6. Composites systems and Entanglement

6.1 Tensor product of Hilbert spaces

Until now we have been concerned with the description and evolution of a single TLS. Although we have seen some examples of how it describes some real physical systems, of course many systems are more complicated and cannot be described by that formalism. We could of course start studying higher dimensional systems, such as more general angular momentum with dimension N. Here we focus instead on systems with dimension $N = 2^n$ (with n integer) because we are interested in studying composite (or multipartite) systems, where two or more TLS systems interact. Let's consider 2 two-level Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, each spanned by the vectors: $|0\rangle_A, |1\rangle_A$ and $|0\rangle_B, |1\rangle_B$. For each space we can define the Pauli Matrices and the identity on the space. They are two distinguishable Hilbert space (we will deal with indistinguishable particles later on). The action of a Pauli matrix on the vector of its own Hilbert space is as usual (e.g. $\sigma_x^A |0\rangle_A = |1\rangle_A$). But operators of the A Hilbert space do not act on the vectors of the other Hilbert space, they leave them unchanged: $\sigma_x^A |0\rangle_B = |0\rangle_B$.
We can define the joint space $\mathcal{H}_{AB}$ by a tensor product $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$, which has dimensions $N = 2^2 \times 2^2 = 2^4 = 16$. When we consider a matrix representation of the Hilbert space, this corresponds to a kronecker product. For example, the kronecker product of two matrices (operators) A and B is given by:

$$A \otimes B = \left(\begin{array}{cc} A_{11}B & A_{12}B \\ A_{21}B & A_{22}B \end{array} \right) = \left(\begin{array}{cccc} A_{11}B_{11} & A_{11}B_{12} & A_{12}B_{11} & A_{22}B_{11} \\ A_{11}B_{21} & A_{11}B_{22} & A_{12}B_{21} & \dots \\ A_{21}B_{11} & A_{21}B_{12} & \dots & \dots \\ A_{21}B_{12} & & & \end{array} \right)$$

that is, a 4×4 matrix. In the same way, the vector states of the joint Hilbert space are defined by the kronecker products of the basis states of the two spaces. For example:

$$|0\rangle_A \otimes |1\rangle_B = \left[\begin{array}{c} 0 \\ 1 \end{array} \right] \otimes \left[\begin{array}{c} 1 \\ 0 \end{array} \right] = \left[\begin{array}{c} 0 \\ 0 \\ 1 \\ 0 \end{array} \right]$$

A basis set for a two-qubit system (two TLS) is given by the four states: $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$.
Notation-wise, we normally do not write the identity: $\sigma_x^A \otimes 1_B = \sigma_x^A$.

If one spin space is spanned by 4 matrices, the joint domain A and B is spanned by 16 operators, which are the combinations of operators from the two spaces: $\{1, \sigma_x^A, \sigma_x^B, \dots, \sigma_x^A\sigma_y^B, \dots \sigma_z^A\sigma_z^B\}$.
The joint space is still an Hilbert space. If $|a\rangle$ is a vector in the $\mathcal{H}_A$ space and $|b\rangle$ in the $\mathcal{H}_B$ space, taking a vector in the joint space $|a\rangle \otimes |b\rangle$ it has the properties of a linear vector:

$$(|a_1\rangle + |a_2\rangle) \otimes |b\rangle = |a_1\rangle \otimes |b\rangle + |a_2\rangle \otimes |b\rangle$$

and

$$c(|a\rangle \otimes |b\rangle) = c\,|a\rangle \otimes |b\rangle = |a\rangle \otimes c\,|b\rangle$$

(notice that the scalar can be pushed trough as desired).
If A is an operator in $\mathcal{H}_A$ and B in $\mathcal{H}_B$, each operator acts on its own domain: $AB(|a\rangle \otimes |b\rangle) = (A\,|a\rangle) \otimes (B\,|b\rangle)$. If $\mathcal{H}_C = \mathcal{H}_{AB}$ is the joint Hilbert space, any operator in it can be written as a linear combination of operators in the two spaces: $C = \sum_{i,j} c_{i,j} A_i B_j$, where i and j run on the two domains and $\{A_i\}$, $\{B_j\}$ form complete sets (a basis for the operator spaces).
The inner product of vectors in the joint space are

$$(\langle b_1| \otimes \langle a_1|)(|a_2\rangle \otimes |a_2\rangle) = \langle a_1|\, a_2\rangle \,\langle b_1|\, b_2\rangle.$$

A ket of a joint space can also be written as $|a, b\rangle$, that is, a ket can be specified by as many quantum number as required to fully characterize the state.

6.1.1 Product Operator Basis

We can generalize these considerations to more than two TLS (or qubits or spin-$\frac{1}{2}$). We thus define a composite Hilbert space of dimension $N = 2^n$, where n is the number of qubits, as the tensor product of the Hilbert space for each qubit: $\mathcal{H} = \bigotimes_{i=1}^n \mathcal{H}_i$. A basis for this operator space is the product operator basis (also called generalized Pauli operators). Elements of this basis are defined as

$$P_l = \bigotimes_{j=1}^{n} P_l^{(j)},$$

where each $P_l^{(j)}$ is either a Pauli matrix $\{\sigma_x, \sigma_y, \sigma_z\}$ or the identity $\mathbb{1}$ in the space of the qubit j. Notice that $P_l^\dagger = P_l$ (hermitian) and $\mathrm{Tr}\,\{P_l P_{l'}\} = N\delta_{l,l'}$ (that is, the basis is orthogonal, but nor normalized).

