• EXPLORING THE FUNDAMENTS OF QUANTUM MECHANICS USING QUANTUM OPTICS : EPR-PARADOX AND BELL'S INEQUALITIES

- In the previous lectures we have had a look to some of the most important topics of quantum optics including the quantization of the EM field, squeezing, coherence (1st and 2nd order), the interaction of light and atoms, spontaneous emission, resonance fluorescence and parametric amplifiers. We have introduced some basic methodological tools as coherent states, P-Q-W Representations, stochastic methods (master equation, quantum regression theorem and Fokker-Planck equation) and correlation functions.

- In the next set of lectures we will depart from the topic of open systems (i.e. the stochastic processes we saw in the last lectures) and have a look to other major research area in quantum optics, which is directly linked to some of the most important problems lying at the very basics of quantum mechanics. We will in particular have a look to the famous EPR paradox and the Bell inequalities, and how these inequalities have been studied using quantum optics tools. Later on we will have a look in a forthcoming lecture on the ideas of quantum ~~[illegible]~~ teleportation, quantum cryptography and q-computing.

These ~~two~~ topics ~~[illegible]~~ are ~~[illegible]~~ basic "ingredients" of the very fruitful field of quantum information theory. This is a major research topics in nowadays physics, with major exciting developments in recent years as quantum cryptography or quantum computing. Unfortunately these topics lie well beyond the scope of these lectures. I would just ~~[illegible]~~ now that these topics constitute currently one of the major research areas in quantum optics (also in other fields).

• THE EINSTEIN-PODOLSKY-ROSEN ARGUMENT

- The EPR paradox uses a phenomenon predicted by quantum mechanics, known as quantum entanglement, to show that measurements performed on spatially separated parts of a quantum system have an instantaneous effect on one another. This effect is known as nonlocal behaviour (or quantum weirdness or "spooky" action at distance).

- The basic step in the EPR argument is to introduce correlated pure states of 2 particles (it may be photons, electrons, or whatever) of the form:

$$|\psi\rangle = \sum_n |a_n\rangle_1 \otimes |b_n\rangle_2$$

where $\{|a_n\rangle_1\} \longrightarrow$ orthonormal eigenstates of the operator $\hat{A}_1$ of particle 1

$\{|b_n\rangle_2\} \longrightarrow$ orthonormal eigenstates of the operator $\hat{B}_2$ of particle 2

These states may be created by especially designed sources (we will see an example later for the case of photons). For photons we may work with polarization states, for electrons we could work with spin states.

- The states as the state $|\psi\rangle$ above are called <u>entangled</u> states of the two particles. Note that we cannot associate

either particle in the state $|\psi\rangle$ with a definite state.

- Example: for the case of electrons, we may consider a source that creates two entangled electrons, such that if the spin of electron ① is pointing upward along z ($\uparrow$), the electron ② points downwards ($\downarrow$) and viceversa: $|\psi\rangle = (|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle)/\sqrt{2}$ → spin singlet

The spin of the 2 electrons is entangled.

- Note that the correlations between particles persist even if in the course of the experiment the particles became spatially separated after their creation at the source.

- Now suppose one were to measure $\hat{A}_1$ on particle ① long after the pair creation, and the 2 particles are far apart. If the result is some eigenvalue a_n, particle ① must thereafter be considered to be in the state $|a_n\rangle_1$, while particle 2 must be considered to be in the state $|b_n\rangle_2$.

As the state of particle 2 is now an eigenstate of $\hat{B}_2$, we can then predict with 100% certainty that the physical quantity represented by $\hat{B}_2$ if measured will give the result b_n. Thus we can predict the value of this physical quantity for particle 2 without in any way interacting with it.

- In the example above if the electron ① is measured to be in $|\uparrow\rangle$ then a subsequent measurement of ② will give for sure $|\downarrow\rangle$. And viceversa, if ① is measured to be in $|\downarrow\rangle$ the ② is for sure in $|\uparrow\rangle$.

. Suppose that instead of measuring $\hat{A}_1$ on particle ① we measure some other observable $\hat{C}_1$ with eigenstates $|c_n\rangle_1$.

We can then re-write

$$|\psi\rangle = \sum_n |c_n\rangle_1 \otimes |d_n\rangle_2$$

where $|d_n\rangle_2$ is an eigenstate of some operator $\hat{D}_2$ on ②.

- In the example above we could choose to measure in both electrons the spin along the X axis. According to quantum mechanics the spin singlet state may equally well be expressed as a function of the x-spin states: $|\psi\rangle = (|\uparrow\rangle_x|\downarrow\rangle_x - |\downarrow\rangle_x|\uparrow\rangle_x)/\sqrt{2}$.

So, again, if we measure $|\uparrow\rangle_x$ for 1 we will get in a subsequent measurement on ② 100% surely $|\downarrow\rangle_x$.

- Thus depending on what we choose to measure on particle ① the state of particle ② after the measurement can be an eigenstate of 2 quite different operators.

