Optical Quantum Egineering - IQUPS - March 2017

Philippe Grangier

1. The EPR "paradox" and Bell's inequalities (Lecture 1).

Let us consider two spin 1/2 particles in the singlet state :

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|+_z,\ -_z\rangle - |-_z,\ +_z\rangle)$$

The spin operators of the two particles are denoted as $\vec{\sigma}_1 = \vec{S}_1/(\hbar/2)$ and $\vec{\sigma}_2 = \vec{S}_2/(\hbar/2)$. The kets $|\epsilon_{1z},\ \epsilon_{2z}\rangle$ denote the joint eigenstates of $\sigma_{1z},\ \sigma_{2z}$, with the eigenvalues $\epsilon_{1z} = \pm 1,\ \epsilon_{2z} = \pm 1$. Let us assume that the two particles are spatially separated, so it is possible to measure independantly any spin component for each particle.

The eigenstates $|\pm_{\vec{u}}\rangle$ of a spin measurement along the unit vector $\vec{u}$, with polar angles θ and ϕ in spherical coordinates, are given by :

$$|+_{\vec{u}}\rangle = \cos(\theta/2)e^{-i\phi/2}|+_z\rangle + \sin(\theta/2)e^{i\phi/2}|-_z\rangle$$

$$|-_{\vec{u}}\rangle = -\sin(\theta/2)e^{-i\phi/2}|+_z\rangle + \cos(\theta/2)e^{i\phi/2}|-_z\rangle$$

1. Let us assume that the two particles move in opposite directions along the axis Oy. Calculate the expression of $|\psi\rangle$ in a basis $|\epsilon_{\vec{a}},\ \epsilon_{\vec{b}}\rangle$ of eigenstates $|\pm_{\vec{a}}\rangle$ for particle 1 et $|\pm_{\vec{b}}\rangle$ for particle 2, where $\vec{a}$ and $\vec{b}$ are two unit vectors in the plane xOz ($\phi_1 = \phi_2 = 0$), corresponding to the angles θ_1 et θ_2.

2. One performs an instantaneous measurement of $\sigma_{1a} = \vec{\sigma}_1.\vec{a}$ and $\sigma_{2b} = \vec{\sigma}_2.\vec{b}$ of the spin components along the unit vectors $\vec{a}$ and $\vec{b}$.

a. What are the 4 possibles results, and the probabilities of these results ?

b. What are the possibles results if one considers one particle only ? What are the probabilities of these results ?

c. What is the conditional probability to get the result $+1$ for particle 2, knowing that the measurement on particle 1 has given the result -1 ?

d. Assuming $\vec{a} = \vec{b}$, show that the measurement result for one spin is perfectly determined by the measurement result for the other spin. Find again this conclusion by using the "reduction of the wave packet" postulate. What can be said about the correlation between these measurements results ?

e. Show that the average value in state $|\psi\rangle$ of the product of results $E_Q(\vec{a}, \vec{b}) = \langle\psi|\sigma_{1a}\sigma_{2b}|\psi\rangle$ is given by : $E_Q(\vec{a}, \vec{b}) = -\vec{a}.\vec{b}$. What is the physical meaning of $|E_Q(\vec{a}, \vec{b})| = 1$?

3. Bell's inequalities (1964) : Einstein, Podolsky and Rosen argued in 1935 that when two particles are far enough of each other, the value of the spin for each particle must have a determined value, independant from any measurement realized on the other particle. Following this idea, John Bell built a very general model in which there might be a "hidden variable" λ, determining the results ± 1 for the separate (and remote) measurements of σ_{1a} and σ_{1b}, using two "sign" functions :

$$A(\lambda, \vec{a}) = \pm 1, \quad B(\lambda, \vec{b}) = \pm 1$$

This model is "local", because $A(\lambda, \vec{a})$ does not depend on $\vec{b}$, neither $B(\lambda, \vec{b})$ on $\vec{a}$. Denoting $P(\lambda)$ the probability distribution of the variables λ, normalized as $\int d\lambda P(\lambda) = 1$, one has thus :

$$E_C(\vec{a}, \vec{b}) = \int d\lambda P(\lambda) A(\lambda, \vec{a}) B(\lambda, \vec{b})$$

(i) Considering the 4 vectors $\vec{a}$, $\vec{a}'$, $\vec{b}$, $\vec{b}'$, one defines :

$$s(\lambda) = A(\lambda, \vec{a})B(\lambda, \vec{b}) - A(\lambda, \vec{a})B(\lambda, \vec{b}') + A(\lambda, \vec{a}')B(\lambda, \vec{b}) + A(\lambda, \vec{a}')B(\lambda, \vec{b}')$$

Show that $s(\lambda) = \pm 2$. Hint : write $s(\lambda)$ as

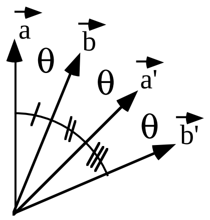
$$\big(A(\lambda, \vec{a}) + A(\lambda, \vec{a}')\big)\, B(\lambda, \vec{b}) - \big(A(\lambda, \vec{a}) - A(\lambda, \vec{a}')\big)\, B(\lambda, \vec{b}')$$

and look at the different possible values of $A(\lambda, \vec{a}) \pm A(\lambda, \vec{a}')$.

