Journal of Mathematical Sciences, Vol. 168, No. 3, 2010

ON THE RING OF LOCAL POLYNOMIAL INVARIANTS FOR A PAIR OF ENTANGLED QUBITS

V. Gerdt,* A. Khvedelidze, and Yu. Palii†** UDC 517.986

The entanglement characteristics of two qubits are encoded in the invariants of the adjoint action of the group $\mathrm{SU}(2)\otimes\mathrm{SU}(2)$ *on the space of density matrices* $\mathfrak{P}_+$*, defined as the space of* 4×4 *positive semidefinite Hermitian matrices. The corresponding ring* $\mathrm{C}[\,\mathfrak{P}_+\,]^{\mathrm{SU}(2)\otimes\mathrm{SU}(2)}$ *of polynomial invariants is studied. A special integrity basis for* $\mathrm{C}[\,\mathfrak{P}_+\,]^{\mathrm{SU}(2)\otimes\mathrm{SU}(2)}$ *is described, and the constraints on its elements imposed by the positive semidefiniteness of density matrices are given explicitly in the form of polynomial inequalities. The suggested basis is characterized by the property that the minimum number of invariants, namely, two primary invariants of degree* $2, 3$ *and one secondary invariant of degree* 4 *appearing in the Hironaka decomposition of* $\mathrm{C}[\,\mathfrak{P}_+\,]^{\mathrm{SU}(2)\otimes\mathrm{SU}(2)}$*, are subject to the polynomial inequalities. Bibliography:* 32 *titles.*

1. Introduction

According to the quantum theory, the nonlocality of the quantum word manifests itself in a way that is very different from the intuitive classical views. At the very outset of the quantum epoch, reflections on that fact created a variety of paradoxes, starting from the Einstein–Podolsky–Rosen paradox and the famous Schrödinger cat neither dead nor alive [1–3]. Only towards the end of the 20th century, with advances in technology, when controlling quantum coherence became reality, the pragmatic approach to the problem posed questions concerning the practical usage of quantum nonlocality. The time for the realization of quantum communications and creation of a quantum computer came [4].

The difference between quantum and classical correlations has a very transparent mathematical background. One can already formulate it comparing the basic states of classical and quantum computers, bits and qubits. While an arbitrary n-bit string can be transformed into another one by a so-called "local transformation" acting on its constituent bits, in the quantum case this is true for one-qubit states only. In other words, the action of "local transformations" ceases to be *transitive* for multi-qubit systems [5, 6]. The action of local transformations splits the space of an arbitrary quantum system into equivalence classes, each class being characterized by different nonlocal properties [7]. Therefore the problem of classification of nonlocalities in a system of n qubits reduces to the mathematical problem of description of orbits of the "local" group action on the space of states [8, 9]. The corresponding orbit space, $\mathcal{E}_n$, is termed as the "*entanglement space*" [5, 6]. For its characterization, the mathematical formalism based on the classical theory of invariants (cf. [10, 11]) is often applied. In this approach, in order to separate orbits, i.e., to introduce coordinates on E_n, one uses polynomials in the elements of the density matrices invariant under the local transformations.

The entanglement space has a highly nontrivial geometric and topological structure [6, 12]. The complexity of $\mathcal{E}_n$ rises sharply as the number of qubits grows. This makes computations very tedious. However, for the simplest, 2-qubit, system, the approach based on the classical theory of invariants allows one to obtain a series of important algebraic results clarifying the properties of $\mathcal{E}_2$, see [9, 13, 14].

There is one further complication with the description of $\mathcal{E}_n$. According to physical requirements, density matrices should be positive semidefinite [15–17]. Therefore, the space of the local group action is not a linear space, but rather a certain semialgebraic variety $\mathfrak{P}_+$. Applying the classical theory of invariants to the construction of the orbit space, one should take into account this circumstance. In the present article, this problem is analyzed, and a detailed solution for the case of 2 qubits is obtained. For this reason, the semidefiniteness of density matrices is formulated explicitly in the form of polynomial inequalities in the scalars of the adjoint action of the group $\mathrm{SU}(2)\otimes\mathrm{SU}(2)$. Moreover, an integrity basis for the polynomial ring $\mathrm{C}[\,\mathfrak{P}_+\,]^{\mathrm{SU}(2)\otimes\mathrm{SU}(2)}$ that includes the minimum number of elements subject to the above inequalities will be presented.