6.2 Quantum Information Processing

Quantum information processing is the study of information processing tasks that can be accomplished (only) using quantum mechanical systems. What do we mean by *only*? What we refers to are tasks that can be possible only if the law of quantum mechanics apply to the system used for processing the information or that are accomplished in a more efficient way if performed by a quantum system (in terms of time or material resources). For example, Peter Shor showed in 1994 that it is possible to find the prime factors of a number using a quantum computer in an exponentially shorter time than in a classical computer. The scaling refers to the fact that if we want to factorize a number represented by n bits of information (e.g. in its binary representation the string is n-character long) it will take a time $T_{cl} \propto 2^n$ for a classical computer to perform the computation, while only a time $T_{qu} \propto n$ to a quantum computer. Although factoring the number 15 is easy[14], factoring large numbers is a very time-consuming task, so much that encryption is based on number factoring (as the reverse operation, finding the product of two numbers, is instead an easy task).

[14] Why do I mention here 15? Because that is the number that has been possible to factorize until now by a quantum computer:
L.M.K Vandersypen, M. Steffen, G. Breyta, C.S. Yannoni, M.H. Sherwood and I.L. Chuang, *Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance*, Nature **414** 883-887 (2001)

While it is still a debate of where the power of quantum computation comes from, two main ingredients seems to have a preeminent role. Quantum superposition (in the form of parallelism that allows to compute all the possible solutions of a problem at once) and interference (that leads to algorithms that select a constructive interference for the correct solution, so that we obtain the right answer with high probability once we measure the quantum system and collapse the superposition state). As it is implied in this last statement, not all the tasks can be made more efficient on a quantum computer and in fact it has proven quite hard to find quantum algorithms (although the known ones are quite powerful).

Quantum information processing has ramifications well beyond quantum computation. Very active areas of research - and of practical results - are quantum communications, simulations, sensors, and of course on the theory side, quantum control, quantum complexity, entanglement theory, decoherence, etc.

Here we will adopt some of the language and tools of quantum information to explore ideas that connect to the very foundation of quantum theory. We will start by describing operations that can be performed on a quantum computer. As at its heart a quantum computer is just a QM physical system, these operations simply describe the evolution of the system itself.

In the same way as classical computer are physical systems, circuits made of wires and gates, a quantum computer is also composed of wires and quantum gates. The wires are used to carry the information around, while the gates perform operations, manipulate the information. Quantum gates however have the properties of being linear and *invertible*, as they represent the unitary evolution of a quantum system (a collection of TLS or qubits). This is different than usual classical gates, although invertible classical gates were already known.

6.3 Operators on two Qubits

There are several operators which are normally used in quantum computation and that describe the possible evolution of the system.
- Not$^A = \sigma_A^x \otimes 1_B$; Not$^B = 1_A \otimes \sigma_B^x$.
- Hadamard gate: $H = (\sigma_x + \sigma_z)/\sqrt{2}$.
- Controlled Not: rotate B conditionally on the state in the A subspace. Introducing the idempotents[15] (or projectors) $E^+ = |0\rangle\ \ 0|$ and $E^- = |1\rangle\ \ 1|$, the CNOT is $C^A NOT^B = E_A^+ + E_A^- \sigma_B^x$:

$$C^A NOT^B = \left(\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{array}\right)$$

If somebody has taken some computer science classes, you can realize that the truth table of the cnot gate is quite similar to that of a XOR gate. We can also just have general single qubit gates, U, that describe any general rotation on a single qubit. If we combine this single qubit rotations with the CNOT gates on any pair of qubit, we are able to build any possible algorithm (or computation) on the system. That also means that we are able to enforce any possible evolution of the system, by letting it evolve under these two types of gates. We says that they are universal gates.

A	B	AB
0	0	00
0	1	01
1	0	11
1	1	10

Table 2: Truth table of the CNOT (1st qubit controller, 2nd qubit target)

[15] Idempotents since they square to themselves

A. Measurement in the σ_x basis

At the end of a circuit, the qubits are measured. While usually it is implicit that the qubits are measured in their computational basis ($|0\rangle,\ |1\rangle$), which corresponds to the eigenvalues of the operator σ_z, this does not always has to been the case. The eigenvectors of σ_x form an equivalently good basis. We could have expressed a state vector as: $|\psi\rangle_z = a\,|0\rangle + b\,|1\rangle \to |\psi\rangle_x = c\,|0\rangle_x + d\,|1\rangle_x = c\,|+\rangle + d\,|-\rangle$ (the last expression is a notation encountered often). The coefficients c and d can be calculated with a change of basis. First, notice that the eigenvectors of σ_x in the z-basis are given by the eigenvectors of the matrix