(ii) Using the above, demonstrate Bell's inequality : $|S_C| \leq 2$ with

$$S_C = E_C(\vec{a}, \vec{b}) - E_C(\vec{a}, \vec{b}') + E_C(\vec{a}', \vec{b}) + E_C(\vec{a}', \vec{b}')$$

4. Conflict between Quantum Mechanics and Hidden Variables Theories. Consider the choice of angles given on the figure below :



(i) Show that :

$$S_Q = E_Q(\vec{a}, \vec{b}) - E_Q(\vec{a}, \vec{b}') + E_Q(\vec{a}', \vec{b}) + E_Q(\vec{a}', \vec{b}')$$

can be written as : $S_Q = \cos(3\,\theta) - 3\cos(\theta)$.

(ii) Show that there is a conflict between the calculated predictions for S_Q and S_C for some values of θ. Conclusion ?

2. QND measurement of a spin component (Lecture 2).

On wants to perform a measurement on a qubit "a" by using an indirect (rather than direct) measurement, called a "Quantum Non Demolition" (QND) measurement. For instance, if the qubit is a spin 1/2 particle, one will not use a Stern-Gerlach magnet, but rather get the spin "a" to interact with another spin "b" during a time τ, and read out the result on spin "b". For this purpose, let us denote $\vec{\sigma}_{a,b} = \vec{S}_{a,b}/(\hbar/2)$ the spin observables for the two qubits, and $|az : \pm 1\rangle$, $|bz : \pm 1\rangle$ the eigenstates of the observables σ_{az} and σ_{bz}. After the interaction, one measures (directly) the state of qubit b, and one wants to infer the states of qubit a.

1. Let us denote $|ax : \pm 1\rangle$ et $|ay : \pm 1\rangle$ the eigenstates of σ_{ax} et σ_{ay}. Write down these states in the basis $\{|az : \pm 1\rangle\}$. Write also the expression of $|ax : \pm 1\rangle$ as a function of $|ay : \pm 1\rangle$.

2. We assume that the qubits are motionless (e.g. they are trapped), and that their interaction is described by the hamiltonian $H_m = \hbar g\ \sigma_{az}\ \sigma_{bx}/2$, acting during a duration τ. All other effects will be negelected during the interaction time. Show that H_m, σ_{az} and σ_{bx} are commuting operators. Write down their eigenstates, and give the corresponding eigenvalues.

3. Let us assume that the initial state of the pair of qubits is $|\psi_+(0)\rangle = |az : +\rangle \otimes |by : +\rangle$, and adjust the duration of the interaction so that $g\tau = \pi/2$. Calculate the system's final state $|\psi(\tau)\rangle$. Answer the same question if the initial state is $|\psi_-(0)\rangle = |az : -\rangle \otimes |by : +\rangle$. Give an interpretation of these results by considering the expression of H_m and Bloch's sphere for the qubit b, in the two cases where the qubit a is in either of the two states $\{|az : \pm 1\rangle\}$.

4. Starting from the initial state $|\psi(0)\rangle = (\alpha|az : +\rangle + \beta|az : -\rangle) \otimes |by : +\rangle$, one measures the spin component of qubit b along Oz, after the interaction has been carried out and turned off.

What are the possible results, and what are their probabilities ? After this measurement, what can be said about the component along Oz for qubit a ? Justify the name "QND measurement" given to this kind of process.

3. Schmidt decomposition (Lecture 2, density matrix)

One considers two quantum systems (e.g. two particles) described in two Hilbert spaces $\mathcal{E}_A$ et $\mathcal{E}_B$. The most general state of the particles pair is :

$$|\psi_{AB}\rangle = \sum_{i,j} c_{ij} |u_i\rangle_A |v_j\rangle_B$$

where $\{|u_i\rangle_A\}$ et $\{|v_j\rangle_B\}$ are orthogonal and normalized basis of $\mathcal{E}_A$ and $\mathcal{E}_B$.

1. Show that one can write $|\psi_{AB}\rangle = \sum_i |u_i\rangle_A |w_i\rangle_B$ and give the expression for $|w_i\rangle_B$.
2. Let us consider the density operator $\rho = |\psi_{AB}\rangle\langle\psi_{AB}|$ for the two particles, and define the reduced density operators : $\rho_A = Tr_B(\rho)$, and $\rho_B = Tr_A(\rho)$. Give the expression for ρ_A as a function of the scalar products $\langle w_i|w_j\rangle$.
3. Let us assume that ρ_A is diagonal in the basis $\{|u_i\rangle_A\}$, i.e. one has :

$$\rho_A = \sum_i p_i \, (|u_i\rangle|\langle u_i|)_A.$$

Show that the vectors $\{|w_j\rangle_B\}$ are orthogonal. What is the value of the modulus $|w_j\rangle_B$?

