Chapter 4

Quantum entanglement

In this chapter we study the nature of a special type of correlation displayed by the entangled states. These correlations have no classical counterpart, in other words, they cannot be described by classical probability distributions. They are genuine quantum mechanical correlations built up in the states of composite quantum systems.

We first take a close look at the so-called Bell states which violate the famous Bell inequalities*[1]. These states display the essence of entanglement and the CHSH inequality provides an experimentally testable signature of it. We then describe three applications: a quantum key distribution protocol (Ekert 1991), quantum teleportation and dense coding. We stress here that all three of them have been experimentally realized.

In quantum information processing one tries to use entanglement as a quantifiable ressource, much like energy or information, and it would be very convenient to be able to measure the degree or quantity of entanglement. It is not yet clear that such a meaningful and useful measure exists. We will come back to this point in later chapters.

4.1 Bell states

Production of Bell states. We have seen in chapter 2 that in order to produce entangled states the Qbits must "interact", at some point in time. The prototypical example of entangled states are the Bell states which form a basis of $C^2 \otimes C^2$. Here we show how these can be produced from the unitary

[1]There is a class of such nequalities named after John Bell who derived the first ones. In this chapter we derive the more transparent Clauser-Horne-Shimony-Holt (CHSH) inequality.

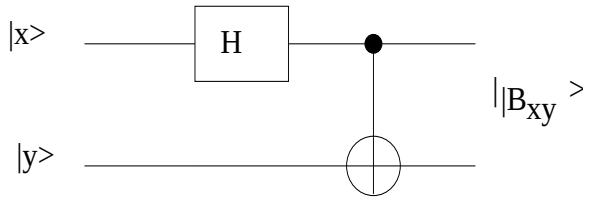

Figure 4.1: Quantum circuit producing Bell states

gate

$$U = (CNOT) \cdot (H \otimes I) \tag{4.1}$$

This is a 4×4 matrix equal to the usual matrix product of the two 4×4 matrices $CNOT$ and $H \otimes I$. The *Control Not* gate provides the interaction between the two bits. It is defined as the NOT gate acting on the second bit provided the first one*[2] equals 1

$$CNOT|x, y\rangle = |x, y \oplus x\rangle$$

The matrices H and I are the usual 2×2 Hadamard and identity matrices. The circuit representation of the unitary gate $U = (CNOT) \cdot (H \otimes I)$ is depicted in figure 1.

Let us calculate the action of this circuit on a tensor product state $|x\rangle \otimes |y\rangle = |x, y\rangle$.

$$\begin{aligned}
(CNOT) \cdot (H \otimes I)|x, y\rangle &= (CNOT)\frac{1}{\sqrt{2}}\big(|0\rangle + (-1)^x|1\rangle\big) \otimes |y\rangle \\
&= \frac{1}{\sqrt{2}}CNOT|0, y\rangle + \frac{(-1)^x}{\sqrt{2}}CNOT|1, y\rangle \\
&= \frac{1}{\sqrt{2}}|0, y\rangle + \frac{(-1)^x}{\sqrt{2}}|1, y \oplus 1\rangle) \\
&= |B_{xy}\rangle
\end{aligned}$$

More excplicitely we have

$$|B_{00}\rangle = \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big) = U|00\rangle$$

$$|B_{01}\rangle = \frac{1}{\sqrt{2}}\big(|01\rangle + |10\rangle\big) = U|01\rangle$$

$$|B_{10}\rangle = \frac{1}{\sqrt{2}}\big(|00\rangle - |11\rangle\big) = U|10\rangle$$

[2] called the control bit

$$|B_{11}\rangle = \frac{1}{\sqrt{2}}\big(|01\rangle - |10\rangle\big) = U|11\rangle$$

These four states are a unitary "rotation" of the four canonical basis states of $C^2 \otimes C^2$ and thus also form a basis, called the Bell basis.

Here the interaction is effected by the $CNOT$ gate: building such a gate in a laboratory requires bringing two particles supporting the Qbits $|x\rangle$, $|y\rangle$ close enough in space and time (interactions are local). Photons do not interact directly with one another (Maxwell equations are linear) but they can interact indirectly through their direct interaction with matter (one speaks of non-linear optics). Localized sources producing pairs of entangled photons are excited atoms or nuclei. Electron spin can also be entangled because the combination of the Coulomb interaction with the Pauli principle can cause magnetic correlations of this type. In fact this kind of entanglement is very common place: in a hydrogen molecule the spin part of the chemical valence bond*[3] between two hydrogen atoms is the state

$$|B_{11}\rangle = \frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle)$$

The reader should check that

$$|B_{00}\rangle = \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big) = \frac{1}{\sqrt{2}}\big(|\gamma\gamma\rangle + |\gamma_\perp\gamma_\perp\rangle\big) \tag{4.2}$$

This has remarquable consequences as the following discussion will show. For the sake of the argument we suppose that Alice has captured one photon in her lab and Bob has captured the other photon in his lab (figure 2). Irrespective how remote the two labs are, it is always true that the two photons have come from a common localized source. Now we look at the outcome of several simple measurements that Alice and Bob might do each in their own lab, *assuming that they cannot communicate the outcomes*. We will consider the three specific situations wher: Alice measures first/Bob measures after; Bob measures first/Alice measures after; Alice and Bob measure simultaneously[4].

- *Alice measures first and Bob after.* The "measurement apparatus" of Alice is formed by the projectors $\{|\alpha\rangle\langle\alpha| \otimes I, |\alpha_\perp\rangle\langle\alpha_\perp| \otimes I\}$ so that,

[3] the antisymmetry of the spin part allows the orbital part to be in the symmetric energetically favorable state (Heitler-London theory)

[4] For the moment assume a Newtonian picture for space-time, but we will see that the time ordering of events is irrelevant so that the discussion is also valid with a relativistic picture of space-time.

