APPPHYS225 - Thursday 30 October 2008

A bit more on partial traces and reduced density operators

Recall that there exist nonfactorizable pure states in the joint Hilbert space of two subsystems, *e.g.*,

$$|\Psi_{AB}\rangle = \frac{1}{\sqrt{2}}(|0_A\rangle \otimes |0_B\rangle + |1_A\rangle \otimes |1_B\rangle) \neq |\Psi_A\rangle \otimes |\Psi_B\rangle.$$

There is no way to assign a pure state to system A or B individually.

Suppose our friend Charlie comes into our lab and takes away system B, after $|\Psi_{AB}\rangle$ has been prepared. Clearly we can still make measurements on system A. It is also true, although perhaps not entirely obvious, that the statistics of any measurements we might choose to make on system A will be independent of whatever Charlie happens to do with system B – we assume that A and B can no longer physically interact after they have been separated.

Hence we would like to have a compact representation of everything we know about system A alone, starting from the statement that the initial joint state of the AB system was $|\Psi_{AB}\rangle$. What do we mean by compact? It may not be entirely clear if both A and B are two-dimensional systems – pure states in H_{AB} have four complex coefficients, the same as a reduced density operator on H_A alone. But consider the more general entangled state,

$$|\Psi_{AB}\rangle = \frac{1}{\sqrt{2}}(|0_A\rangle \otimes |\Psi_B^0\rangle + |1_A\rangle \otimes |\Psi_B^1\rangle), \quad \langle \Psi_B^0 | \Psi_B^1 \rangle = 0,$$

when H_A is still two-dimensional but H_B is (for example) fifty-dimensional. Then state vectors in H_{AB} have one hundred complex coefficients, but the reduced density operator still only has four.

Let's get back to our example with $N_A = N_B = 2$. One of the things that Charlie might choose to do with system B is to perform a measurement, say of the set $\{\mathbf{P}_0^B, \mathbf{P}_1^B\}$. Working from the initial state in the joint Hilbert space, we know that the outcome probabilities will bef

$$\Pr(0_B) = \langle \Psi_{AB} | \mathbf{1}^A \otimes \mathbf{P}_0^B | \Psi_{AB} \rangle = 0.5,$$
$$\Pr(1_B) = 0.5.$$

Likewise, the corresponding post-measurement states of the joint system will be

$$|\Psi_{AB}\rangle \mapsto \frac{\mathbf{1}^A \otimes \mathbf{P}_0^B |\Psi_{AB}\rangle}{\sqrt{\langle \Psi_{AB} | \mathbf{1}^A \otimes \mathbf{P}_0^B | \Psi_{AB} \rangle}} = |0_A\rangle \otimes |0_B\rangle$$

or

$$|\Psi_{AB}\rangle \mapsto \frac{\mathbf{1}^A \otimes \mathbf{P}_1^B |\Psi_{AB}\rangle}{\sqrt{\langle \Psi_{AB} | \mathbf{1}^A \otimes \mathbf{P}_1^B | \Psi_{AB} \rangle}} = |1_A\rangle \otimes |1_B\rangle$$

But we see that the post-measurement state of system A alone is definitely either $|0_A\rangle$ or $|1_A\rangle$, each with 50% probability. *If Charlie doesn't tell us the measurement result*, we are left with a mixed ensemble of quantum states for A. The density operator that

represents this ensemble is

$$\boxed{\rho_A = \frac{1}{2}(|0_A\rangle\langle 0_A| + |1_A\rangle\langle 1_A|),}$$

