangle + a_1|1_b\rangle,$$

where a_0, a_1 are arbitrary complex coefficients known only to Charlie! The total *resource cost* of the procedure is one entangled pair plus two bits of classical communication.

In quantum information theory, we would say that teleportation demonstrates an equivalence between quantum bits (*qubits*), entanglement “bits” (*e-bits*), and classical bits (*c-bits*):

$$1 \text{ qubit} = 1 \text{ e-bit} + 2 \text{ c-bits}.$$

Here a qubit is implicitly defined as the amount of information represented by the state of a two-level quantum system.