Advanced Quantum Physics
Week 6

Michel Ferrero
Thomas Schäfer

Fall 2019

Separable and entangled states

We have previously seen that the tensor product Hilbert space is the relevant object to describe a system with several degrees of freedom. If we consider two degrees of freedom, the tensor product Hilbert space is

$$\mathcal{G} = \mathcal{E} \otimes \mathcal{F}$$

The most general state $|\Psi\rangle \in \mathcal{G}$ is written as a linear combination of states in the tensor product basis

$$|\Psi\rangle = \sum_{m,n} c_{m,n} |e_m\rangle \otimes |f_n\rangle$$

Sometimes this expression can be simplified and brought to the form

$$|\Psi\rangle_{\text{separable}} = |e\rangle \otimes |f\rangle$$

where

$$|e\rangle = \sum_m a_m |e_m\rangle$$
$$|f\rangle = \sum_n b_n |f_n\rangle$$

In this case, we say that $|\Psi\rangle_{\text{separable}}$ is a *separable* or a *product* state. A state is separable if its coefficients in the tensor product basis can be written as $c_{m,n} = a_m b_n$ for all m, n. When, instead, a state cannot be written as just a product of an element of $\mathcal{E}$ times an element of $\mathcal{F}$, that state is said to be *entangled*.

The existence of entangled states in quantum mechanics has been at the origin of many debates about the interpretation of quantum mechanics.

The Einstein–Podolsky–Rosen paradox

In 1935, Einstein, Podolsky and Rosen published an article (Phys. Rev. 47, 777) where they discuss the very special and counter-intuitive nature of entangled states. In particular, they have shown that it is not possible to reconcile quantum mechanics with a realistic physical theory that would be local. For them, this was a proof that quantum mechanics was incomplete and that there had to be a more general deterministic supertheory of which quantum mechanics would be a special case. The article by Einstein, Podolsky and Rosen (EPR) was soon followed by a response of Nils Bohr that triggered a long debate about the interpretation of quantum mechanics and the nature of physical reality.

Deterministic versus non-deterministic theory

Let us consider the following quantum spin state expressed in the basis $\{|+\rangle_z, |-\rangle_z\}$ of eigenvectors of the $\hat{S}_z$ operator

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

A measurement of $\hat{S}_z$ on this state gives $+\hbar/2$ or $-\hbar/2$ with probability 1/2. One could say that this is like flipping a coin: the result is either heads or tails with probability 1/2. There is a fundamental difference though. In principle, if one knew exactly all the details about the coin, its precise position, its speed, the forces that act on it, one could predict the result of the toss. The description of the result in statistical terms is merely an expression of our ignorance about all these initial conditions. The situation in different in the usual interpretation of quantum mechanics. The fact that we find the result $+\hbar/2$ with probability 1/2 is not a result of our ignorance about the quantum state. It is inherent to the state $|\Sigma\rangle$. Einstein did not like this non-deterministic aspect of quantum mechanics ("God does not play dice"). He was hoping that there was a deterministic supertheory that would yield the same results as those predicted by quantum mechanics. Phrased differently, he was thinking that a full description of quantum particles would involve other variables, often called *hidden variables*, whose evolution would be completely deterministic. The knowledge of these hidden variables would allow to know the outcome of an experiment. Quantum mechanics would then just be a way to cope with our ignorance about what these hidden variables are, just like we don't know all the precise initial conditions of the coin. If we consider systems of just one particle, one cannot exclude that this interpretation is correct. However, *entangled states* provide a way to actually check whether a hidden variable theory is correct. Indeed, a local deterministic theory imposes some constraints, known as the *Bell inequality*, that can be verified experimentally.

The EPR argument by David Bohm

The article by Einstein, Podolsky and Rosen describes an experiment intended to demonstrate an inherent paradox in the early formulations of quantum theory. At the time, it was impossible to actually realize the experiment, so it was just a thought experiment. The original way the paradox was presented was somewhat confusing and several years later, in 1952, David Bohm modified the EPR paradox example to make it easier to understand. In this more popular formulation, two spin-1/2 particles a and b are prepared in a singlet state

$$|\Sigma_{\mathrm{s}}\rangle = \frac{1}{\sqrt{2}} \left(|+;-\rangle_z - |-;+\rangle_z\right)$$

where we have introduced the notation

$$|\sigma_a;\sigma_b\rangle_z \equiv |\sigma_a\rangle_z \otimes |\sigma_b\rangle_z$$