which is in fact identical to the reduced density operator

$$\begin{aligned}
\tilde{\rho}_A &= \mathrm{Tr}_B\,[|\Psi_{AB}\rangle\langle\Psi_{AB}|] \\
&= \frac{1}{2}\mathrm{Tr}_B\,[(|0_A0_B\rangle + |1_A1_B\rangle)(\langle 0_A0_B| + \langle 1_A1_B|)] \\
&= \frac{1}{2}\left\{\begin{array}{l}\boxed{\langle 0_B|[|0_A0_B\rangle\langle 0_A0_B| + |0_A0_B\rangle\langle 1_A1_B| + |1_A1_B\rangle\langle 0_A0_B| + |1_A1_B\rangle\langle 1_A1_B|]|0_B\rangle} \\ \boxed{+\langle 1_B|[|0_A0_B\rangle\langle 0_A0_B| + |0_A0_B\rangle\langle 1_A1_B| + |1_A1_B\rangle\langle 0_A0_B| + |1_A1_B\rangle\langle 1_A1_B|]|1_B\rangle}\end{array}\right\} \\
&= \frac{1}{2}\{|0_A\rangle\langle 0_A| + |1_A\rangle\langle 1_A|\}.
\end{aligned}$$

What if Charlie decides to perform the measurement corresponding to $\{\mathbf{P}_x^B, \mathbf{P}_y^B\}$, where

$$\begin{aligned}
\boxed{\mathbf{P}_x^B = \frac{1}{2}(|0_B\rangle\langle 0_B| + |0_B\rangle\langle 1_B| + |1_B\rangle\langle 0_B| + |1_B\rangle\langle 1_B|),} \\
\boxed{\mathbf{P}_y^B = \frac{1}{2}(|0_B\rangle\langle 0_B| - |0_B\rangle\langle 1_B| - |1_B\rangle\langle 0_B| + |1_B\rangle\langle 1_B|).}
\end{aligned}$$

Then $\langle \mathbf{1}^A \otimes \mathbf{P}_x^B\rangle = \langle \mathbf{1}^A \otimes \mathbf{P}_y^B\rangle = 0.5$ still, but the resulting post-measurement states are

$$\begin{aligned}
x\ :\ |\Psi_{AB}\rangle &\mapsto \frac{\mathbf{1}^A \otimes \mathbf{P}_x^B|\Psi_{AB}\rangle}{\sqrt{\langle\Psi_{AB}|\mathbf{1}^A \otimes \mathbf{P}_x^B|\Psi_{AB}\rangle}} \\
&\propto \mathbf{1}^A \otimes \mathbf{P}_x^B \frac{1}{\sqrt{2}}(|0_A\rangle \otimes |0_B\rangle + |1_A\rangle \otimes |1_B\rangle) \\
&\propto \mathbf{1}^A \otimes \left\{\frac{1}{2}(|0_B\rangle\langle 0_B| + |0_B\rangle\langle 1_B| + |1_B\rangle\langle 0_B| + |1_B\rangle\langle 1_B|)\right\}\frac{1}{\sqrt{2}}(|0_A\rangle \otimes |0_B\rangle + |1_A\rangle \otimes |1_B\rangle) \\
&\propto \{|0_A\rangle \otimes |0_B\rangle + |1_A\rangle \otimes |0_B\rangle + |0_A\rangle \otimes |1_B\rangle + |1_A\rangle \otimes |1_B\rangle\} \\
&= \frac{1}{2}(|0_A\rangle \otimes |0_B\rangle + |0_A\rangle \otimes |1_B\rangle + |1_A\rangle \otimes |0_B\rangle + |1_A\rangle \otimes |1_B\rangle) \\
&= \frac{1}{2}(|0_A\rangle + |1_A\rangle) \otimes (|0_B\rangle + |1_B\rangle), \\
y\ :\ |\Psi_{AB}\rangle &\mapsto \frac{1}{2}(|0_A\rangle \otimes |0_B\rangle - |0_A\rangle \otimes |1_B\rangle - |1_A\rangle \otimes |0_B\rangle + |1_A\rangle \otimes |1_B\rangle) \\
&= \frac{1}{2}(|0_A\rangle - |1_A\rangle) \otimes (|0_B\rangle - |1_B\rangle).
\end{aligned}$$

Hence the post-measurement state of sytem A considered alone will be either $\frac{1}{\sqrt{2}}(|0_A\rangle + |1_A\rangle)$ or $\frac{1}{\sqrt{2}}(|0_A\rangle - |1_A\rangle)$ with $p = 0.5$, and the density operator for this ensemble is still

$$\begin{aligned}
\boxed{\tilde{\rho}_A = \frac{1}{4}(|0_A\rangle + |1_A\rangle)(\langle 0_A| + \langle 1_A|) + \frac{1}{4}(|0_A\rangle - |1_A\rangle)(\langle 0_A| - \langle 1_A|)} \\
\boxed{= \frac{1}{2}(|0_A\rangle\langle 0_A| + |1_A\rangle\langle 1_A|),}
\end{aligned}$$

which is once again our good old reduced density operator for A.

