Quantum Information Theory and Geometry of Quantum States

M. Kuś

Centrum Fizyki Teoretycznej, Polska Akademia Nauk
al. Lotników 32/46, 02-668 Warszawa, Poland

(Received November 5, 2001)

The advantages of quantum information processing and transmission over corresponding classical operations are connected to the existence in composite quantum-mechanical systems states without classical counterparts — the so-called entangled states. The paper shows and examines various applications of entangled states in the quantum information theory. Recent results connected with characterization and geometry of entangled states are examined with the emphasis on some unsolved mathematical problems.

PACS numbers: 03.65.Ud, 03.67.–a

1. Introduction

One of the most spectacular and interesting achievements of quantum mechanics in the last years of twentieth century was the theory of quantum computation. A fully operational quantum computer exists until now only on paper in the form of various ideas of theoretical physicist, and we are still, it seems, quite far from a practical construction, but the theory itself poses many challenging and unsolved problems, extremely interesting from the point of view of fundamentals of quantum mechanics.

The promises of quantum information theory encompass such things as exponential speed up of computations [1], absolutely secure communication [2, 3], faster data search [4], more effective information transmission [5], and other equally spectacular phenomena like e.g. quantum teleportation [6]. It is thus quite natural to ask about properties of quantum-mechanical systems, distinguishing them from their classical counterparts, which are responsible for the advantages of quantum computers and quantum communication channels. Although an exhaustive answer

is by no means neither straightforward nor unique, one observes that in nearly all above mentioned applications, the prominent role is played by the phenomenon of entanglement — a property of quantum systems not present on the classical level.

In the rest of the paper we shall define entangled states, exhibit the roles played by them in various applications in quantum information theory and finally concentrate on their properties and criteria allowing to distinguish them among all other "not-so-interesting" quantum states.

2. Entangled states

Each system pretending to become useful in transmission or processing of quantum information consists of (usually many) subsystems. States of each subsystem encode parts of information to be processed through subsequent transformations according to rules of quantum mechanics. So far this parallels exactly classical information processing and it is not clear where from the advantages of quantum computing should come. The main difference is in the structure of space of states of composite system between classical and quantum systems.

In most applications which will be interesting for us in the following, quantum systems are characterized in terms of states in finite-dimensional Hilbert spaces — one should think of some generalized spin systems as models of them. Hence in fact the corresponding Hilbert space is simply a many-dimensional complex space ($\mathcal{H} = \mathrm{C}^N$, say), with the natural scalar product $\langle\cdot|\cdot\rangle$ structure. The complete characterization of a state of the system is given by a density matrix ρ, i.e. a Hermitian ($\rho^\dagger = \rho$), positive-definite ($\langle x|\rho|x\rangle \geq 0$ for each $|x\rangle \in \mathcal{H}$), trace-one ($\mathrm{Tr}\rho = 1$) operator acting on $\mathcal{H}$ ($\rho : \mathcal{H} \to \mathcal{H}$). Knowing ρ we can calculate expectation value of any observable represented by a Hermitian operator A as

$$\langle A\rangle = \mathrm{Tr}A\rho. \tag{2.1}$$

A particular situation occurs when the state ρ is a projection operator

$$\rho = \rho^2, \tag{2.2}$$

so the eigenvalues of ρ are equal to 0 or 1. Since, from the definition, $\mathrm{Tr}\rho = 1$, only one eigenvalue equals 1, and the operator ρ is a projection on a one-dimensional space

$$\rho = |\psi\rangle\langle\psi|. \tag{2.3}$$

In this case the state is called *pure* and is customary identified with the vector $|\psi\rangle \in \mathcal{H}$ (we assume $\| \psi \|^2 := \langle\psi|\psi\rangle = 1$ and identify vectors differing by a phase factor). The expectation value of an observable A in a pure state ψ (2.1) reads thus

$$\langle A\rangle = \mathrm{Tr}\,(A|\psi\rangle\langle\psi|) = \langle\psi|A|\psi\rangle. \tag{2.4}$$

All states which are not pure (i.e. do not fulfill (2.2)) are called *mixed*.