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

that is:

$$|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2} \qquad |-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$$

The operator that perform the change of frame is therefore the Hadamard matrix: $|\psi\rangle_x = H\,|\psi\rangle_z$. This is also the reason why, instead of measuring in the x-basis, we can perform an Hadamard operation to bring back the qubit to the z-basis, and measure in this more usual basis.
The representations of gates, qubits and wires is usually done via diagrams like the following:

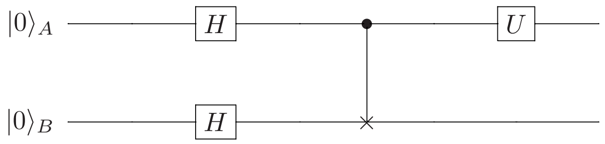

Fig. 9: Quantum circuit, showing Hadamard, CNot gate and a general gate U

6.4 No cloning Theorem

We are going to study some properties of quantum states that distinguish them from classical states. One property that has been known for a long time, without stirring much interest before it was considered again in the optics of quantum computation is the impossibility of copying a quantum state. This impossibilities seemed to doom quantum computation, because it seemed to forbid correction codes, but quantum resources offer other ways to perform error correction.
The so-called *No-cloning* theorem, states that:
■ Theorem: It is impossible to make a perfect copy of an unknown, pure state by an unitary operation.

Proof: I want to copy an arbitrary state $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ on the blank initial state $|i\rangle$ using a unitary operator U. The final state is therefore:

$$U\,|\psi\rangle \otimes |i\rangle \overset{?}{=} |\psi\rangle \otimes |\psi\rangle$$

for any state $|\psi\rangle$ in the domain of the first system. If I assume to be able to copy any arbitrary state, I can assume that I can copy at least another state $|\varphi\rangle$, which is not the state $|\psi\rangle$ and not orthogonal to it. For this second state we have:

$$U\,|\varphi\rangle \otimes |i\rangle = |\varphi\rangle \otimes |\varphi\rangle$$

Equating the inner products of the RHS and LHS of the two equations above, we obtain:

$$\begin{array}{ccc} \varphi, i|\, U^\dagger U\,|\psi, i\rangle & = & \varphi, \varphi|\, \psi, \psi\rangle = \\ \varphi\,|\psi\rangle\ \ i\,|i\rangle & = & \varphi\,|\psi\rangle\ \ \varphi\,|\psi\rangle \\ \varphi\,|\psi\rangle & = & \varphi\,|\psi\rangle^2 \end{array}$$

The last equation is verified iif $\varphi|\psi\rangle = 1$ or $\varphi|\psi\rangle = 0$. In the first case, the two states are in effect the same state (up to a normalization factor or a global phase, which are not important). In the second case the two states are orthogonal, in contradiction with the hypothesis. □

A unitary operator cannot copy an arbitrary state. If we find an operator that can clone one state, it can only copy that state and states which are orthogonal to it, but it cannot clone all the other states. In a Hilbert space it is therefore possible to define an operator that clones the basis states, but not an arbitrary superposition of them.

Example of ”Cloning”

Consider the action of the CNOT gate on the state $|\psi\rangle|0\rangle$, where $|\psi\rangle$ is the state we would like to clone and $|0\rangle$ is the blank bit we want to copy on. If $|\psi\rangle = |0\rangle$, the CNOT gives us the state $|00\rangle$, if it is $|1\rangle$ we obtain the state: $|11\rangle$. So it seems that it is possible to copy the state of the first qubit on the second qubit. But notice that for the moment we have only verified that we can copy two orthogonal state. If we have a more general state: $|\psi\rangle = a|0\rangle + b|1\rangle$, the action of the CNOT will give us:

$$CNOT|\psi, 0\rangle = CNOT(a|00\rangle + b|10\rangle) = a|00\rangle + b|11\rangle$$

$$\neq |\psi, \psi\rangle = (a|0\rangle + b|1\rangle)(a|0\rangle + b|1\rangle).$$

Notice that approximate cloning is possible[16] (that is, it is possible to obtain an approximate copy of an arbitrary state up to an error ϵ. The error is usually measured as the deviation from unity of the inner product of the original and ”cloned” state: $\epsilon = 1 - |\langle\psi|\varphi\rangle|$).

[16] Valerio Scarani, Sofyan Iblisdir, Nicolas Gisin and Antonio Acin, *Quantum cloning*, Rev. Mod. Phys. **77**, 1225 - 1256 (2005) *Abstract* - The impossibility of perfectly copying (or cloning) an unknown quantum state is one of the basic rules governing the physics of quantum systems. The processes that perform the optimal approximate cloning have been found in many cases. These ”quantum cloning machines” are important tools for studying a wide variety of tasks, e.g., state estimation and eavesdropping on quantum cryptography. This paper provides a comprehensive review of quantum cloning machines both for discrete-dimensional and for continuous-variable quantum systems. In addition, it presents the role of cloning in quantum cryptography, the link between optimal cloning and light amplification via stimulated emission, and the experimental demonstrations of optimal quantum cloning.