We thus see that taking a partial trace over subsystem B is like performing an

‘imaginary’ complete measurement on B and then ignoring the result. As with the trace itself, it doesn’t matter what basis we imagine the measurement is made in as long as it is complete and projective.

Recall that a pair of systems that starts out in a factorizable initial state can evolve into an entangled state via Hamiltonian evolution. How can we check for the ‘generation’ of entanglement in such a scenario?

Let’s work again with our same two two-dimensional quantum systems. Let the initial state be

$$\begin{aligned} |\Psi_{AB}(0)\rangle &= \tfrac{1}{2}(|0_A\rangle + |1_A\rangle) \otimes (|0_B\rangle + |1_B\rangle) \\ &= \tfrac{1}{2}(|0_A\rangle \otimes |0_B\rangle + |0_A\rangle \otimes |1_B\rangle + |1_A\rangle \otimes |0_B\rangle + |1_A\rangle \otimes |1_B\rangle), \end{aligned}$$

and suppose the Hamiltonian is

$$\mathbf{H} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix},$$

where the ordering of basis states in H_{AB} is

$$|0_A\rangle \otimes |0_B\rangle, \quad |0_A\rangle \otimes |1_B\rangle, \quad |1_A\rangle \otimes |0_B\rangle, \quad |1_A\rangle \otimes |1_B\rangle.$$

The unitary evolution operator is

$$\mathbf{T}(t,0) = \exp\left(\frac{-i}{\hbar}\mathbf{H}t\right).$$

After a time $t = \frac{1}{2}\pi\hbar$,

$$\mathbf{T}(t,0) = \begin{pmatrix} e^{-i\pi/2} & 0 & 0 & 0 \\ 0 & e^{-i\pi/2} & 0 & 0 \\ 0 & 0 & e^{-i\pi/2} & 0 \\ 0 & 0 & 0 & e^{+i\pi/2} \end{pmatrix} = \begin{pmatrix} -i & 0 & 0 & 0 \\ 0 & -i & 0 & 0 \\ 0 & 0 & -i & 0 \\ 0 & 0 & 0 & i \end{pmatrix},$$

and

$$\begin{aligned} |\Psi_{AB}(t)\rangle &= \mathbf{T}(t,0)|\Psi_{AB}(0)\rangle \\ &= \tfrac{-i}{2}(|0_A\rangle \otimes |0_B\rangle + |0_A\rangle \otimes |1_B\rangle + |1_A\rangle \otimes |0_B\rangle - |1_A\rangle \otimes |1_B\rangle), \end{aligned}$$

which certainly looks like an entangled state.

How do we know that this is an entangled state? Probably by inspection, but let’s also check the trace of $\tilde{\boldsymbol{\rho}}_A^2$. First off, the joint density operator is

$$
\begin{aligned}
\boldsymbol{\rho}_{AB} &= |\Psi_{AB}(t)\rangle\langle\Psi_{AB}(t)| \\
&= \tfrac{1}{4}(|0_A0_B\rangle\langle 0_A0_B| + |0_A0_B\rangle\langle 0_A1_B| + |0_A0_B\rangle\langle 1_A0_B| - |0_A0_B\rangle\langle 1_A1_B| \\
&\quad + |0_A1_B\rangle\langle 0_A0_B| + |0_A1_B\rangle\langle 0_A1_B| + |0_A1_B\rangle\langle 1_A0_B| - |0_A1_B\rangle\langle 1_A1_B| \\
&\quad + |1_A0_B\rangle\langle 0_A0_B| + |1_A0_B\rangle\langle 0_A1_B| + |1_A0_B\rangle\langle 1_A0_B| - |1_A0_B\rangle\langle 1_A1_B| \\
&\quad - |1_A1_B\rangle\langle 0_A0_B| - |1_A1_B\rangle\langle 0_A1_B| - |1_A1_B\rangle\langle 1_A0_B| + |1_A1_B\rangle\langle 1_A1_B|).
\end{aligned}
$$