Let us observe that states form a convex set in the space of all linear operators acting on $\mathcal{H}$, i.e. when ρ_1 and ρ_2 are states (i.e. Hermitian, positive definite, trace-one operators), so is their convex linear combination

$$\rho := \alpha_1\rho_1 + \alpha_2\rho_2, \tag{2.5}$$

with $\alpha_1,\ \alpha_2$ real and positive and $\alpha_1+\alpha_2 = 1$. Invoking the spectral decomposition of an arbitrary density matrix ρ we can write it as a convex combination of pure states

$$\rho = \sum_{i=1}^{N} \lambda_i |\psi_i\rangle\langle\psi_i|, \tag{2.6}$$

$$\lambda_i \geq 0, \tag{2.7}$$

$$\sum_{i=1}^{N} \lambda_i = 1, \tag{2.8}$$

where λ_i are the eigenvalues of ρ with the corresponding, normalized eigenvectors $|\psi_i\rangle$ and (2.7), (2.8) are consequences of positivity and the trace-one conditions respected by ρ.

Let us consider now two quantum systems A and B described by the states in, respectively, Hilbert spaces $\mathcal{H}_A = \mathrm{C}^{\mathcal{M}}$ and $\mathcal{H}_B = \mathrm{C}^{\mathcal{N}}$. The Hilbert space of the composite system $A+B$ is the tensor product of $\mathcal{H}_A$ and $\mathcal{H}_B$

$$\mathcal{H} := \mathcal{H}_{A+B} = \mathcal{H}_A \otimes \mathcal{H}_B, \tag{2.9}$$

and its states are operators acting in $\mathcal{H}$.

Let us, for the moment, limit our attention to the pure states of the composite system. If $|\psi_1\rangle$ and $|\psi_2\rangle$ are pure states of the system A whereas $|\phi_1\rangle$ and $|\phi_2\rangle$ — pure states of B, then, in principle*

$$|\Psi\rangle := \alpha|\phi_1\rangle \otimes |\psi_1\rangle + \beta|\phi_2\rangle \otimes |\psi_2\rangle, \quad |\alpha|^2 + |\beta|^2 = 1 \tag{2.10}$$

is a state of the composite system $A+B$. More generally, if $\{|e_i\rangle\}_{i=1}^{M}$ and $\{|f_i\rangle\}_{i=1}^{N}$ are bases in $\mathcal{H}_A$ and $\mathcal{H}_B$, then each vector (pure state) in $\mathcal{H}$ can be written as

$$|\psi\rangle = \sum_{ij} c_{ij}|e_i\rangle \otimes |f_j\rangle, \tag{2.11}$$

with some complex coefficients c_{ij}.

It is now clear that quantum mechanics admits more states for a composite system than the classical physics. Indeed, in the classical case if states of the subsystem A and B are described by sets coordinates $\{x_\mu^{(A)}\}$ and $\{x_\nu^{(B)}\}$ (e.g. phase-space canonical variables), then the state of the composite system is characterized by the set of coordinates $\{x_\mu^{(A)}, x_\nu^{(B)}\}$. It means that the (phase-)space of the composite system has the structure of the Cartesian product of the spaces of

*barring superselection rules

the subsystems, rather than the tensor product of the quantum case. The so-called product states of the form

$$|\Psi\rangle = |\psi\rangle \otimes |\phi\rangle, \quad |\psi\rangle \in \mathcal{H}_A, \quad |\phi\rangle \in \mathcal{H}_B \tag{2.12}$$

have their counterparts on the classical level, whereas all other quantum states lack classical interpretation. States fulfilling (2.12) are also called *separable*, all other states, i.e. those which cannot be written as simple tensors (tensor products of two states) but rather as nontrivial linear combinations of products like (2.12) go under the name of *entangled* states.

Entangled states together with their non-classical, and to some extent, paradoxical properties came to prominence already in 1935 with the publication of the famous paper "Can quantum-mechanical description of physical reality be considered complete" by Albert Einstein, Boris Podolsky, and Nathan Rosen [7]. In a version of the argument later proposed by Bohm [8] a molecule containing two atoms in a state with the zero total spin, with the spin of each atom equal to $\hbar/2$, disintegrates without changing the total angular momentum, and the atoms separate and cease to interact any longer. The spin degrees of freedom of the atoms are described by the singlet (entangled!) wave function

$$\frac{1}{\sqrt{2}}\left(|+\rangle_1 \otimes |-\rangle_2 - |-\rangle_1 \otimes |+\rangle_2\right), \tag{2.13}$$

where the obvious notation for the "spin-up" and "spin-down" states of the individual atoms were used. A measurement of a particular spin component of one atom gives with certainty the outcome of the measurement of the same component of the spin for the other one without any need of actually performing the second measurement. Now, according to Einstein, Rosen, and Podolsky: *If, without in any way disturbing a system, we can predict with certainty (i.e. with a probability equal to unity) the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity.* In this sense, the particular value of the chosen spin component of the second atom must be *the element of physical reality*, since we can predict it without disturbing the atom, moreover it existed in the second atom even before the measurement, since at the moment of the measurement the atoms are separated and do not interact. The paradox appears if we realize that we could have chosen to measure an orthogonal component of the spin of the first atom, thus coming to the conclusion that the corresponding value for the second atom is also *the element of physical reality* existing in the second atom even before the measurement. But according to quantum mechanics we cannot specify with certainty two orthogonal components of spin, the quantum-mechanical description must be, according to Einstein, Podolsky, and Rosen, incomplete.