6.5 Entanglement and EPR paradox

It is nearly 70 years ago that Schrödinger gave the name *Verschraenkung* to a correlation of quantum nature. This term was then rather loosely translated to *entanglement*. Over the decades the meaning of the word *entanglement* has changed its flavor, going from a negative statement by Einstein and coworkers *"An entangled wavefunction does not describe the physical reality in a complete way"*, to more quantitative definitions (Bell, *"A correlation that is stronger than any classical correlation"*) to more practical ones (C. Bennett: *"A resource that enables quantum teleportation"*, P. Shor: *"that allows for faster algorithms"*).
A simple definition of entanglement is possible for pure, bipartite systems (i.e. composed of two subsystems).

$\mathcal{D}$: **Entanglement** A pure state $|\psi\rangle$ is called separable iff it can be written as $|\psi\rangle = |\varphi\rangle_1 \otimes |\varphi\rangle_2$, otherwise it is entangled. An example for a pure separable state is $|00\rangle$; examples for pure entangled states are the Bell states

$$\left|\Phi^{\pm}\right\rangle = (|00\rangle \pm |11\rangle)/\sqrt{2}$$

$$\left|\Psi^{\pm}\right\rangle = (|01\rangle \pm |10\rangle)/\sqrt{2}$$

We will see some measure of entanglement and also some difficulties arising for example in defining and measuring entanglement for more complex systems.
Why is entanglement a difficult property to quantify and more importantly, to grasp its meaning?
We will review the so-called EPR paradox which makes it manifest some of the weirdness of QM as associated to entanglement.
In 1935 Einstein published a paper with some coworkers that asked :
Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?[17]

We will rephrase their result in a slightly different way (due to Bohm) and following the presentation in Ballentine's book[18].

6.5.1 Bell Inequalities

Let us suppose that we are capable of making a state $|\psi\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$ of two identical spin-1/2 particles, with the two particles traveling with equal momenta in opposite directions. For example, they could originate in the decay of an unstable particle of zero spin and zero momentum, in which case momentum conservation implies that the particles move in opposite directions and have spin with zero sum.
Two experimentalists, conventionally named Alice and Bob (A,B), measure the spin component of each particle along a certain axis when the particles are very far apart compared with the range of any force of mutual interaction and when they have not interacted with each other for a long time.
Alice measures the spin component on the $\hat{a}$ axis for the particle traveling to the left, particle a, while Bob measures the component along the $\hat{b}$ axis of the particle traveling to the right, particle b. Let us first study the case where Alice and Bob both use the z-axis, $\hat{a} = \hat{b} = \hat{z}$. For the moment we can just think of the spins as a property of the particles, as it could be e.g. the color of a ball.
Alice measures the z component of the spin of particle a, S_z^a, with the result $\pm\frac{1}{2}$, and Bob measures S_z^b. They obtain a series of random results, when they repeat the experiment. After the series of measurements has been completed, Alice and Bob meet and compare their results. They conclude that the results for each pair exhibit a perfect (anti-)correlation. When Alice has measured $+1/2$ for particle a, Bob has measured $-1/2$ for particle b and vice versa.
Upon reflection, this result is not very surprising. It can occur also for classical particles (or travelers!). Two travelers a and b, each carrying a suitcase, depart in opposite directions from the origin and eventually are checked by two customs inspectors Alice and Bob. One of the suitcases contains a red ball and the other a green ball, but the travelers have picked up their closed suitcases at random and do not know what color the ball inside is. If Alice checks the suitcase of traveler A, she has a 50% chance of finding a green ball. But if in fact she finds a green ball, clearly Bob

[17] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 - 780 (1935)
[18] L. E. Ballentine, *Quantum Mechanics A Modern Development*, World Scientific Publishing (1998)

will find a red ball with 100% probability. Correlations between the two suitcases were introduced at the time of departure, and these correlations reappear as a correlation between the results of Alice and Bob.
However, the situation becomes weirder if Alice and Bob decide to use the x axis instead of the z axis for another series of measurements. In the classical case, this would correspond to the fact the ball hidden in the suitcases possess another property (for example they are shiny or matte). Again, one would obtain the same result of perfect anti-correlation of the results (try e.g. expressing the Bell state in the x basis).
In the usual classical picture of the world, one would assume –as stated by Einstein– the hypothesis of Locality and Realism (both of these hypothesis should be true at the same time). What do these hypotheses entail?

1. Realism: At preparation, particles a and b possess both the properties (color and gloss for the classical balls and σ_x, σ_z, with $\sigma_{x,z} = x(z) = \pm 1$ for the quantum particles).

2. Locality: When I measure particle a I cannot modify instantaneously the result of measuring particle b, since b already had its own properties and there is no action at distance (faster than light).