. However, the EPR argument raises now a crucial point. What if (as in the example with the spins) the two operators on particle ② $\hat{B}_2$ and $\hat{D}_2$ do not commute? Two operators which don't commute fulfill a Heisenberg uncertainty principle operating between them: a quantum state cannot possess a definite value for both variables.

If we measure the spin-z of electron ①, and for electron ② we measure the x-spin, according to quantum mechanics

if ① is in $|\uparrow\rangle$, then ② is in a 50-50 superposition of $|\uparrow\rangle_x$ and $|\downarrow\rangle_x$. The outcome of the measurement on the electron ② is fundamentally impossible to predict until the measurement is produced.

* So how does ② know, at the same time, which way to point if we decide to measure z-spin in ① and also how to point if we decide to measure x-spin in ①?

Using the usual Copenhagen interpretation rules that the wavefunction collapses at the time of measurement, there must be either action at distance or the electron must know more than it is supposed to.

* The original formulation of the EPR argument is then the following. If (as shown above) without in anyway disturbing a system we can predict with certainty the value of a physical quantity, then there exists an element of physical reality corresponding to that quantity.

Next, EPR defined a complete physical theory as one in which every element of physical reality is accounted for.

The aim of their argument was actually to show that the previous experiment shows that quantum mechanics is incomplete.

* let's see how these concepts apply to the above gedanken experiment. If we measure in ① the z-spin then the z-spin of ② is 100% known without disturbing it. So it's an element of reality. The same if we measure in ① the x-spin, then the x-spin of ② is 100% known without disturbing. So the x-spin is also an element of reality.

- But a quantum state cannot posses a definite value for both x-spin and z-spin. Then there are 2 ways out

[• Quantum mechanics is incomplete
[• Quantum mechanics is complete, but the x-spin and the z-spin cannot be elements of reality at the same time. This means that ~~the~~ the measurement on ① has an instantaneous effect on the elements of reality of ②. However this violates another principle, namely locality.

* So either there's a more complete theory than quantum mechanics (we will discuss this in a moment) or we have to give up locality.

- let's try to understand first <u>the concept of locality</u>. At first sight it seems that locality, i.e. physical processes at one place can't have immediate effects on another location, seems to be a consequence of special relativity.

• Special relativity states that information can't be transmitted faster than the speed of light without violating causality.

• However, in the EPR Gedanken experiment causality is preserved since an observer (let's call her Alice) measuring ① has no way to transmit messages (i.e. information) to an observer (let's call him Bob) at particle ②, just by manipulating her measurement axis.

- Whichever axis she uses, she has 50-50 chances of getting ↑ or ↓, completely at random.
- Bob, in one measurement he is allowed to make, has 50-50 to get ↑ or ↓ regardless of whether or not his axis is aligned to Alice's.

Hence the EPR Gedanken experiment doesn't involve faster-than-light signaling, and hence causality is not violated.

• However, since locality is such a powerful physical intuition, EPR didn't want to abandon it, and hence suggested the other possibility, i.e. that quantum mechanics is not a complete theory.

• This brings us to the idea of hidden variables.

• Hidden variables

• EPR suggested that there is some yet undiscovered theory of nature to which quantum mechanics acts as a kind of statistical approximation. Unlike quantum mechanics, the more complete theory contains variables corresponding to all elements of physical reality. There must be some unknown mechanism acting on these variables to give rise to Heisenberg's uncertainty principle. Such a theory is called a hidden-variable theory

• Let's understand this with the electron spin example. One supposes that the quantum spin-singlet states emitted by the source are approximative descriptions for "true" physical states possessing definite z-spin and x-spin. The electron going to Alice has always opposite spin momentums as that of Bob. e.g. Alice $(-z, +x)$, Bob $(+z, -x)$ and so on.

Therefore if Bob measurement is aligned to Alice's, he will get necessarily the opposite of what Alice gets.

Assuming we restrict to the z and x-axes such hidden variable theory is experimentally indistinguishable from quantum mechanics.

- Of course in reality we have an infinite number of possible axes, so there's to be an infinite number of hidden variables. However this is not a killer argument.

- A much more serious (and one could say almost conclusive) argument against hidden variables came from the theory of John Bell, and the so-called Bell inequalities. We will have a look to this very fundamental issue now, and we will show later how a quantum-optics experiment proved indeed that EPR were actually wrong in their claim.