Next we take the partial trace over B:

$$
\begin{aligned}
\tilde{\boldsymbol{\rho}}_A &= \mathrm{Tr}_B\,[\boldsymbol{\rho}_{AB}] \\
&= \langle 0_B|\boldsymbol{\rho}_{AB}|0_B\rangle + \langle 1_B|\boldsymbol{\rho}_{AB}|1_B\rangle \\
&= \tfrac{1}{4}(|0_A\rangle\langle 0_A| + |0_A\rangle\langle 1_A| + |1_A\rangle\langle 0_A| + |1_A\rangle\langle 1_A| \\
&\quad + |0_A\rangle\langle 0_A| - |0_A\rangle\langle 1_A| - |1_A\rangle\langle 1_A| + |1_A\rangle\langle 1_A|) \\
&= \tfrac{1}{2}(|0_A\rangle\langle 0_A| + |1_A\rangle\langle 1_A|) \\
&= \tfrac{1}{2}\mathbf{1}^A.
\end{aligned}
$$

Hence $\tilde{\boldsymbol{\rho}}_A^2 = \frac{1}{4}\mathbf{1}^A$, and $\mathrm{Tr}[\tilde{\boldsymbol{\rho}}_A^2] = \frac{1}{2}$, which is clearly less than one. Since density operators that correspond to pure states are projectors, we conclude that no pure state can be assigned to subsystem A when the joint state of the AB system is $|\Psi_{AB}(t)\rangle$.

Entanglement vs. classical correlation

Still working with two-dimensional H_A and H_B, etc.

Consider the joint density operator

$$
\boldsymbol{\rho}_{AB} = \tfrac{1}{2}(|0_A0_B\rangle\langle 0_A0_B| + |1_A1_B\rangle\langle 1_A1_B|).
$$

This corresponds to a mixed preparation where, with equal probability, the joint pure state is either $|0_A0_B\rangle$ or $|1_A1_B\rangle$. Hence, we don't know whether A or B is $|0\rangle$ or $|1\rangle$, but we do know that *they have to be the same*. Formally,

$$
\begin{aligned}
&\langle \mathbf{P}_0^A \otimes \mathbf{P}_0^B\rangle = 0.5, \quad \langle \mathbf{P}_0^A \otimes \mathbf{P}_1^B\rangle = 0, \\
&\langle \mathbf{P}_1^A \otimes \mathbf{P}_0^B\rangle = 0, \quad \langle \mathbf{P}_1^A \otimes \mathbf{P}_1^B\rangle = 0.5.
\end{aligned}
$$

This kind of situation, where some property of A is random but nonetheless tied to some property of B, is called 'classical' or 'probabilistic' correlation.

Now consider the entangled pure state

$$
|\Psi_{AB}\rangle = \frac{1}{\sqrt{2}}(|0_A0_B\rangle + |1_A1_B\rangle).
$$

It is still the case that

$$
\begin{aligned}
&\langle \mathbf{P}_0^A \otimes \mathbf{P}_0^B\rangle = 0.5, \quad \langle \mathbf{P}_0^A \otimes \mathbf{P}_1^B\rangle = 0, \\
&\langle \mathbf{P}_1^A \otimes \mathbf{P}_0^B\rangle = 0, \quad \langle \mathbf{P}_1^A \otimes \mathbf{P}_1^B\rangle = 0.5.
\end{aligned}
$$

Is there any difference between the type of correlation embodied in $|\Psi_{AB}\rangle$ and that embodied in $\boldsymbol{\rho}_{AB}$?

