Additional lecture notes FYS4110

Joakim Bergli

November 6, 2019

1 Experimental tests of Bell's inequalities

1.1 Generation of entangled pairs

How do we generate entangled pairs of photons? There are as far as I know two ways that have been used in practice: Atomic cascades and parametric downconversion in nonlinear crystals. The first was used in the initial experiments, while the latter is used in all modern experiments.

Atomic cascades The principle of this is quite simple: An atom, ususally calcium, that has a very short lived excited state is excited to a state with higher energy than this state. The atom will then after some time spontaneously decay to the short lived state, emitting one photon. It will stay in the short lived state only for a short time, and then emit a second photon. Because the angular momentum of the electron changes by ± 1 in an electric dipole transition, and if one chooses the initial and final states to have the same angular momentum, the polarizations of the tho photons must be correlated.

Parametric downconversion This is a process which takes place in nonlinear crystals. By this, we mean a material where the polarization is not a linear function of the applied electric field. In principle, this is the case for all crystals, but only some have strong nonlinearity so that the effect is not too small. Examples are beta barium borate (BBO) or potassium titanyl phosphate (KTP). In general, the polarization of a material in the presence of an applied electric field E is (for simplicity we write the equations for an isotropic material, even if the usual materials used inexperiments are birefringent)

$$P = \epsilon_0 \chi^{(1)} E + \epsilon_0 \chi^{(2)} E^2 + \cdots$$

where $\chi^{(1)}$ is the usual linear electric susceptibility, while $\chi^{(2)}$ describes the lowest order nonlinearity. This gives the displacement vector

$$D = \epsilon_0 E + P = \epsilon E + \epsilon_0 \chi^{(2)} E^2$$

where $\epsilon = (1 + \chi^{(1)})\epsilon_0$. The energy (Hamiltonian) is

$$H = \frac{1}{2} \int d^3 r D \cdot E = \frac{\epsilon}{2} \int d^3 r E^2 + \frac{\epsilon_0}{2} \int d^3 r \chi^{(2)} E^3$$

The second term gives the nonlinear interaction in the crystal. We know that the electric field is given by the expression

$$E(r,t) = i \sum_{ka} \sqrt{\frac{\omega}{2\epsilon_0 V}} \epsilon_{ka} \left[a_{ka} e^{i(kr - \omega t)} - a_{ka}^\dagger e^{-i(kr-\omega t)} \right].$$

This means that E^3 will contain a term proportional to $\hat{a}_{ka}\hat{a}^\dagger_{k'a'}\hat{a}^\dagger_{k''a''}$ which means that one photon is annihilated and two are created. That is, one photon is split in two. A more detailed analysis is needed to determine the relations between the energies and polarizations of the two photons, and they will depend on the specific crystal and direction of propagation of the photons. In general, the two photons are entangled, and by choosing the proper direction and polarization of the incoming and outgoing beams one can control the exact state.

1.2 CHSH inequality

In the lecture notes, section 2.3.2, there is a discussion of one form of Bell inequality. Here we present a different form, the CHSH inequality.[1]

We consider two spin-$\frac{1}{2}$ particles propagating in opposite directions and reaching detectors A and B. Both detectors can be oriented to measure spin along any axis we choose, but we need only two different for each detector. We call them a and a' for A and b and b' for B. In a local realistic theory we would have two functions $A(a,\lambda)$ and $B(b,\lambda)$ both with value either $+1$ or -1 depending on whether the spin is parallell or antiparallell to the given axis. Here λ represents any set of hidden variables which is needed to fully specify the state in addition to the usual quantum state. These functions give in a fully deterministic way the outcome of the experiment with a given direction of the measurement axis and given values of the hidden variables. Consider now the quantity

$$S(\lambda) = A(a,\lambda)[B(b,\lambda) + B(b',\lambda)] + A(a',\lambda)[B(b,\lambda) - B(b',\lambda)].$$

For given values of b, b' and λ, we must have that $B(b,\lambda)$ and $B(b',\lambda)$ either have the same or opposite signs. This means that one of the square brackets is 0 and the other ± 1. $S(\lambda)$ can then only take the values ± 2. The average

$$\langle S(\lambda)\rangle = \int d\lambda \rho(\lambda) S(\lambda)$$

must then satisfy

$$-2 \le \langle S(\lambda)\rangle \le 2.$$

We also need the maximal quantum value for S. Take the state

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

and the observables

$$A = \sigma_a = \mathbf{a}\cdot\sigma = \begin{pmatrix} a_z & a_x - ia_y \\ a_x + ia_y & -a_z \end{pmatrix}$$

where $\mathbf{a} = (a_x, a_y, a_z)$ is the unit vector giving the direction of spin measurement, and we have similar expressions for the other observables. We then have

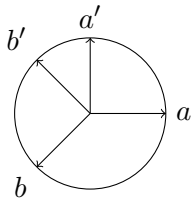
$$\begin{aligned}\langle\psi|\sigma_a\otimes\sigma_b|\psi\rangle &= \frac{1}{2}\left[\langle\uparrow\downarrow|\sigma_a\otimes\sigma_b|\uparrow\downarrow\rangle - \langle\uparrow\downarrow|\sigma_a\otimes\sigma_b|\downarrow\uparrow\rangle - \langle\downarrow\uparrow|\sigma_a\otimes\sigma_b|\uparrow\downarrow\rangle + \langle\downarrow\uparrow|\sigma_a\otimes\sigma_b|\downarrow\uparrow\rangle\right] \\ &= \frac{1}{2}\left[a_z(-b_z) - (a_x - ia_y)(b_x + ib_y) - (a_x + ia_y)(b_x - ib_y) + (-a_z)b_z\right] = -\mathbf{a}\cdot\mathbf{b}.\end{aligned}$$

[1] After J. F. Clauser, M. A. Horne, A. Shimony, and B. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).