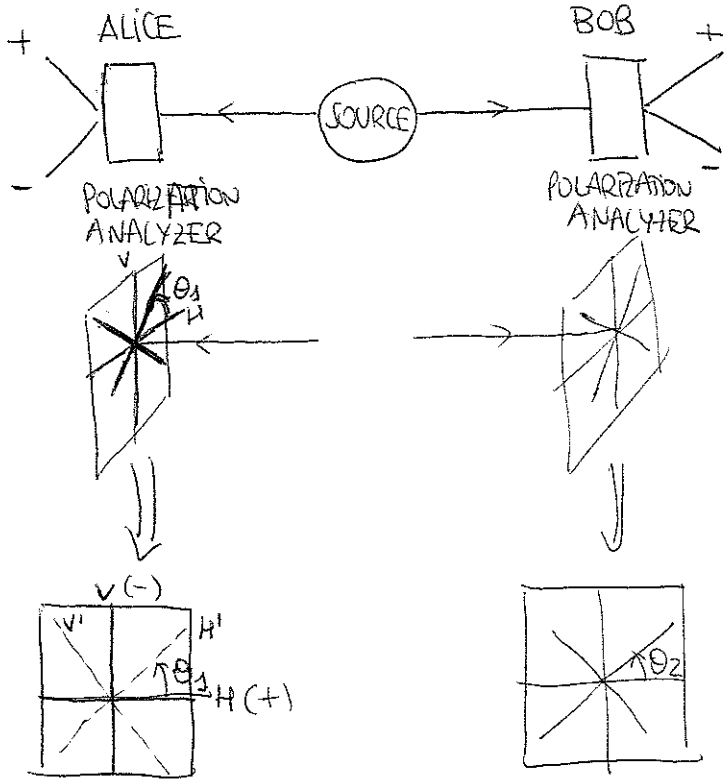
• BELL INEQUALITIES

- As we will see in a moment, the predictions of quantum mechanics in the EPR gedanken experiment are not exactly the same as those from hidden variable theories. These differences may be expressed in the form of inequalities, which are called Bell-inequalities, and that have been experimentally tested.

- For simplicity of the argument we will discuss a particular experimental situation, being interested in the different predictions from quantum mechanics and hidden-variables.

- We will be interested in entangled photon pairs. The interesting degree of freedom here is the photon polarization (which plays the same role as the spin in our previous electronic example).
- The two photons are emitted in opposite directions with entangled polarization states.

Each photon passes through separate polarization analyzers (they play the role of the detectors of spin in the previous example), emerging in either the horizontal (+) channel, or the vertical (-) channel of each analyzer.



- Initially we assume the horizontal polarization as orthogonal to the plane of the experiment
- However, we are free to rotate the polarizers in the plane orthogonal to the propagation direction of the photons. They may be rotated at different angles θ_1 (Alice) or θ_2 (Bob).

- Let $\hat{a}_\pm \equiv$ annihilation operator for $\pm$ polarized mode for the field traveling to Alice

$\hat{b}_\pm \equiv$ annihilation operator for $\pm$ polarized mode for the field traveling to Bob.

• The (entangled) state of the two photons may be written as

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(\hat{a}_+^\dagger \hat{b}_+^\dagger + \hat{a}_-^\dagger \hat{b}_-^\dagger\right)|0\rangle$$

where $|0\rangle$ is the vacuum state.

Using the notation $|n_1 n_2 n_3 n_4\rangle \equiv \left\{\begin{array}{l} n_1 \text{ photons in } a_+ \\ n_2 \text{ photons in } a_- \\ n_3 \text{ " in } b_+ \\ n_4 \text{ " in } b_- \end{array}\right\}$

Then

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left[|1010\rangle + |0101\rangle\right]$$

If the photon is detected by Alice in +, then Bob detects it in +.
This is of course just another version of the EPR experiment.

• As mentioned above, we are free to measure the polarization in any direction by rotating the polarizers. The detected modes are then obtained by rotating the modes $\hat{a}_\pm$ and $\hat{b}_\pm$:

$$\text{Alice} \rightarrow \begin{array}{l} \hat{c}_+ = \hat{a}_+ \cos\theta_1 + \hat{a}_- \sin\theta_1 \\ \hat{c}_- = -\hat{a}_+ \sin\theta_1 + \hat{a}_- \cos\theta_1 \end{array}$$

$$\text{Bob} \rightarrow \begin{array}{l} \hat{d}_+ = \hat{b}_+ \cos\theta_2 + \hat{b}_- \sin\theta_2 \\ \hat{d}_- = -\hat{b}_+ \sin\theta_2 + \hat{b}_- \cos\theta_2 \end{array}$$

• As discussed previously in our lectures (p. 40) the detectors placed after the polarizers (polarizer + detector ≡ polarization analyzer) measure the intensities $\langle I_{1,2}^\pm \rangle$, while the "click"-correlators measure $\langle I_1^+ I_2^+ \rangle$, etc. (remember p. 49)

• Of course all these correlations and averages depend on θ_1 and θ_2.

• let's now suppose that there's a more complete theory in which these correlations also depend on the variable λ which remains hidden from direct determination and for which only a statistical description is possible. The hidden variable λ is distributed according to some distribution $\rho(\lambda)$.

