# Quantum entanglement

**Maciej Lewenstein**

Maciej Lewenstein has obtained his degree in Physics from Warsaw University. From 1980 he worked at the Center for Theoretical Physics of the Polish Academy of Sciences. He received his doctoral degree in 1983 at the University of Essen and habilitation in 1986 in Warsaw. He became a full Professor in Poland in 1993. In 1995 he joined "Service de Photones, Atomes et Molecules" of CEA in Saclay. In 1998 he became a full professor and a head of the quantum optics theory group at the University of Hannover. In 2005 he started a new theory group at the "Insitut de Ciencias Fotoniques" in Barcelona. His research interests include: quantum optics, quantum information and statistical physics.

**Chiara Macchiavello**

Chiara Macchiavello finished her degree in Physics in 1991 and her PhD in 1995 at the University of Pavia. She held a post-doctoral for two years at the University of Oxford. Since 1998 she has been an Assistant Professor at the University of Pavia. Her research interests include quantum information processing and quantum optics.

**Dagmar Bruss**

Since 2003 Dagmar Bruss is a professor at the Institute of Theoretical Physics at the University of Duesseldorf, Germany. Her research interests include the foundations of quantum information theory, classification of entanglement and quantum optical implementations of quantum computation.

## Abstract
Entanglement is a fundamental resource in quantum information theory. It allows performing new kinds of communication, such as quantum teleportation and quantum dense coding. It is an essential ingredient in some quantum cryptographic protocols and in quantum algorithms. We give a brief overview of the concept of entanglement in quantum mechanics, and discuss the major results and open problems related to the recent scientific progress in this field.


## Introduction
Entanglement is a property of the states of quantum systems that are composed of many parties, nowadays frequently called Alice, Bob, Charles etc. Entanglement **expresses particularly strong correlations between these parties,** persistent even in the case of large separations among the parties, and going beyond simple intuition.

Historically, the concept of entanglement goes back to the famous **Einstein-Podolski-Rosen (EPR) "paradox"**. Einstein, who discovered relativity theory and the modern meaning of causality, was never really happy with quantum mechanics. In his opinion every reasonable physical theory should exhibit a so called local realism.

Suppose that we consider two particles, one of which is sent to Alice and one to Bob, and we perform independent local measurements of "reasonable" physical observables on these particles. Of course, the results might be correlated, because the particles come from the same source. But Einstein wanted really to restrict the correlations for "reasonable" physical observables to the ones that result from statistical distributions of some hidden (i.e. unknown to us and not controlled by us) variables that characterize the source of the particles. Since quantum mechanics did not seem to produce correlations consistent with a local hidden variable (LHV) model, Einstein concluded that quantum mechanics is not a complete theory. Erwin Schrödinger, in answer to Einstein's doubts, introduced in 1935 the term "Verschränkung" (in English "entanglement") in order to describe these particularly strong quantum mechanical correlations.

Entanglement was since then a subject of intense discussions among experts in the foundations of quantum mechanics and philosophers of science (and not only science). It took, however, nearly 30 years until John Bell was able to set the framework for experimental investigations on the question of local realism. Bell formulated his famous inequalities, which have to be fulfilled in any multiparty system described by a LHV model. Alain Aspect and coworkers in Paris have demonstrated in their seminal experiment in 1981 that **quantum mechanical states violate these inequalities**. Recent very precise experiments of Anton Zeilinger's group in Vienna confirmed fully Aspect's demonstrations. **All these experiments indicate the correctness of quantum mechanics**, and despite various loopholes, they exclude the possibility of LHV models describing properly the physics of the considered systems.

Entanglement has become again the subject of cover pages news in the 90's, when quantum information was born. It was very quickly realized that **entanglement is one of the most important resources for quantum information processing**. Entanglement is a necessary ingredient for quantum cryptography, quantum teleportation, quantum dense coding, and if not necessary, then at least a much desired ingredient for quantum computing.