Although in our opinion, apart from the final conclusion, the argument touches the heart of the matter concerning differences between classical and quantum physics, it can be easily blurred by deliberating the notion of physical reality

etc., locality etc. Fortunately in a beautiful paper [9], Bell showed that existence of entangled states has measurable consequences not predictable by any reasonable classical theory. The argument can be shortly summarized as follows [10]. Let us measure the spin component of the first atom along the directions $\boldsymbol{e}_1$, $\boldsymbol{e}_2$ at angles 0 and $\pi/2$ and the components of the second atom spin along $\boldsymbol{f}_1$, $\boldsymbol{f}_2$ at angles $\pi/4$ and $3\pi/4$ (all in the same plane). Let us calculate the following correlation function for the above measurements:

$$E(\boldsymbol{e}_i, \boldsymbol{f}_j) = P_{++}(\boldsymbol{e}_i, \boldsymbol{f}_j) + P_{--}(\boldsymbol{e}_i, \boldsymbol{f}_j) - P_{+-}(\boldsymbol{e}_i, \boldsymbol{f}_j) - P_{-+}(\boldsymbol{e}_i, \boldsymbol{f}_j), \tag{2.14}$$

where $P_{\pm,\pm}(\boldsymbol{e}_i, \boldsymbol{f}_j)$ is the probability of measuring $\pm\hbar/2$ along $\boldsymbol{e}_i$ and, at the same time, $\pm\hbar/2$ along $\boldsymbol{f}_j$. Straightforward quantum-mechanical calculations give

$$S := E(\boldsymbol{e}_1, \boldsymbol{f}_1) - E(\boldsymbol{e}_1, \boldsymbol{f}_2) + E(\boldsymbol{e}_2, \boldsymbol{f}_1) + E(\boldsymbol{e}_2, \boldsymbol{f}_2) = -2\sqrt{2}. \tag{2.15}$$

The same calculation can be done on a classical level. "Classical" means here that we think of quantum mechanics as a statistical theory, where the full characterization of the state of quantum-mechanical system is given in terms of some "hidden" classical variables and quantum-mechanical probabilities are expressible in terms of (unknown) classical probability distributions of the hidden variables. It can be shown that, independently on the distribution of hidden variables, the classical expectation value of S must fulfill

$$-\sqrt{2} \leq S \leq \sqrt{2}, \tag{2.16}$$

in a clear contradiction with (2.15). The experiments of Aspect et al. [11] performed on correlated photon pairs rather than spins, confirmed the above predictions of quantum theory.

As already mentioned, entangled states play also a prominent role in nearly all proposed applications of quantum information theory. Few examples below will confirm this statement.

2.1. Quantum computing

Undoubtedly, the result of Shor, who showed that notoriously hard problem of factorizing big numbers into their prime factors can be solved efficiently (i.e. exponentially faster than with the help of a classical computer) [1], was the most spectacular and striking achievements of the theory of quantum computing. The fact that quantum computers can perform some tasks much faster than classical ones was shown, for the first time, by Deutsch and Jozsa [12]. Below we follow the reasoning and notation of Vedral and Plenio [13]. Let us suppose that we are given a computer which calculates values of a function transforming the two-element set $\{0, 1\}$ into itself

$$f : \{0, 1\} \rightarrow \{0, 1\}. \tag{2.17}$$

Obviously, there are four such (distinct) functions: two of them are constant taking always value 0 or 1 independently on the argument, two are not constant having

distinct values for the arguments 0 and 1. Let us suppose further that we want to check to which class the function computed by our device belongs, i.e. whether it is constant or not constant function. Definitely we have to run our computer twice: first let it calculate the value at 0 and then at 1. Only after the second run of the computer we can answer the question. However, quantum mechanics gives the method answering the question by performing the calculation of $\boldsymbol{f}$ only once! To this end we shall represent the digits of input and output as states of a two-level quantum system (so-called qubits), for example spin 1/2 particle. We shall need two such qubits, to achieve the goal. Let us choose some basis in the two-dimensional space of a qubit and denote the orthonormal basis states (e.g. two states with opposite projection of the spin on a chosen axis) by $|0\rangle$ and $|1\rangle$. They will represent digits 0 and 1 in our computation. The actual computation of the function f by our quantum computer consists of the following transformation of two qubits:

$$|x\rangle \otimes |y\rangle \mapsto |x\rangle \otimes |[y + f(x)]\mathrm{mod}2\rangle, \tag{2.18}$$

achieved by some quantum-mechanical manipulation of spins. If we now prepare the input in the state (we dismiss unimportant normalization factors in the following):

$$|\psi\rangle \ := \ |0\rangle \otimes |0\rangle - |0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle - |1\rangle \otimes |1\rangle, \tag{2.19}$$

we obtain after the quantum-mechanical evolution (2.18):

$$|\Psi\rangle = |0\rangle \otimes |f(0)\rangle - |0\rangle \otimes |\overline{f(0)}\rangle + |1\rangle \otimes |f(1)\rangle - |1\rangle \otimes |\overline{f(1)}\rangle, \tag{2.20}$$

where $\overline{x} = (x+1)\mathrm{mod}2$, i.e. $\overline{0} = 1$ and $\overline{1} = 0$. The final state is *entangled*, and can be rewritten in the form

$$|\Psi\rangle = |0\rangle \otimes (|f(0)\rangle - |\overline{f(0)}\rangle) + |1\rangle \otimes (|f(1)\rangle - |\overline{f(1)}\rangle). \tag{2.21}$$

If the function f is constant, this reduces to

$$|\Psi\rangle = (|0\rangle + |1\rangle) \otimes (|f(0)\rangle - |\overline{f(0)}\rangle), \tag{2.22}$$

and in the opposite case of a not constant f to

$$|\Psi\rangle = (|0\rangle - |1\rangle) \otimes (|f(0)\rangle - |\overline{f(0)}\rangle). \tag{2.23}$$

Hence, measurement of the first qubit in the basis $\{|0\rangle+|1\rangle\ |0\rangle-|1\rangle\}$ (i.e. measuring an observable having eigenvectors $|0\rangle+|1\rangle$ and $|0\rangle-|1\rangle$) gives unambiguous answer on the posed question about the character of f. The goal was achieved after a single run of the computer. Obviously the success of quantum approach relied on the existence of an entangled state (2.20) obtained from the separable input state in the course of quantum evolution.

2.2. Dense coding

Quantum information, stored in qubits can be processed and transmitted like its classical counterpart. At first sight, if we want to transmit information stored in some sequence of qubits, each in one of the basis states $|0\rangle$ or $|1\rangle$, we have to send them to the receiver who should then perform appropriate measurements, hence transmission of the one bit of information consists of sending one qubit, just like in the classical case. Let us suppose, however, that the sender and the receiver share an entangled pair of qubits in the state

$$|\psi_1\rangle = |0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle. \tag{2.24}$$

Now the sender can communicate two classical bits by sending only one qubit. Indeed, let us observe that from the state $|\psi_1\rangle$ one can generate three other states

$$|\psi_1\rangle = |0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle, \tag{2.25}$$

$$|\psi_2\rangle = |0\rangle \otimes |0\rangle - |1\rangle \otimes |1\rangle, \tag{2.26}$$

$$|\psi_3\rangle = |1\rangle \otimes |0\rangle + |0\rangle \otimes |1\rangle, \tag{2.27}$$

$$|\psi_4\rangle = |0\rangle \otimes |1\rangle - |1\rangle \otimes |0\rangle, \tag{2.28}$$

by manipulating only first qubit, namely by applying to the first qubit of $|\psi_1\rangle$ unitary transformations

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \tag{2.29}$$

where we used the customary convention that the basis states $|0\rangle$ and $|1\rangle$ are represented by column vectors

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}. \tag{2.30}$$

The states (2.25)–(2.28) form an orthogonal basis in the Hilbert space of the sender. Her choice of one out of four of the operations (2.29) corresponds to $\log_2 4 = 2$ bits of classical information, but sending her (single!) qubit to her partner allows the receiver to distinguish the four possibilities by:

1. performing the following unitary transformation on two qubits

$$U := \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \tag{2.31}$$

where, by extending our convention we represent the product vectors as

$$|0\rangle \otimes |0\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \quad |0\rangle \otimes |1\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix},$$

$$|1\rangle \otimes |0\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \quad |1\rangle \otimes |1\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}, \tag{2.32}$$

2. measuring the second qubit to distinguish (2.25), (2.28) from (2.26), (2.27),
3. operating with

$$U_1 := \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \tag{2.33}$$

on the first qubit, and finally

4. measuring the first qubit.