Hence:

$$\langle I_1^{\pm} I_2^{\pm} \rangle_{\theta_1,\theta_2} = \int d\lambda\, \rho(\lambda)\, I_1^{\pm}(\lambda,\theta_1,\theta_2)\, I_2^{\pm}(\lambda,\theta_1,\theta_2)$$

where I_1^{+} denotes the expected intensity at detector Alice given a value for λ

• It's reasonable to assume (as in EPR) that for a given value of λ the results at Alice cannot depend on the angle θ_2 chosen by Bob (and viceversa). This is the locality assumption that we discussed before; hence:

$$I_1^{\pm}(\lambda,\theta_1,\theta_2) = I_1^{\pm}(\lambda,\theta_1)$$

$$I_2^{\pm}(\lambda,\theta_1,\theta_2) = I_2^{\pm}(\lambda,\theta_2)$$

• let's consider now the following correlation functions:

$$E(\theta_1,\theta_2) \equiv \frac{\langle (I_1^{+} - I_1^{-})(I_2^{+} - I_2^{-}) \rangle}{\langle (I_1^{+} + I_1^{-})(I_2^{+} + I_2^{-}) \rangle}$$

or in other words:

$$E(\theta_1,\theta_2) \equiv \frac{\langle : (\hat{c}_+^{\dagger}\hat{c}_+ - \hat{c}_-^{\dagger}\hat{c}_-)(\hat{d}_+^{\dagger}\hat{d}_+ - \hat{d}_-^{\dagger}\hat{d}_-) : \rangle}{\langle : (\hat{c}_+^{\dagger}\hat{c}_+ + \hat{c}_-^{\dagger}\hat{c}_-)(\hat{d}_+^{\dagger}\hat{d}_+ + \hat{d}_-^{\dagger}\hat{d}_-) : \rangle}$$

normal order

* Assuming a local hidden variable theory:

$$E(\theta_1,\theta_2) = \frac{\int \rho(\lambda)d\lambda\,[I_1^+(\lambda,\theta_1) - I_1^-(\lambda,\theta_1)][I_2^+(\lambda,\theta_2) - I_2^-(\lambda,\theta_2)]}{\int \rho(\lambda)\,d\lambda\,[I_1^+(\lambda,\theta_1) + I_1^-(\lambda,\theta_1)][I_2^+(\lambda,\theta_2) + I_2^-(\lambda,\theta_2)]}$$

note that $I_1^+(\lambda,\theta_1) + I_1^-(\lambda,\theta_1) = I_1(\lambda) \equiv$ intensity measured when we remove the polarizer, and hence independent of θ_1

$$= \frac{\int d\lambda\, \rho(\lambda) I_1(\lambda) I_2(\lambda) \left[\frac{I_1^+(\lambda,\theta_1) - I_1^-(\lambda,\theta_1)}{I_1(\lambda)}\right]\left[\frac{I_2^+(\lambda,\theta_2) - I_2^-(\lambda,\theta_2)}{I_2(\lambda)}\right]}{\int d\lambda \rho(\lambda) I_1(\lambda) I_2(\lambda)}$$

let $f(\lambda) \equiv \rho(\lambda) I_1(\lambda) I_2(\lambda)$; $N = \int f(\lambda)\,d\lambda$

$$= \frac{1}{N}\int d\lambda f(\lambda)\, S_1(\lambda,\theta_1)\, S_2(\lambda,\theta_2)$$

where $S_j(\lambda,\theta_j) \equiv \dfrac{I_j^+(\lambda,\theta_j) - I_j^-(\lambda,\theta_j)}{I_j(\lambda)}$ $\quad j = 1,2$

clearly $|S_j(\lambda,\theta_j)| \leq 1$

• Let's have a look now to how $E(\theta_1,\theta_2)$ changes when we change the orientation of the polarizers ~~the old orientation~~

~~$E(\theta_1,\theta_2) - E(\theta_1,\theta_2') = \frac{1}{N}\int d\lambda f(\lambda)\,[S_1(\lambda,\theta_1)S_2(\lambda,\theta_2) - S_1(\lambda,\theta_1')S_2(\lambda,\theta_2')]$~~

~~$= \frac{1}{N}\int d\lambda f(\lambda)\{S_1(\lambda,\theta_1)S_2(\lambda,\theta_2)[1 \pm S_1(\lambda,\theta_1')S_2(\lambda,\theta_2')]$~~

~~$- S_1(\lambda,\theta_1)S_2(\lambda,\theta_2')[1 \pm S_1(\lambda,\theta_1')S_2(\lambda,\theta_2)]\}$~~

• let's consider

$$E(\theta_1,\theta_2) - E(\theta_1,\theta_2') + E(\theta_1',\theta_2') + E(\theta_1',\theta_2)$$

$$= \int \frac{d\lambda}{N} f(\lambda) \begin{bmatrix} S_1(\lambda,\theta_1) S_2(\lambda,\theta_2) - S_1(\lambda_1,\theta_1) S_2(\lambda,\theta_2') \\ + S_1(\lambda,\theta_1') S_2(\lambda,\theta_2') + S_1(\lambda,\theta_1') S_2(\lambda,\theta_2) \end{bmatrix}$$

$$= \int \frac{d\lambda}{N} f(\lambda) \begin{bmatrix} S_1(\lambda,\theta_1)\left(S_2(\lambda,\theta_2) - S_2(\lambda,\theta_2')\right) \\ + S_1(\lambda,\theta_1')\left(S_2(\lambda,\theta_2) + S_2(\lambda,\theta_2')\right) \end{bmatrix}$$