Therefore we get

$$\langle S\rangle = \langle \sigma_a \otimes \sigma_b + \sigma_a \otimes \sigma_{b'} + \sigma_{a'} \otimes \sigma_b - \sigma_{a'} \otimes \sigma_{b'}\rangle = -\mathbf{a}\cdot\mathbf{b} - \mathbf{a}\cdot\mathbf{b}' - \mathbf{a}'\cdot\mathbf{b} + \mathbf{a}'\cdot\mathbf{b}'.$$

If we choose the axes all to be in the same plane according to this scheme



we see that

$$\mathbf{a}\cdot\mathbf{b} = \mathbf{a}\cdot\mathbf{b}' = \mathbf{a}'\cdot\mathbf{b} = -\frac{1}{\sqrt{2}}, \qquad \mathbf{a}'\cdot\mathbf{b}' = \frac{1}{\sqrt{2}}.$$

This gives

$$\langle S\rangle = 2\sqrt{2} > 2$$

One can show that this is the maximal value one can get for any state and observables.

1.3 First experiments

The first experiments that conclusively showed a violation of Bell's inequalities were by Aspect in 1981.[2] The source of entangled pairs of photons was an atomic cascade using calcium atoms, and the detectors were placed at a maximal distance of 6 m on opposite sides of the source.

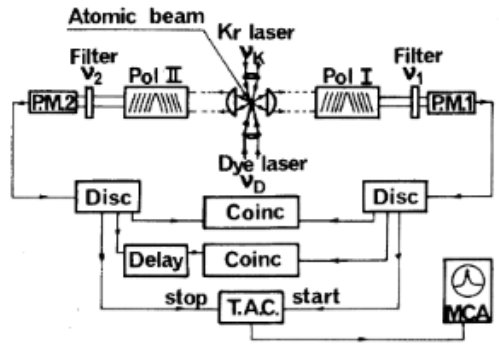


FIG. 2. Schematic diagram of apparatus and electronics. The laser beams are focused onto the atomic beam perpendicular to the figure. Feedback loops from the fluorescence signal control the krypton laser power and the dye-laser wavelength. The output of discriminators feed counters (not shown) and coincidence circuits. The multichannel analyzer (MCA) displays the time-delay spectrum.

[2] A. Aspect *et al.*, Phys. Rev. Lett. **47**, 460 (1981). Similar experiments were performed earlier (see Stuart J. Freedman and John F. Clauser, Phys. Rev. Lett. **28**, 938 (1972)) but with much smaller detection rates and therefore much less statistics.

The detectors are not able to measure the polarization of each photon. Insetad, detectors that are insensitive to polarization are used, and polarizers are put in front of the detectors. This means that one can not directly measure correlation functions, since we only get coincidence detection if both photons are polarized along the direction specified by their polarizers. To account for this, one has to rewrite the CHSH inequality in terms of directly observable quantitites, to get

$$-1 \leq \left[R(\mathbf{a},\mathbf{b}) + R(\mathbf{a},\mathbf{b}') + R(\mathbf{a}',\mathbf{b}) - R(\mathbf{a}',\mathbf{b}') - R_1(\mathbf{a}') - R_2(\mathbf{b})\right]/R_0 \leq 0 \qquad (1)$$

where $R(\mathbf{a},\mathbf{b})$ is the rate of coincidences with polarizer A in orientation $\mathbf{a}$, and polarizer B in orientation $\mathbf{b}$, $R_1(\mathbf{a}')$ is the coincidence rate with polarizer B removed and polarizer A in orientation $\mathbf{a}'$, (and similarly for $R_2(\mathbf{b})$), and R_0, is the coincidence rate with the two polarizers removed. The result of the experiment was $S_{exp} = 0.126 \pm 0.014$ violating inequality (1) by 9 standard deviations.

1.4 Loopholes

There were at least two serious concerns regarding the early experiments. These are usually expressed in terms of loopholes: Ways in which the experiments can show violation of Bell's inequalities while they still may not be really violated.

Locality loophole
The locality requirement in the derivation of Bell's inequality [Lecture notes Section 2.3.2] includes the assumption that the probability distribution $\rho(\lambda)$ for the hidden variable λ is independent of the settings of the two polarizers. But if somehow the process that creates the entangled pairs is affected by the setings of the polarizers that are going to select which measurement we will perform. Then the process creating the photon pair can make pairs with different polarizations depending on the settings of the polarizers, and one can violate Bells inequalities even in a classical thory. The way to close this loophole is to have the direction of the polarizers undecided at the time of creation of the photons (or at least the creation event should be outside of the future lightcones of the events were the polarizers are set).

Detection loophole
The photon detectors are far from perfect, detecting maybe 20% of the photons. If the efficiency of the detectors depends on the hidden variables, one can violate Bells inequality in local hidden variable models. To close this loophole directly on photons, one would have to have better detectors, so that the probablity of misdetection (not detecting a photon present or detecting one that is not present) is sufficiently small. Alternatively, one can create a pair of entangled particles of some other type than photons, where detectors are already good. It is this latter option that is chosen in practice, as we will discuss below.

Both of these may seem paraniod, in the sense that it seems very likely that they are not going to really affect the experiments. In particular, it seems difficult to understand how the settings of the polarizers can affect the process creating the entangled pairs, even if the polarizers are set before the photons are created. I have no idea which physical mechanism should be responsible for this process. But as matters of principle, they still are valid objections, and since one is trying to test the fundamental limitations of any classical theory, it is worth to try to close all loopholes.