Particle a goes towards Alice while particle b goes towards Bob. Alice will measure the spin along the axis $\vec{u}_a$, while Bob will measure it along $\vec{u}_b$. These two measurements are strongly correlated. Indeed, if Alice and Bob choose the same direction $\vec{u}_a = \vec{u}_b = \hat{z}$ then Alice will find $+\hbar/2$ and Bob will find $-\hbar/2$ with probability 1/2. With probability 1/2 Alice will find $-\hbar/2$ and Bob $+\hbar/2$. However it will never happen that both Alice and Bob measure $+\hbar/2$ (or $-\hbar/2$). This perfect anti-correlation between the measurements of Alice and Bob does not depend on the specific axis that they choose. Indeed, one can show that the singlet state is always written as

$$|\Sigma_{\mathrm{s}}\rangle = \frac{1}{\sqrt{2}} \left(|+;-\rangle_{\vec{u}} - |-;+\rangle_{\vec{u}}\right)$$

no matter the direction $\vec{u}$. This is because the singlet has zero angular momentum and therefore full rotational symmetry.

Anti-correlations like this are not uncommon. For example, consider that you have two envelopes that each contain money. You have been told that one of them contains a 5 dollar bill and the other contains a 10 dollar bill. If you open one envelope and it contains a 5 dollar bill, then you know for sure that the other envelope contains the 10 dollar bill. In that case, before you open the envelope, it has a well-defined amount of money in it. For Einstein, Podolsky and Rosen, if you are sure you will obtain a given result, it means that the result is somewhat part of the physical properties of the object. As they state in their paper:

If, without in any way disturbing a system, we can predict with certainty (i.e., with probability equal to unity) the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity.

Following this argument, one would conclude that there is an element of physical reality in particle b corresponding to Bob's measurement of the spin along the z direction, because we can predict with certainty what the result will be (after Alice's measurement) without perturbing the system. Now, the same argument would predict that there is such an element of physical reality for the spin along the x direction as well. This would mean that one could in principle know both the result of a measurement along z or along x. This is in contradiction with Heisenberg's uncertainty principle and constitutes the basis of the paradox.

The arguments above are based on the idea of locality of a physical theory. The EPR paradox supposes that the measurement of Bob is made on a system that has not been disturbed in any way. It assumes that the measurement made by Alice (who is far away) cannot influence the state of the spin of Bob. This is however not true in the interpretation of quantum mechanics supported by Bohr and Heisenberg. In their interpretation, often called the *Copenhagen interpretation* of quantum mechanics, the wavefunction collapses instantaneously after a measurement is performed. In other words, the measurement of Alice, instantaneously changes the spin state, even at very long distances, and at the moment when Bob makes his measurement the wavefunction has collapsed into a spin state with opposite spin with respect to Alice's measurement.

There are therefore two very different interpretations of the experiment. For Einstein, Podolsky and Rosen there is an element of physical reality encoded in some hidden parameters governed by a larger theory that still has to be discovered, but that would probably feel more comfortable (as Einstein said: "I like to think the moon is there even if I am not looking at it"). Alternatively, one can accept quantum mechanics with its inherent non-locality and where physical reality does not exist before the measurement is actually made.

Bell's inequality

In 1964, John Stewart Bell published an article that provided a mathematical formulation of the notion of local hidden variables. This has lead to the possibility to realize an experiment that would be able to show whether quantum mechanics or hidden variable theories are correct. His formulation states that, in a local hidden variable theory, for any pair of particles (a,b) one would have some parameter λ that would entirely determine the result of the measurements of Alice and Bob. This means that there must be some function $A(\lambda, \vec{u}) = \pm\hbar/2$ for Alice and some function $B(\lambda, \vec{u}) = \pm\hbar/2$ for Bob that describe the outcome of the experiment. Let us then introduce the correlation function $E(\vec{u}_a, \vec{u}_b)$ defined as the average value of the product of the results of Alice and Bob. This correlation function always has the property

$$|E(\vec{u}_a, \vec{u}_b)| \leq 1$$

Now for a local hidden variable theory, this average value can be written as

$$E(\vec{u}_a, \vec{u}_b) = \frac{4}{\hbar^2} \int \mathcal{P}(\lambda) A(\lambda, \vec{u}_a) B(\lambda, \vec{u}_b) d\lambda,$$

where $\mathcal{P}(\lambda)$ is the distribution function of λ. The function $\mathcal{P}(\lambda)$ can be anything, it only has to satisfy

$$\mathcal{P}(\lambda) \geq 0 \qquad \int \mathcal{P}(\lambda) d\lambda = 1$$

Constraints for local hidden variable theories

Let us now define the quantity

$$S = E(\vec{u}_a, \vec{u}_b) + E(\vec{u}_a, \vec{u'}_b) + E(\vec{u'}_a, \vec{u'}_b) - E(\vec{u'}_a, \vec{u}_b)$$