Our plan is as follows. We start, in Secs. 2 and 3, with a brief review of necessary notions from quantum mechanics placing them into a context suitable for the characterization of entanglement within the classical

*Joint Institute for Nuclear Research, Dubna, Russia, e-mail: gerdt@jinr.ru.

**Razmadze Mathematical Institute, Tbilisi, Georgia, e-mail: akhved@jinr.ru.

†Institute of Applied Physics, Chisinau, Moldova, e-mail: palii@jinr.ru.

Translated from *Zapiski Nauchnykh Seminarov POMI*, Vol. 373, 2009, pp. 104–123. Original article submitted September 21, 2009.

theory of invariants. Further, in Sec. 4, we derive a system of polynomial inequalities in the Casimir operators of the enveloping algebra su(4) that describes the space $\mathfrak{P}_+$. Taking into account these inequalities, in the last section we construct an integrity basis for the ring $\mathrm{C}[\,\mathfrak{P}_+\,]^{\mathrm{SU}(2)\otimes\mathrm{SU}(2)}$.

2. The space of states

A generic mixed state of an n-level quantum system is described by an $n \times n$ complex matrix, the density matrix ϱ (see [15, 16]) satisfying the following conditions[1]:

(i) *Hermicity*: $\varrho = \varrho^+$,
(ii) *finite trace*: $\mathrm{Tr}(\varrho) = 1$,
(iii) *positive semidefiniteness*: $\varrho \geq 0$.

The mixed states form a subspace $\mathfrak{P}_+$ of the space of Hermitian $n \times n$ matrices. It is instructive, before considering a generic n-level system, to start with the simplest two-level quantum-mechanical model.

2.1. Qubit

In the quantum theory of information, an abstract quantum-mechanical model with two classical states (levels) holds a special place and, independently of its physical realization, bears the universal name – *qubit*.

The state of a qubit is given by a density matrix that coincides with the standard density matrix of the nonrelativistic spin 1/2:

$$\varrho = \frac{1}{2}\,(1 + \boldsymbol{\alpha}\cdot\boldsymbol{\sigma})\,, \tag{1}$$

where $\boldsymbol{\sigma}$ is the set of Pauli matrices[2] and $\boldsymbol{\alpha}$ is the expectation defined as

$$\boldsymbol{\alpha} = \mathrm{Tr}\,(\boldsymbol{\sigma}\varrho)\,.$$

In the representation (1), requirements (i) and (ii) are taken into account by construction. Condition (iii) restricts the parameter space to the unit ball

$$\boldsymbol{\alpha}^2 \leq 1, \tag{2}$$

while for pure states of the qubit, the expectation $\boldsymbol{\alpha}$ lies in the Bloch 2-sphere

$$\boldsymbol{\alpha}^2 = 1. \tag{3}$$

2.2. Qudit

By analogy with a qubit, a special term for a state of a d-level quantum system, "*qudit*," was introduced. The generalization of the representation (1) to the case of qudits reads as follows (see [18]):

$$\varrho = \frac{1}{d}\left(\mathbb{I}_d + \sqrt{\frac{d(d-1)}{2}}\,\boldsymbol{\xi}\cdot\boldsymbol{\lambda}\right), \tag{4}$$

where $\boldsymbol{\xi} = \langle\boldsymbol{\lambda}\rangle \in \mathbb{R}^{d^2-1}$ is a (d^2-1)-dimensional Bloch vector. In the expansion (4), the components of the vector $\boldsymbol{\lambda} = (\lambda_1, \lambda_2, \ldots, \lambda_{d^2-1})$ represent the elements of the algebra su(d) normalized by the conditions

$$\lambda_i\lambda_j = \frac{2}{d}\,\delta_{ij}\mathbb{I}_d + (d_{ijk} + i\,f_{ijk})\lambda_k\,,$$

where δ_{ij} is the Kronecker symbol, d_{ijk} and f_{ijk} are the structure constants of the algebra, totally symmetric and antisymmetric, respectively:

$$d_{abc} = \frac{1}{4}\,\mathrm{Tr}(\{\lambda_a, \lambda_b\}\lambda_c), \qquad f_{abc} = -\frac{i}{4}\,\mathrm{Tr}([\lambda_a, \lambda_b]\lambda_c),$$

[1] The special class of idempotent matrices, satisfying $\varrho^2 = \rho$, corresponds to the so-called *pure states*, whose description reduces to the usage of rays in a Hilbert space. A mixed state is a mixture of pure states.