1.5 Delayed choice experiments

Closing the locality loophole often goes under the name of delayed choice experiments, because one does not decide the settings of the polarizers until after the photons are created. Since the speed of light is large, one has to be very fast unless one can have a large distance between the two detectors.

The first delayed choice experiments were performed in 1982[3], and were not very much more convincing than the original experiment. We include a discussion here only to show the ingenuity of experimentalists in designing the switching of the polarizers in the very short time available. The distance from the source to the detectors was about 6 m, giving a time of about 20 ns for a light signal to propagate from the polarizer in front of the detecto to the source. There is no way to rotate a physical polarizer in this time, so instead they used two detectors with independent polarizers in front. This means that one can change the polarization by deciding which detector the light is sent to. To do this very fast, they had a water bath with transducers (a type of loudspeaker) on both ends. These created a standing ultrasound wave with a frequency of about 25 MHz in the water. This means that at a certain phase of the acoustic wave, the amplitude of density variations in the water is zero. The light is then passing the water unaffected. A quarter of a period later, the density variation is maximal, and this will scatter the light. Since the density variation is periodic in space, it acts as a grating, Bragg reflecting the incoming light if it is incident at the proper angle.

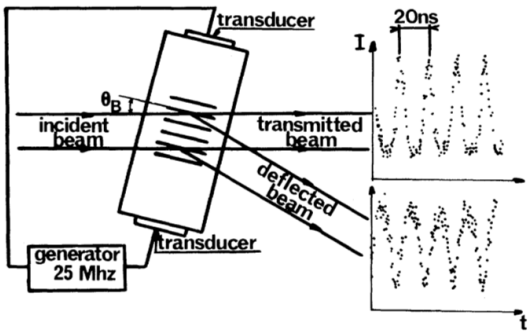


FIG. 3. Optical switch. The incident light is switched at a frequency around 50 MHz by diffraction at the Bragg angle on an ultrasonic standing wave. The intensities of the transmitted and deflected beams as a function of time have been measured with the actual source. The fraction of light directed towards other diffraction orders is negligible.

In this way, the detector that the light hits is switched at twice the acoustic frequency, about every 10 ns. The results were the same as without this elaborate switching device, and in full agreement with quantum mechanics, and violating the Bell inequality. However, in terms of closing the locality loophole, it is not fully convincing. As they write

> The new feature of this experiment is that we change the settings of the polarizers, at a rate greater than c/L. The ideal scheme has not been completed since the change is not truly random, but rather quasiperiodic. Nevertheless, the two switches on the two sides are driven by different generators at different frequencies. It is then very natural to assume that they function in an uncorrelated way.

[3] A. Aspect, J. Dalibard and G. Roger, Phys. Rev. Lett. **49**, 1804 (1982).

So in principle, both the process creating the entangled pairs and the detector on the other side of the setup could "know" the settings of both the polarizers on one side, as well as the state of the switch, since this can be predicted from the fact that it is periodic. It would be really strange if information, encoded in some hard to imagine phyical signal, could be influencing the detectors and the photon source in just the right way.

Still, to be conclusive, the setings of the polarizers should be really random. How can this be achieved? Using a quantum random generator, of course! [4] This is implemented by a weak light source, emitting a stream of well-spaced photons. Each photon is directed to a 50/50 beamsplitter, and is either reflected or transmitted with equal probabilities. A detector is placed in each output of the beamsplitter, and a detection in one gives the random bit "0", while a detection in the other gives "1". Thus, the outcomes are random to the degree that a quantum system collapses randomly to one of the eigenstates in a measurement.

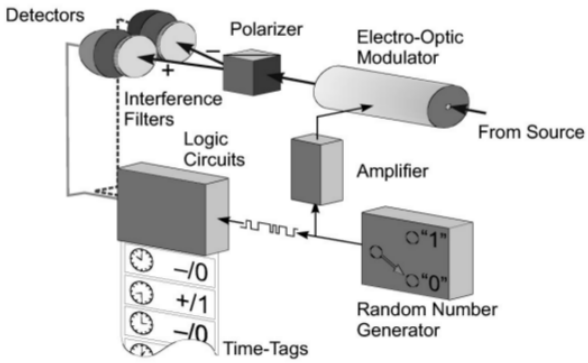


FIG. 2. One of the two observer stations. A random number generator is driving the electro-optic modulator. Silicon avalanche photodiodes are used as detectors. A "time tag" is stored for each detected photon together with the corresponding random number "0" or "1" and the code for the detector "+" or "−" corresponding to the two outputs of the polarizer.

The switching of the beam into one or the other detector is now achieved by an electro-optic modulator, which is a device that rotates the polarization of the photon if a voltage is applied to it. A polarizing beamsplitter then sends the photon to one or the other detector depending on the polarization of the photon. It can change its rate in a time of about 30 ns. To get sufficient time for this and the detectors to fire, the distance from the source to either detector was about 200 m, giving a time of about 1.3 μs for light to cross from one detector to the other. The photons were sent though optical fibres, to minimize loss of photons (by absorption or scattering) on the way. As is seen in the following figure, they were well within the constrints of locality, thus conclusively closing the locality loophole.

[4] Gregor Weihs, Thomas Jennewein, Christoph Simon, Harald Weinfurter, and Anton Zeilinger, Phys. Rev. Lett. **81**, 5039 (1998).