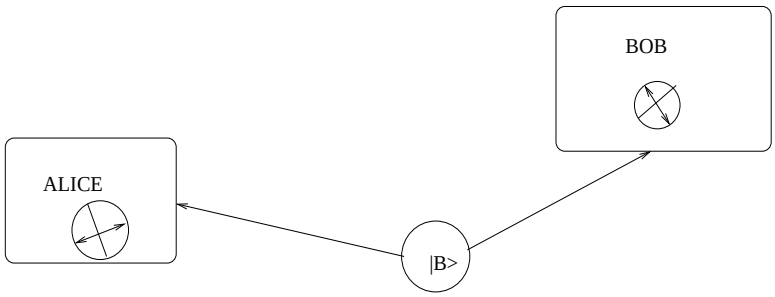

Figure 4.2: Alice and Bob share an entangled pair

according to the measurement postulate, the Bell state collapses to one of the projections (remember we have to normalize after projecting)

$$|\alpha\rangle\langle\alpha| \otimes I|B_{00}\rangle = \frac{1}{\sqrt{2}}|\alpha\alpha\rangle \rightarrow |\alpha\rangle \otimes |\alpha\rangle, \qquad \text{with prob } \frac{1}{2}$$

$$|\alpha_\perp\rangle\langle\alpha_\perp| \otimes I|B_{00}\rangle = \frac{1}{\sqrt{2}}|\alpha_\perp\alpha_\perp\rangle \rightarrow |\alpha_\perp\rangle \otimes \alpha_\perp\rangle, \qquad \text{with prob } \frac{1}{2}$$

Therefore Alice observes *her photon* in the collapsed state $|\alpha\rangle$ or $|\alpha_\perp\rangle$. Bob, on his side, does not know anything, and doesnt even know that Alice has performed measurements ! In order for him to learn something he can try to perform a measurement on his photon. But he has to choose a basis $\{|\beta\rangle, |\beta_\perp\rangle\}$. Given that his photon is in the state $\alpha\rangle$, his photon collapses to $\beta\rangle$ with prob $\cos^2(\alpha - \beta)$ or to $|\beta_\perp\rangle$ with prob $\sin^2(\alpha - \beta)$. Similarly, given that his photon is in the state $\alpha_\perp$ we get the same result with $\cos^2$ and $\sin^2$ interchanged. The fact that Bob does not know the initial state of his photon or that he does not even known what Alice has done should not bother you: the point is that he does a specific experiment (measurement in the $\beta, \beta_\perp$ basis) and finds a net outcome. The net outcome in Bob's lab is that the photon is in the state $\perp \beta\rangle$ with prob $\frac{1}{2}$ or $|\beta_\perp\rangle$ with prob $\frac{1}{2}$.

- *Bob measures first and Alice after.* The same discussion shows that, if Bob performs measurements first (in the $\beta, \beta_\perp$ basis) while Alice sleeps and Alice measures after (in the $(\alpha, \alpha_\perp$ basis) the net outcome of each party is the same.

- *Bob and Alice measure simultaneously.* You might think (?) that if both parties perform *simultaneous* local measurements the whole scenario is different. Let us try. Suppose Alice and Bob perform simultaneous measurements in the basis

$$\{|\alpha, \beta\rangle, |\alpha, \beta_\perp\rangle, |\alpha_\perp, \beta\rangle, |\alpha_\perp, \beta_\perp\rangle\}$$

The Bell state

$$|B_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|\gamma\gamma\rangle + |\gamma_\perp\gamma_\perp\rangle)$$

will collapse to one of the four basis states. So Alice will be in possession of a photon in state $|\alpha\rangle$ or $|\alpha_\perp\rangle$ and Bob in possession of a photon in the state $|\beta\rangle$ or $|\beta_\perp\rangle$. The situation is exactly the same than in the previous situations ! It is very instructive to compute the probabilities of the respective collapsed states (which are nothing else than the basis states). One finds that these are*[5]

$$\frac{1}{2}\cos^2(\alpha-\beta),\ \frac{1}{2}\sin^2(\alpha-\beta),\ \frac{1}{2}\sin^2(\alpha-\beta),\ \frac{1}{2}\cos^2(\alpha-\beta)$$

In her lab Alice finds that the probability of her outcomes $|\alpha\rangle$ (resp $|\alpha_\perp\rangle$) is $\frac{1}{2}$ (resp $\frac{1}{2}$) as in the previous scenarios; and the same holds true for Bob. Therefore the conclusions that Alice and Bob infer from their simultaneous local measurements are the same than in the non-simultaneous cases above.

To summarize the situation, we see that when Alice or/and Bob perform successive or simultaneous local measurements on their photons, whatever is their choice of basis they find the photon in one of the two chosen basis states with probability $\frac{1}{2}$. In other words the entropy of the probability distribution of their local outcomes is maximal (it equals $\ln 2$ bits) and they may infer that their photon is in a "maximaly disordered state". In fact if they dont know that the source produced an entangled pair or if nobody tells them that the two photons are entangled they have no way of even noticing that the pair is entangled. It seems that we have no way of knowing if we are entangled to some distant Alien in the universe, just by performing local experiments in our part of the universe (scary no ?!). We will see in the next section that Alice and Bob can assert that their photons are entangled and that the only way for them to know that is to communicate. Here by communicate we mean the perfect or approximate transmission of a classical message.

Let us also point out that here we have discussed the situation having in mind a Newtonian picture of space-time. In other words the meaning of the words "before", "simultaneous" and "after" is the "usual" one. However this is only an approximation and one might question if a proper account of Minkowskian space-time would change our conclusions. According to relativity these words are relative to each observer's frame of reference. What

[5] fortunately independent of γ

has an absolute meaning is the space-time interval which may be space-like, time-like (or zero). If the local measurement events (events are points in space-time) of Alice and Bob are separated by a space-like vector they cannot possibly be a causal connection or between the events and in particular it is garanteed that Alice and Bob cannot establish a classical communication link during the experiment. On the other hand if the measurement events are separated by a time-like vector it is conceivable that there is a causal connection between the events, however unless Alice and Bob set up such a communication link, there is no reason to believe that there is a causal connection between the outcomes since they are exactly the same as in the case of space-like separation.

4.2 Bell inequalities and Aspect experiment

We saw in the last section that if there is no communication between Alice and Bob they can only infer that the photons are in a maximaly disordered state. In this section we will see that by doing repeated measurements and by communicating the results afterwards, Alice and Bob can assert if the state produced by the source is entangled or not.