In the EPR paper, the authors argue that since QM does not give a description coherent with these hypotheses, there must be a more complete theory able to fully describe reality while respecting these hypotheses.
The search for a theory of *hidden variables* is still open, but it has been shown already that local realism is in conflict with experiment.
The Bell inequalities want to show that these two hypotheses cannot be true together for quantum mechanics. They describe a more general experiment to what done until now.
I - Assume that A measure her particles along the axis $\vec{a} = \vec{z}$ while B along the axis $\vec{b}$ such that $\vec{b} \cdot \vec{z} = \cos\vartheta$. The results of the measurements are $\left\langle \sigma_z^A \right\rangle = a$ and $\left\langle \sigma_b^B \right\rangle = b$ and we are interested in the correlation $\ ab\rangle$. This is given by

$$\left\langle \sigma_z^A \sigma_b^B \right\rangle = \frac{1}{2}(\langle 01|\, \sigma_z^A \sigma_b^B \,|01\rangle + \langle 01|\, \sigma_z^A \sigma_b^B \,|10\rangle + \langle 10|\, \sigma_z^A \sigma_b^B \,|01\rangle + \langle 10|\, \sigma_z^A \sigma_b^B \,|10\rangle$$

$$= \frac{1}{2}\left(\langle 0|\sigma_z^A|0\rangle\langle 1|\sigma_b^B|1\rangle + \cancel{\langle 0|\sigma_z^A|1\rangle}\ 1|\sigma_b^B|0\rangle + \langle 1|\sigma_z^A|1\rangle\langle 0|\sigma_b^B|0\rangle + \cancel{\langle 1|\sigma_z^A|0\rangle}\ 0|\sigma_b^B|1\rangle\right)$$

$$= \frac{1}{2}\left(\langle 1|\sigma_b^B|1\rangle - \langle 0|\sigma_b^B|0\rangle\right) = -\cos\vartheta$$

where the last equation comes from the fact that $\sigma_b^B = \cos\vartheta\sigma_z^B + \sin\vartheta\sigma_\perp^B$.
II - Now we choose two other directions $\vec{a}'$ and $\vec{b}'$ each rotated by some angle φ with respect to the original directions. Then what we have done is a collective rotation of the coordinate frame, but we have seen already that the Bell state is unchanged by such a rotation. Thus by repeating the same analysis we will find that $\langle a'b'\rangle = \langle ab\rangle = -\cos\vartheta$.
III - Consider then the following experiment:
A can measure either $\vec{a}$ or $\vec{a}'$
B can measure either $\vec{b}$ or $\vec{b}'$
and we want to look at the correlation of the outcomes $\langle ab\rangle$, $\langle a'b\rangle$, $\langle ab'\rangle$ and $\langle a'b'\rangle$. The quantity we are interested in is actually $\langle S\rangle = \langle ab\rangle + \langle a'b'\rangle + \langle ab'\rangle - \langle a'b\rangle$. There are two possible strategies:
a) One can measure each correlation in separate experiments (i.e. we measure separately $\langle ab\rangle$ etc.). We then expect the results $\langle ab\rangle = -\cos\vartheta_{ab}$, $\langle a'b\rangle = -\cos\vartheta_{a'b}$ etc. and

$$S\rangle = -(\cos\vartheta_{ab} + \cos\vartheta_{a'b'} + \cos\vartheta_{ab'} - \cos\vartheta_{a'b})$$

b) One can look at the outcome of the quantity $S_k = (\sigma_a^A\sigma_b^B)_k + (\sigma_{a'}^A\sigma_{b'}^B)_k + (\sigma_a^A\sigma_{b'}^B)_k - (\sigma_{a'}^A\sigma_b^B)_k$ at each k^{th} experiment. Then the expectation value is $\ S\rangle = \lim_{N\to\infty}\frac{1}{N}\sum_k S_k$. Notice that this definition of the quantity S_k implies that even in experiments were we measure e.g. along $\vec{a}$ (i.e. we measure σ_a^A and not $\vec{a}'$, $\sigma_{z'}^A$ still has a well-defined value (realism). We can rewrite S_k as

$$S_k = \sigma_a^A(\sigma_b^B + \sigma_{b'}^B)_k - \sigma_{a'}^A(\sigma_b^B - \sigma_{b'}^B)_k$$

In each measurement, the possible results for σ_b^B are ± 1 (and the same for $\sigma_{b'}^B$) so that the possible outcomes for $\sigma_b^B + \sigma_{b'}^B$ are $\{0, +2, -2\}$ and the same for the difference. Whenever $\sigma_b^B + \sigma_{b'}^B = \pm 2$ we have however that $\sigma_b^B - \sigma_{b'}^B = 0$ and vice-versa. Thus the possible outcomes for S_k are $\pm 2\sigma_a$ or $\pm 2\sigma_{a'}$ or finally $S_k = \pm 2$ (since outcomes for σ_a are ± 1 and we assume that the act of measuring B does not change the outcome of A). Then, the expectation value for any possible choice of the axis direction is bounded by

$$-2 < \langle S\rangle < +2$$

If we now go back to the first strategy *a)* and choose as the measurement axes

$$\vec{a} = \vec{z}, \qquad \vec{a}' = \vec{x}, \qquad \vec{b} = \vec{z} - \vec{x}, \qquad \vec{b}' = \vec{z} + \vec{x}$$

we find :

$$\langle ab \rangle = -\cos\vartheta_{ab} = -1/\sqrt{2} \qquad \langle a'b' \rangle = -\cos\vartheta_{ab} = -1/\sqrt{2}$$
$$\langle ab' \rangle = -\cos\vartheta_{ab'} = -1/\sqrt{2} \qquad \langle a'b \rangle = -\cos\vartheta_{ab} = 1/\sqrt{2}$$

which yields

$$\langle S \rangle = \langle ab \rangle + \langle a'b' \rangle + \langle ab' \rangle - \langle a'b \rangle = -\frac{4}{\sqrt{2}} = -2\sqrt{2} < -2$$

Thus the two hypothesis that we assumed in *b)* to arrive at the conclusion $-2 < \langle S \rangle < +2$ must be wrong (or at least one of them: which one?)