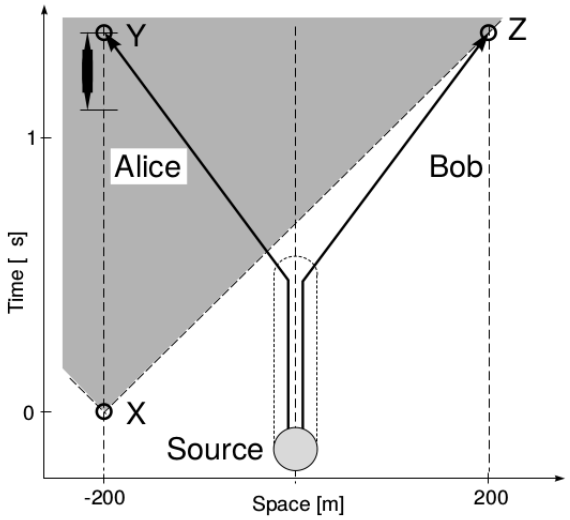


FIG. 1. Spacetime diagram of our Bell experiment. Selecting a random analyzer direction, setting the analyzer, and finally detecting a photon constitute the measurement process. This process on Alice's side must fully lie inside the shaded region which is invisible to Bob's during his own measurement. For our setup this means that the decision about the setting has to be made after point "X" if the corresponding photons are detected at spacetime points "Y" and "Z", respectively. In our experiment the measurement process (indicated by a short black bar) including the choice of a random number took less than only one-tenth of the maximum allowed time. The vertical parts of the kinked photon world lines emerging from the source represent the fiber coils at the source location, which are obviously irrelevant to the locality argument.

To further ensure that no unwanted communication was possible, they independently registered all events with timestamps provided by local clocks and only looked for coincidences (one photon detected at each end at the same time, thus being one entangled pair) afterwards. Previous experiments took the signals from each detector to a common coincidence detector, and one could worry that this allowed for some type of influece of one detector in the measurements of the other. The results were still perfectly in agreement with quantum mechanics, and violating Bell's inequality.

1.6 Entangled ions

To improve the efficiency of photon detectors sufficiently is not realistic at present. Therefore one must work with some other system than photons, where detection of the state is more certain. However, creating an entangled pair of anything else, and transporting the away from each other to sufficient distance so that one can measure their state faster than any signal can go from one to the other is equally difficult (or more). Decoherence from interactions with the environment will eat away all the entanglement logn before they are far enough apart. The trick is to use photons to transport the entanglement to two sufficiently separated places, transfer the entanglement to trapped ions (this process is called entanglement swapping, and we will discuss the principle of this in section 4, and then measure the ion state. The efficiency in the detection of the ionic state is quite good, and sufficient to close the detection loophole.

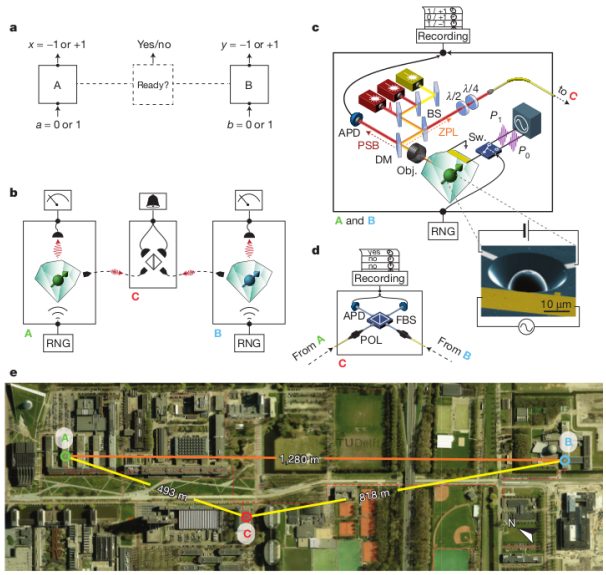
As far as I know, the first such experiments were by Rowe [5] using Beryllium ions. However, the

[5] M. A. Rowe et al., Nature **409**, 791 (2001)

two ions were still in the same trap, and not very far from each other. Better were the experiments[6] where two separate traps were used, but the distance was still only about 1 m, and while the detection loophole was closed, the locality loophole was definitely not.

1.7 Loophole free Bell test

The first experiments to close all loopholes were made in 2015[7]. This experiment is using a special defect, a Nitrogen-Vacancy (NV) centre in diamond instead of ions to be prepared in a Bell state. Photons are exchanged and entanglement is swapped to the NV centres. Then the state of each NV centre is measured, and the efficiency of the detectors is about 92%, sufficient to close the detection loophole. The distance between the two detectors was about 1.3 km, giving sufficient time to perform the basis selection and measurement in time to also close the locality loophole.



The result was that $S = 2.42$, for the first time confirming violation of Bel's inequality with all Loopholes closed.

2 Interaction free measurements

In the lecture notes, section 3.1, there is a discussion of the interaction free measurements of Elitzur and Vaidman. The conclusion was that it is possible to detect the presence of an object without any photon ever interacting with it. Just the possibility of such interaction was sufficient. But it was not always successful. Here we find the success rate and see how to improve it in several ways and determine the optimal success rate.

2.1 The success rate in the original version

In the original version as discussed in the lecture notes, the photon is always detected in detector A if there is no object in the lower arm of the interferometer. If there is an object, we have that the state

[6]

[7] Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres B. Hensen *et al.*, Nature **526**, 682 (2015).

evolves according to

$$|0\rangle \to \frac{1}{\sqrt{2}}|0\rangle + i\frac{1}{\sqrt{2}}|1\rangle \to i\frac{1}{\sqrt{2}}|1\rangle + \frac{1}{\sqrt{2}}|lost\rangle \to -\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|lost\rangle \to -\frac{1}{2}|0\rangle - i\frac{1}{2}|1\rangle + \frac{1}{\sqrt{2}}|lost\rangle$$

where $|lost\rangle$ indicates that the photon is absorbed by the object, and no detection occurs. This means that the probabilities of the different outcomes are

$$\text{A: } \frac{1}{4} \qquad \text{B:} \frac{1}{4} \qquad \text{No detection: } \frac{1}{2}$$

Only if we get the photon in detector B can we tell that the object is there and that the photon did not interact with it. So the probability that we succeed with detecting the object without interaction is only $\frac{1}{4}$.