The procedure that we are going to describe was initialy invented by John Bell who was refelcting on a famous paper of Einstein-Podolsky-Rosen. The later claimed that the entangled states do not provide a "complete" description of the correlations present in the system, and where seeking a "classical" theory of these corelations. Bell's approach to the problem is to try to decide if the correlations in a real pair of entangled photons (produced by an excited atomic source say) *can be described* or *cannot be described* by *a classical theory*. The general idea is that if a pair of photons is described by a classical theory then appropriate correlation functions of the measurements of Alice and Bob satisfy very special constraints. These constraints are violated if the pair is described by a quantum mechanical Bell state. We will see that Bell's approach is able to discrimnate between a huge set of classical theories and QM. Famous experiments of Aspect-Grangier-Roger have shown that standard QM wins!

The experimental protocol. A source S produces, at each instant of time n, a pair of photons. We do not have any prejudice as to what is the state or the description of the pair. One photon flies to Alice's lab and the other flies to Bob's lab. In each lab our two protagonists operate independently: for the moment they do not communicate and do not care what the other one does.

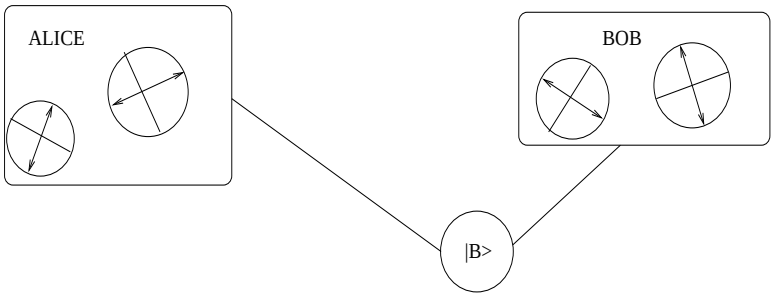

Figure 4.3: Experimental set up

- At each time instant n, Alice randomly uses analyzers

$$\{|\alpha\rangle, |\alpha_\perp\rangle\} \qquad \text{or} \qquad \{|\alpha'\rangle, |\alpha'_\perp\rangle\}$$

to measure the polarization of her photon. When she records a click in the detector she sets $a_n = +1$ or $a'_n = +1$ and when the detector does not click she sets $a_n = -1$ or $a'_n = -1$. She keeps track of her choices for the analyzer at each n.

- At each time instant n, Bob uses randomly analyzers

$$\{|\beta\rangle, |\beta_\perp\rangle\} \qquad \text{or} \qquad \{|\beta'\rangle, |\beta'_\perp\rangle\}$$

to measure the polarization of his photon. When he records a click in the detector he sets $b_n = +1$ or $b'_n = 1$ and when the detector does not click he sets $b_n = -1$ or $b'_n = -1$. He keeps track of his choices of analyzers for each n.

- Now there is a classical communication phase. Alice and Bob meet and discuss all their measurements. They classify them according to the four exprimental setups. Given n the arrangement of analyzers were

$$1 = (\alpha, \beta),\ 2 = (\alpha, \beta'),\ 3 = (\alpha', \beta),\ 4 = (\alpha', \beta')$$

For each arrangement they compute the following empirical averages

$$\frac{1}{N_1}\sum_{n_1} a_{n_1} b_{n_1},\ \frac{1}{N_2}\sum_{n_2} a_{n_2} b'_{n_2},\ \frac{1}{N_3}\sum_{n_1} a'_{n_3} b_{n_3},\ \frac{1}{N_4}\sum_{n_4} a'_{n_4} b'_{n_4}$$

Then they compute the following correlation function

$$X_{exp} = \frac{1}{N_1}\sum_{n_1} a_{n_1} b_{n_1} + \frac{1}{N_2}\sum_{n_2} a_{n_2} b'_{n_2} - \frac{1}{N_3}\sum_{n_1} a'_{n_3} b_{n_3} + \frac{1}{N_4}\sum_{n_4} a'_{n_4} b'_{n_4}$$

Prediction of classical theories. We assume that the quantities that Alice and Bob measure correspond to well defined observables A, A', B, B' that have simultaneous definite values a, a', b, b' even when there is no observer. This is the hypothesis of "realism" and is discussed in more detail later. Furthermore we assume that the outcomes of Alice and Bob can be modeled by a joint probability distribution*[6]

$$P_{class}(a, a', b, b')$$

Here by a, b, a' and b' we mean the random variables modelling the measurement outcomes. The expectation with respect to P_{class} is denoted by $\mathbf{E}_{class}$. The corresponding theoretical prediction for *each* empirical average above is

$$\mathbf{E}_{class}[ab],\ \mathbf{E}_{class}[ab'],\ \mathbf{E}_{class}[a'b],\ \mathbf{E}_{class}(a'b')$$

and using *only the linearity of expectation*

$$X_{class} = \mathbf{E}_{class}[ab + ab' - a'b + a'b']$$

Notice that

$$ab + ab' - a'b + a'b' = a(b + b') + a'(b' - b)$$

and that

$$-2 \leq a(b + b') + a'(b' - b) \leq 2$$

Indeed if $b = b'$ then only the first term survives which leads to the inequality; while if $b \neq b'$ only the second term survives which again leads to the inequality. Thus we have for the expectation,

$$-2 \leq X_{class} \leq 2$$

This is one of the simplest Bell type inequalities which was derived by Clauser-Horne-Shimony-Holt and is called the CHSH inequality.

In order to derive this result we havent assumed anything about the state of preparation of the source. We have only assumed that the experimental results can be cast into a probability distribution. In fact this is not a priori so obvious. There are four experimental arrangements so that when Alice and Bob meet they have four histograms that can be fitted to 4 probability distributions:

$$P_1(a, b),\ P_2(a', b),\ P_3(a, b'),\ P_4(a', b')$$

and we ask if these are the marginals of a common $P_{class}(a, a', b, b')$. It is not a priori clear that nature always gives us histograms that are marginals

[6]this second assumption follows from the assumption of "realism" combined with "locality". This is explained in the next paragraph

of a common distribution. In fact this is *not* always the case: after all any of you can construct four probability distributions that are not marginals of a common one, and this is an outcome of your brain viewed as a physical system. So why is the assumption leading to the CHSH inequality very reasonable ? Below we do not attempt to provide the most general argument.

Let us admit that the laws of physics are "local". By this we mean that when Alice (resp. Bob) perform measurements that are space-like separated (no communication possible with slower than the speed of light signals) Alice's experimental outcomes (resp. Bob's) depend only on her own local choice of analyzers. This is an assumption that nobody, among physicists, wants to abandon because it underlies all the known fundamental laws of physics.