[2] The explicit form of the σ-matrices is given below, in Sec. 5, formulas (24).

with

$$\{\lambda_a, \lambda_b\} = \lambda_a\lambda_b + \lambda_b\lambda_a, \quad [\lambda_a, \lambda_b] = \lambda_a\lambda_b - \lambda_b\lambda_a.$$

As in the case of a qubit, properties (i) and (ii) of the density matrix of a qudit are already taken into account in the decomposition (4). The nonnegativity requirement (iii) imposes further restrictions, more subtle than (2). A complete characterization of the qudit Bloch vector space $\mathbf{B}(\mathbb{R}^{d^2-1})$ in an arbitrary dimension is an open problem. However, some general properties of this space are already known. Particularly, it can be shown that $\mathbf{B}(\mathbb{R}^{d^2-1})$ is a convex subset of the (d^2-1)-dimensional unit ball

$$\boldsymbol{\xi}^2 \leq 1, \tag{5}$$

and all pure states are concentrated on its surface. More precisely, pure states of the qudit are determined by the equation

$$\boldsymbol{\xi}^2 = 1, \quad \boldsymbol{\xi} \vee \boldsymbol{\xi} = \boldsymbol{\xi}, \tag{6}$$

where

$$(\boldsymbol{\xi} \vee \boldsymbol{\xi})_k := \sqrt{\frac{d(d-1)}{2}}\,\frac{1}{d-2}\,d_{ijk}\xi_i\xi_j.$$

2.3. Composite states

From the standpoint of quantum information theory, of greatest interest are states composed of several qubits. According to the composite system axiom of quantum theory [4], the space of states of the system obtained by joining two systems A and B is a subspace of the tensor product of their individual Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$:

$$\mathcal{H} \subset \mathcal{H}_A \otimes \mathcal{H}_B. \tag{7}$$

The definition (7), in conjunction with the superposition principle, is the source of the appearance of correlations in the joint system that have no classical analog. If a mixed state ϱ, describing the joint system $A+B$, admits a (not necessarily unique) representation of the form

$$\varrho = \sum_{j=1}^{M} \omega_j\, \varrho_j^A \otimes \varrho_j^B, \quad \omega_j > 0\,, \quad \sum_{j=1}^{M} \omega_j = 1, \tag{8}$$

where ϱ_j^A and ϱ_j^B are the density matrices of the subsystems, then this joint state is called *separable* [7]. For such a state, correlations between the subsystems are classically conceivable. But the states of the form (8) are far from exhausting all possible states of the combined system. States that cannot be written in the form (8) are called *entangled*.

For a pair consisting of an r-qudit and an s-qudit, it is useful to represent the density matrix in the so-called Fano form [19, 20]:

$$\varrho = \frac{1}{rs}\left(\mathbb{I}_{rs} + \sum_{i=1}^{r^2-1} a_i\,\lambda_i \otimes \mathbb{I}_s + \sum_{i=1}^{s^2-1} b_i\,\mathbb{I}_r \otimes \tau_i + \sum_{i=1}^{r^2-1}\sum_{j=1}^{s^2-1} c_{ij}\lambda_i \otimes \tau_j\right). \tag{9}$$