Consider a new set of projectors $\{\mathbf{P}_x^A \otimes \mathbf{P}_x^B, \mathbf{P}_x^A \otimes \mathbf{P}_y^B, \mathbf{P}_y^A \otimes \mathbf{P}_x^B, \mathbf{P}_y^A \otimes \mathbf{P}_y^B\}$, where

$$\mathbf{P}_x = |x\rangle\langle x|, \quad |x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle),$$

$$\mathbf{P}_y = |y\rangle\langle y| = \mathbf{1} - \mathbf{P}_x, \quad |y\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

Then for the mixed initial state,

$$\begin{aligned}
\langle \mathbf{P}_x^A \otimes \mathbf{P}_y^B \rangle &= \langle x_A y_B | \boldsymbol{\rho}_{AB} | x_A y_B \rangle \\
&= \frac{1}{2}\langle x_A y_B | (|0_A 0_B\rangle\langle 0_A 0_B| + |1_A 1_B\rangle\langle 1_A 1_B|) | x_A y_B \rangle \\
&= \frac{1}{2}\left(|\langle x_A y_B | 0_A 0_B \rangle|^2 + |\langle x_A y_B | 1_A 1_B \rangle|^2 \right) \\
&= \frac{1}{2}\left(\frac{1}{4} + \frac{1}{4} \right) = \frac{1}{4}.
\end{aligned}$$

Hence we see that the correlation between A and B is not as strong in the x, y basis as in the $0, 1$ basis, when the initial state is $\boldsymbol{\rho}_{AB}$. What about $|\Psi_{AB}\rangle$?

$$\begin{aligned}
\langle \mathbf{P}_x^A \otimes \mathbf{P}_y^B \rangle &= |\langle x_A y_B || \Psi_{AB} \rangle|^2 \\
&= \frac{1}{\sqrt{2}} |\langle x_A y_B | (|0_A 0_B\rangle + |1_A 1_B\rangle)|^2 \\
&= \frac{1}{\sqrt{2}} \left| \frac{1}{2} - \frac{1}{2} \right|^2 \\
&= 0.
\end{aligned}$$

$$\langle \mathbf{P}_y^A \otimes \mathbf{P}_x^B \rangle = |\langle y_A x_B || \Psi_{AB} \rangle|^2 = 0.$$

For this particular entangled state, A and B remain perfectly correlated even under the specified change of measurement basis. While one should not over-generalize, entanglement can in many scenarios be less basis-dependent than classical correlation.

Entanglement is a very special property of composite *quantum* systems. As you might guess from even this simple example, there are scenarios in which entanglement can be 'utilized' to perform otherwise impossible tasks in communication and information processing - this basic idea motivations much of what is now called quantum information theory. However, the tensor-product rule for representation of joint states also places some limitations on what we can do with composite quantum systems, as we'll see later in our discussions of the no-cloning and no-broadcasting theorems.

Nonlocality and Bell Inequalities

(Based on the discussion in Chris Isham's book, *Lectures on Quantum Theory: Mathematical and Structural Foundations* (Imperial College Press, 1995).)

Say we have two experimenters, Alice and Bob, whose labs are located many

kilometers apart. Their labs are basically identical, actually, each consisting of one particle 'detector' that has one meter, one switch, and a bell. The meter is for reading out the result of a measurement (which we assume to be either ± 1), while the switch is used to select which of two types of measurements the experimenter would like to make. On Alice's side we'll label the two possibilities A and A', and on Bob's side B and B'. The bell rings each time a particle hits the detector, letting the experimenter know when he or she can read out the result of his/her selected measurement.

So where do these particles come from? Midway between Alice's lab and Bob's there is a 'pair source.' This source always produces particles in pairs, sending one to Alice and the other to Bob. We assume that the particles have some internal degree of freedom, which is what Alice's and Bob's detectors are designed to measure. The pair source prepares the internal states of the particles in some unknown, possibly random fashion.

The 'experiment' consists of the following procedure. The source prepares and emits one pair of particles per unit of time, so Alice and Bob know that they may expect to receive particles at a regular rate. Once per unit time, they each (independently) select a random setting for their switch, wait for their bell to ring, and then read off and write down the measurement result.