4. Show that $|\psi_{AB}\rangle = \sum_i \sqrt{p_i}\, |u_i\rangle_A |\tilde{w}_i\rangle_B$ where $\{|\tilde{w}_j\rangle_B\}$ is a normalized orthogonal basis, to be specified.
5. This expression is called the Schmidt decomposition of the pure state $|\psi_{AB}\rangle$. Using this decomposition, give a simple expression for ρ_B, and show that ρ_A et ρ_B have the same non-zero eigenvalues. The number of non-zero eigenvalues is called the *Schmidt number.*
6. The pure state $|\psi_{AB}\rangle$ is *separable* iff it can be written as a factorized expression $|\psi_{AB}\rangle = |\phi_A\rangle|\chi_B\rangle$. A non-separable state is *entangled.* Show that a state is separable iff the Schmidt number is equal to one. The Schmidt number is a (rough) measure of entanglement.

4. Security of quantum cryptography. (Lecture 3)

The goal of this exercice is to establish a proof of the security of quantum cryptography, inspired from an article by F. Grosshans and N. Cerf (arXiv:quant-ph/0311006). This is not the most general and powerful proof currently available, but it gives a good feeling of the issue. The proof relies on two theorems, that we will not demonstrate;

(a) a theorem by Csiszar and Körner : If a quantum protocol provides mutual quantum informations I_{AB} and I_{BE} between Alice, Bob and Eve, then Alice and Bob can use classical data processing to distill a secret key with size

$$\Delta I = I_{AB} - I_{BE}$$

One is using I_{BE} rather than I_{AE} because the distillation of the key includes the information about which photons were actually received by Bob. This is called an "inverse reconciliation protocol" because quantum and classical informations are going in opposite directions (Alice to Bob for quantum, and Bob to Alice for classical).

(b) the “entropic Heisenberg inequalities” (arXiv:quant-ph/0110025): If Bob measures two (generally non-commuting) observables B_X et B_Y on a system described by a density matrix ρ, the Shannon entropies associated with these measurements are constrained by :

$$H(B_X|\rho) + H(B_Y|\rho) \geq -2\ \log_2 c$$

where $c = max_{i,j}|\langle x_i|y_j\rangle|$ is the maximum value of the overlap between the eigenstates of B_X et B_Y. This inequality is physically very close to the usual Heisenberg inequalities, but it involves entropies rather than variances. .

Let us consider a statistical ensemble $\mathcal{A}$ of quantum states prepared by Alice and sent to Bob. The eavesdropper Eve will attack the communication by entangling ancilla qubits with the qubits sent by Alice, in order to extract the maximum amount of information.

This situation can be studied by assuming (without loss of generality) that Alice, Bob et Eve share a tripartite entangled pure state $|\Psi\rangle$. Rather than sending a qubit to Bob, Alice performs a measurement on her own part of $|\Psi\rangle$. The random (classical) result that she obtains corresponds to the random choice she would have for sending a qubit to Bob. The two approaches (either “prepare and measure scheme”, or “entangled scheme”) are thus completely equivalent, because Alice owns the same information in both cases, and the density matrix seen by Eve and Bob is also the same in both cases.

(a) Assuming that Bob measures the observable B_X, write down the mutual informations I_{BA} et I_{BE} as a function of Bob's entropy $H(B_X)$ and of the conditional entropies $H(B_X|A)$ et $H(B_X|E)$. Calculate the secret bit rate ΔI as a function of the conditional entropies.

(b) The measurements done by Alice and (maybe) by Eve project the initial entangled state on a new state which Bob will receive. Using the entropic Heisenberg inequalities, find a lower bound for the sum $H(B_X|E) + H(B_Y|A)$ of conditional entropies corresponding to the measurements carried out respectively by Eve and Alice.

(c) Using the previous result find a lower bound for ΔI without using I_{BE}, which is unknown by Alice and Bob. Since the observables B_X et B_Y play the same role in the protocol, one will assume that $H(B_X|A) = H(B_Y|A) = H(B|A)$.

(d) Calculate c for the BB84 protocol where the exchanged quantum system is a polarized photon, with possible polarization orientations 0, 45, 90, 135 degrees. Deduce the security condition for BB84, expressed as a function of the mutual information I_{AB}.

(e) Calculate I_{AB} as a function of the binary entropy $H(e)$ when the error rate of the transmission line is e. Deduce a condition on the error rate e to be able to exchange a secret key through the transmission line.