In Eq. (9), the matrices λ_i and τ_i are basis elements of the algebras $\mathrm{su}(r)$ and $\mathrm{su}(s)$, respectively. The real $(r^2-1)\times(s^2-1)$ matrix $C = ||c_{ij}||$ is the so-called "*correlation matrix*." The meaning of the parameters $\boldsymbol{a} = (a_1, \ldots, a_{r^2-1})$ and $\boldsymbol{b} = (b_1, \ldots, b_{s^2-1})$ becomes clear after performing the partial trace operation (see [5])

$$\varrho^{(A)} := \mathrm{Tr}_B(\varrho) = \frac{1}{r}(\mathbb{I}_r + \boldsymbol{a}\cdot\boldsymbol{\lambda}), \quad \varrho^{(B)} := \mathrm{Tr}_A(\varrho) = \frac{1}{s}(\mathbb{I}_s + \boldsymbol{b}\cdot\boldsymbol{\tau}). \tag{10}$$

The vectors $\boldsymbol{a}$ and $\boldsymbol{b}$ are Bloch vectors for the subsystems whose states are described by the matrices $\varrho^{(A)}$ and $\varrho^{(B)}$, respectively.

The entanglement properties of density matrices (9), as well as of more general multipartite systems, admit a formulation in terms of invariants of the so-called local group [9]. In the next section, the corresponding notions will be introduced.

3. The entanglement space

3.1. The local invariance

On the space of density matrices of an n-level system, the adjoint action of the group $\mathrm{SU}(n)$ is defined:

$$\varrho \quad \to \quad \varrho' = U^\dagger \varrho\, U. \tag{11}$$

If a quantum system is obtained by combining r-subsystems with $n_1, n_2, \ldots, n_r$ levels together, the nonlocal properties of the composite system are in correspondence with a certain decomposition of the unitary operations (11). Namely, among all the unitary actions we distinguish the group of so-called *local unitary transformations* (LUT)

$$\mathrm{SU}(n_1) \otimes \mathrm{SU}(n_2) \otimes \cdots \otimes \mathrm{SU}(n_r), \tag{12}$$

acting independently on the density matrix of each subsystem:

$$\varrho^{(n_i)} \quad \to \quad \varrho^{(n_i)\prime} = g^\dagger \varrho^{(n_i)}\, g\,, \quad g \in \mathrm{SU}(n_i), \quad i = 1, 2, \ldots, r. \tag{13}$$

Two states of the composite system connected by a LUT transformation (12) have the same nonlocal properties. They can be changed only by the remaining unitary actions from

$$\frac{\mathrm{SU}(n)}{\mathrm{SU}(n_1) \otimes \mathrm{SU}(n_2) \otimes \cdots \otimes \mathrm{SU}(n_r)}, \tag{14}$$

generating the class of nonlocal transformations.

As was mentioned in the introduction, the action of LUT is not transitive. The equivalence of states with respect to the action (12) gives rise to a decomposition of the space of matrices into equivalences classes (orbits). The union of these classes, i.e., the orbit space, is usually called the "entanglement space" $\mathcal{E}_n$.

3.2. The orbit space and local polynomial invariants

The main motivation for the study of $\mathcal{E}_n$ is the necessity to work out qualitative criterions and quantitative measures for degrees of nonlocality [6, 12].

As was mentioned above, a canonical method for describing the orbit space $\mathcal{E}_n$ is the theory of invariants [11]. Within this approach, starting from the works by Linden and Popescu, a series of interesting results clarifying the mathematical contents of the entanglement phenomenon have been obtained. Considerable progress has been achieved for pure states. As an example, we refer to the construction of Hilbert series for multipartite systems of qubits [21] and the classification of pure entangled states based on the theory of hyperdeterminants [22].

The analysis of the orbit space for systems in mixed states is much more vague. The general questions concerning the construction of a basis for the ring of local invariants for mixed states were considered in [13, 14]. With this aim, algorithmic methods of computer algebra were used [23, 24].[3]

According to the theory of invariants [11], the ring of polynomial invariants $\mathbb{C}[V]^G$, of a linear space V over the field of complex numbers $\mathbb{C}$, under the action of a group G is the graded algebra

$$\mathbb{C}[V]^G = \bigoplus_{k=1}^{\infty} A_k\,,$$

where A_k is the space of homogeneous invariant polynomials of degree k.