References

• A. Einstein, B. Podolsky, and N. Rosen, *Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?* Phys. Rev. **47**, 777 - 780 (1935)
Abstract – In a complete theory there is an element corresponding to each element of reality. A sufficient condition for the reality of a physical quantity is the possibility of predicting it with certainty, without disturbing the system. In quantum mechanics in the case of two physical quantities described by non-commuting operators, the knowledge of one precludes the knowledge of the other. Then either (1) the description of reality given by the wave function in quantum mechanics is not complete or (2) these two quantities cannot have simultaneous reality. Consideration of the problem of making predictions concerning a system on the basis of measurements made on another system that had previously interacted with it leads to the result that if (1) is false then (2) is also false. One is thus led to conclude that the description of reality as given by a wave function is not complete.

• J. S. Bell, *On the Einstein Podolsky Rosen Paradox,* Physics **1**, 195-200 (1964)

• N.D. Mermin *Bringing home the atomic world: Quantum mysteries for anybody* American Journal of Physics, **49** (10), 940-943 (1981)
Abstract – A simple device is described, based on a version of Bell's inequality, whose operation directly demonstrates some of the most peculiar behavior to be found in the atomic world. To understand the design of the device one has to know some physics, but the extraordinary implications of its behavior should be evident to anyone. Except for a preface and appendix for physicists, the paper is addressed to the general reader.

• Alain Aspect, Philippe Grangier, and Gerard Roger, *Experimental Tests of Realistic Local Theories via Bell's Theorem*, Phys. Rev. Lett. **47**, 460 - 463 (1981)
Abstract – We have measured the linear polarization correlation of the photons emitted in a radiative atomic cascade of calcium. A high-efficiency source provided an improved statistical accuracy and an ability to perform new tests. Our results, in excellent agreement with the quantum mechanical predictions, strongly violate the generalized Bell's inequalities, and rule out the whole class of realistic local theories. No significant change in results was observed with source-polarizer separations of up to 6.5 m.

• Alain Aspect, Philippe Grangier, and Gerard Roger, *Experimental Realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: A New Violation of Bell's Inequalities*, Phys. Rev. Lett. **49**, 91 - 94 (1982)
Abstract – The linear-polarization correlation of pairs of photons emitted in a radiative cascade of calcium has been measured. The new experimental scheme, using two-channel polarizers (i.e., optical analogs of Stern-Gerlach filters), is a straightforward transposition of Einstein-Podolsky-Rosen-Bohm gedankenexperiment. The present results, in excellent agreement with the quantum mechanical predictions, lead to the greatest violation of generalized Bell's inequalities ever achieved.

6.6 Teleportation (Bennet, Peres, Brassard)

Two parties -Alice and Bob- want to transfer an unknow quantum state. They share a resource prior to the transfer, a pair of qubit in one of the Bell States, let say $|\Phi^+\rangle = (|00\rangle + |11\rangle)/2$. Alice possesses also another qubit in an unknow pure state $|\psi\rangle = a|0\rangle + b|1\rangle$, that she wishes to send to Bob. The circuit below shows the steps in the teleportation algorithm, starting with the gates that create the Bell State on the ancilla qubits.

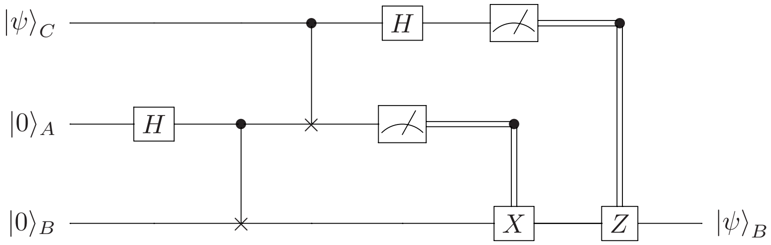

Fig. 10: Circuit for teleportation: the qubit $|\psi\rangle_C$ (initially in Alice's hands) is teleported to Bob ($|\psi\rangle_B$) by using two qubits in a Bell pair $|\Phi\rangle^+_{AB}$.