At the same time the theory of entanglement is related to some of the open questions of mathematics, or more precisely linear algebra and functional analysis. A solution of the entanglement problem could help to characterize the so called positive linear maps, i.e. linear transformations of positive definite operators (or physically speaking quantum mechanical density matrices, see below) into positive definite operators.

## Entanglement of pure states

In quantum mechanics (QM) a state of a quantum system corresponds to a vector |Psi> in some vector space, called **Hilbert space**. Such states are called **pure states**. One of the most important properties of QM is that **linear superpositions** of state-vectors are also legitimate state-vectors. **This superposition principle lies at the heart of the matter-wave dualism and of quantum interference phenomena.**

Entanglement is also a result of superposition, but in the composite space of the involved parties. Let us for the moment focus on two parties, Alice and Bob. It is then easy to define states which are not entangled. Such states are product states of the form $|\Phi\rangle = |a\rangle|b\rangle$, i.e. Alice has at her disposal $|a\rangle$, while Bob has $|b\rangle$. Product states obviously carry no correlations between Alice and Bob. **Entangled pure states may be now defined as those which are superpositions of at least two product states, such as**

$$|\Phi\rangle = \alpha_1|a_1\rangle|b_1\rangle + \alpha_2|a_2\rangle|b_2\rangle + \text{etc.}$$

but cannot be written as a single product state in any other basis. All entangled pure states contain strong quantum mechanical correlations, and do not admit LHV models.

## Entanglement of mixed states and the separability problem

Verify whether a given state-vector is a product state or not is a relatively easy task. In practice, however, we often either do not have full information about the system, or are not able to prepare a desired state perfectly. In effect in everyday situations we deal practically always with statistical mixtures of pure states. There exists a very convenient way to represent such mixtures as so called density operators, or matrices. A density matrix rho corresponding to a pure state-vector $|\Phi\rangle$ is a projector onto this state. More general density matrices can be represented as sums of projectors onto pure state-vectors weighted by the corresponding probabilities.

The definition of entangled mixed states for composite systems has been formulated by Reinhard Werner from Braunschweig in 1989. In fact, this definition determines which states are not entangled. Non-entangled states, called separable states, are mixtures of pure product states, i.e. convex sums of projectors onto product vectors:

$$\rho = \Sigma_i\, p_i|a_i\rangle|b_i\rangle\langle a_i|\langle b_i|, \qquad (*)$$

where $0 \leq p_i \leq 1$ are probabilities, i.e. $\Sigma_\iota\ p_i = 1$. The physical interpretation of this definition is simple: a separable state can be prepared by Alice and Bob by using local operations and classical communication. Checking whether a given state is separable or not is a notoriously difficult task, since one has to check whether the decomposition (*) exists or not. This difficult problem is known under the name of "separability or entanglement problem", and has been a subject of intensive studies in the recent years.

## Simple entanglement criteria

The difficulty of the separability problem comes from the fact that rho admits in general an infinite number of decompositions into a mixture of some states, and one has to check whether among them there exists at least one of the form (*). One of the most powerful necessary conditions for separability has been found by one of the fathers of quantum information, the late Asher Peres. Peres (Technion, Haifa) observed that since Alice and Bob may prepare separable states using local operations, Alice may safely reverse the time arrow in her system, which will change the state, but will not produce something unphysical. In general, such a partial time reversal is not a physical operation, and can transform a density operator (which is positive definite) into an operator that is no more positive definite. In fact this is what happens with all pure entangled states. Mathematically speaking partial time reversal corresponds to partial transposition of the density matrix (only on Alice's side). We arrive in this way at the Peres criterion: ***If a state*** $\rho$ ***is separable then its partial transposition has to be positive definite.*** This criterion is usually called positive partial transpose condition, or shortly PPT condition. Amazingly, the PPT condition is not only necessary for separability, but it is also a sufficient condition for low dimensional systems such as two qubits (dimension 2x2)and a system composed of one qubit and one qutrit (dimension 2x3). In higher dimensions, starting from 2x4 and 3x3, this is no longer true: there exist entangled states with positive partial transpose, which are called PPT entangled states.