The special unitary groups $\mathrm{SU}(n)$ belong to the class of reductive algebraic groups. The ring of invariants for these groups is finitely generated [11], and $\mathbb{C}[V]^G$ is the Cohen–Macaulay algebra [26]. However, the straightforward application of this construction to problems of quantum entanglement is complicated by the fact that the space V on which the group G acts is not a linear space. As was emphasized in the introduction, density matrices are positive semidefinite, and, therefore, the representation space V is a nonlinear semidefinite algebraic

[3] Unfortunately, the application of the existing algorithmic methods, including the Gröbner bases technique, to the analysis of the ring of polynomial invariants for multipartite systems is not effective due to the sharp growth of the number of algebraic operations with the increase of the number of qubits.

manifold. Below we suggest a solution to this issue, exemplified by the problem of describing the system of a qubit pair.

Let us start with the construction of the ring $\mathbb{C}[\mathcal{H}_{4\times4}]^{\mathrm{SU}(2)\otimes\mathrm{SU}(2)}$ of invariants of the adjoint action on the space of 4×4 Hermitian matrices $\mathcal{H}_{4\times4}$. In order to define the ring $\mathbb{C}[\mathfrak{P}_+]^{\mathrm{SU}(2)\otimes\mathrm{SU}(2)}$, note that the space of positive definite matrices $\mathfrak{P}_+$ is a subspace of $\mathcal{H}_{4\times4}$ invariant under the action of SU(4). As we demonstrate below, the subset $\mathfrak{P}_+$ admits a representation as a set of polynomial inequalities[4]

$$P_a(\mathfrak{C}_2,\mathfrak{C}_3,\mathfrak{C}_4)\geq 0,\quad a=1,2,3, \tag{15}$$

in three invariants, $\mathfrak{C}_2,\mathfrak{C}_3$, and $\mathfrak{C}_4$, of the enveloping algebra of the group SU(4). On the other hand, since $\mathfrak{C}_2,\mathfrak{C}_3,\mathfrak{C}_4$ are at the same time invariants of $\mathrm{SU}(2)\otimes\mathrm{SU}(2)$, one can construct a basis in $\mathbb{C}[\mathcal{H}_{4\times4}]^{\mathrm{SU}(2)\otimes\mathrm{SU}(2)}$ that includes these invariants. As a result, having this basis and taking into account the inequalities (15), we will be able to characterize the ring $\mathbb{C}[\mathfrak{P}_+]^{\mathrm{SU}(2)\otimes\mathrm{SU}(2)}$ completely. According to the considerations in the subsequent sections, a basis of the ring can be chosen in such a way that only the primary invariants of degree 2, 3 and one secondary invariant of degree 4 present in the Hironaka decomposition of the ring (see [11]) are constrained by the polynomial inequalities (15).

4. The nonnegativity of the density matrix

To succeed in our program of constructing an optimal homogeneous basis for the ring $\mathbb{C}[\mathfrak{P}_+]^{\mathrm{SU}(2)\otimes SU(2)}$, let us start with the requirement of positive semidefiniteness of density matrices. Below this requirement will be formulated in the form of inequalities constraining the values of invariants of the adjoint action of the group $\mathrm{SU}(n)$ on $\mathfrak{P}_+$.

4.1. $\mathfrak{P}_+$ in terms of Casimirs of $\mathrm{SU}(n)$

A Hermitian operator is positive semidefinite if and only if all its characteristic numbers are nonnegative. The condition of nonnegativity of a Hermitian operator can be formulated solely in terms of the coefficients of its characteristic equation:

$$|\mathbb{I}_n\,x-\varrho|=x^n-S_1x^{n-1}+S_2x^{n-2}-\ldots+(-1)^nS_n=0. \tag{16}$$

The coefficients S_k in Eq. (16) are the sums of principal minors of kth order:

$$S_k=\sum_{1\leq i_1<\ldots<i_k\leq n}\varrho\begin{pmatrix}i_1&\ldots&i_k\\ i_1&\ldots&i_k\end{pmatrix},\quad k=1,\ldots,n.$$

Since the matrix ϱ is Hermitian, all its characteristic numbers are real. If they are nonnegative, then all S_k are nonnegative as well, since S_k are symmetric polynomials in the roots x_k of the characteristic equations:

$$S_k=\sum_{1\leq i_1\leq\ldots\leq i_k\leq n}\prod_{j=1}^{k}x_{i_j}.$$

The converse statement is correct as well; the nonnegativity of the coefficients S_k implies the nonnegativity of the roots x_k. The proof of this observation [27] follows from the Descartes theorem [30]: the number of positive roots (taking into account their multiplicities) equals the number of sign changes in the sequence of coefficients of the polynomial equation.