Hence after ten rounds, *e.g.*, Alice's and Bob's lab books might look something like this:

Alice		**Bob**	
A	-1	B'	-1
A	$+1$	B'	-1
A'	$+1$	B	$+1$
A	$+1$	B	$+1$
A'	-1	B	-1
A'	-1	B'	$+1$
A	$+1$	B	-1
A'	-1	B'	$+1$
A	$+1$	B'	$+1$
A	-1	B	$+1$

Although this experimental scenario seems extremely general, it turns out that we have already specified enough to derive some important predictions about the statistics of Alice's and Bob's measurement records!

Let's start by making some reasonable assumptions about the overall behavior of the experiment:

1. ***Local determinism*** – we might like to believe that the result of Alice's measurement (either A or A') is *locally* determined by the physical state of the particle she receives from the pair source. It should not depend on the

state of Bob's particle, since in this scenario Bob could be really far away! And the result of Alice's measurement certainly should not depend on Bob's choice of measurement – that is, whether Alice's meter reads $+$ or -1 should not depend on whether Bob has his switch set to B or B'...

2. ***Objective reality*** – Even though Alice (and Bob) must choose to make one measurement or the other (A or A') on any given particle, each particle 'knows' what its value is for both measurements. That is, sufficient information to determine the outcome of either measurement is encoded in the internal state of each particle.

Under these assumptions, we can write down the following model for this experiment. In each round, the pair souce produces a pair of particles with the following information encoded in their internal states:

$$A_n = \pm 1, \quad A'_n = \pm 1, \quad B_n = \pm 1, \quad B'_n = \pm 1.$$

Here the four possible measurement labels are treated as random variables, with the subscript labelling the round. As a logical consequence of local determinism and objective realism, we can assume the existence of a *joint probability distribution* $\Pr(A, A', B, B')$. Hence, it should be meaningful to consider correlation functions of all four random variables simultaneously, and these correlation functions should be measurable by Alice and Bob.

Consider the following function of the random variables,

$$g_n = A_n B_n + A'_n B_n + A_n B'_n - A'_n B'_n.$$

Were we to tabulate the 16 possible values of g_n, we would magically find that $g_n = \pm 2$. However, an easier way to see this is to note that the last term in the sum is equal to the product of the first three, since $A_n^2 = (A'_n)^2 = B_n^2 = (B'_n)^2 = +1$:

$$\begin{aligned} A'_n B'_n &= (A_n B_n)(A'_n B_n)(A_n B'_n) \\ &= A_n^2 B_n^2 A'_n B'_n. \end{aligned}$$

Then if $A'_n B'_n = +1$, the set $\{A_n B_n, A'_n B_n, A_n B'_n\}$ has either zero or two -1's, hence $g_n = A_n B_n + A'_n B_n + A_n B'_n - A'_n B'_n$ must be either $+2$ or -2. If on the other hand $A'_n B'_n = -1$, the set must have either zero or two $+1$'s, hence g_n must be either -2 or $+2$.

In any case, it follows that

$$\begin{aligned} \left| \frac{1}{N} \sum_{n=1}^{N} g_n \right| &= \frac{1}{N} \left| \sum_{n=1}^{N} A_n B_n + \sum_{n=1}^{N} A'_n B_n + \sum_{n=1}^{N} A_n B'_n - \sum_{n=1}^{N} A'_n B'_n \right| \\ &\leq 2. \end{aligned}$$

This is one form (due to Clauser, Horne, Shimony, and Holt) of Bell's famous inequality. It should be noted that at this point, all we have relied on in our derivation is basic probability theory! Hence the Bell Inequality is a *model-independent* prediction about measurement statistics in a world that is locally deterministic and allows objective realism.