Furthermore let us suppose, following our classical intuition, or following Einstein, that the outcomes of experiments should be well defined prexisting functions*[7] of the system's state and the experimental set up (this is called "realism" by some people). In mathematical terms there should be a function such that

$$a = f_{\mathcal{A}}(\alpha;\lambda),\ a' = f_{\mathcal{A}}(\alpha';\lambda),\ b = f_{\mathcal{B}}(\beta;\lambda),\ b' = f_{\mathcal{B}}(\beta';\lambda)$$

Here λ is a set of variables accounting for the state of the system and whatever is needed to compute the experimental outcome. It has become custommary to call them "hidden variables".

The hidden variables may be random or deterministic*[8] and their set of values is described by a probability distribution $h(\lambda)$. According to "local realism" the histograms of Alice and Bob are modelled by

$$P_1(a,b) = \int d\lambda h(\lambda)\delta(a - f_{\mathcal{A}}(\alpha,\lambda))\delta(b - f_{\mathcal{B}}(\beta,\lambda))$$

$$P_2(a,b') = \int d\lambda h(\lambda)\delta(a - f_{\mathcal{A}}(\alpha,\lambda))\delta(b' - f_{\mathcal{B}}(\beta',\lambda))$$

$$P_3(a',b) = \int d\lambda h(\lambda)\delta(a' - f_{\mathcal{A}}(\alpha',\lambda)\delta(b - f_{\mathcal{B}}(\beta,\lambda))$$

$$P_4(a',b') = \int d\lambda h(\lambda)\delta(a' - f_{\mathcal{A}}(\alpha',\lambda)\delta(b' - f_{\mathcal{B}}(\beta',\lambda))$$

[7] we could also frame the discussion in a slightly more genneral context where the outcome is described by a probability distribution $p_{\mathcal{A}}(a|\alpha,\lambda)$. here we have $p_{\mathcal{A}}(a|\alpha,\lambda) = \delta(a - f_{\mathcal{A}}(\alpha,\lambda)$. The conclusions are however the same, but this remark is interesting because it shows that it is not determinism that is at stake here.

[8] in this case the distribution is simply a Dirac $\delta(\lambda - \lambda_0)$

Evidently these are the marginals of a common probability distribution

$$P_{class}(a,a',b,b') = \int d\lambda h(\lambda)\delta(a-f(\alpha,\lambda))\delta(a'-f(\alpha',\lambda))\delta(b-f(\beta,\lambda))\delta(b'-f(\beta,\lambda))$$

Prediction of QM for a Bell state. First of all we notice that according to the quantum formalism the measurements of Alice and Bob are measurements of the 4 observables (hermitian matrices)

$$A = |\alpha\rangle\langle\alpha| - |\alpha_\perp\rangle\langle\alpha_\perp|, \qquad A' = |\alpha'\rangle\langle\alpha'| - |\alpha'_\perp\rangle\langle\alpha'_\perp|$$

and

$$B = |\beta\rangle\langle\beta| - |\beta_\perp\rangle\langle\beta_\perp|, \qquad B' = |\beta'\rangle\langle\beta'| - |\beta'_\perp\rangle\langle\beta'_\perp|$$

At each time instant n the state of the photon pair is described by some ket $|\Psi\rangle \in \mathcal{C}^2 \otimes \mathcal{C}^2$. The quantum mechanical prediction for the four empirical averages of Alice and Bob is

$$\langle\Psi|A\otimes B|\Psi\rangle,\ \langle\Psi|A\otimes B'|\Psi\rangle,\ \langle\Psi|A'\otimes B|\Psi\rangle,\ \langle\Psi|A'\otimes B'|\Psi\rangle$$

and for the correlation function

$$X_{QM} = \langle\Psi|A\otimes B|\Psi\rangle + \langle\Psi|A\otimes B'|\Psi\rangle - \langle\Psi|A'\otimes B|\Psi\rangle + \langle\Psi|A'\otimes B'|\Psi\rangle$$

Now let us compute this quantity for the Bell state

$$|\Psi\rangle = |B_{00}\rangle$$

The first average is best computed by expressing the Bell state as $\frac{1}{\sqrt{2}}(|\alpha\alpha\rangle + |\alpha_\perp\alpha_\perp\rangle)$.

$$\begin{aligned}
\langle B_{00}|A\otimes B|B_{00}\rangle &= \frac{1}{2}\langle\alpha\alpha|A\otimes B|\alpha\alpha\rangle + \frac{1}{2}\langle\alpha_\perp\alpha_\perp|A\otimes B|\alpha_\perp\alpha_\perp\rangle \\
&+ \frac{1}{2}\langle\alpha\alpha|A\otimes B|\alpha_\perp\alpha_\perp\rangle + \frac{1}{2}\langle\alpha_\perp\alpha_\perp|A\otimes B|\alpha\alpha\rangle \\
&= \frac{1}{2}\langle\alpha|A|\alpha\rangle\langle\alpha|B|\alpha\rangle + \frac{1}{2}\langle\alpha_\perp|A|\alpha_\perp\rangle\langle\alpha_\perp|B|\alpha_\perp\rangle \\
&= \frac{1}{2}\cdot 1\cdot\big(|\langle\alpha|\beta\rangle|^2 - |\langle\alpha|\beta_\perp\rangle|^2\big) + \frac{1}{2}\cdot(-1)\cdot\big(|\langle\alpha_\perp|\beta\rangle|^2 - |\langle\alpha_\perp|\beta_\perp\rangle|^2\big) \\
&= \frac{1}{2}\big(\cos^2(\alpha-\beta) - \sin^2(\alpha-\beta)\big) - \frac{1}{2}\big(\sin^2(\alpha-\beta) - \cos^2(\alpha-\beta)\big) \\
&= \cos^2(\alpha-\beta) - \sin^2(\alpha-\beta) = \cos 2(\alpha-\beta)
\end{aligned}$$

Performing similar calculations for the other averages we find

$$X_{QM} = \cos 2(\alpha-\beta) + \cos 2(\alpha-\beta') - \cos 2(\alpha'-\beta) + \cos 2(\alpha'-\beta')$$