Thus the nonnegativity of a density matrix can be written in an invariant way as the condition of nonnegativity of the coefficients of its characteristic equation:

$$S_k\geq 0,\quad k=1,\ldots,n. \tag{17}$$

[4] A description of $\mathfrak{P}_+$ similar to that given here can be found in [27–29].

We give, for further use, the explicit form of a few first coefficients S_k, written in terms of the n-dimensional Bloch vector $\boldsymbol{\xi}$ [27, 28]:

$$S_2 = \frac{1}{2!}\frac{n-1}{n}(1 - \boldsymbol{\xi}\cdot\boldsymbol{\xi}),$$
$$S_3 = \frac{1}{3!}\frac{(n-1)(n-2)}{n^2}(1 - 3\,\boldsymbol{\xi}\cdot\boldsymbol{\xi} + 2\,(\boldsymbol{\xi}\vee\boldsymbol{\xi})\cdot\boldsymbol{\xi}),$$
$$S_4 = \frac{1}{4!}\frac{(n-1)(n-2)(n-3)}{n^3}(1 - 6\,\boldsymbol{\xi}\cdot\boldsymbol{\xi} + 8\,(\boldsymbol{\xi}\vee\boldsymbol{\xi})\cdot\boldsymbol{\xi} + 3\frac{n-1}{n-3}(\boldsymbol{\xi}\cdot\boldsymbol{\xi})^2 - 6\frac{n-2}{n-3}(\boldsymbol{\xi}\vee\boldsymbol{\xi})\cdot(\boldsymbol{\xi}\vee\boldsymbol{\xi})).$$

Apart from the restrictions (17), there are upper bounds on S_k due to the normalization condition $\mathrm{Tr}(\varrho) = 1$, $\mathrm{Tr}(\varrho^k) \le 1$ for $k \ge 2$. Note that the equality is achieved for pure states, and the maximum values of S_k are achieved for equal eigenvalues x_i of the density matrix.

Finally, the positive semidefiniteness and normalizability conditions for the density matrices of an n-level system can be written as the following set of inequalities:

$$0 \le \frac{k!\,n^{k-1}}{(n-1)(n-2)\dots(n-k+1)}\,S_k \le 1, \qquad k = 2,\dots,n. \tag{18}$$

The coefficients S_k, $k = 1,\dots,n$, of the characteristic equation are invariants of the adjoint action of the group $\mathrm{SU}(n)$. They are algebraically independent and can be represented as polynomials in the Casimir operators of the corresponding enveloping algebra. Below, the case $n = 4$, related to the 2-qubit system, is considered in detail, and inequalities (18) are rewritten directly in terms of the Casimir operators of the enveloping algebra su(4).

4.2. Restrictions on invariants of su(4)

The group SU(4) has three Casimir operators whose expressions in terms of the components of the 15-dimensional Bloch vector $\boldsymbol{\xi}$ (see (4)) can be written as

$$\mathfrak{C}_2 = \boldsymbol{\xi}\cdot\boldsymbol{\xi}, \tag{19}$$
$$\mathfrak{C}_3 = \boldsymbol{\xi}\vee\boldsymbol{\xi}\cdot\boldsymbol{\xi}, \tag{20}$$
$$\mathfrak{C}_4 = \boldsymbol{\xi}\vee\boldsymbol{\xi}\cdot\boldsymbol{\xi}\vee\boldsymbol{\xi}. \tag{21}$$