After these operations the receiver determines unambiguously the initial state of two qubits, recovering thus two classical bits of information out of a single qubit sent to him. Once more the prominent role played by the entangled states (2.25)–(2.28) is to be stressed.

2.3. Quantum cryptography

At least one of the proposed quantum cryptographic schemes makes an explicit use of entangled states. The main idea of quantum cryptography is to provide means of transmitting information between a sender and a receiver in such a way that from the transmitted data both parties can extract the part about which they are sure to be not available to the third party who wants to intercept (eavesdrop) the communication. If the transmitted information consists of random bits it can be later used to construct a secure quantum key for further secret communication. In order to check whether the transmission was intercepted Ekert [3] proposed the following scheme based on the Bell scheme described above. The communication takes place with the help of singlet states (2.13), each party measures the spin of the particle coming to him/her from the source. The first party measures the spin along the directions $\boldsymbol{e}_1$, $\boldsymbol{e}_2$, or $\boldsymbol{e}_3$, where $\boldsymbol{e}_1$, $\boldsymbol{e}_2$ are the directions described previously and $\boldsymbol{e}_3$ is characterized by the angle $\pi/4$. At the same time second party measures the second spin along $\boldsymbol{f}_1$, $\boldsymbol{f}_2$, or $\boldsymbol{f}_3$, the last one at angle $\pi/2$. If the measurements of the both parties happen to be along the same directions e.g. $\boldsymbol{e}_3$ and $\boldsymbol{f}_1$, then $E(\boldsymbol{e}_i, \boldsymbol{f}_j) = -1$. After measuring a string of qubits the parties announce publicly the *directions* (but used in each measurement) and the

results of the measurements in which directions did not coincide. Out of these results they can calculate the value of S and check whether it conforms with its quantum-mechanical value (2.15). If the communication was intercepted by an eavesdropper (i.e. one of the qubits was measured by him), the quantum correlation present in the entangled state are destroyed, and since he does not know subsequent orientation of the measuring apparatus of the legitimate party, the only thing he can do in an attempt to remain undetected is to resend a qubit with random polarization (with some probability distribution). This however is equivalent to averaging over classical probability distribution which the communicating party will discover by finding the calculated value of S within the classical limits (2.16). If there is no evidence of eavesdropping, the results of measurements in which both directions coincide give both parties strictly correlated results (recall that $E(\boldsymbol{e}_i, \boldsymbol{f}_j) = -1$ in this case) which comprise the secret shared information.

3. Mixed states entanglement

In the previous sections we pointed out some unusual and useful properties of pure entangled states. But pure states are only particular and rather special instances of states available for quantum systems. In particular, if the system in question interacts or interacted with some other system(s) on which we perform measurements, the final state of our system will be, in general, a mixed rather than pure one. The generalization of the notion of entanglement to mixed states was proposed by Werner [14]. A mixed state ρ of a bipartite quantum system is separable if it is a convex combination of product states

$$\rho = \sum_i^k p_i \rho_i^A \otimes \rho_i^B, \quad p_i \geq 0, \quad \sum_i^k p_i = 1, \tag{3.1}$$

where ρ_i^A, ρ_i^B are legitimate (i.e. Hermitian and positive definite) density matrices of the subsystems. States which are not separable are, by the definition, entangled. If ρ is pure, the above definitions of separability and entanglement coincide with the original ones for pure states. Moreover, according to this definition, separable states can be obtained "from scratch", i.e. from an initially uncorrelated state by local manipulations in each subspace (i.e. admissible quantum operations, like quantum evolution, measurements etc. applied separately to each part), and, what is more important, cannot exhibit correlations which cannot be reproduced by classical systems (cf. [14]).

It is easy to check whether a *pure* state of a composite system is separable or entangled. To this end let us observe that a change of the bases in both spaces in (2.11) by local unitary transformations

$$|e_i\rangle = \sum_k^M U_{ik} |e'_k\rangle, \quad |f_j\rangle = \sum_l^N V_{jl} |f'_l\rangle, \tag{3.2}$$

amounts to

$$|\psi\rangle = \sum_{ij} (U^{\mathrm{T}} C V)_{ij} |e'_i\rangle \otimes |f'_j\rangle, \tag{3.3}$$

where $^{\mathrm{T}}$ means transposition and C is the matrix of the coefficients c_{ij}. From the linear algebra (cf. e.g. [15]) it is known that for an arbitrary rectangular $M \times N$ complex matrix C one can find a pair of unitary matrices W_1 and W_2 of dimensions $M \times M$ and $N \times N$ respectively, such that $W_1 C W_2^{\dagger} = D$ where $D_{ij} = 0$ for $i \neq j$ and $D_{ii} \geq 0$ for $i = 1, 2, \ldots, \min(M, N)$. Choosing $U^{\mathrm{T}} = W_1$ and $V = W_2^{\dagger}$ in (3.3) we arrive at the so-called Schmidt decomposition of the pure state $|\psi\rangle$:

$$|\psi\rangle = \sum_{i=1}^{\min(M,N)} D_{ii} |e'_i\rangle \otimes |f'_i\rangle. \tag{3.4}$$