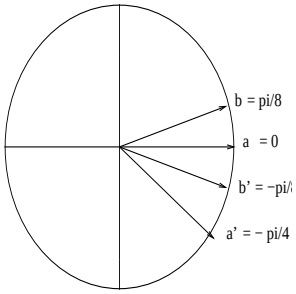

Figure 4.4: Optimal choice of analyzer orientation

This quantity is maximized for the following choice of angles (and all global rotations of this choice of course, figure 4),

$$\alpha = 0,\ \alpha' = -\frac{\pi}{4},\ \beta = \frac{\pi}{8},\ \beta' = -\frac{\pi}{8}$$

and equals

$$X_{QM} = \cos\frac{\pi}{4} + \cos\frac{\pi}{4} - \cos\frac{3\pi}{4} + \cos\frac{\pi}{4} = 2\sqrt{2}$$

We see that the CHSH inequality is violated ! For the three other Bell states on finds the same result. In the exercises you will show that this is the maximum possible violation over all quantum states of $C^2 \otimes C^2$. In this sense the Bell states are maximaly entangled.

Experiments. In a famous set of experiments performed in the 80's Aspect and collaborators showed that experiment agrees with QM and not with classical theories. The difficulty of these experiments is that to be really convincing one must rotate the analysers of Alice and Bob fast enough so that the measurement events are separated by a space-like interval. Otherwise one may always argue that some form of classical communication, that will conspire to make up the results, happens in the system (on speaks of locality loophole). This is the challenge that the Aspect experiments were the first to address, as compared with other slightly earlier experiments. This locality loophole has been since then conclusively settled by more recent experiments*[9].

These experiments tell us that we have to abandon the "local realism". QM does not give up locality (fundamental models of interactions are local) but rather it gives up realism (at least in the sense described above). Indeed when Alice performs a measurement her outcome does not depend on what

[9]see the review by Aton Zeilinger "Experiment and the foundations of quantum physics", in Reviews of Modern Physics **71**, S288-S297 (1999)

Bob does (this is locality) but at the same time it is not a well defined function $f(\cdot, \lambda)$ independent of her choice of analyzers (in this sense realism doesnt hold). There cannot exist such a function depending on hidden variables λ with distribution $h(\lambda)$, which accounts for the experimanetal results. QM predicts that the four histograms of Bob and Alice are

$$\begin{aligned} P_1(a,b) &= \frac{1}{4}(1 + ab\cos 2(\alpha - \beta)) \\ P_2(a,b) &= \frac{1}{4}(1 + ab'\cos 2(\alpha - \beta')) \\ P_3(a',b) &= \frac{1}{4}(1 + a'b\cos 2(\alpha' - \beta)) \\ P_4(a',b') &= \frac{1}{4}(1 + a'b'\cos 2(\alpha' - \beta')) \end{aligned}$$

There special choices of the angles $\alpha, \beta, \alpha', \beta'$ for which these *are not the marginals of a common distribution* $P_{class}(a, b, a', b')$ otherwise we would have $|X| \leq 2$: this is just a mathematical fact[10]. Now, nature produces these four histograms in an experiment satisfying locality in the sense that all analyser choices of Alice and Bob are independent. But she plays a very subtle magic trick with us: *the correlations that are built up in Bell's states are non-local* in the sense that correlations are present in the measurement outcomes even though the measurements on the photons are purely local (e.g space like separted). Alice and Bob cannot notice these non local correlations by purely local means in their own lab. They have to meet or to communicate by exchanging matter.

It is sometimes said that QM is non-local: this has to be understood in the sense that quantum mechanical states of the Hilbert space can be non-local, in other words arbitrarily extended; however the physical laws of interactions are, as far as we know, local, in other words decay with distance till they become negligible.

As you can begin to suspect it does not make much sense to stick to "classical intuition", "local realism" or anything of this sort. You will have to develop a new "quantum like intuition"...

4.3 Ekert protocol for QKD

A nice application of the CHSH inequality is a protocol for the generation of a secret key by two parties. We assume that a localized source of EPR

[10] In some sense they are the marginals of a quantum state

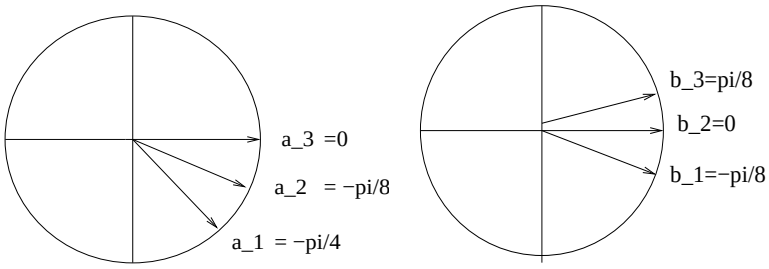

Figure 4.5: Alice and Bob's random choices of analyzers

particles delivers entangled Qbits to Alice and Bob at each time instant n in the state

$$|B_{00}\rangle = \frac{1}{2}(|00\rangle + |11\rangle) = \frac{1}{2}(|\theta\theta\rangle + |\theta_\perp\theta_\perp\rangle)$$

Moreover they have also established a noiseless communication channel.

The protocol:

- Alice has analyzers oriented in directions $\mathbf{a}_1$, $\mathbf{a}_2$, $\mathbf{a}_3$ and records the results of measurements, at each time instant, for the observables

  $$A(\mathbf{a}) = (+1)|\mathbf{a}\rangle\langle\mathbf{a}| + (-1)|\mathbf{a}_\perp\rangle\langle\mathbf{a}_\perp|$$

  where she chooses $\mathbf{a}$ randomly among $\mathbf{a}_1$, $\mathbf{a}_2$, $\mathbf{a}_3$ (figure 5).

- Bob has three analyzers oriented along $\mathbf{b}_1$, $\mathbf{b}_2$, $\mathbf{b}_3$ and records the results of measurements, at each time instant, for the observables

  $$B(\mathbf{b}) = (+1)|\mathbf{b}\rangle\langle\mathbf{b}| + (-1)|\mathbf{b}_\perp\rangle\langle\mathbf{b}_\perp|$$

  where he chooses $\mathbf{b}$ randomly among $\mathbf{b}_1$, $\mathbf{b}_2$, $\mathbf{b}_3$ (figure 5).

- Alice and Bob start a public discussion over the communication channel: they inform each other on what vectors they used at each time instant.