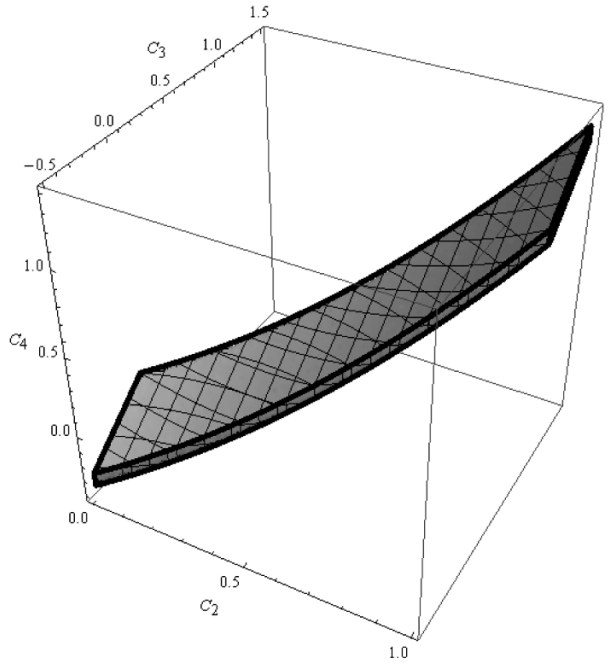

FIG. 1. The allowed region for the values of the Casimirs $\mathfrak{C}_2, \mathfrak{C}_3, \mathfrak{C}_4$.

Since the coefficients S_1, S_2, S_3 of the characteristic equation of the density matrix for an arbitrary 4-level system are expressible via these Casimir operators,

$$S_2 = \frac{3}{8}(1 - \mathfrak{C}_2),$$
$$S_3 = \frac{1}{16}(1 - 3\mathfrak{C}_2 + 2\mathfrak{C}_3),$$
$$S_4 = \frac{1}{256}((1 - 3\mathfrak{C}_2)^2 + 8\mathfrak{C}_3 - 12\mathfrak{C}_4),$$

the set (18) reduces to the following constraints on SU(4)-invariants:

$$\begin{aligned} &0 \le \mathfrak{C}_2 \le 1, \\ &0 \le 3\mathfrak{C}_2 - 2\mathfrak{C}_3 \le 1, \\ &0 \le (1 - 3\mathfrak{C}_2)^2 + 8\mathfrak{C}_3 - 12\mathfrak{C}_4 \le 1. \end{aligned} \tag{22}$$

In the space spanned by the invariants $\mathfrak{C}_2, \mathfrak{C}_3, \mathfrak{C}_4$, inequalities (22) define a bounded domain, which is depicted on Fig. 1.

5. The ring of local invariants $\mathbb{C}[\mathfrak{P}_+]^{\mathrm{SU}(2)\otimes\mathrm{SU}(2)}$

Consider the density matrix of two qubits parameterized in the Fano form [18, 19]:

$$\varrho = \frac{1}{4}\,[\,\mathbb{I}_2 \otimes \mathbb{I}_2 + \boldsymbol{a}\cdot\boldsymbol{\sigma} \otimes \mathbb{I}_2 + \mathbb{I}_2 \otimes \boldsymbol{b}\cdot\boldsymbol{\sigma} + c_{ij}\,\sigma_i \otimes \sigma_j\,], \tag{23}$$

where 3-component vectors $\boldsymbol{a} = (a_1, a_2, a_3)$, $\boldsymbol{b} = (b_1, b_2, b_3)$ are the Bloch vectors of the constituent qubits, and $\sigma_i,\ i = 1, 2, 3$, are the Pauli matrices forming a basis of the algebra su(2):

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{24}$$

The correlation matrix C of the pair of qubits has 9 elements $c_{ij},\ i, j = 1, 2, 3$.

First, following our program of constructing the ring of invariants $\mathbb{C}[\mathfrak{P}]^{\mathrm{SU}(2)\otimes\mathrm{SU}(2)}$ outlined in Sec. 3.2, we identify the space of parameters $\boldsymbol{a}, \boldsymbol{b}$, and C with $\mathbb{R}^{15}$, for a moment ignoring all restrictions implied by the condition of nonnegativity of density matrices. Besides, we linearize the adjoint action (11) of the local group $\mathrm{SU}(2) \otimes \mathrm{SU}(2)$:

$$V_A \ \to\ V'_A = L_{AB}V_B \quad A, B = 1, \ldots, 15, \tag{25}$$

with a 15×15 matrix $L \in \mathrm{SU}(2) \otimes \mathrm{SU}(2) \otimes \overline{\mathrm{SU}(2) \otimes \mathrm{SU}(2)}$.