Bell observed that in a local hidden variable theory, this quantity must satisfy $|S| \leq 2$. Indeed, in this case S can be written as

$$S = \frac{4}{\hbar^2} \int \mathcal{P}(\lambda)\mathcal{S}(\lambda)d\lambda,$$

where we have introduced

$$\mathcal{S}(\lambda) = A(\lambda, \vec{u}_a)B(\lambda, \vec{u}_b) + A(\lambda, \vec{u}_a)B(\lambda, \vec{u'}_b) + A(\lambda, \vec{u'}_a)B(\lambda, \vec{u'}_b) - A(\lambda, \vec{u'}_a)B(\lambda, \vec{u}_b)$$

The latter can also be expressed as

$$\mathcal{S}(\lambda) = A(\lambda, \vec{u}_a)\big[B(\lambda, \vec{u}_b) + B(\lambda, \vec{u'}_b)\big] + A(\lambda, \vec{u'}_a)\big[B(\lambda, \vec{u'}_b) - B(\lambda, \vec{u}_b)\big]$$

Because $B(\lambda, \vec{u}_b)$ and $B(\lambda, \vec{u'}_b)$ can only take values $\pm\hbar/2$, it is clear that either the first of the second line will vanish and the overall result will always be $\pm\hbar^2/2$. It follows that the integral above will be bounded above and below

$$-2 \leq S \leq 2 \qquad \text{or} \qquad |S| \leq 2$$

This inequality is known as *Bell's inequality.* It is a strong constraint for local hidden variable theories. We will now see whether it can be broken within a quantum mechanical theory.

Violation of Bell's inequality in quantum mechanics

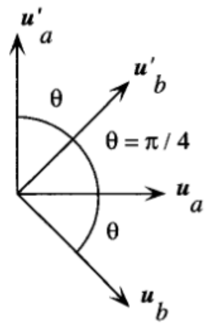
In quantum mechanics, the correlator $E(\vec{u}_a, \vec{u}_b)$ is written as

$$E(\vec{u}_a, \vec{u}_b) = \frac{4}{\hbar^2} \left\langle \hat{S}_{\vec{u}_a} \otimes \hat{S}_{\vec{u}_b} \right\rangle$$

A direct consequence of the Cauchy-Schwartz inequality is that $|E(\vec{u}_a, \vec{u}_b)| \leq 1$. We can compute the correlator on the entangled spin singlet state introduced above. We find that

$$E(\vec{u}_a, \vec{u}_b) = \frac{4}{\hbar^2} \langle \Sigma_{\rm s} | \hat{S}_{\vec{u}_a} \otimes \hat{S}_{\vec{u}_b} | \Sigma_{\rm s} \rangle = -\vec{u}_a \cdot \vec{u}_b$$

Let us choose the $\vec{u}$-vectors as in the figure below



We then have $\vec{u}_a \cdot \vec{u}_b = \vec{u}_a \cdot \vec{u'}_b = \vec{u'}_a \cdot \vec{u'}_b = -\vec{u'}_a \cdot \vec{u}_b = 1/\sqrt{2}$ and the expectation value of the correlator is found to be

$$S = -2\sqrt{2} < -2$$

We see that in the quantum mechanical treatment, the entangled state $|\Sigma_s\rangle$ violates Bell's inequality! If the conditions described above can be realized, there is then a way to check whether Bell's inequality is satisfied or not and whether there is room for a possible local hidden variable theory.

Experimental verification

Experiments trying to check Bell's inequality were performed with photons rather than with spin-1/2 particles. With photon, vertical and horizontal polarizations are considered rather than up or down spins. First experimental tests were realized between 1970 and 1975 but did not lead to conclusive results. It was the experiments of Fry and Thomson in Texas in 1976 and those of Aspect and his group in Orsay between 1980 and 1982 that have undeniably shown the violation of Bell's inequality. The Orsay group found that the relevant quantity S' for this experiment was $S' = 2.697 \pm 0.015$ when Bell's inequality would impose $S' \leq 2$. The experimental value clearly violates Bell's inequality and agrees with the value computed in quantum mechanics $S' = 2.70$. These experiments have therefore shown that a local hidden variable theory cannot exist for this experiment.