- They do a security check to ensure that no eavesdropper is present. Alice and Bob select all time instants when the basis choices were

  $$(\mathbf{a}_3, \mathbf{b}_3),\ (\mathbf{a}_3, \mathbf{b}_1),\ (\mathbf{a}_1, \mathbf{b}_1),\ (\mathbf{a}_1, \mathbf{b}_3)$$

  Note that these are the same four analyzer arrangements used for the Bell inequalities (figure 6). For such configurations and only for such

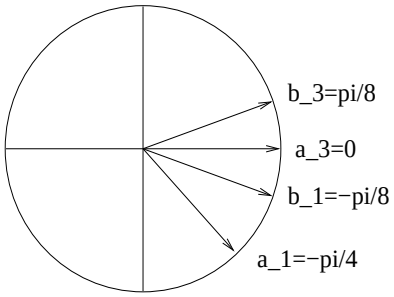

Figure 4.6: CHSH configuration

ones they exchange their measurement results. Each party computes a correlation coefficient

$$\begin{aligned} X_{\text{exp}} = Av(a_n(\mathbf{a}_3)b_n(\mathbf{b}_3)) &+ Av(a_n(\mathbf{a}_3)b_n(\mathbf{b}_1)) \\ &- Av(a_n(\mathbf{a}_1)b_n(\mathbf{b}_3)) + Av(a_n(\mathbf{a}_1)b_n(\mathbf{b}_1)) \end{aligned}$$

where Av is the empirical average. In a perfect world they should find $X_{exp} = 2\sqrt{2}$. We will see later that when an eavesdropper is present they will certainly find $X_{exp} \leq 2$ because the effect of the eavesdropper is to destroy the entanglement of the EPR pair and the system behaves "classicaly". The security check thus consists in checking that

$$X_{exp} > 2$$

If the test passes they conclude there is no eavesdropper and generate the key, if not they stop communication.

- The key generation process is as follows. For every time n such that they used the same basis - that is $(\mathbf{a}_3, \mathbf{b}_2)$ or $(\mathbf{a}_2, \mathbf{b}_1)$ - they know for sure that

$$a_n = b_n = 1, \qquad \text{or} \qquad a_n = b_n = -1$$

(one can also check that in this case $\langle B_{00}|A \otimes B|B_{00}\rangle = \cos 2(\hat{\mathbf{a}, \mathbf{b}}) = 1$). This is a common subsequence of ± 1 that they keep secret and forms their shared secret key.

Attacks from Eve. Let us consider the simplest measurement attack in which Eve captures each photon of the EPR pair and makes a measurement (figure 7). Then she sends each photon (in the resulting state) to Alice and Bob. She measures Alice's photon in the basis $\{\mathbf{e}_a, \mathbf{e}_a^{\perp}\}$ and Bob's photon

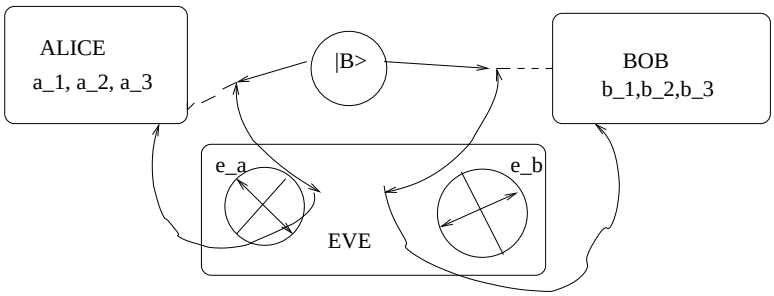

Figure 4.7: Eve collapses the pair in a tensor product state

in the basis $\{\mathbf{e}_b, \mathbf{e}_b^\perp\}$. Her strategy for the sucessive choices of basis at each time instant is described by a probability distribution

$$\rho(\mathbf{e}_a, \mathbf{e}_b) \geq 0, \qquad \int\int d^2\mathbf{e}_a d^2\mathbf{e}_b \, \rho(\mathbf{e}_a, \mathbf{e}_b) = 1$$

After Eve's measurement the pair of photons is left in one of the four tensor product states

$$|\mathbf{e}_a, \mathbf{e}_b\rangle, \ |\mathbf{e}_a, \mathbf{e}_b^\perp\rangle, \ |\mathbf{e}_a^\perp, \mathbf{e}_b\rangle, \ |\mathbf{e}_a^\perp, \mathbf{e}_b^\perp\rangle$$

with corresponding probabilities

$$|\langle \mathbf{e}_a, \mathbf{e}_b | B_{00}\rangle|^2 = \frac{1}{2}\cos^2(\widehat{\mathbf{e}_a, \mathbf{e}_b}), \qquad |\langle \mathbf{e}_a, \mathbf{e}_b^\perp | B_{00}\rangle|^2 = \frac{1}{2}\sin^2(\widehat{\mathbf{e}_a, \mathbf{e}_b})$$

$$|\langle \mathbf{e}_a^\perp, \mathbf{e}_b | B_{00}\rangle|^2 = \frac{1}{2}\sin^2(\widehat{\mathbf{e}_a, \mathbf{e}_b}), \qquad |\langle \mathbf{e}_a^\perp, \mathbf{e}_b^\perp | B_{00}\rangle|^2 = \frac{1}{2}\cos^2(\widehat{\mathbf{e}_a, \mathbf{e}_b})$$

Let us compute the correlation coefficient that Alice and Bob would find during the security test. Given Eve's choice $(\mathbf{e}_a, \mathbf{e}_b)$ we have

$$\begin{aligned} X(\mathbf{e}_a, \mathbf{e}_b) = \frac{1}{2}\cos^2(\widehat{\mathbf{e}_a, \mathbf{e}_b}) S(\mathbf{e}_a, \mathbf{e}_b) \ &+ \ \frac{1}{2}\sin^2(\widehat{\mathbf{e}_a, \mathbf{e}_b^\perp}) S(\mathbf{e}_a, \mathbf{e}_b^\perp) \\ &+ \ \frac{1}{2}\sin^2(\widehat{\mathbf{e}_a^\perp, \mathbf{e}_b}) S(\mathbf{e}_a^\perp, \mathbf{e}_b) + \frac{1}{2}\cos^2(\widehat{\mathbf{e}_a^\perp, \mathbf{e}_b^\perp}) S(\mathbf{e}_a^\perp, \mathbf{e}_b^\perp) \end{aligned}$$

where $S(\mathbf{v}, \mathbf{w})$ is the correlation coefficient corresponding to Eve's measurement outcome $|\mathbf{v}\rangle$, $|\mathbf{w}\rangle$,

$$S(\mathbf{v}, \mathbf{w}) = \langle \mathbf{v}, \mathbf{w} | A(\mathbf{a}_3) \otimes B(\mathbf{b}_3) + A(\mathbf{a}_3) \otimes B(\mathbf{b}_1) - A(\mathbf{a}_1) \otimes B(\mathbf{b}_3) + A(\mathbf{a}_1) \otimes B(\mathbf{b}_1) | \mathbf{v}, \mathbf{w}\rangle$$