2.2 First improvement: Repeated trials

We can immediately improve on the probability of success by noting that if we get outcome A, the measurement is inconclusive, but no interaction took place. We can then repeat the experiment with a new photon and have another chance. If this still gives A, we repeat again until B or no detection. The total probability of success is

$$p = \frac{1}{4} + \frac{1}{4^2} + \frac{1}{4^3} + \cdots = \frac{1}{3}$$

2.3 Second improvement: Optimized mirrors

Above, we have used a symmetric beam splitter that has the same probability for transmission and reflection. We can also consider spliters that are assymetric, and optimize the reflection and transmission probabilities. Instead of Eq (3.1) from the lecture notes, we now use for the first beamsplitter

$$|0\rangle \to a|0\rangle + ib|1\rangle \qquad |1\rangle \to a|1\rangle + ib|0\rangle \tag{2}$$

with $a^2 + b^2 = 1$. For the second beamsplitter we interchange the coefficients a and b

$$|0\rangle \to b|0\rangle + ia|1\rangle \qquad |1\rangle \to b|1\rangle + ia|0\rangle \tag{3}$$

We will see that the best result is obtained if $b > a$, so that the first beamsplitter is mostly reflective while the second is mostly transmittive. The fact that the beamsplitters are complementary to each other in the sense that a and b are interchanged ensures that we still have all photons detected by detector A if the box is empty:

$$|0\rangle \to a|0\rangle + ib|1\rangle \to ia|1\rangle - b|0\rangle \to iab|1\rangle - a^2|0\rangle 1 - b^2|0\rangle - iab|1\rangle = -|0\rangle$$

If the box is full we have the evolution of the state

$$|0\rangle \to a|0\rangle + ib|1\rangle \to ib|1\rangle + a|lost\rangle \to -b|0\rangle + a|lost\rangle \to -b^2|0\rangle - iab|1\rangle + a|lost\rangle$$

This gives the probabilities of the different outcomes

$$\text{A: } b^4 \qquad \text{B: } a^2b^2 \qquad \text{No detection: } a^2$$

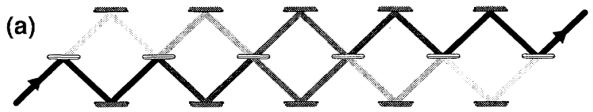
The probability of success in repeated trials is then

$$p = a^2b^2 + (b^4)a^2b^2 + (b^4)^2a^2b^2 + \cdots = \frac{a^2b^2}{1-b^4} = \frac{b^2}{1+b^2}$$

In the limit $b \to 1$ we have $p \to \frac{1}{2}$. Large b mens that the first beamsplitter is mostly reflective, so that the photon most likely will not hit the object. It also means that the probability of getting the result A is close to one, which means that we have to repeat the experiment before evetually getting B and concluding that the oject is there without interaction, or having no detection, which means that the photon reached the object.

2.4 Third improvement: Quantum repeated trials

One can do even better by exploiting quantum interference[8]. Instead of really detecting the photon and collapsing the wavefunction after each trial, one can send the outcome into a second identical interferometer, and then to another and so on. This is illustrated in the figure below, where the darkness of the lines indicates the probability amplitude at that point.



The number of beamsplitters is N, and they are identical with the action

$$|0\rangle \to a|0\rangle + ib|1\rangle \qquad\qquad |1\rangle \to a|1\rangle + ib|0\rangle \tag{4}$$

where now $|0\rangle$ represents a photon moving up and $|1\rangle$ one moving down. We choose

$$a = \sin\frac{\pi}{2N} \qquad\qquad b = \cos\frac{\pi}{2N}$$

and analyze first the case where there is no object. If we let the state after beamsplitter n be $c_n|0\rangle + d_n|1\rangle$ we have that the action of one step in the interferometer is

$$c_n|0\rangle + d_n|1\rangle \overset{mirrors}{\longrightarrow} id_n|0\rangle + ic_n|1\rangle \overset{beamsplitter}{\longrightarrow} (-bc_n + iad_n)|0\rangle + (iac_n - bd_n)|1\rangle$$

which gives the recurrence relations

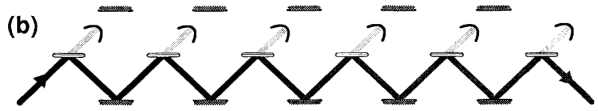
$$c_{n+1} = -bc_n + iad_n \qquad\qquad d_{n+1} = iac_n - bd_n$$

With $c_1 = a = \sin\frac{\pi}{2N}$ and $d_n = ib = i\cos\frac{\pi}{2N}$ it is not difficult to see that the solution is

$$c_n = (-1)^{n+1}\sin\frac{\pi n}{2N} \qquad\qquad d_n = (-1)^{n+1}i\cos\frac{\pi n}{2N}$$

After N beamsplitters we then have $c_N = (-1)^{N+1}$ and $d_N = 0$ so a photon injected into the interferometer will always exit up. To repeat the option of interacting with the object for each beamsplitter, we need to have not a single object, but one for each step, as illustrated in the following figure (this seems a bit unrealistic, but it is soon to be fixed).