Note that

$$S_1(\lambda,\theta_1)\left[S_2(\lambda,\theta_2) - S_2(\lambda,\theta_2')\right] + S_1(\lambda,\theta_1')\left[S_2(\lambda,\theta_2) + S_2(\lambda,\theta_2')\right]$$

$$\leq |S_1(\lambda,\theta_1)|\,|S_2(\lambda,\theta_2) - S_2(\lambda,\theta_2')| + |S_1(\lambda,\theta_1')|\,|S_2(\lambda,\theta_2) + S_2(\lambda,\theta_2')|$$

$$\leq |S_2(\lambda,\theta_2) - S_2(\lambda,\theta_2')| + |S_2(\lambda,\theta_2) + S_2(\lambda,\theta_2')| \leq 2$$

by assuming without lack of generality $S_2(\lambda,\theta_2) \geq S_2(\lambda,\theta_2') \geq 0$

• Note that the last bound (2) may be obtained then:

$$|S_2(\lambda,\theta_2) - S_2(\lambda,\theta_2')| + |S_2(\lambda,\theta_2) + S_2(\lambda,\theta_2')|$$

$$= S_2(\lambda,\theta_2) - S_2(\lambda,\theta_2') + S_2(\lambda,\theta_2) + S_2(\lambda,\theta_2')$$

$$= 2\,S_2(\lambda,\theta_2) \leq 2$$

Hence:

$$\boxed{E(\theta_1,\theta_2) - E(\theta_1,\theta_2') + E(\theta_1',\theta_2') + E(\theta_1',\theta_2) \leq 2}$$

This is an example of Bell inequality known as the Clauser-Horne-Shimony-Holt (CHSH) inequality

For simplicity of the notation we call the l.h.s. B: $\boxed{B \leq 2}$

. We will see that the state $|\psi\rangle$ violates this inequality

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left[\hat{a}_+^\dagger \hat{b}_+^\dagger + \hat{a}_-^\dagger \hat{b}_-^\dagger\right]|0\rangle$$

Note that: $\hat{a}_+ = \hat{c}_+ \cos\theta_1 - \hat{c}_- \sin\theta_1$

$\hat{a}_- = \hat{c}_+ \sin\theta_1 + \hat{c}_- \cos\theta_1$

Hence:

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left\{\begin{array}{l}[\hat{c}_+^\dagger \cos\theta_1 - \hat{c}_-^\dagger \sin\theta_1][\hat{d}_+^\dagger \cos\theta_2 - \hat{d}_-^\dagger \sin\theta_2] \\ + [\hat{c}_+^\dagger \sin\theta_1 + \hat{c}_-^\dagger \cos\theta_1][\hat{d}_+^\dagger \sin\theta_2 + \hat{d}_-^\dagger \cos\theta_2]\end{array}\right\}|0\rangle$$

$$= \frac{1}{\sqrt{2}}\left\{\begin{array}{l}\cos(\theta_1-\theta_2)\left[\hat{c}_+^\dagger \hat{d}_+^\dagger + \hat{c}_-^\dagger \hat{d}_-^\dagger\right] \\ + \sin(\theta_1-\theta_2)\left[\hat{c}_+^\dagger \hat{d}_-^\dagger + \hat{c}_-^\dagger \hat{d}_+^\dagger\right]\end{array}\right\}|0\rangle$$

$$= \frac{1}{\sqrt{2}}\left\{\cos(\theta_1-\theta_2)\left[|1010\rangle + |0101\rangle\right] + \sin(\theta_1-\theta_2)\left[|1001\rangle + |0110\rangle\right]\right\}$$

Hence:

$$E(\theta_1,\theta_2) = \frac{\langle\psi|:\left[\hat{c}_+^\dagger \hat{c}_+ - \hat{c}_-^\dagger \hat{c}_-\right]\left[\hat{d}_+^\dagger \hat{d}_+ - \hat{d}_-^\dagger \hat{d}_-\right]:|\psi\rangle}{\langle\psi|:\left[\hat{c}_+^\dagger \hat{c}_+ + \hat{c}_-^\dagger \hat{c}_-\right]\left[\hat{d}_+^\dagger \hat{d}_+ + \hat{d}_-^\dagger \hat{d}_-\right]:|\psi\rangle}$$

$$= \cos^2(\theta_1-\theta_2) - \sin^2(\theta_1-\theta_2) = \cos\left[2(\theta_1-\theta_2)\right]$$

. Let's choose $\theta_1, \theta_1', \theta_2, \theta_2'$ such that

$$\phi = \theta_2 - \theta_1 = \theta_2' - \theta_1' = \theta_1' - \theta_2$$

Then $\theta_1 - \theta_2' = -3\phi$

· Hence $B = 3\cos 2\phi - \cos 6\phi$

let's choose $\phi = 22.5°$. Then $B = 2\sqrt{2} > 2$

Hence, the state $|4\rangle$ violates the CHSH inequality!

· This violation was convincingly demonstrated in an already classical experiment performed in 1982 by Aspect et al. In that experiment a cascade 2-photon transition in calcium-40 was employed to generate the EPR pairs, and the polarization analyzers were essentially beam splitters with polarization-dependent transmittivity.

