

Quantum Entanglement and Symmetry

Dariusz Chruściński and Andrzej Kossakowski

Institute of Physics, Nicolaus Copernicus University,
Grudziądzka 5/7, 87-100 Toruń, Poland

E-mail: darch@fizyka.umk.pl; kossak@fizyka.umk.pl

Abstract.

One of the main problem in Quantum Information Theory is to test whether a given state of a composite quantum system is entangled or separable. It turns out that within a class of states invariant under the action of the symmetry group this problem considerably simplifies. We analyze multipartite invariant states and the corresponding symmetric quantum channels.

1. Introduction

Quantum Entanglement is one of the key features which distinguish quantum mechanics from the classical one. Recent development of Quantum Information Theory [1] shows that quantum entanglement does have important practical applications and it serves as a basic resource for quantum cryptography, quantum teleportation, dense coding and quantum computing.

A fundamental problem in Quantum Information Theory is to test whether a given state of a composite quantum system is entangled or separable. Surprisingly this so called *separability problem* has no simple solution. Several operational criteria have been proposed to identify entangled states. Each of these criterion is only necessary and in general one needs to perform infinite number of tests to be sure that a given state is separable. It is therefore desirable to possess a class of states for which one may easily check separability and test various concepts of Quantum Information Theory.

The basic idea of this paper is to construct such classes using symmetry arguments. Symmetry plays a prominent role in modern physics. In many cases it enables one to simplify the analysis of the corresponding problems and very often it leads to much deeper understanding and the most elegant mathematical formulation of the corresponding physical theory. As is well known bipartite symmetric states turned out to be very useful for the investigation of quantum entanglement. Symmetry considerably simplifies computation of various important quantities like e.g. entanglement of formation and other important entanglement measures. Moreover, they play crucial role in entanglement distillation.

We propose a natural generalization of symmetric states to multipartite case with even number of parties. It turns out that within a class of multipartite symmetric states the separability problem is easy to solve. Finally, using duality between states of composite systems and quantum channels we discuss basic properties of symmetric channels corresponding to multipartite case. It is hoped that multipartite invariant state discussed in this paper may serve as a useful laboratory for testing various concepts from quantum information theory.

2. Entanglement and separability problem

In this section we recall basic features of entangled states.

2.1. Pure states

Consider a bipartite quantum system living in $\mathcal{H}_{\text{total}} = \mathcal{H}_A \otimes \mathcal{H}_B$. We call $\psi \in \mathcal{H}_{\text{total}}$ separable (or classically correlated) iff $\psi = \psi_A \otimes \psi_B$ with $\psi_A \in \mathcal{H}_A$ and $\psi_B \in \mathcal{H}_B$. Otherwise ψ is entangled (or nonseparable). Suppose now, that we are given a state ψ from $\mathcal{H}_{\text{total}}$. How to check whether ψ is separable or entangled? This so called separability problem is easy to solve do the following

Theorem 1 (Schmidt) *For any normalized $\psi \in \mathcal{H}_{\text{total}}$ there exist two orthonormal basis (depending on ψ !) $\{e_\alpha\}$ in \mathcal{H}_A and $\{f_\beta\}$ in \mathcal{H}_B such that*

$$\psi = \sum_{\alpha} \lambda_{\alpha} e_{\alpha} \otimes f_{\alpha} , \quad (1)$$

where $\lambda_{\alpha} \geq 0$ and $\sum_{\alpha} \lambda_{\alpha}^2 = 1$.

Denote by $\text{SR}(\psi)$ the Schmidt rank of ψ , that is, a number of non-vanishing Schmidt coefficients in (1). Hence, ψ is separable if and only if $\text{SR}(\psi) = 1$.

2.2. Mixed states

For mixed states the problem is much more complicated. Following Werner [2] we call a state represented by a density matrix ρ separable iff it can be represented as the following convex combination

$$\rho = \sum_k p_k \rho_k^{(A)} \otimes \rho_k^{(B)} , \quad (2)$$

where $\rho_k^{(A)}$ ($\rho_k^{(B)}$) are mixed state in \mathcal{H}_A (\mathcal{H}_B) and $\{p_k\}$ is a probability distribution (i.e. $p_k \geq 0$ and $\sum_k p_k = 1$).