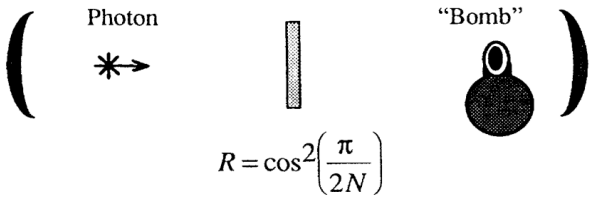
[8]This idea and the real experiment are discussed in Kwiat et al., Phys. Rev. Lett. **74**, 4763 (1995).



To get the outcome $|1\rangle$ (photon exiting down) at the end of the chain, we need to have reflection on all the beamsplitters, so that we never get absorbed by any object. This would indicate the presence of the object since it is impossible if the object is not there. The probability for this is $p = \cos^{2N} \frac{\pi}{2N}$. For large N we can expand this to get

$$p = \cos^{2N} \frac{\pi}{2N} = 1 - \frac{\pi^2}{4N} + \cdots$$

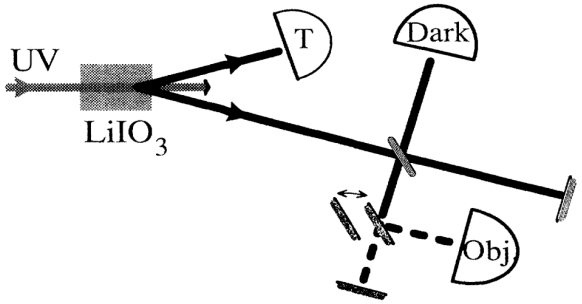
which approaches 1 in the limit $N \to \infty$. This means that we succeed in close to all cases if N is large. It is not easy to imagine successfully building this device with large N since it requires a long chain of optical elements which would be difficult to align, and also it is not so elegant to have N objects to be detected and not just one. Fortunately, the whole chain can be collapsed, and one beamsplitter used repeatedely.



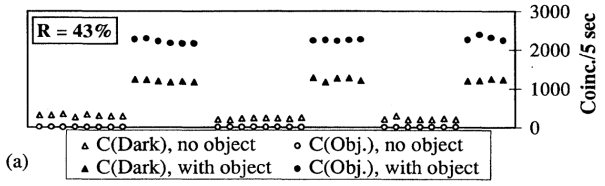
We use two mirrors and one beamsplitter in the middle, creating two optical cavities coupled by the beamsplitter. A photon is inserted into the left cavity at time T = 0. For a beam splitter reflectivity of $\cos \frac{\pi}{2N}$, and in the absence of any absorber, the photon will with certainty be located in the right cavity at time $T_N = N \times$ (round-trip time), due to interference effects. Therefore, a detector inserted into the left cavity at time T_N would not fire. However, in the presence of an absorber or scatterer in the right cavity, the photon wave function is continually projected back onto the left cavity. Making the coupling weaker (i.e. , increasing the reflectivity) and the number N greater, one can reduce the probability that the photon ever leaves the first cavity when the object is in the second. A detector inserted into the left cavity will then nearly always fire at time T_N. Again, the probability of an interaction-free measurement can be made arbitrarily close to 1.

2.5 The real experiment

The real experiment was less ambitious, and used only a single pass through an interferometer. The setup is shown below



A laser beam is passing through a crystal of $LiIO_3$, which creates entangled pairs. One photon of the pair is sent to detector T to confirm that another photon enters the interferometer. The second phothon is split by a beamsplitter and reflected back using two mirrors. The object whose presence is to be detected is implemented as a mirror that can be outside of the beam, corresponding to no object, or in the beam, deflecting the photon. To make an additional check, it is not absorbed but sent to a detector (marked "Obj"). In the absence of an object, the interferometer is such that all photons are sent back to the source, and no photons exit in the direction of the detector marked "Dark", so this detector should never detect any photons in the absence of an object. In the presence of the object, there is no amplitude to return from the lower branch of the interferometer, the destructive interference is removed, and photons can reach the "Dark" detector. This shows up as coincidences between the detectors "T" and "Dark" as was indeed observed.



(a)

3 Quantum cryptography

One of the ways in which one can explit quantum mechanics in communication is in cryptography, in particular in distributing cryptographic keys in a secure way. Here we describe the principles of quantum key distribution and some examples of experiments.

3.1 Secure classical communication: one time pad

One of the simplest ways to construct a classical code is to replace each letter in the alphabet with another, which is called a substitution cipher. This is easy to code and decode: To code you need a table of the type a→r, b→m, ..., and to decode you need the reverse table r→a, m→b, ... These tables are referred to as the encoding and decoding keys, respectively. Unfortunately, it is also easy to break this code, at least if you have a reasonably long coded message to study and know the language it is written in. The point is that some letters are more common than others, so we can guess that a letter occuring frequently in the coded message is corresponding to one of the frequently occuring letters. To do even better, one can look at groups of letters or short words, and one will be able to reconstruct the decoding key, and break the code. It becomes much more difficult to decode if the same key is not used all the time. This was the principle for example of the famous Enigma system used during WW2. There, the key was implemented as a series of wheels with contacts for each letter and wires connecting them. After each letter was encrypted, the wheels were rotated, so that effectively each letter was encoded using a new key, although according to some pattern that provides some help in an attept to break the code. However, we get the idea that if we could really use a new key for each letter, the code could never be broken.

In our digital world, we are happy only to send 0 and 1, so we replace the alphabet by just those two symbols. Then there are only two possible keys:

$$\begin{matrix} 0 \to 0 \\ 1 \to 1 \end{matrix} \quad \text{or} \quad \begin{matrix} 0 \to 1 \\ 1 \to 0 \end{matrix}$$

These are conveniently represented by addition mod 2. Adding 0 gives the first key, adding 1 (mod 2) gives the second key. This means that if both the encoder and decoder have access to the same random sequence of bits (with equal probabilities for 0 and 1 and no correlations between any bits), they can do the following.