· That experiment gave results in good agreement with quantum theory, clearly violating the Bell inequality.

· In the light of these (and other similar) experiments, it seems that local hidden variable theories do not provide a correct answer, whereas quantum mechanics does!

• Quantum teleportation

* Quantum entanglement and EPR-like experiments have extremely interesting consequences. We have no time in this course to have a look to all of them, but just as an example, let's have a look to the idea of quantum teleportation (which perhaps some of you have heard of). We will briefly see other examples later.

* Suppose that Alice has a state (let's call it a qubit)

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

($|0\rangle$ and $|1\rangle$ can be polarizations $|\leftrightarrow\rangle$ and $|\updownarrow\rangle$ for a photon, or spin $|\uparrow\rangle$, $|\downarrow\rangle$ for an electron)

* Suppose that Alice wants to teleport $|\psi\rangle$ to Bob, but of course Alice can't know the state.

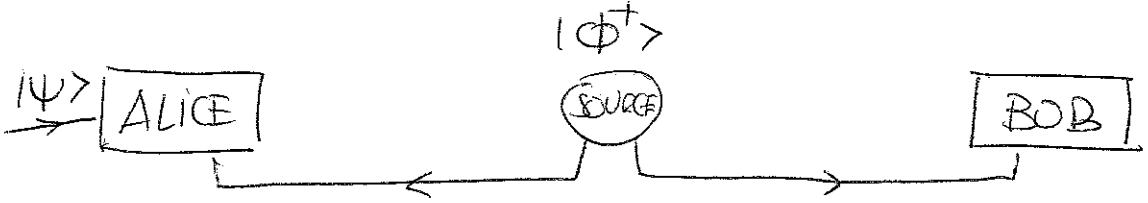
* In the following teleportation scheme we assume that Alice and Bob share a maximally entangled state, for instance one of the so-called Bell states:

$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}\left[|0\rangle_A \otimes |0\rangle_B \pm |1\rangle_A |1\rangle_B\right]$$

$$|\psi^{\pm}\rangle = \frac{1}{\sqrt{2}}\left[|0\rangle_A \otimes |1\rangle_B \pm |1\rangle_A |0\rangle_B\right]$$

All these states are of the EPR type discussed before.

- Alice takes one of the particles of the pair, and Bob the other. Let's assume that they share $|\Phi^+\rangle$.



So Alice has two particles, the one whose state wants to teleport, and one of the EPR pair, and Bob has one.

The total state of the system is given by

$$|\Psi\rangle \otimes |\Phi^+\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle)$$

in Alice

$$= \frac{1}{\sqrt{2}}\left[\alpha|100\rangle|0\rangle + \alpha|101\rangle|1\rangle + \beta|10\rangle|0\rangle + \beta|11\rangle|1\rangle\right]$$

in Bob

- Since:

$$|00\rangle = \frac{1}{\sqrt{2}}\left[|\Phi^+\rangle + |\Phi^-\rangle\right]$$

$$|11\rangle = \frac{1}{\sqrt{2}}\left[|\Phi^+\rangle - |\Phi^-\rangle\right]$$

$$|01\rangle = \frac{1}{\sqrt{2}}\left[|\Psi^+\rangle + |\Psi^-\rangle\right]$$

$$|10\rangle = \frac{1}{\sqrt{2}}\left[|\Psi^+\rangle - |\Psi^-\rangle\right]$$

Then:

$$|\Psi\rangle \otimes |\Phi^+\rangle = \frac{1}{2}\left\{\begin{array}{l} |\Phi^+\rangle \otimes [\alpha|0\rangle + \beta|1\rangle] + |\Phi^-\rangle \otimes [\alpha|0\rangle - \beta|1\rangle] \\ + |\Psi^+\rangle \otimes [\beta|0\rangle + \alpha|1\rangle] + |\Psi^-\rangle [-\beta|0\rangle + \alpha|1\rangle] \end{array}\right\}$$

- After the teleportation Alice gets an entangled state, but no copy of $|\psi\rangle$ is left there. I will come to this point in a moment
- There's no "real" teleportation of matter or energy. Only the state
- There's no superluminal communication (remember the telephone call from Alice to Bob!)
- The 2 classical bits sent by Alice contain no information about α and β.

- NO CLONING THEOREM
- The fact that there's no copy (see above) is consistent with the so called no-cloning theorem, which ~~is actually~~ forbids the creation of identical copies of an arbitrary unknown quantum state. It's actually rather easy to

proof:

Let $|\psi\rangle_A$ the state we want to copy, and $|e\rangle_B$ some initial state. Let's suppose that there's some unitary operator such that

$U \equiv$ acts as a copier

$$U|\psi\rangle_A|e\rangle_B = |\psi\rangle_A|\psi\rangle_B$$

For some other $|\phi\rangle_A$

$$U|\phi\rangle_A|e\rangle_B = |\phi\rangle_A|\phi\rangle_B$$

Hence $$\left[\langle e|_B\langle\phi|_A U^\dagger\right]\left[U|\psi\rangle_A|e\rangle_B\right] = \langle\phi|_B\langle\phi|_A|\psi\rangle_A|\psi\rangle_B$$

$$= \langle\phi|\psi\rangle^2$$

* Up to now we have done nothing else than re-writing the state. The actual teleportation starts when Alice measures her two qubits in the Bell basis (we won't enter into how this may be done). Depending on the result of her measurement the 3-particle state collapses into:

1) $|\Phi^+\rangle \otimes [\alpha|0\rangle + \beta|1\rangle]$
2) $|\Phi^-\rangle \otimes [\alpha|0\rangle - \beta|1\rangle]$
3) $|\Psi^+\rangle \otimes [\beta|0\rangle + \alpha|1\rangle]$
4) $|\Psi^-\rangle \otimes [-\beta|0\rangle + \alpha|1\rangle]$

The entanglement originally shared between Alice and Bob is now broken.

Alice, after her measurement, has a complete knowledge of the state of the 3 particles. She now sends the result of her measurement to Bob via a classical channel (e.g. a telephone). (She just need two classical bits, since she uses binary notation to denote from $0 \rightarrow 3$).

1) If Alice tells $|\Phi^+\rangle \rightarrow$ Bob does nothing
2) If Alice tells $|\Phi^-\rangle \rightarrow$ Bob applies $\hat{\sigma}_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
3) If Alice tells $|\Psi^+\rangle \rightarrow$ Bob applies $\hat{\sigma}_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
4) If Alice tells $|\Psi^-\rangle \rightarrow$ Bob applies $i\hat{\sigma}_y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$

At the end Bob gets $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, i.e. the state has been teleported to Bob, and none of them knows actually what is α and β!

* But $U^\dagger U = 1 \longrightarrow \langle e|_B \langle \psi|_A U^\dagger U |\phi\rangle_A |e\rangle_B = \langle \psi|\phi\rangle$

Hence $\langle \psi|\phi\rangle = \langle \psi|\phi\rangle^2$

which isn't true in general. Therefore U can't clone a general quantum state, proving the no cloning theorem.

* Quantum cryptography

- Other important field of application of the fundamentals of quantum mechanics is quantum cryptography, i.e. we want to share and transmit information using a code such that it is only known by the receptor, and such that any spy in the middle could be detected.

* Quantum cryptography enables the two parties (let's call them again Alice and Bob) to produce a shared random bit string which can be used as a key to encryption and decryption of messages

- The security of quantum cryptography relies on the foundations of quantum mechanics, in contrast to traditional public key cryptography which relies on the computation of some mathematical functions. Whereas traditional cryptography can't provide any indication of eavesdropping, quantum cryptography does, since the process of measuring a quantum system in general disturbs it.

- By using quantum superposition or quantum entanglement and transmitting the information in quantum states, one can implement a communication system that detect eavesdropping.

* There are different methods for quantum cryptography. In the following we will describe one that actually does not use quantum

entanglement, but rather quantum superposition. Historically it's basically the 1st method to be proposed. Since it was proposed by Bennett and Brassard in 1984, it's called the BB84 method.

- In the BB84 scheme, Alice wants to send a private key to Bob.
- She begins with two strings of bits [redacted]
a and b, each n-bits long.
- She then encodes these 2 strings as a string of n qubits (remember that a qubit is a state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Originally BB84 was thought for photon polarization states, but any 2 pairs of conjugate states would be employed either, e.g. spins for ~~electrons~~ are in our previous examples).

Let's denote the qubit-string as:

$$|\psi\rangle = \bigotimes_{i=1}^{n} |\psi_{a_i b_i}\rangle$$

where a_i, b_i → i^{th} bit of a and b respectively $\left.\begin{matrix} a_i = 0,1 \\ b_i = 0,1 \end{matrix}\right\}$

Together a_i, b_i give an index for the following 4 qubit states:

$|\psi_{00}\rangle = |0\rangle$ (horizontal pol.) [+ BASIS]

$|\psi_{10}\rangle = |1\rangle$ (vertical pol.)

$|\psi_{01}\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ (45°)

$|\psi_{11}\rangle = |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ (-45°) [X BASIS]

- Note that the bit b_i decides in which basis a_i is encoded (either the +-Basis or the ×-Basis)
- Note that the qubits are in states which aren't mutually ~~[illegible]~~ all of them orthogonal, and hence we can't distinguish them without knowing b_i.
- Then Alice sends $|\psi\rangle$ over a public quantum channel. In the case of photons this channel is generally an optical fiber or even free space.

Bob receives the string of qubits.

- Bob proceeds to generate a string of random bits b' of the same length of b. Then according to this bits b' he chooses the + or × basis to measure the qubit string he has received from Alice. ~~He~~ Then obtains an array a' of bits, which will in general differ from the original a.
- At this point Bob announces (via telephone, e.g.) that he has received the transmission. Then Alice publically (Teleph.) says what is b. Then Bob tells (Teleph.) to Alice which $b_i \neq b_i'$, and both Alice and Bob discard the qubits in a and a' where $b_i \neq b_i'$.