Alice then transforms her unknown qubit and her part of the shared pair to the Bell State basis by a cnot and a hadamard gate. She then measures them in this new basis and via a classical communication channel, tells the result of the measurement to Bob. Bob performs then an operation on his qubit (the second half of the entangled pair) based on whatever the measurement result was:

if $|00\rangle$ → do nothing
if $|01\rangle$ → σ_x
if $|10\rangle$ → σ_z
if $|11\rangle$ → $\sigma_x \sigma_z$

This operation leaves Bob's qubit in the same state of the one initially owned by Alice. Notice that no superluminal speed of information transmission is proven by quantum teleportation, since classical communication is needed. Also, no cloning of an unknown, arbitrary state is happening (which is forbidden by quantum mechanics), since the original state is destroyed in the process.
The state of the 3 qubits at each step is as follows:

1. $|\psi 00\rangle \xrightarrow{H_A} (|\psi 00\rangle + |\psi 10\rangle)/\sqrt{2}$ (with $|\psi\rangle = a|0\rangle + b|1\rangle$)
2. $\xrightarrow{C_A NOT_B} (|\psi 00\rangle + |\psi 11\rangle)/\sqrt{2} = |\psi\rangle\,|\Phi\rangle^+$
3. $\xrightarrow{C_B NOT_A} (a|000\rangle + b|110\rangle + a|011\rangle + b|101\rangle)/\sqrt{2}$
4. $\xrightarrow{H_C} \left[|00\rangle(a|0\rangle + b|1\rangle) + |01\rangle(a|1\rangle + b|0\rangle) + |10\rangle(a|0\rangle - b|1\rangle) + |11\rangle(a|1\rangle - b|0\rangle)\right]/2$
5. $\xrightarrow{Meas.+U_C} |\psi\rangle_B = a|0\rangle + b|1\rangle$

References

• A. Fedrizzi, R. Ursin, T. Herbst, M. Nespoli, R. Prevedel, T. Scheidl, F. Tiefenbacher, T. Jennewein & A. Zeilinger, *High-fidelity transmission of entanglement over a high-loss free-space channel*, Nature Physics **5**, 389 - 392 (2009)
Abstract – Quantum entanglement enables tasks not possible in classical physics. Many quantum communication protocols1 require the distribution of entangled states between distant parties. Here, we experimentally demonstrate the successful transmission of an entangled photon pair over a 144 km free-space link. The received entangled states have excellent, noise-limited fidelity, even though they are exposed to extreme attenuation dominated by turbulent atmospheric effects. The total channel loss of 64 dB corresponds to the estimated attenuation regime for a two-photon satellite communication scenario. We confirm that the received two-photon states are still highly entangled

by violating the Clauser-Horne-Shimony-Holt inequality by more than five standard deviations. From a fundamental point of view, our results show that the photons are subject to virtually no decoherence during their 0.5-ms-long flight through air, which is encouraging for future worldwide quantum communication scenarios.
Building on work done in:

- R. Ursin, et al (& A. Zeilinger), *Entanglement-based quantum communication over 144 km*, Nature Physics **3**, 481 - 486 (2007)

Abstract – Quantum entanglement is the main resource to endow the field of quantum information processing with powers that exceed those of classical communication and computation. In view of applications such as quantum cryptography or quantum teleportation, extension of quantum-entanglement-based protocols to global distances is of considerable practical interest. Here we experimentally demonstrate entanglement-based quantum key distribution over 144 km. One photon is measured locally at the Canary Island of La Palma, whereas the other is sent over an optical free-space link to Tenerife, where the Optical Ground Station of the European Space Agency acts as the receiver. This exceeds previous free-space experiments by more than an order of magnitude in distance, and is an essential step towards future satellite-based quantum communication and experimental tests on quantum physics in space.

- T. Schmitt-Manderbach, et al *Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km* Phys. Rev. Lett. **98**, 010504 (2007)

6.7 Deutsch-Jozsa algorithm

To illustrate the power of quantum computation, we present one of the simplest quantum algorithm, the Deutsch-Josza algorithm. The algorithm's goal is to decide whether a given function $f(x)$ is *constant* for all values of x or *balanced*, that is, equal to 1 for half of the values of x and to 0 for the other half. The goal is to make this decision with the minimum possible number of evaluations of the function value on trial x and with a given probability of arriving at the correct answer.
If the function f is defined on a space of dimension 2^n (i.e. x can be stored in a n-bit string), the classical algorithm can decide the function with at least $\frac{2^n}{2}+1$ queries, while the quantum one only needs one query. The steps of the algorithm are illustrated in the following picture, where $\mathbf{H}$ is the Hadamard gate and $\mathbf{U}_f$ is a unitary gate which transform the state $|x,y\rangle$ to $U_f|x,y\rangle = |x, y\oplus f(x)\rangle$ ($\oplus$ indicates the addition modulo 2).
In the case where f is a function from 1 bit to 1 bit, there are only 4 possible f, two constant and two balanced ($f_1(x)=1$, $f_2(x)=0$, $f_3(x)=x$, $f_4(x)=\bar{x}=NOTx$). Since U_f gives the sum $y\oplus x$, these functions correspond to the following U_i:

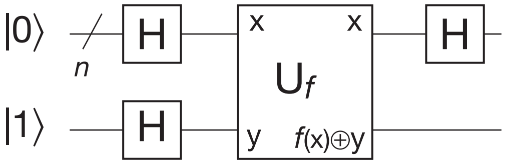

Fig. 11: Circuit implementing the Deutsch-Josza algorithm.