There exist several other necessary or sufficient separability criteria which have been established and frequently discussed in recent years. For example, states that are close to the completely chaotic state (whose density operator is equal to the normalized identity) are necessarily separable. There exist also other criteria that employ entropic inequalities, uncertainty relations, or an appropriate reordering of the density matrix (so called realignment criterion) etc. There exists, however, no general simple operational criterion of separability that would work in systems of arbitrary dimension.

## Entanglement witnesses

The set of all states P is obviously compact and convex. If $\rho_1$ and $\rho_2$ are legitimate states, so is their convex mixture. The set of separable states S is also compact and convex (see **Figure 1**). From the theory of convex sets and Hahn-Banach theorem we conclude that for any entangled state there exists a hyperplane in the space of operators separating rho from S. Such a hyperplane defines uniquely a Hermitian operator W (observable) which has the following properties: The expectation value of W on all separable states, $\langle W \rangle \geq 0$, whereas its expectation value on $\rho$ is negative, i.e. $\langle W \rangle_\rho < 0$.

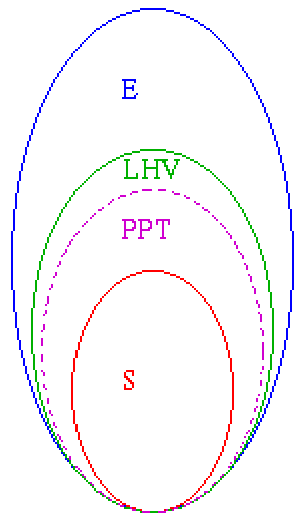


**Figure 1**

Such an observable is for obvious reasons called entanglement witness, since it "detects" the entanglement of $\rho$. Every entangled state has its witnesses; the problem obviously is to find appropriate witnesses for a given state. To find out whether a given state is separable one should check whether its expectation value is non-negative for all witnesses. Obviously this is a necessary and sufficient separability criterion, but unfortunately it is not operational, in the sense that there is no simple procedure to test for all witnesses.

Nevertheless, witnesses provide a very useful tool to study entanglement, especially if one has some knowledge about the state in question. They provide a sufficient entanglement condition, and may be obviously optimized (see **Figure 2**) by shifting the hyperplane in a parallel way towards S.

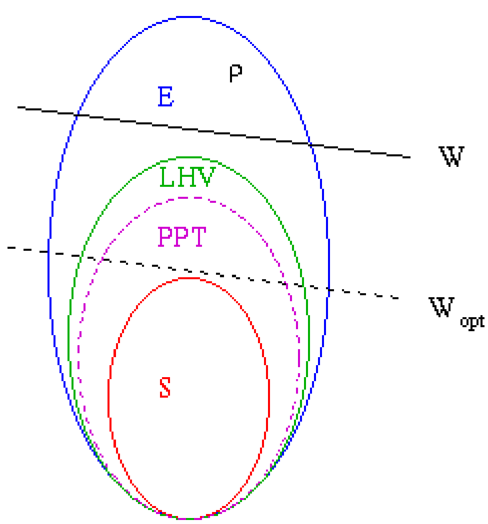


**Figure 2**

## Bell inequalities

After introducing the concept of separability and entanglement for mixed states, it is legitimate to ask what is the relation of mixed state entanglement and the existence of a LHV model, which requires that the state cannot violate any of the Bell-like inequalities. Let us discuss an example of such inequalities, the so called Clauser-Horne-Shimony-Holt inequality for two qubits. Let us assume that Alice and Bob measure two binary observables each, namely $A_1$, $A_2$, and $B_1$, $B_2$. The observables are random variables taking the values +1 or – 1, correlated possibly through some dependence on local hidden variables. It is easy to see that in the classical world, if $B_1 + B_2$ is zero, then $B_1 - B_2$ is either +2 or −2, and vice versa. Therefore if we define $s = A_1(B_1 + B_2) + A_2(B_1 - B_2)$, we obtain that $2 \geq s \geq -2$. This inequality holds also after averaging over various realizations. On the other hand, it can be shown that by taking suitable sets of observables for Alice and Bob we can find pure and even mixed quantum states that violate this inequality.