In the remaining (say k) bits both Alice and Bob measured in the same basis. Then Alice takes $k/2$ of them randomly, telling (Teleph.) to Bob which bits she has chosen, and then announces (Teleph.) the value of these bits. Bob also announces (Teleph.)

publically the values of his corresponding K_i bits. They make a check to see if they match. Ideally, in absence of any noise, if they mismatch then something fishy happened in the quantum communication, some eavesdropper was having a look. In reality some noise may be present, so some careful statistical analysis may be needed, but we won't enter into that.

- The rest of the bits can be employed for sharing a key for encoding/decoding, if the "security check" was positive.
- For a graphic representation see p. (156) and (157).
- There are other quantum cryptography schemes, based on entanglement, but we won't study them here.
- Quantum cryptography has been experimentally realized in many labs, and recently over distances of over hundred kilometers (via fiber or in free space)

Quantum cryptography is already at a commercial level, being employed by some banks and organizations.

BB84 graphically

ALICE →

a	0	0	1	1	0	1	0	1	1	0	0	0
b	1	0	1	0	0	1	1	1	0	1	1	0

} → $|\psi\rangle$

① ALICE send via a quantum channel $|\psi\rangle$ to BOB

ALICE —$|\psi\rangle$, QUANTUM→ BOB

?EVE?

② BOB generates b', and measures on $|\psi\rangle$ to get a'

b'	1	1	1	0	1	1	0	1	0	0	1	1
a'	0	0	1	1	0	1	1	1	1	0	0	1

③ He sends a message to Alice

ALICE ←"I GOT IT", CLASSICAL— BOB

④ Alice tells which basis she used (which is b)

ALICE —b, CLASS.→ BOB

⑤ Bob checks which $b'_i \neq b_i$

b'	1	1	1	0	1	1	0	1	0	0	1	1
b	1	0	1	0	0	1	1	1	0	1	1	0

ALICE ←WHICH ARE WRONG, CLASS— BOB

⑥ Both discard the mismatched ones

2, 5, 7, 10, 12

· After ⑥

ALICE ⟶ a ⟶ 0 1 1 1 1 1 0

BOB ⟶ a' ⟶ 0 1 1 1 1 0 0

⑦ * ALICE chooses say the bits 1, 3, 7 ⟶ 0, 1, 0

ALICE —for the check (1,3,7) / CLASS.→ BOB

I get 0, 1, 0 →

← I get 0, 1, 0

⑧ The channel is safe, let's use the rest 1111 as our secret key.

• QUANTUM COMPUTERS

* To finish our necessarily very brief review on quantum foundations let's briefly have a look to the idea of quantum computer, which probably some of you have heard of.

* A quantum computer is any device that makes direct use of quantum mechanical phenomena (as superposition and entanglement) to perform operations with data.

* Whereas classical computers work with bits, quantum computers work with qubits ($\alpha|0\rangle+\beta|1\rangle$), a concept we have already encountered in p. (147).

* It's easy to understand the fundamental conceptual difference between bit and qubit.

- Consider a 3-bit register. At any given time, the bits can just be in a given definite state, say 110.

- On the contrary, a qubit can be in a superposition of all the classically allowed states:

$$|4\rangle = a|000\rangle + b|001\rangle + c|010\rangle + d|011\rangle +$$
$$+ e|100\rangle + f|101\rangle + g|110\rangle + h|111\rangle$$

where $a,\dots,h$ are complex coefficients. This linear superposition and the possibility of quantum interference plays a crucial role in quantum computers.

- Quantum computers (and the associated quantum algorithms) may allow to solve some untractable problems with classical computers.

* For example, integer factorization is believed to be computationally unfeasible with an ordinary computer for large integers that are the product of only a few prime numbers. Actualy, most of the public key ciphers are based on this difficulty (as eg. RSA, which is employed to protect WEB pages, email, etc).

On the contrary, a quantum computer can solve this problem in an exponentially faster way by means of the so-called Shor's algorithm.

* Other problem which can be speeded-up with a quantum computer (although not exponentially) is quantum database search, e.g. when you have a look to a telephone book but you just to know the telephone number, and you look for a name! In a classical way it would tolle you a number of steps proportional to the number of entries in the telephone book. A quantum computer may do it with a number of steps proportional to the square root of the number of entries! This is done by the so-called Grover's algorithm.

. We have here no time to have a look to this algorithms, but it should be clear to you that if quantum computer become a reality at large scale, they may revolutionize completely our society.

. There are however some important practical issues to overcome, as e.g. quantum decoherence (provided by the interaction with a reservoir).

- There's a number of possible candidates for the implementation of quantum computers, including trapped ions, quantum dots, defects in diamonds, cold gases, superconductors, etc.

- At the moment only small scale quantum computers have been demonstrated, although this may change within the very next future, opening a new era in computing!

- With these comments I would like to finish this very brief overview on the foundations of quantum mechanics. Once more, although this is not directly related with say "standard" quantum optics, nowadays many quantum opticians work on this field, since many experimental and theoretical tools of "standard" quantum optics are certainly of use for these problems.

- This is a very exciting research field, and I invite you to have a further look to it!