Surprisingly the separability problem has in this case no simple solution. Peres [3] was first who derived very simple necessary separability criterion, namely if ρ is separable, then its partial transposition

$$(\mathbb{1}_A \otimes \tau_B) \rho \geq 0 , \quad (3)$$

where τ_B denotes transposition on $\mathcal{B}(\mathcal{H}_B)$. States with the above property are called PPT (Positive Partial Transpose). Actually, it turns out that if $\dim \mathcal{H}_A \cdot \dim \mathcal{H}_B = 6$, then this criterion is also sufficient, i.e. all PPT states in $2 \otimes 2$, $2 \otimes 3$ and $3 \otimes 2$ systems are separable.

It turns out that the separability problem may be reformulated in terms of mathematical theory of positive maps: let $M_n(\mathbb{C})$ denote an algebra of $n \times n$ complex matrices. A linear map $\Lambda : M_n(\mathbb{C}) \longrightarrow M_m(\mathbb{C})$ is positive iff $\Lambda(X) \geq 0$ for any semi-positive $X \in M_n(\mathbb{C})$. Moreover, if $\mathbb{1}_k \otimes \Lambda$ is positive, where $\mathbb{1}_k$ is an identity map on $M_k(\mathbb{C})$, then Λ is k -positive. Finally, if Λ is k -positive for all k , then it is completely positive (CP). The structure of CP maps is well known. Any such map may be represented as follows

$$\Lambda_{\text{CP}}(X) = \sum_{\alpha} S_{\alpha} X S_{\alpha}^* , \quad (4)$$

where S_{α} are so called Sudarshan-Kraus operators [4]. The importance of positive maps follows from the following

Theorem 2 ([5]) *A mixed state ρ in $\mathcal{H}_{\text{total}}$ is separable iff*

$$(\mathbb{1}_A \otimes \Lambda) \rho \geq 0 , \quad (5)$$

for all positive maps $\Lambda : \mathcal{B}(\mathcal{H}_B) \longrightarrow \mathcal{B}(\mathcal{H}_A)$.

Note, that when Λ is CP, then (5) is trivially satisfied. Therefore, only positive maps which are not CP may be used to detect entanglement. The above theorem shows that in general one needs infinitely many test (each defined by a positive map) to be sure that a state is separable. The main problem, however, is that the structure of positive maps which are not CP is still unknown. Moreover, we know only few examples of such maps (see [6] for a recent review).

2.3. Multipartite states

The above discussion may be easily generalized to multipartite case. A state ρ in $\mathcal{H}_{\text{total}} = \mathcal{H}_1 \otimes \dots \otimes \mathcal{H}_N$ is fully separable (or N -separable) iff it can be represented as the convex combination of product N -partite states:

$$\rho = \sum_k p_k \rho_k^{(1)} \otimes \dots \otimes \rho_k^{(N)}, \quad (6)$$

where $\rho_k^{(l)}$ is a mixed state in \mathcal{H}_l and $\{p_k\}$ is a probability distribution. In analogy to Theorem 2 one has the following result:

Theorem 3 ([7]) *An N -partite mixed state ρ in $\mathcal{H}_{\text{total}}$ is separable iff*

$$(\mathbb{1}_1 \otimes \Lambda) \rho \geq 0, \quad (7)$$

for all linear maps $\Lambda : \mathcal{B}(\mathcal{H}_2 \otimes \dots \otimes \mathcal{H}_N) \longrightarrow \mathcal{B}(\mathcal{H}_1)$ such that

$$\Lambda(\rho^{(2)} \otimes \dots \otimes \rho^{(N)}) \geq 0, \quad (8)$$

for all states $\rho^{(k)}$ in \mathcal{H}_k .

Note that there is a crucial difference between bipartite and N -partite case with $N > 2$. For $N = 2$ one needs only positive maps whereas for $N > 2$ a larger class of maps has to be considered, that is, maps which are not necessarily positive but which are positive on separable states.