Are Bell-like inequalities similar in this respect to witnesses, i.e. for a given entangled state can one always find a Bell-like inequality that "detects" it? The answer to this question is no, and has been already given by R. Werner in 1989. Even for two qubits there exist entangled states that admit an LHV model, i.e. cannot violate any Bell-like inequality.

This observation indicates already that there is more structure in the "eggs" of **Figure 1** and **Figure 2**. Separable states are evidently inside the PPT egg, according to the Peres condition. They admit an LHV model, i.e. they are also inside the LHV egg. But what about PPT entangled states? Do they violate some Bell-like inequality? Peres has formulated a conjecture that this not the case, and there is a lot of evidence that this conjecture is correct, although a rigorous proof is still missing.

## The distillability problem and bound entanglement

**Above we have classified quantum states according to the property of being either separable or entangled.** An alternative classification approach is based on the possibility of distilling the entanglement of a given state. In a distillation protocol the entanglement of a given state is increased by performing local operations and classical communication on a set of identically prepared copies. In this way one obtains fewer, but "more entangled", copies. This kind of technique was originally proposed in 1996 by Bennett and coworkers in the context of quantum teleportation, in order to achieve faithful transmission of quantum states over noisy channels. It also has applications in quantum cryptography as a method for quantum privacy amplification in entanglement based protocols in the presence of noise, as pointed out by David Deutsch and coworkers from Oxford.

The distillability problem poses the question whether a given quantum state can be distilled or not. A separable state can never be distilled because the average entanglement of a set of states cannot be increased by local operations. Furthermore, the positivity of the partial transpose ensures that no distillation is possible. Thus, a given PPT entangled state is not distillable, and is therefore called bound entangled. There may even exist undistillable entangled states which do not have the PPT property. However, this conjecture is not proved at the moment.

The first example of a PPT entangled state has been found by Pawel Horodecki from Gdansk in 1997. These states are so called edge states, which means that they cannot be written as a mixture of a separable state and a PPT entangled state. Particularly simple families of states have been suggested by Charles Bennett and coworkers at IBM, New York. They have found the so called unextendible product bases (UPB), i.e. sets of orthogonal product state-vectors, with the property that the space orthogonal to this set does not contain any product vector. It turns out that the projector onto this space is a PPT state, which obviously has to be entangled since it does not contain any product vector in its range (note that all state-vectors in the decomposition of a separable state $\rho$ into a mixture of product states belong automatically to the range of $\rho$).

The existence of bound entanglement is a mysterious invention of Nature. It is an interesting question to ask whether bound entanglement is a useful resource to perform quantum information processing tasks. It was shown so far that this is not the case for communication protocols such as quantum teleportation and quantum dense coding (i.e. a protocol that allows to enhance the transmission of classical information, using entanglement). However, surprisingly, it is possible to distill a secret key in quantum cryptography, starting from certain bound entangled states.

## Entanglement detection

As discussed above, entanglement is a precious resource in quantum information processing. Typically in a real world experiment noise is always present and it leads to a decrease of entanglement in general. Thus, it is of fundamental interest for experimental applications to be able to test the entanglement properties of the generated states. A traditional method to this aim is represented by the Bell inequalities, a violation of which indicates the presence of entanglement. However, as mentioned above, not every entangled state violates a Bell inequality. So, not all entangled states can be detected by using this method. Another possibility is to perform complete state tomography, which allows determining all the elements of the density matrix. This is a useful method to get a complete knowledge of the density operator of a quantum system, but to detect entanglement it is an expensive process as it requires an unnecessary large number of measurements. If one has certain knowledge about the state the most appropriate technique is the measurement of the witness observable, which can be achieved by few local measurements. A negative expectation value clearly indicates the presence of entanglement.