Original message	0	1	1	0	1	1	0	$\cdots$
Random sequence	1	1	0	1	0	1	0	$\cdots$
Coded message	1	0	1	1	1	0	0	$\cdots$
Same random sequence	1	1	0	1	0	1	0	$\cdots$
Decoded message	0	1	1	0	1	1	0	$\cdots$

To encode the message, one adds the random sequence (mod 2). To decode, one adds the same random sequence again (which is the same as subtracting (mod 2)). As long as the random sequence is truly random, the encoded message will be equally random, and it is absolutely impossible to break the code. It is important that there are no patterns in the random sequence. For example is it tempting to have a sequence of finite length and then start from the beginning again once you reach the end. This would introduce a pattern that in principle could be discovered and used to break the code (although in practice it could be extremely difficult if the message is not many times the length of the random sequence). To make it principally unbreakable, each bit in the random sequence can be used only once, and it is therefore referred to as a one time pad. The disadvantage of this type of code is that it requires the sender and receiver to share the random sequence at some time before they can communicate, either by meeting or sending the information in some way they trust nobody can intercept.

What if I am in some remote place and run out of random sequence and have some really secret message for a freind back home? Or I find that I want to send a secret to someone I never met? If we can somehow generate the same random sequence in two places while at the same time being certain that nobody, even if they listen to all communication between us, will get any information about the sequence, we can use this as a one time pad to encode the message. This trick can be performed if we are able to send and measure particles in well defined quantum states (like electrons with spin of photons with polarization) as well as classical signals.

3.2 Quantum key distribution

We have two parties A and B that want to establish a common random sequence, which we will call the key, to be used as a one time pad. A first generates one random sequence of bits to be used as the key (or at least parts of it will be the key). A also generates an additional random sequence specifying the basis which she will use to encode the key in a two-level quantum system. If the bit specifying the basis is 0, she will use the basis of eigenstates of σ_z which we denote $\{|\uparrow\rangle, |\downarrow\rangle\}$, while if the basis bit is 1 she will use the basis of eigenstates of σ_x which we denote $\{|\rightarrow\rangle, |\leftarrow\rangle\}$ and which are defined by

$$|\rightarrow\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle + |\downarrow\rangle) \qquad |\leftarrow\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle - |\downarrow\rangle).$$

The encoding of the key bit is then

$$\text{If basis bit is 0: } \begin{array}{l} 0 \rightarrow |\uparrow\rangle \\ 1 \rightarrow |\downarrow\rangle \end{array} \qquad \text{If basis bit is 1: } \begin{array}{l} 0 \rightarrow |\rightarrow\rangle \\ 1 \rightarrow |\leftarrow\rangle \end{array}$$

For each bit A now prepares a two-level system in the corresponding state and sends it to B. B has no idea which basis was used to prepare the states, so he can do no better than randomly measuring

according to one of the bases for each particle that arrives. When B uses the same basis for measurement as A used for preparation, the result of the masurement is perfectly determined, and agrees with the state that A pepared. In the cases where different bases are used, the result is random and there is no correlation between that prepared state and the result. Both A and B now send their random bases to each other using any type of classical communication. This can be done without any encryption, it does not matter if anyone gets to know this information. The cases where the bases are different are useless and discarded, but for those with a common basis we are guranteed that B knows the corresponding bit in A's random key. The process is exemplified in the following table:

A random key	1	0	1	1	0	1	0	$\cdots$
A random basis	0	0	1	0	1	0	1	$\cdots$
A state	$\vert\downarrow\rangle$	$\vert\uparrow\rangle$	$\vert\leftarrow\rangle$	$\vert\downarrow\rangle$	$\vert\rightarrow\rangle$	$\vert\downarrow\rangle$	$\vert\rightarrow\rangle$	$\cdots$
B random basis	0	1	1	0	0	0	1	$\cdots$
B measures	$\downarrow$	$\rightarrow$	$\leftarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\rightarrow$	$\cdots$
Bits that we use	1	$-$	1	1	$-$	1	0	$\cdots$

What happens if somebody tries to evesdrop and listen to the communication, quantum or classical? It is clear that the information on the basis for A and B, communicated on the open classical channel does not provide any information on the key, and is therefore useless to intercept. What about intercepting the quantum channel? We will not provide a full proof of the security of the protocol[9], but illustrate what happens in an example. One possible way to gain information from the quantum channel is if the evesdropper (E) measures the particles. It is clear that the state is affected by the measurement, and we assume in this example that E will pass on the state after the measurement (which is now the eigenstate corresponding to the measurement outcome). Since experiments are (almost?) exclusively using photons, these are absorbed during detection, and E will instead resend the state corresponding to the measured result. This type of attempt to steal the information is therefore known as measure and resend attack. At the time of the exchange of quantum information, E has no idea about the basis that is used by A or B for that particle, this is only given by classical communication later. So E can do no better than randomly chossing a basis for the measurement. We only have to consider those cases were the basis of A and B are the same, since these are the only that are going to be used. Sometimes E will measure in same basis as the one used by A and B, in which case the state will not be modified, and E gets the information about the key at that bit. E can then decode that bit if she intercepts the coded message. If E uses a basis different from A, the state will be modified, and the result of the measurement will not be correlated with the actual value A has for that bit. The fact that the state is changed also means that B may not get the same value as A for the key at that point. In the example below, we have not specified what happens when A and B do not use the same basis, as these bits are discarded anyway. We have marked with circles those places where the keys for E or B are different

[9] See Nielsen and Chuang, Quantum Computation and Quantum Information

from the one of A.