Hence experimental violations of the Inequality actually tell us something about Nature, not just quantum theory. As it turns out, one can actually go to the lab and

perform experiments of precisely the type described above, and find that this inequality is strongly violated! For example, see

- G. Weihs *et al.*, "Violation of Bell's Inequality under Strict Einstein Locality Conditions," Phys. Rev. Lett. **81**, 5039-5043 (1998);
- W. Tittel *et al.*, "Violation of Bell Inequalities by Photons More Than 10 km Apart," Phys. Rev. Lett. **81**, 3563-3566 (1998);
- A. Aspect, "Bell's inequality test: more ideal than ever," Nature **398**, 189-190 (1999);
- C.-Z. Peng *et al.*, "Experimental Free-Space Distribution of Entangled Photon Pairs Over 13 km: Towards Satellite-Based Global Quantum Communication," Phys. Rev. Lett. **94**, 150501 (2005).

In experiments of this type, the key is to construct a source that produces pairs of photons an *entangled* state such as

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

In each round of the experiment, Alice's two measurements correspond to the observables $\mathbf{A} = \boldsymbol{\sigma}_z^a$ and $\mathbf{A}' = \cos\phi\,\boldsymbol{\sigma}_z^a + \sin\phi\,\boldsymbol{\sigma}_x^a$, where

$$\boldsymbol{\sigma}_z^a = |0_a\rangle\langle 0_a| - |1_a\rangle\langle 1_a|,$$
$$\boldsymbol{\sigma}_x^a = |0_a\rangle\langle 1_a| + |1_a\rangle\langle 0_a|.$$

On Bob's side we choose $\mathbf{B} = \boldsymbol{\sigma}_z^b$ and $\mathbf{B}' = \cos\phi\,\boldsymbol{\sigma}_z^b - \sin\phi\,\boldsymbol{\sigma}_x^b$. The eigenvalues of $\mathbf{A}$ and $\mathbf{B}$ are clearly ± 1, and it turns out that those of $\mathbf{A}'$ and $\mathbf{B}'$ are also ± 1. For example, the eigenstates of $\cos\phi\,\boldsymbol{\sigma}_z + \sin\phi\,\boldsymbol{\sigma}_x$ are simply

$$|\tilde{0}\rangle = \cos\frac{\phi}{2}|0\rangle + \sin\frac{\phi}{2}|1\rangle,$$
$$|\tilde{1}\rangle = \sin\frac{\phi}{2}|0\rangle - \cos\frac{\phi}{2}|1\rangle.$$

Hence $\mathbf{A}'$ corresponds to projectors on a basis that is rotated from that of $\mathbf{A}$ by an angle $\phi/2$ (and similarly a rotation of $-\phi/2$ for $\mathbf{B}, \mathbf{B}'$).

Now we can compute the necessary correlation functions using the standard quantum probability rules:

$$\frac{1}{N}\sum_{n=1}^{N} A_n B_n = \langle \mathbf{A} \otimes \mathbf{B} \rangle$$
$$= \langle \mathbf{P}_0^a \mathbf{P}_0^b \rangle + \langle \mathbf{P}_1^a \mathbf{P}_1^b \rangle - \langle \mathbf{P}_0^a \mathbf{P}_1^b \rangle - \langle \mathbf{P}_1^a \mathbf{P}_0^b \rangle$$
$$= -1.$$

Similarly,

$$\frac{1}{N}\sum_{n=1}^{N} A_n B'_n = \langle \mathbf{P}_0^a \cos\phi\, \boldsymbol{\sigma}_z^b \rangle - \langle \mathbf{P}_0^a \sin\phi\, \boldsymbol{\sigma}_x^b \rangle - \langle \mathbf{P}_1^a \cos\phi\, \boldsymbol{\sigma}_z^b \rangle + \langle \mathbf{P}_1^a \sin\phi\, \boldsymbol{\sigma}_x^b \rangle$$

$$= -\frac{1}{2}\cos\phi - \frac{1}{2}\cos\phi = -\cos\phi.$$

$$\frac{1}{N}\sum_{n=1}^{N} A'_n B_n = \langle \mathbf{P}_0^b \cos\phi\, \boldsymbol{\sigma}_z^a \rangle + \langle \mathbf{P}_0^b \sin\phi\, \boldsymbol{\sigma}_x^a \rangle - \langle \mathbf{P}_1^b \cos\phi\, \boldsymbol{\sigma}_z^a \rangle - \langle \mathbf{P}_1^b \sin\phi\, \boldsymbol{\sigma}_x^a \rangle$$