The numbers D_{ii} are called Schmidt coefficients. It is now clear that $|\psi\rangle$ is separable if and only if there is only one non-vanishing Schmidt coefficient.

The situation complicates in the case of mixed states. A simple and practical necessary criterion of separability is known, but there are no known sufficient conditions for higher dimensional composite systems. To formulate Peres' [16] necessary condition for separability let us make the following observations: first an arbitrary state ρ can be written in the form

$$\rho = \sum_{i}^{k} p_i \rho_i^A \otimes \rho_i^B, \tag{3.5}$$

by choosing some bases $\{\rho_l^A\}$ and $\{\rho_k^B\}$ in the spaces of linear Hermitian operators acting in $\mathcal{H}_A$ and $\mathcal{H}_B$. The coefficients p_i are real, but otherwise restricted only by the (unimportant in the present argumentation) trace condition. Also neither ρ_i^A nor ρ_j^B need all to be positive definite (the positive definiteness is obeyed only by ρ itself). We define the *partial transposition* as

$$\rho^{\mathrm{T}_B} := \sum_{i}^{k} p_i \rho_i^A \otimes (\rho_i^B)^{\mathrm{T}}. \tag{3.6}$$

Now, as observed by Peres, if ρ is separable i.e. (3.1) is fulfilled, then ρ^{T_B} is positive definite, i.e. is also a legitimate density matrix for the composite system. For low dimensional ($M = N = 2$, $M = 2$, $N = 3$, and $M = 3$, $N = 2$) systems the above condition is also sufficient [17].

The result of partial transposition depends on the basis in subspace $\mathcal{H}_B$. If we change the bases of $\mathcal{H}_A$ and $\mathcal{H}_B$ by a local transformation $U \otimes V$, i.e. by unitary rotations U and V in the spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively (in fact, since the overall phase factor does not play any role, we can assume $\det U = 1 = \det V$, i.e. $U \in \mathrm{SU}(M)$, $V \in \mathrm{SU}(N)$), the matrix ρ will be transformed according to

$$\rho' = U \otimes V \rho (U \otimes V)^{\dagger} = \sum_{i}^{k} p_i U \rho_i^A U^{\dagger} \otimes V \rho_i^B V^{\dagger}. \tag{3.7}$$

Consequently, the partial transposition gives

$$\rho'^{\mathrm{T}_B} = \sum_i^k p_i U \rho_i^A U^\dagger \otimes (V \rho_i^B V^\dagger)^{\mathrm{T}} = U \otimes V^* \rho^{\mathrm{T}_B} (U \otimes V^*)^\dagger, \tag{3.8}$$

where * denotes the complex conjugation. From (3.8) it follows that the spectrum of ρ^{T_B} is basis-independent.

4. Entanglement measures and geometry of entangled states

Having exposed useful and unusual properties of entangled state we would like to conclude this review by enumerating and discussing some unsolved or only partially solved problems of entanglement. As mentioned above, the criterion based on positivity of partial transpose is, in general, only a necessary one. The quest for separability criteria and checks remains one of the major effort of quantum information theory (see [18] for a survey of recent results and developments). Another issue is how to quantify entanglement. Since, as the examples of Sec. 2 show that entanglement can be treated as a quantum information resource, it is reasonable to pose the question about the amount of entanglement in a particular state or, in other words, to ask if a particular state is "more entangled" than the other one. Such a measure of entanglement should fulfill the following three conditions [19]: it vanishes if and only if ρ is separable, it is invariant under local unitary operations, and its expectation value is non-increasing under general local operations (see [19] for details). Such a measure in the case of two qubits was constructed by Wootters [20] in the form of the *concurrence* defined as

$$c(\rho) = \max\{0, c_1 - c_2 - c_3 - c_4\}, \tag{4.1}$$

where $c_1 \geq c_2 \geq c_3 \geq c_4$ are the square roots of the (real and positive) eigenvalues of the matrix

$$X := \Sigma \rho^* \Sigma \rho, \quad \Sigma = \sigma_2 \otimes \sigma_2, \quad \sigma_2 := \begin{bmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{bmatrix}. \tag{4.2}$$

It is, however, not clear how to construct a similar measure for higher dimensional systems.