3. Bipartite symmetric states

Consider a bipartite quantum system living in $\mathcal{H}_{\text{total}} = \mathcal{H}_A \otimes \mathcal{H}_B$. Let G be a compact Lie group together with two irreducible unitary representations $\mathfrak{D}^{(A)}$ and $\mathfrak{D}^{(B)}$:

$$\mathfrak{D}^{(A)}(g) : \mathcal{H}_A \longrightarrow \mathcal{H}_A, \quad \mathfrak{D}^{(B)}(g) : \mathcal{H}_B \longrightarrow \mathcal{H}_B, \quad (1)$$

for any element $g \in G$. We call a state ρ of the composite system $\mathfrak{D}^{(A)} \otimes \mathfrak{D}^{(A)}$ -invariant iff

$$[\rho, \mathfrak{D}^{(A)}(g) \otimes \mathfrak{D}^{(A)}(g)] = 0, \quad (2)$$

for each $g \in G$. The most prominent example of a symmetric state was constructed by Werner [2]: take $\mathcal{H}_A = \mathcal{H}_B = \mathbb{C}^d$, $G = U(d)$ and let $\mathfrak{D}^{(A)} = \mathfrak{D}^{(B)}$ be a defining representation of $U(d)$ in \mathbb{C}^d (i.e. we represent elements from $U(d)$ by $d \times d$ unitary matrices). Now, the commutant of $U(d) \times U(d)$ is spanned by identity $I^{\otimes 2} = I_d \otimes I_d$ and the flip operator \mathbb{F} defined by $\mathbb{F}(\varphi \otimes \psi) = \psi \otimes \varphi$. Note that in the standard basis $\{e_1, \dots, e_d\}$ in \mathbb{C}^d the flip operator may be represented as follows

$$\mathbb{F} = \sum_{i,j=1}^d e_{ij} \otimes e_{ji}, \quad (3)$$

where $e_{ij} = |e_i\rangle\langle e_j|$. Now, building two orthogonal projectors:

$$Q^0 = \frac{1}{2}(I^{\otimes 2} + \mathbb{F}) , \quad (4)$$

$$Q^1 = \frac{1}{2}(I^{\otimes 2} - \mathbb{F}) , \quad (5)$$

one obtains the following general form of $U \otimes U$ -invariant Werner states:

$$\rho = q_0 \tilde{Q}^0 + q_1 \tilde{Q}^1 , \quad (6)$$

where $q_\alpha \geq 0$, $q_0 + q_1 = 1$ and we use the following notation: $\tilde{A} = A/\text{Tr}(A)$. It is well known [2] that a Werner state (6) is separable iff it is PPT. This may be easily translated into the following condition upon coefficients q_α : $q_1 \leq 1/2$.

4. Multipartite symmetric states

Now, generalization to multipartite system is simple: consider an N -partite system living in

$$\mathcal{H}_{\text{total}} = \mathcal{H}_1 \otimes \dots \otimes \mathcal{H}_N ,$$

together with a compact Lie group G and N irreducible unitary representations

$$\mathfrak{D}^{(k)} : \mathcal{H}_k \longrightarrow \mathcal{H}_k , \quad k = 1, \dots, N .$$

N -partite state ρ is $\mathfrak{D}^{(1)} \otimes \dots \otimes \mathfrak{D}^{(N)}$ -invariant iff

$$[\rho, \mathfrak{D}^{(1)}(g) \otimes \dots \otimes \mathfrak{D}^{(N)}(g)] = 0 , \quad (1)$$

for each $g \in G$. This problem was considered in [8, 9] for $N = 3$ in the case of $\mathcal{H}_k = \mathbb{C}^d$ and $G = U(d)$. The complete list of separability conditions for $U \otimes U \otimes U$ -invariant states were found. However, the detailed analysis of separability for $U^{\otimes N}$ -invariant states for $N > 3$ is not straightforward.