The average correlation coefficient found by Alice and Bob when Eve operates is

$$X = \int\int d^2\mathbf{e}_a d^2\mathbf{e}_b \, \rho(\mathbf{e}_a, \mathbf{e}_b) X(\mathbf{e}_a, \mathbf{e}_b)$$

We leave it as an exercise to check that $|S(\mathbf{v}, \mathbf{w})| \leq 2$ which then leads to

$$|X| \leq 2$$

Thus Alice and Bob notice the presence of Eve. Note that Eve could manipulate (unitarily) the pair after her measurements in order to send other photon states to Alice and Bob. However if she re-entangles the photons she behaves as a new source for Alice and Bob, and she gets no information from their measurements.

Finaly let us note that if Eve copies the EPR pair (this can be done with a machine that copies the four orthogonal Bell states) and waits for the public discussion before doing the measurements, she gets no information about the secret key. Indeed her measurement operate on a different pair and thus there is only half of the time will she get the same result than Alice and Bob. This is equivalent to flip a coin at each time instant and cannot yield information.

Experiments. see in Review of Modern Physics **74** p 145-190 (2002) the extensive article "Quantum cryptography" by N. Gisin, G. Ribordy, W. Tittel, H. Zbinden.

4.4 Quantum teleportation

Suppose that Alice and Bob are spatialy separated and that Alice possesses a Qbit state,

$$|\Phi\rangle = \alpha|0\rangle + \beta|1\rangle, \qquad |\alpha|^2 + |\beta|^2 = 1$$

The state (i.e α and β) is not necessarily known to Alice and is not known to Bob. They also share an EPR pair

$$|B_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle$$

and have at their disposal a classical communication channel.

We are going to explain that by sending only two classical bits of information over the clasical channel, Alice can *teleport* the state to Bob. Here *teleportation* means that $|\Phi\rangle$ is destroyed in Alice's lab and is reconstructed in Bob's lab. Note that destruction of $|\Phi\rangle$ in Alice's lab is to be expeceted because of the no-cloning theorem. After the teleportation process, Bob knows that he possesses the state $|\Phi\rangle$ but still does not know the state itself (i.e he does not know α and β). The teleportation process itself does not involve physical transport of matter - except for the two classical bits that Alice

communicates to Bob. Of course this later communication phase cannot happen at speeds greater than that of light, so that the whole teleportation process does not violate the principles of relativity. We also note that the material support of the state $|\Phi\rangle = \alpha|0\rangle + \beta|1\rangle$ is not necessarily the same in Alice's and Bob's lab. Thus in principle a photon polarization state can be teleported to a distant electron spin state !

Teleportation can be summarized by the following "law"

$$\text{teleporting 1 Qbit} \;=\; \text{sending 2 Cbits} \;+\; \text{sharing 1 EPR pair}$$

and can be thought of, as some form of communication between Alice and Bob which share a classical channel and an "EPR like channel". The quantum state $|\Phi\rangle$ in Alice's lab is erased on her side and reproduced in Bob's lab - the information contained in α and β has not been communicated.

The protocol.

- A source produces an EPR pair of particles in the Bell state $|B_{00}\rangle_{23}$. One particle, called particle 2 is sent to Alice and one particle , called particle 3 is sent to Bob. The Hilbert space of the entangled system 23 is $\mathcal{H}_2 \otimes \mathcal{H}_3 = C^2 \otimes C^2$.

- Alice prepare a particle, called 1, in the state $|\Phi\rangle_1 = \alpha|0\rangle + |\beta\rangle$. The Hilbert space of particle 1 is $\mathcal{H}_1 = C^2$.

- The total Hilbert space of the composite system 123 is $\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \mathcal{H}_3 = C^2 \otimes C^2 \otimes C^2$ and the total state is

  $$|\Psi\rangle = |\Phi\rangle_1 \otimes |B_{00}\rangle_{23}$$

  At this point a short calculation will facilitate the subsequent discussion

  $$|\Psi\rangle = \frac{\alpha}{\sqrt{2}}|000\rangle + \frac{\beta}{\sqrt{2}}|100\rangle + \frac{\alpha}{\sqrt{2}}|011\rangle + \frac{\beta}{\sqrt{2}}|111\rangle$$

- Alice makes a local measurement in her lab, i.e on partiles 12. She uses an apparatus that has measurement basis of $\mathcal{H}_1 \otimes \mathcal{H}_2$

  $$\{|B_{00}\rangle_{12}, |B_{01}\rangle_{12}, |B_{10}\rangle_{12}, |B_{11}\rangle_{12}\}$$

  The associated projectors for the total system are

  $$P_{00} = |B_{00}\rangle\langle B_{00}| \otimes I_3, P_{01} = |B_{01}\rangle\langle B_{01}| \otimes I_3, P_{10} = |B_{10}\rangle\langle B_{10}| \otimes I_3, P_{11} = |B_{11}\rangle\langle B_{11}| \otimes I_3$$

As usual the outcome of the measurement is one of the four possible collapsed states*[11] (check this calculation and also that the probability of each outcome is $\frac{1}{4}$)

$$P_{00}|\Psi\rangle = \frac{1}{2}|B_{00}\rangle_{12} \otimes (\alpha|0\rangle_3 + \beta|1\rangle_3)$$

$$P_{01}|\Psi\rangle = \frac{1}{2}|B_{01}\rangle_{12} \otimes (\beta|0\rangle_3 + \alpha|1\rangle_3)$$

$$P_{10}|\Psi\rangle = \frac{1}{2}|B_{10}\rangle_{12} \otimes (\alpha|0\rangle_3 - \beta|1\rangle_3)$$

$$P_{11}|\Psi\rangle = \frac{1}{2}|B_{11}\rangle_{12} \otimes (-\beta|0\rangle_3 - \alpha|1\rangle_3)$$

- Depending on the random outcome Bob has one of the four states

$$\begin{aligned} \alpha|0\rangle_3 + \beta|1\rangle_3 &= |\Phi\rangle \\ \beta|0\rangle_3 + \alpha|1\rangle_3 &= X|\Phi\rangle \\ \alpha|0\rangle_3 - \beta|1\rangle_3 &= Z|\Phi\rangle \\ \beta|0\rangle_3 - \alpha|1\rangle_3 &= iY|\Phi\rangle \end{aligned}$$

  but he does not know the state he has.