All these methods have been successfully implemented in various experiments. Recently another method for the detection of entanglement was suggested based on the physical approximation of the partial transpose. It remains a challenge to implement this idea in the laboratory because it requires the implementation of non local measurements.

## Entanglement measures

When classifying a quantum state as being entangled, a natural question is to **quantify the amount of entanglement** it contains. For pure quantum states there exists a well defined entanglement measure, namely the von Neumann entropy of the density operator of a subsystem of the composite state. For mixed states the situation is more complicated. There are several different possibilities to define an entanglement measure. The so called entanglement cost describes the amount of entanglement one needs in order to generate a given state. An alternative measure is the entanglement of formation, which is a more abstract definition. A further possibility to quantify entanglement is given by the minimum distance to separable states. Finally, motivated by physical applications, one can introduce the distillable entanglement which quantifies the extractable amount of entanglement.

Unfortunately all of these quantities are very difficult to compute in general. For example, in order to determine the entanglement of formation one has to find the decomposition of the state that leads to the minimum average von Neumann entropy of a subsystem and this is a very challenging task. So far a complete analytical formula for the entanglement of formation only exists for composite systems of two qubits.

## Entanglement in multipartite systems

So far, we have restricted ourselves to the case of composite systems with two subsystems, so called bipartite systems. When considering more than two parties, i.e multipartite systems, the situation becomes much more complex. For example, for the most simple tripartite case of three qubits, a pure state can be either completely separable, or biseparable (i.e. one of the three parties is not entangled with the other two), or genuinely entangled among all three parties. The latter class again consists of inequivalent subclasses, the so called GHZ and W states. This concept can be generalized to mixed states. For more than three parties it is easy to imagine that the number of subclasses grows fast.

In recent years there has been much progress in the creation of multipartite entangled states in the laboratory. The existence of genuine multipartite entanglement has also been demonstrated experimentally by using the concept of witness operators.

Even if the full classification of multipartite entanglement is a formidable task, certain classes of states, the so called graph states, have been completely characterized and shown to be useful both for quantum computational and quantum error correction protocols. Moreover, a deeper understanding of entanglement has proved to be very fruitful in connection with statistical properties of physical systems. All of these problems are discussed in more details in other sections of this publication.

## References

**[1]** Einstein, P. Podolsky and N. Rosen, Phys. Rev. **47**, 777 (1935)
**[2]** J.S. Bell, Physics **1**, 195 (1964)
**[3]** P. Horodecki, Phys. Lett. A **232**, 333 (1997)
**[4]** M. Lewenstein et al., J. Mod. Opt. **47**, 2481 (2000)
**[5]** A. Peres, Phys. Rev. Lett. **77**, 1413 (1996)

**[6]** E. Schrödinger, Naturwissenschaften **23**, 807 (1935)
**[7]** R.F. Werner, Phys. Rev. A **40**, 4277 (1989)

**Contact information of the author of this article**

Maciej Lewenstein
Institut de Ciènces Fotòniques (ICFO)
C/Jordi Girona 29, Nexus 29
08034 Barcelona
Spain
Email: maciej.lewenstein@icfo.es

Chiara Macchiavello
Istituto Nazionale di Fisicadella Materia, Unita' di Pavia
Dipartimento di Fisica "A. Volta"
via Bassi 6
I-27100 Pavia
Italy
Email: chiara@unipv.it

Prof. Dr. Dagmar Bruss
Inst. fuer Theoretische Physik III
Heinrich-Heine-Universitaet Duesseldorf
Universitaetsstr. 1, Geb. 25.32
D-40225 Duesseldorf,
Germany
Email: bruss@thphy.uni-duesseldorf.de