Recently, in a series of papers [10, 11, 12] we proposed another class of symmetric multipartite states constructed as follows: let $N = 2K$ and consider

$$\mathcal{H}_{\text{total}} = \mathcal{H}_1 \otimes \dots \otimes \mathcal{H}_K \otimes \mathcal{H}_1 \otimes \dots \otimes \mathcal{H}_K .$$

Now, a $2K$ -partite state ρ is $\mathfrak{D}^{(1)} \otimes \dots \otimes \mathfrak{D}^{(K)} \otimes \mathfrak{D}^{(1)} \otimes \dots \otimes \mathfrak{D}^{(K)}$ -invariant iff

$$[\rho, \mathfrak{D}^{(1)}(g_1) \otimes \dots \otimes \mathfrak{D}^{(K)}(g_K) \otimes \mathfrak{D}^{(1)}(g_1) \otimes \dots \otimes \mathfrak{D}^{(K)}(g_K)] = 0 , \quad (2)$$

for each $g_k \in G$ ($k = 1, \dots, K$). Note that definition (2) is much more restrictive than (1) and hence a class of states invariant under (2) is smaller than a class of states (with $N = 2K$) invariant under (1).

As an example consider the simplest case: $\mathcal{H}_1 = \dots = \mathcal{H}_K = \mathbb{C}^d$ and let $G = U(d)$ be represented in a natural way on \mathbb{C}^d . Defining the K -vector $\mathbf{U} = (U_1, \dots, U_K)$ together with $\mathbf{U} \otimes \mathbf{U} = U_1 \otimes \dots \otimes U_K \otimes U_1 \otimes \dots \otimes U_K$ we may rewrite the definition of $\mathbf{U} \otimes \mathbf{U}$ -invariant state as follows

$$[\rho, \mathbf{U} \otimes \mathbf{U}] = 0 , \quad (3)$$

for each $\mathbf{U} \in U(d) \times \dots \times U(d)$. Now, to parameterize the space of $\mathbf{U} \otimes \mathbf{U}$ -invariant states let us denote by $\boldsymbol{\sigma}$ a binary K -vector and introduce a set of $2K$ -partite operators

$$\mathbf{Q}^{\boldsymbol{\sigma}} = Q_{1|K+1}^{\sigma_1} \otimes \dots \otimes Q_{K|2K}^{\sigma_K} , \quad (4)$$

where each $Q_{j|j+K}^{\sigma_j}$ is a bipartite operator acting on $\mathcal{H}_j \otimes \mathcal{H}_{j+K}$. One easily shows that

- (i) \mathbf{Q}^σ are $\mathbf{U} \otimes \mathbf{U}$ -invariant,
- (ii) $\mathbf{Q}^\alpha \cdot \mathbf{Q}^\beta = \delta_{\alpha\beta}$,
- (iii) $\sum_{\sigma} \mathbf{Q}^\sigma = \mathbb{1}^{\otimes 2K}$,

that is, \mathbf{Q}^σ define orthogonal resolution of identity in $\mathcal{H}_{\text{total}}$. Therefore, any $\mathbf{U} \otimes \mathbf{U}$ -invariant state ρ may be uniquely represented as follows

$$\rho = \sum_{\sigma} q_{\sigma} \tilde{\mathbf{Q}}^{\sigma}, \quad (5)$$

with $q_{\sigma} \geq 0$ and $\sum_{\sigma} q_{\sigma} = 1$. To investigate multi-separability of (5) let us define a family of generalized partial transpositions parameterized by a binary K -vector $\sigma = (\sigma_1, \dots, \sigma_K)$:

$$\tau_{\sigma} = \tau^{\sigma_1} \otimes \dots \otimes \tau^{\sigma_K}. \quad (6)$$

We call a $2K$ -partite state σ -PPT iff $(\mathbb{1}^{\otimes K} \otimes \tau_{\sigma})\rho \geq 0$. It is not difficult to show that states which are σ -PPT for all binary K -vectors σ define $(2^K - 1)$ -dimensional simplex [10]. Its vertices (extremal states) are characterized as follows:

- 1 extremal state corresponding to $q_{\sigma} = (1, 0, 0, \dots, 0)$,
- K extremal states with $q_{\sigma} = 1/2$ for each σ with $|\sigma| = 1$,
- $\binom{K}{2}$ extremal states with $q_{\sigma} = 1/4$ for each σ with $|\sigma| = 2$,
- ...
- 1 extremal state corresponding to $q_{\sigma} = 2^{-K}(1, 1, \dots, 1)$,

where $|\sigma| = \sigma_1 + \dots + \sigma_K$. Hence, a necessary condition for multi-PPT property reads as follows

$$q_{\sigma} \leq \frac{1}{2^{|\sigma|}}. \quad (7)$$

It is clear that for $K = 1$, i.e. in a bipartite case, (7) reproduces condition $q_1 \leq 1/2$. Now, it may be proved [10] that all extremal multi-PPT states are $2K$ -separable. Hence a $2K$ -partite $\mathbf{U} \otimes \mathbf{U}$ -invariant state ρ is separable iff it is σ -PPT for all binary K -vectors σ .

5. Duality and symmetric quantum channels

It is well known that the space of density operators in $\mathcal{H}_{\text{total}} = \mathcal{H} \otimes \mathcal{H}$ is isomorphic with the space of trace-preserving CP maps $\Phi : \mathcal{B}(\mathcal{H}) \longrightarrow \mathcal{B}(\mathcal{H})$. Such maps are called quantum channels. An example of such isomorphism is given by [13]

$$\Phi \longrightarrow \rho_{\Phi} = (\mathbb{1} \otimes \Phi) P^+, \quad (1)$$

where $P^+ = (1/d) \sum_{i,j=1}^d e_{ij} \otimes e_{ij}$ denotes the projector onto the maximally entangled state in $\mathcal{H}_{\text{total}}$. Consider now an irreducible unitary representation \mathfrak{D} of G acting on \mathcal{H} . A quantum channel Φ is \mathfrak{D} -invariant iff

$$\Phi(\mathfrak{D}(g) X \mathfrak{D}(g)^*) = \mathfrak{D}(g) \Phi(X) \mathfrak{D}(g)^*, \quad (2)$$

for each $g \in G$ and $X \in \mathcal{B}(\mathcal{H})$. Clearly, Φ is \mathfrak{D} -invariant iff ρ_{Φ} is $\mathfrak{D} \otimes \mathfrak{D}$ -invariant.

Let $\Phi^{\sigma} : M_d(\mathbb{C}) \longrightarrow M_d(\mathbb{C})$ be a quantum channel corresponding to $\tilde{\mathbf{Q}}^{\sigma}$ ($\sigma = 0, 1$). Therefore, a channel corresponding to the Werner state (6) is given by $\Phi = q_0 \Phi^0 + q_1 \Phi^1$. Let

$$\Phi_K : M_d(\mathbb{C})^{\otimes K} \longrightarrow M_d(\mathbb{C})^{\otimes K}, \quad (3)$$

be a quantum channel invariant under $U(d) \times \dots \times U(d)$, i.e.

$$\Phi_K \left((U_1 \otimes \dots \otimes U_K) X (U_1 \otimes \dots \otimes U_K)^* \right) = (U_1 \otimes \dots \otimes U_K) \Phi_K(X) (U_1 \otimes \dots \otimes U_K)^* , \quad (4)$$

with $U_1, \dots, U_K \in U(d)$. It is clear that a $2K$ -partite state

$$\rho = (\mathbb{1}^{\otimes K} \otimes \Phi_K) (P_{1|K+1}^+ \otimes \dots \otimes P_{K|2K}^+) , \quad (5)$$

is $\mathbf{U} \otimes \mathbf{U}$ -invariant. Observe that any $U(d) \times \dots \times U(d)$ -invariant channel may be uniquely represented as follows

$$\Phi_K = \sum_{\sigma} q_{\sigma} \Phi^{\sigma_1} \otimes \dots \otimes \Phi^{\sigma_K} , \quad (6)$$

and hence it corresponds to $\mathbf{U} \otimes \mathbf{U}$ -invariant state (5). In terms of Φ_K the N -separability of ρ is equivalent to the following set of conditions:

$$\tau_{\sigma} \circ \Phi_K = \sum_{\sigma} q_{\sigma} (\tau^{\sigma_1} \circ \Phi^{\sigma_1}) \otimes \dots \otimes (\tau^{\sigma_K} \circ \Phi^{\sigma_K}) , \quad (7)$$

is CP for all σ . Finally, note that reduction with respect to $(i|i+K)$ pair leads to a $2(K-1)$ -partite invariant state or equivalently $U(d) \times \dots \times U(d)$ -invariant channel Φ_{K-1} . For example reduction with respect to the last pair $(K|2K)$ gives $\Phi_{K-1} : M_d(\mathbb{C})^{\otimes K-1} \longrightarrow M_d(\mathbb{C})^{\otimes K-1}$ defined by

$$\Phi_{K-1} \circ \text{Tr}_K = \text{Tr}_K \circ \Phi_K , \quad (8)$$

where Tr_K denotes the trace with respect to the K th factor. It is clear that

$$\Phi_{K-1} = \sum_{\sigma} q'_{\sigma} \Phi^{\sigma_1} \otimes \dots \otimes \Phi^{\sigma_{K-1}} , \quad (9)$$

where $q'_{(\sigma_1, \dots, \sigma_{K-1})} = \sum_{\sigma_K} q_{(\sigma_1, \dots, \sigma_K)}$.

6. Conclusions

Construction of $2K$ -partite symmetric states may be easily generalized for other groups, e.g. orthogonal group $O(d)$ [11] and $SU(2)$ [12]. Moreover, we may define states with other symmetry properties: for example in a bipartite case one may consider states invariant under $\mathfrak{D}^{(A)} \otimes \overline{\mathfrak{D}^{(B)}}$. If $G = U(d)$ such states are called isotropic [14] and they do play important role in applications of Quantum Information Theory. In a similar way one may introduce isotropic-like states in a multipartite setting. It is hoped that the multipartite state discussed in this paper may serve as a very useful laboratory for testing various concepts from quantum information theory and they may shed new light on the more general investigation of multipartite entanglement.

Acknowledgments

This work was partially supported by the Polish Ministry of Science and Higher Education Grant No 3004/B/H03/2007/33.

References

- [1] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information*, Cambridge University Press, Cambridge, 2000.
- [2] R.F. Werner, Phys. Rev. A **40**, 4277 (1989).
- [3] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996); P. Horodecki, Phys. Lett. A **232**, 333 (1997).

- [4] E.C.G. Sudarshan, P. M. Mathews, and J. Rau, Phys. Rev. **121**, 920 (1961); T. F. Jordan and E. C. G. Sudarshan, J. Math. Phys. **2**, 772 (1961); K. Kraus, Ann. Phys. (N.Y.) **64**, 311 (1971); K. Kraus, *States, Effects and Operations*, Springer-Verlag, Berlin, 1983.
- [5] M. Horodecki, P. Horodecki and R. Horodecki, Phys. Lett A **223** 1 (1996).
- [6] D. Chruściński and A. Kossakowski, *On the structure of entanglement witnesses and new class of positive indecomposable maps*, quant-ph/0606211 (to appear in Open Systems and Inf. Dynamics).
- [7] M. Horodecki, P. Horodecki and R. Horodecki, Phys. Lett A **283** 1 (2001).
- [8] K.G.H. Vollbrecht and R.F. Werner, Phys. Rev. A **64**, 062307 (2001).
- [9] T. Eggeling and R.F. Werner, Werner, Phys. Rev. A **63**, 042111 (2001).
- [10] D. Chruściński and A. Kossakowski, Phys. Rev. A **73**, 062313 (2006).
- [11] D. Chruściński and A. Kossakowski, Phys. Rev. A **73**, 062314 (2006).
- [12] D. Chruściński and A. Kossakowski, Open Systems Inf. Dyn. **14**, 25 (2007).
- [13] A. Jamiolkowski, Rep. Math. Phys. **3** (1972) 275
- [14] M. Horodecki and P. Horodecki, Phys. Rev. A **59**, 4206 (1999).