- Alice knows that the outcome of the measurement (in her lab) is one of the four Bell states. She can thus use the Bell basis to re-measure (this will not perturb Bob's particle this time) and determine her outcome. This outcome can be encoded by two classical bits

$$00, 01, 10, 11$$

  that she sends to Bob over the classical communication channel. As soon as Bob receives Alice's message he knows that she has finished her operations and he has the two bits of information needed to decide which *unitary* operation he has to perform on his state in order to recover $|\Phi\rangle$,

$$\begin{aligned} I(\alpha|0\rangle_3 + \beta|1\rangle_3) &= |\Phi\rangle \\ X(\beta|0\rangle_3 + \alpha|1\rangle_3) &= |\Phi\rangle \\ Z(\alpha|0\rangle_3 - \beta|1\rangle_3) &= |\Phi\rangle \\ -iY(\beta|0\rangle_3 - \alpha|1\rangle_3) &= |\Phi\rangle \end{aligned}$$

[11] up to normalization

4.5 Dense coding

Suppose Alice and Bob have established a quantum channel over which they can send Qbits (for example a optic fiber over which photons travel). We will study the capacity of such a noisy channel later in the course but for the moment let us address a simpler question. Assume that Alice and Bob share an EPR pair. How much information does one Qbit convey over the quantum channel ?

The answer is that 2 classical bits of information can be transmitted by Alice to Bob, by sending only 1 Qbit as long as they share an EPR pair. The protocol that achieves this is called *dense coding*.

We will come back to the problem of communicating classical/quantum messages over noisy quantum channels assisted/or not by entanglement in later chapters. As we will see even for simple analogs of Shannon's channel coding theorem there are various open questions.

Dense coding can be summarized as follows:

$$\text{communicating 2 Cbits} = \text{sending 1 Qbit} + \text{sharing 1 EPR pair}$$

This "law" may seem complementary to the one of teleportation. Note however that here only two particles are involved and it is the Qbit that is physicaly transported form Alice to Bob.

Protocol.

- An EPR pair in the state $|B_{00}\rangle$ is prepared by a source and each particle sent to Alice and Bob.
- Alice wants to communicate two bits of information to Bob:
  - To send 00 she leaves her particle intact (or applies the unitary gate I) and physicaly sends her particle to Bob. Bob receives the particle and is now in possession of the whole state
  $$|B_{00}\rangle$$
  - To send 01 she applies the unitary gate X to her particle and then physicaly sends her particle to Bob. Bob is now in possession of the pair in the state
  $$X_1 \otimes I_2 |B_{00}\rangle = |B_{01}\rangle$$

  - To send 10 she applies the unitary gate Z to her particle and then physicaly sends her particle. Bob is now in possession of the pair in the state
$$Z_1 \otimes I_2 |B_{00}\rangle = |B_{10}\rangle$$
  - To send 11 she applies the unitary gate iY to her particle and then physicaly sends her particle. Bob is now in possession of the pair in the state
$$(iY)_1 \otimes I_2 |B_{00}\rangle = |B_{11}\rangle$$

- Bob now has the EPR pair 12 in some state $|B_{xy}\rangle$. In order to determine the two Cbits that Alice sent he must decide which Bell state he has. Since he knows that he has one of the four Bell states in his lab, he can do a local measurement in the Bell basis, and access the information xy.

Measurement in the Bell basis. One might think that measuring in the Bell basis is a theoretician's wishful thinking. In fact this has been realized experimentaly, and although explaining how is beyond the scope of this course, we give here an argument that shows that, in principle, it suffices to have H and $CNOT$ gates (the simplest unitary gates) together with polarization analyzers (the simplest measurement apparatus).

We have seen at the beginning of this chapter that Bell states can be generated as $|B_{xy}\rangle = (CNOT)(H \otimes I)|xy\rangle$. The projectors on the Bell basis states are therefore related to the ones over the Z basis,

$$|B_{xy}\rangle\langle B_{xy}| = (CNOT)(H \otimes I)|xy\rangle\langle xy|(H \otimes I)(CNOT)$$

(here we have used that the Hadamard and control not matrices are hermitian). The projectors $|xy\rangle\langle xy|$ correspond to the analyzer-photodetector apparatus for photons or to spin analyzers (Stern-Gerlach analyzer) for spins (Z basis). The circuit representation of a measurement device in the Bell basis in given on figure 8. The input is any state $|\Psi\rangle$, and the output is one of the four states
$$|B_{xy}\rangle \frac{\langle B_{xy}|\Psi\rangle}{|\langle B_{xy}|\Psi\rangle|}$$

Experiments. Quantum teleportation and dense coding have been realized experimentaly. A summary of the subject can be found in "Les dossiers de la recherche" no 18, février 2005, "L'étrange pouvoir de l'intrication quantique", by N. Gisin.

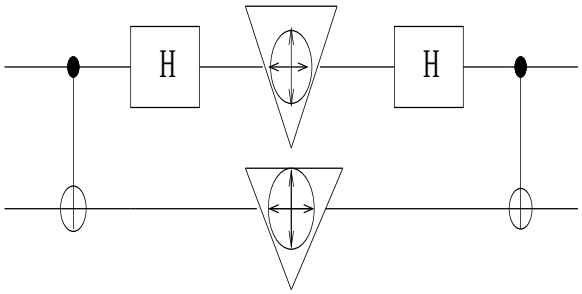

Figure 4.8: Device for Bell basis measurements