$$= -\cos\phi.$$

$$\frac{1}{N}\sum_{n=1}^{N} A'_n B'_n = \langle \cos^2\phi\, \boldsymbol{\sigma}_z^a \boldsymbol{\sigma}_z^b \rangle + \langle \cos\phi \sin\phi\, \boldsymbol{\sigma}_z^a \boldsymbol{\sigma}_x^b \rangle - \langle \cos\phi \sin\phi\, \boldsymbol{\sigma}_x^a \boldsymbol{\sigma}_z^b \rangle$$

$$- \langle \sin^2\phi\, \boldsymbol{\sigma}_x^a \boldsymbol{\sigma}_x^b \rangle$$

$$= \frac{\cos^2\phi}{2}(-1-1) - \frac{\sin^2\phi}{2}(-1-1) = \sin^2\phi - \cos^2\phi$$

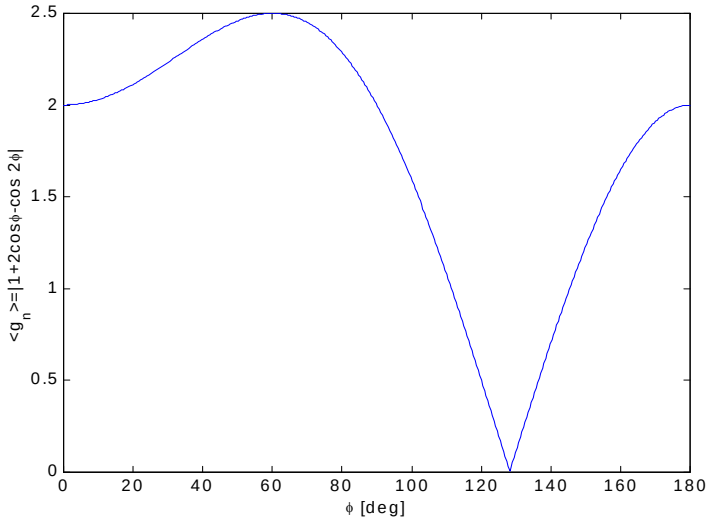
$$= -\cos 2\phi.$$

Finally, we can construct the overall quantity

$$\frac{1}{N}\left|\sum_{n=1}^{N} g_n\right| = |-1 - 2\cos\phi + \cos 2\phi|$$

$$= |1 + 2\cos\phi - \cos 2\phi|.$$

Plotting this, we find that the Bell Inequality is violated ($\langle g_n \rangle > 2$) for $0 < \phi < 90^\circ$:



So what's going on here? From the graph we see that our Bell Inequality can be violated when the two possible measurements that Alice and Bob can perform correspond to projections on nonorthogonal bases. Hence what is being exploited here is the extra-strong "quantum correlation" between two particles that have been prepared in an entangled state such as

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

Recall from our discussion above that the quantum correlation between a and b survives changes of basis, whereas classical correlation

$$\rho_{ab} = \frac{1}{2}(|0_a 1_b\rangle\langle 0_a 1_b| + |1_a 0_b\rangle\langle 1_a 0_b|)$$

does not.

From another point of view, the Bell Inequality we derived above tells us that there is no way to compose a mixed ensemble of factorizable quantum states $\{p_i, |\Psi_a^i\rangle \otimes |\Psi_b^i\rangle\}$ whose behavior simulates that of a *bona fide* entangled state.

Entanglement and information

We have now seen that entangled states such as

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

exhibit quantum correlations that are surprisingly basis-independent, and that they can be used to demonstrate violations of Bell inequalities. Is there any sense in which states like $|\Psi_{ab}\rangle$ can 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

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

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

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 guarenteed 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

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

instead? Noting that

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

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

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

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,

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

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

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

and

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

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 still 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 "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 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, for example, H. K. Lo and H. F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances," Science **283**, 2050 (1999)].