An interesting and challenging approach to this problem was proposed in [21] where it was proved that for any state ρ there exists a unique decomposition

$$\rho = \lambda \rho_{\mathrm{s}} + (1 - \lambda) \delta\rho, \tag{4.3}$$

where ρ_{s} is a separable state and λ is maximal (i.e. it is impossible to find such a decomposition with larger λ without violating positivity or separability of ρ_{s}). Such an optimal decomposition (4.3) can be interpreted as concentrating the whole entanglement in $(1-\lambda)\delta\rho$ or, in other words, subtracting from ρ the maximal possible

separable part $\lambda\rho_{\rm s}$. The parameter $(1-\lambda)$ could thus serve as a quantification of the entanglement contained in ρ. To make such a characterization fully functional, one should find an effective, analytic method of finding the optimal decomposition (4.3). Until now it was possible only in the simplest case of two qubits [22], where as it was shown in [21] the entangled part $\delta\rho$ in (4.3) is a pure state

$$\delta\rho = |\psi\rangle\langle\psi|. \tag{4.4}$$

Moreover, we were able to show that:

1. if the rank (the number of non-vanishing eigenvalues) of $\rho_{\rm s}$ is maximal (i.e. equal to 4) $\delta\rho$ is a maximally entangled pure state: i.e. a state which can be obtained from the singlet by local unitary transformations in each space

$$|\psi\rangle = U_1 \otimes U_2 \Big(|0\rangle\otimes|1\rangle - |1\rangle\otimes|0\rangle \Big). \tag{4.5}$$

   The concurrence $c(\psi) := c(|\psi\rangle\langle\psi|)$ of such state equals 1 (the maximal allowed value of the concurrence) which explains the name (*maximally entangled*).

2. in the same case of maximal rank of $\rho_{\rm s}$ the quantity $1-\lambda$ coincides with the above defined concurrence $c(\rho)$,

3. in a general case $c(\rho)$ and $(1-\lambda)c(\psi)$ are two inequivalent measures of entanglement connected, however, by the inequality

$$c(\rho) \le (1-\lambda)c(\psi). \tag{4.6}$$

   Similar results for larger dimensions are not known.

By definition, entanglement measures do not discriminate between the states which can be connected by local unitary transformations. It is thus natural to ask "how many" states are equivalent to a given one with respect to the amount of entanglement. Since such states form a continuous family, this is, in fact, a question about the dimensionality and geometry of the manifolds of states obtained from a given state by applying arbitrary local unitary transformations. We were able to fully characterize such manifolds in the simplest case of two qubits [23] and for the pure states of $N\times N$ system [24] (a generalization for $M\times N$, $M\neq N$ is straightforward). In the case of mixed states of two qubits the manifold of states with the same amount of entanglement is, generally, six-dimensional, but for some states (classified in [23]) its dimensionality can shrink to 5, 4, 3, or 0. The manifolds of pure states of $N\times N$ system equivalent to a given one $|\psi\rangle$ are fully characterized by its Schmidt coefficients. More precisely, let

$$|\psi\rangle = \sum_{i=1}^{N} \lambda_i |e_i\rangle\otimes|f_i\rangle \tag{4.7}$$

and let us order the set of the Schmidt coefficients Λ in the following way: $\Lambda = (0 \leq \lambda_1 \leq \lambda_2 \leq \ldots \leq \lambda_N)$. In order to describe the character of the degeneracy we rename them into $\Lambda = (0, \ldots, 0, \nu_1, \ldots, \nu_1, \nu_2, \ldots, \nu_2, \ldots, \nu_K, \ldots, \nu_K)$ where each value ν_n occurs m_n times and m_0 is the number of vanishing Schmidt coefficients. Obviously, $m_0 + \sum_{n=1}^{K} m_n = N$, and m_0 might be equal to zero. Then the dimension of the manifold $\mathcal{M}_\psi$ of states equivalent to $|\psi\rangle$ equals

$$\dim(\mathcal{M}_\psi) = 2N^2 - 2m_0^2 - \sum_{n=1}^{K} m_n^2 - 1. \tag{4.8}$$

In fact, the manifold $\mathcal{M}_\psi$ has a structure of a Cartesian product of two manifolds

$$\mathcal{M}_\psi = \frac{\mathrm{U}(N)}{G_1} \times \frac{\mathrm{U}(N)}{G_2}. \tag{4.9}$$