Note that this does not exclude a possible non-local theory. There are indeed other interpretations of quantum mechanics, such as e.g. the De Broglie-Bohm interpretation, in which particles do have an actual configuration, but while their dynamics is deterministic, it is also explicitly non-local. There are still debates about the interpretation of quantum mechanics, but the Copenhagen interpretation remains the most commonly taught.

Quantum cryptography

We will now discuss another application where entangled states play a key role: quantum cryptography. The goal of quantum cryptography is slightly different from classical cryptography. The aim is not to use quantum mechanics to directly encode a message that no one can decode, but rather to make sure that information that has been transferred has not been intercepted by a spy. Here we describe what is known as *quantum key distribution*. It is a method which enables two parties to produce a shared random secret key known only to them. There are different protocols to implement quantum key distribution and we will focus on the E91 protocol due to Artur Ekert.

Let us imagine that Alice wants to send Bob a binary message. Every bit of information is encoded by a spin-1/2, where "1" is represented by the $|+\rangle_{\vec{u}}$ eigenstate of a measurement along some axis $\vec{u}$, while "0" is represented by the $|-\rangle_{\vec{u}}$ eigenstate.

Generation of an entangled state

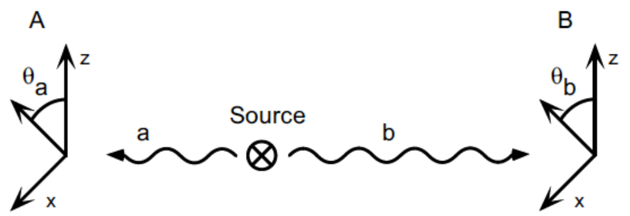
We consider a system of two spin-1/2, denoted a and b. The possible states of this system are written as linear combinations of product states

$$|\sigma;\sigma'\rangle_z \equiv |\sigma\rangle_z \otimes |\sigma'\rangle_z$$

where we have chosen eigenstates of the $\hat{S}_z$ operator. We then suppose that we have a source capable of generating entangled states

$$|\Sigma\rangle = \frac{1}{\sqrt{2}}\left(|+,+\rangle_z + |-,-\rangle_z\right)$$

The a spin is sent to Alice, while the b spin is sent to Bob, as shown in the figure below



It is easy to check that the state $|\Sigma\rangle$ has the same expression using eigenstates $|\sigma\rangle_\theta$ of $\hat{S}_{\vec{u}}$ for any vector $\vec{u} = (\sin\theta, \cos\theta, 0)$

$$|\Sigma\rangle = \frac{1}{\sqrt{2}}\left(|+,+\rangle_\theta + |-,-\rangle_\theta\right)$$

Measurements by Alice and Bob

Alice measures the spin along an axis $\vec{u}_a = (\sin\theta_a, \cos\theta_a, 0)$ forming an angle θ_a with the z axis. The possible outcomes of this measurement are $\pm\hbar/2$ with probability 1/2. If Alice measured $\sigma\hbar/2$, the state right after the measurement will be

$$|\sigma, \sigma\rangle_{\theta_a}$$

Note that this is not an entangled state and therefore a measurement of the b spin can be done independently from the a spin. Here is a summary of the different possibilities for two special cases $\theta_a = 0, \pi/2$

θ_a	measurement	probability	state after measurement
0	$+\hbar/2$	$1/2$	$\|+,+\rangle_z$
0	$-\hbar/2$	$1/2$	$\|-,-\rangle_z$
$\pi/2$	$+\hbar/2$	$1/2$	$\|+,+\rangle_x$
$\pi/2$	$-\hbar/2$	$1/2$	$\|-,-\rangle_x$

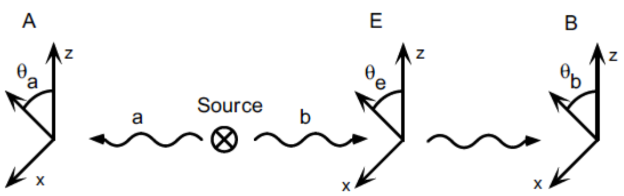
After Alice's measurement, Bob measures the spin b along an axis $\vec{u}_b = (\sin\theta_b, \cos\theta_b, 0)$ that is forming an angle θ_b with the z axis. We introduce the difference between Alice's and Bob's measurement angles $\Delta\theta = \theta_a - \theta_b$. A calculation shows that Bob will obtain the same result as Alice with probability

$$\mathcal{P}_{A=B} = \cos^2\left(\frac{\Delta\theta}{2}\right)$$

If the axis are the same, Bob will obtain the same result as Alice. Otherwise, the probability will be smaller than 1. In the special case where $\Delta\theta = \pi/2$, this probability is 1/2.