Bit number	1	2	3	4	5	6	7	$\cdots$
A random key	1	0	1	1	0	1	0	$\cdots$
A random basis	0	0	1	0	1	0	1	$\cdots$
A state	$\vert\downarrow\rangle$	$\vert\uparrow\rangle$	$\vert\leftarrow\rangle$	$\vert\downarrow\rangle$	$\vert\rightarrow\rangle$	$\vert\downarrow\rangle$	$\vert\rightarrow\rangle$	$\cdots$
E random basis	0	0	0	1	1	1	0	$\cdots$
E measures	$\downarrow$	$-$	$\uparrow$	$\leftarrow$	$-$	$\leftarrow$	$\downarrow$	$\cdots$
Key that E gets	1	$-$	(0)	1	$-$	1	(1)	$\cdots$
E sends to B	$\vert\downarrow\rangle$	$-$	$\vert\uparrow\rangle$	$\vert\leftarrow\rangle$	$-$	$\vert\leftarrow\rangle$	$\vert\downarrow\rangle$	$\cdots$
B random basis	0	1	1	0	0	0	1	$\cdots$
B measures	$\downarrow$	$-$	($\rightarrow$)	$\downarrow$	$-$	($\uparrow$)	$\rightarrow$	$\cdots$
Key that B gets	1	$-$	(0)	1	$-$	(1)	0	$\cdots$

In this example we see several possible outcomes:

1. All can use the same basis, and then also get the same result (Bit 1).
2. E uses the wrong basis, and E and B get the wrong key (Bit 3).
3. E uses the wrong basis, but E and B still get the right key (Bit 4).
4. E uses the wrong basis, and E gets the right key while B gets the wrong key (Bit 6).
5. E uses the wrong basis, and E gets the wrong key while B gets the right key (Bit 7).

The point is that the interference by E results in a certain chance that B will not get the right key, and this can be used to detect the presence of E. Before using this key, A and B will validate by comparing a certain number of bits randomly choosen. The probability that a given bit will give a wrong key to B is $\frac{1}{4}$ since there is a chance $\frac{1}{2}$ that E uses the wrong basis and then a chance $\frac{1}{2}$ that B will get the wrong result. The probability that comparing one specific bit at random will reveal E is then $\frac{3}{4}$. If they compare n bits, the probability that they detect E is $p_n = 1 - \left(\frac{3}{4}\right)$ which becomes very small for not so large n. For example $p_{100} = 3,2 \cdot 10^{-13}$. As we will see below, one can experimentally generate 100 bits in less than a second even over long distances, so only a small fraction of the bits need to be tested in order to ensure virtual certainty about the non-presence of any evesdropper. This picture is complicated by the fact that there will be naturally occuring noise or detector errors, which gives a certain background rate of erroneous key transfers.

4 Entanglement swapping

4.1 Principle

Entanglement is normally a consequence of interaction. If two particles, which initially are in a product state, interact, the final state will generally be entangled. But can we create entaglement between two particles which never have interacted with each other?

Imagine A and B are far from each other and has two TLS each, call them A_1, A_2, B_1 and B_2. We want A_1 and B_1 to end in an entangled state. We let both parties entangle their pair of particles so that they are in the states

$$|\psi_A\rangle = \frac{1}{\sqrt{2}}(|\uparrow_{A_1}\downarrow_{A_2}\rangle - |\downarrow_{A_1}\uparrow_{A_2}\rangle)$$
$$|\psi_B\rangle = \frac{1}{\sqrt{2}}(|\uparrow_{B_1}\downarrow_{B_2}\rangle - |\downarrow_{B_1}\uparrow_{B_2}\rangle)$$

The total state is

$$|\psi\rangle = |\psi_A\rangle\otimes|\psi_B\rangle = \frac{1}{2}\Big[|\uparrow_{A_1}\uparrow_{B_1}\rangle\otimes|\downarrow_{A_2}\downarrow_{B_2}\rangle - |\uparrow_{A_1}\downarrow_{B_1}\rangle\otimes|\downarrow_{A_2}\uparrow_{B_2}\rangle - |\downarrow_{A_1}\uparrow_{B_1}\rangle\otimes|\uparrow_{A_2}\downarrow_{B_2}\rangle + |\downarrow_{A_1}\downarrow_{B_1}\rangle\otimes|\uparrow_{A_2}\uparrow_{B_2}\rangle\Big]$$

Were we have just rearranged the grouping of the particles, but not changed the state in an y way. We now rewrite this state in the Bell basis as defined in Eq. (3.12) in the lecture notes to get

$$|\psi\rangle = \frac{1}{2}\Big[|\phi^+\rangle_{A_1B_1}\otimes|\phi^+\rangle_{A_2B_2} - |\phi^-\rangle_{A_1B_1}\otimes|\phi^-\rangle_{A_2B_2} - |\psi^+\rangle_{A_1B_1}\otimes|\psi^+\rangle_{A_2B_2} + |\psi^-\rangle_{A_1B_1}\otimes|\psi^-\rangle_{A_2B_2}\Big]$$

So far we just rewrote the state. Now, let A and B send their particles A_2 and B_2 to some common point where they are measured in the Bell basis. The state of A_2 and B_2 then collapses to one of the four Bell states and due to the structure of the state $|\psi\rangle$, the particles A_1 and B_1 are left in the same state. So we start from A_1 and A_2 entangled and B_1 and B_2 entangled. After the measurement, A_1 and B_1 are entangled and A_2 and B_2 are entangled. A_1 and B_1 end in an entangled state without ever having interacted with each other.