Here $\frac{\mathrm{U}(N)}{G}$ denotes the quotient manifold obtained by identifying unitary matrices (elements of the group $\mathrm{U}(N)$) if they differ by multiplication by an unitary matrix belonging to the subgroup $G \subset \mathrm{U}(N)$, and $G_1,\ G_2$ are subgroups of $\mathrm{U}(N)$:

$$G_1 = \left\{ U :\ U = \begin{bmatrix} u_0 & & & \\ & u_1 & & \\ & & \ddots & \\ & & & u_K \end{bmatrix} \right\},$$

$$G_2 = \left\{ U :\ U = \begin{bmatrix} v_0 & & \\ & e^{i\phi} & \\ & & I \end{bmatrix} \right\}, \tag{4.10}$$

where u_0 and v_0 are some unitary matrices of dimension m_0, $u_1, \ldots, u_K$ — some unitary matrices of dimensions $m_1, \ldots, m_K$, respectively, $\mathrm{e}^{i\phi}$ — some phase factor (a one-dimensional unitary matrix), and I — the identity matrix of the dimension $N - m_0 - 1$. The generalization of the above results to arbitrary mixed state is not known.

As it is clear from the above even the simplest questions concerning entanglement of states of composite systems are still open, despite the fact that the phenomenon of entanglement is known for more than 65 years and its fundamental meaning for differences between classical and quantum worlds was recognized long ago. The seemingly innocent mathematical problems formulated in terms of finite-dimensional matrices, some of them presented above, are in deep relations with theories of convex sets and so-called completely positive maps [17], geometry of compact group actions [25] and, doubtlessly, in next few years remain an inspiration in mathematical physics.

References

[1] P.W. Shor, in: *Proc. 35th Annual Symp. on Foundations of Computer Science*, IEEE Computer Society Press, Santa Fe 1994, p. 124.

[2] C.H. Bennet, G. Brassard, S. Briedbart, S. Wiesner, in: *Advances in Cryptology: Proc. Crypto '82*, Plenum Press, New York 1982, p. 267.

[3] A. Ekert, *Phys. Rev. Lett.* **67,** 661 (1991).

[4] L.K. Grover, *Phys. Rev. Lett.* **79,** 325 (1997).

[5] C.H. Bennet, S.J. Wiesner, *Phys. Rev. Lett.* **69,** 2881 (1992).

[6] C.H. Bennet, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, W.K. Wootters, *Phys. Rev. Lett.* **70,** 1895 (1993).

[7] A. Einstein, B. Podolsky, N. Rosen, *Phys. Rev.* **47,** 777 (1935).

[8] D. Bohm, *Quantum Theory*, Dover, New York 1989.

[9] J.S. Bell, *Physics* **1,** 195 (1964).

[10] J.F. Clauser, M.A. Horne, A. Shimony, R.A. Holt, *Phys. Rev. Lett.* **23,** 880 (1969).

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

[12] D. Deutsch, R. Jozsa, *Proc. R. Soc. Lond. A* **439,** 553 (1992).

[13] V. Vedral, M. Plenio, *Prog. Quantum Electron.* **22,** 1 (1998).

[14] R.F. Werner, *Phys. Rev. A* **40,** 4277 (1989).

[15] R.A. Horn, C.R. Johnson, *Topics in Matrix Analysis*, Cambridge University Press, Cambridge 1991.

[16] A. Peres, *Phys. Rev. Lett.* **77,** 1413 (1996).

[17] M. Horodecki, P. Horodecki, R. Horodecki, *Phys. Lett. A* **223,** 1 (1996).

[18] M. Lewenstein, D. Bruß, J.I. Cirac, B. Kraus, M. Kuś, J. Samsonowicz, A. Sanpera, R. Tarrach, *J. Mod. Opt.* **47,** 2481 (2000).

[19] V. Vedral, M.B. Plenio, *Phys. Rev. A* **57,** 1619 (1998).

[20] W.K. Wootters, *Phys. Rev. Lett.* **80,** 2245 (1998).

[21] M. Lewenstein, A. Sanpera, *Phys. Rev. Lett.* **80,** 2261 (1998).

[22] T. Wellens, M. Kuś, *Phys. Rev. A* **64,** 052302 (2001).

[23] M. Kuś, K. Życzkowski, *Phys. Rev. A* **63,** 032307 (2001).

[24] M.M. Sinołęcka, K. Życzkowski, M. Kuś, to be published.

[25] P. Heinzner, A.T. Huckleberry, M. Kuś, K. Życzkowski, unpublished.