Here comes the spy Eve

Let us now suppose that $\theta_a = 0$. Eve the spy, hiding between the source and Bob, measures the spin b along an axis $\vec{u} = (\sin\theta_e, \cos\theta_e, 0)$ as shown in the figure below



Just like Bob, the spy Eve will obtain the same result as Alice with probability

$$\mathcal{P}_{A=E} = \cos^2\left(\frac{\theta_e}{2}\right) \qquad \mathcal{P}_{A\neq E} = \sin^2\left(\frac{\theta_e}{2}\right)$$

After this measurement, where both Alice and Eve have obtained $\sigma\hbar/2$, the state of the system is

$$|\sigma\rangle_z \otimes |\sigma\rangle_{\theta_e}$$

Now Bob measures the spin along the z direction on the state that has been measured by Eve. He will obtain the same result as Eve with probability

$$\mathcal{P}_{B=E} = \cos^2\left(\frac{\theta_e}{2}\right) \qquad \mathcal{P}_{B\neq E} = \sin^2\left(\frac{\theta_e}{2}\right)$$

Alice and Bob will obtain the same result either when Eve obtains the same result as Alice and Bob the same result as Eve, or when Eve obtains a different result from Alice and Bob a different result from Eve. All in all Alice and Bob have the same result with probability

$$\mathcal{P}_{A=B} = \frac{1}{4}\left(1+\cos\theta_e\right)^2 + \frac{1}{4}\left(1-\cos\theta_e\right)^2 = \frac{1}{2} + \frac{1}{2}\cos^2\theta_e$$

This is different from the situation with no spy, where Bob would obtain the same result as Alice with certainty. Here it is only when Eve picks the same measurement direction (or opposite direction) as Alice that Bob will obtain the same result as Alice with probability 1.

The encryption protocol

In order to detect whether a spy is trying to intercept the communication between Alice and Bob, they can use the following procedure:

1. Alice and Bob decide on two directions that they will use to make their measurements. For example, they pick x and z.

2. Alice prepares N pairs of spin-1/2 in the state $|\Sigma\rangle$. She sends the b spins to Bob and keeps the a spins.

3. Alice and Bob measure the spin along x or along z. They choose the axis x or z randomly for every new measurement. There is no correlation between the directions chosen by Alice and Bob. They keep track of all the results that they have obtained.

4. Bob selects a fraction F of his N measurements and openly communicates his results as well as the measurement directions to Alice. In practice $F \sim 0.5$.

5. For these FN measurements, Alice compares her results with those obtained by Bob. If they used the same measurement axis they must obtain the same result. Any discrepancy would be an indication that a spy is trying to read the message.

6. If no spy is found, Alice tells Bob that she is confident the message has not been intercepted. Bob tells Alice what measurement axis he used for the remaining $(1-F)N$ spins. But this time, he does not tell her the results he obtained.

7. Alice chooses a sequence where she used the same axis as Bob and openly tells Bob. For this sequence, Alice and Bob know they have obtained the same results and that they are the only ones to know these results. Alice can therefore use this sequence to construct a key to encode her secret message to Bob.

The spy cannot know a priori what axis Alice and Bob will choose. So the measurement angle of the spy must be chosen randomly. It is easy to show that no matter what strategy is used to choose θ_e the probability that Alice and Bob obtain the same result is $3/4$ if the message has been intercepted. In order to detect the presence of a spy, Alice and Bob must have chosen the same axis (probability $1/2$) and must have obtained different results (probability $1 - 3/4 = 1/4$. The spy remains undetected with probability $7/8$. For $FN = 200$ measurements, this probability shrinks to

$$\left(\frac{7}{8}\right)^{200} = 2,5 \times 10^{-12}$$

Needless to say, that it is very unlikely that the spy goes unnoticed...