$$\begin{array}{lcl} f_1 & \rightarrow & U_1 = \mathbf{1}_x \otimes U_{Not,y} \\ f_2 & \rightarrow & U_2 = \mathbf{1}_x \otimes \mathbf{1}_y \\ f_3 & \rightarrow & U_3 = U_{CNot} \\ f_4 & \rightarrow & U_4 = U_{CNot}U_{Not,y} \end{array} \tag{2}$$

Deutsch's algorithm is a perfect illustration of all that is miraculous, subtle, and disappointing about quantum computers. It calculates a solution to a problem faster than any classical computer *ever* can. It illustrates the subtle interaction of superposition, phase-kick back, and interference. Finally, unfortunately, is solves a completely pointless problem.
We begin by illustrating how superposition of quantum state creates *quantum parallelism* or the ability to compute on many states simultaneously.

Given a function $f(x) : \{0,1\} \to \{0,1\}$ using a quantum computer, use two qubits $|x, y\rangle$ and transform them into $|x, y \oplus f(x)\rangle$ (where $\oplus$ represents addition modular two). We use two qubits since we wish to leave the input x or the query register, "un-changed". The second qubit, y, acts as a result register. Let U_f be the unitary transform that implements this.

Suppose we wish to calculate $f(0)$, then we could input x as $|0\rangle$, and y, our output register, as $|0\rangle$ and apply the U_f transform, to obtain $|0\rangle \otimes |0\rangle = |0,0\rangle \to |0, 0 \oplus f(0)\rangle$. If instead we want to calculate $f(1)$, then we could input x as $|1\rangle$, yielding the transformation : $|1\rangle \otimes |0\rangle = |1,0\rangle \to |1, 0 \oplus f(1)\rangle$. In a quantum computer we can actually query the results of 0 and 1 simultaneously using quantum parallelism. For this, let x equal $(|0\rangle + |1\rangle)/\sqrt{2}$ and y equal 0. From the input $|\psi_1\rangle = \frac{|0,0\rangle + |1,0\rangle}{\sqrt{2}}$ we obtain the output $|\psi_2\rangle = \frac{|0,f(0)\rangle + |1,f(1)\rangle}{\sqrt{2}}$. U_f is applied to $|0\rangle$ and $|1\rangle$ simultaneously. This is known as quantum parallelism but there is still a problem since measurement produces either $|0, f(0)\rangle$ or $|1, f(1)\rangle$. Hence we need to be clever about what type of question we ask, and how we go about extracting the answer. For this we use the circuit in the figure, which exploits another quantum mechanical property: *interference*.

The initial state is $|\psi_0\rangle = |0,1\rangle$. We then apply the H gate to the query and result registers to obtain: $|\psi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

Now, let's examine $y \oplus f(x)$:

Suppose $f(x) = 0$. Then $y \oplus f(x) = y \oplus 0 = \frac{1}{\sqrt{2}}(|0 \oplus 0\rangle - |1 \oplus 0\rangle) = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

Suppose $f(x) = 1$. Then $y \oplus f(x) = y \oplus 1 = \frac{1}{\sqrt{2}}(|0 \oplus 1\rangle - |1 \oplus 1\rangle) = \frac{1}{\sqrt{2}}(-|0\rangle + |1\rangle)$

We can compactly describe this behavior as $y \oplus f(x) = (-1)^{f(x)}\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

Thus, U_f transforms $|x\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ into:

$(-1)^{f(x)}|x\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

Or we can say that:

$U_f\left[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right] = \frac{1}{2}\left[(-1)^{f(0)}|0\rangle(|0\rangle - |1\rangle) + (-1)^{f(1)}|1\rangle(|0\rangle - |1\rangle)\right]$

Suppose f is constant, that is $f(0) = f(1)$, then:

$U_f\left[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right] = \pm\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

Suppose instead that f is balanced, that is $f(0) \neq f(1)$, then:

$U_f\left[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right] = = \pm\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

Now apply the Hadamard gate to the first qubit. Just before the measurement the system is in the state

$$|\psi_f\rangle = \begin{cases} \pm\frac{1}{\sqrt{2}}|0\rangle(|0\rangle - |1\rangle) & \text{if} \quad f(0) = f(1) \\ \pm\frac{1}{\sqrt{2}}|1\rangle(|0\rangle - |1\rangle) & \text{if} \quad f(0) \neq f(1) \end{cases}$$

Since in our case $f(0) \oplus f(1) = 0 \Leftrightarrow f(0) = f(1)$ we can write this as $|\psi_f\rangle = \pm|f(0) \oplus f(1)\rangle\left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right]$ Hence it is possible to measure the first qubit to find $f(0) \oplus f(1)$.

The Deutsch-Jozsa algorithm is a generalization of Deutsch's algorithm to a function $f(x) : \{2^n\} \to \{0,1\}$ that f is either constant or balanced. The algorithm just generalize to a larger number of qubits.

22.51 Quantum Theory of Radiation Interactions
Fall 2012