Thus our preliminary task is to build the ring of polynomial invariants of the linear action of the group $\mathrm{SU}(2) \otimes \mathrm{SU}(2) \otimes \overline{\mathrm{SU}(2) \otimes \mathrm{SU}(2)}$ on the linear space $\mathbb{R}^{15}$. Note that the linearization (25) allows us to use a prompt following from the Molien formula for the generating function of invariants for a representation π_G of a compact group G, see [24]:

$$M(q) = \int\limits_G \mathrm{d}\,\mu_G\,\frac{1}{\det\,||\,\mathrm{id} - q\pi_G||}, \tag{26}$$

where the integral is taken over the group G with the Haar measure $\mathrm{d}\,\mu_G$.

The Molien function provides information on the structure of the ring of polynomial invariants. First, its formal expansion in powers of the parameter q, the so-called Hilbert–Poincare series

$$M(q) = \sum_{k\ge 0} d_k q^k \ \in \mathbb{Z}[q],$$

points out the dimension, d_k, of the space of homogeneous invariants of degree k. Second, being a rational function, (26) admits, for $q < 1$, a (non-unique) representation of the form

$$M(q) = \frac{\sum\limits_{k=0}^{r} q^{\deg J_k}}{\Pi_{m=1}^{n}(1 - q^{\deg K_m})}.$$

From this form of the Molien function one can conclude on the number and order of the primary (K_i, $i = 1, 2, \ldots, n$) and secondary (J_i, $i = 1, 2, \ldots, r$) invariants of the Cohen–Macaulay algebra

$$\mathbb{C}[V]^G = \bigoplus_{k=0}^{r} J_k \, \mathbb{C}[K_1, K_2, \ldots, K_n]. \tag{27}$$

As computations show, the Molien function for mixed states of two qubits can be written as (see [13, 14])

$$M(q) = \frac{1 + q^4 + q^5 + 3q^6 + 2q^7 + 2q^8 + 3q^9 + q^{10} + q^{11} + q^{15}}{(1-q)(1-q^2)^3(1-q^3)^2(1-q^4)^3(1-q^6)}. \tag{28}$$

According to (28), a basis of the ring consists of 10 primary invariants of degrees $1, 2, 2, 2, 3, 3, 4, 4, 4, 6$ and 15 secondary invariants of degrees $4, 5, 6, 6, 6, 7, 7, 8, 8, 9, 9, 9, 10, 11, 15$.

A more detailed information on the dependence of invariants on the coefficients of the decomposition (23) can be extracted using the so-called method of multi-parameter generating functions [24]. In our case, the multi-parameter generating function depends not only on one parameter q, but is a function of three parameters, $F(a, b, c)$. The contribution from the variables $\boldsymbol{a}$, $\boldsymbol{b}$, and c_{ij} to the Molien function is now taken with a weight determined by the independent parameters a, b, and c, respectively.

It is worth noting that the generating function $F(a, b, c)$ was found as early as in the middle 1970s [31, 32], in connection with the so-called "*missing index*" problem, which arose in the nuclei spectrum classification. The corresponding mathematical formulation of the problem and its solution can be found, e.g., in [31]. In the remaining part of our presentation, we will mainly follow the article [32].

Consider the space of all polynomials in fifteen variables a_i, b_i, c_{ij} $i, j = 1, 2, 3$. In view of the adjoint action of the local group, the space of Bloch parameters is decomposed into irreducible representations of the group $SO(3) \otimes SO(3)$. More precisely, the variables a_i, b_i, c_{ij} are being transformed according to the representations $D_1 \times D_0$, $D_0 \times D_1$, and $D_1 \times D_1$, respectively. Since the subspace $P_{s,t,q}[a_i, b_i, c_{ij}]$ of homogeneous polynomials in the variables a_i, b_i, c_{ij} of degree s, t, q is invariant under the action of $\mathrm{SU}(2) \otimes \mathrm{SU}(2)$, all invariants C can be classified according to their degrees of homogeneity, $C^{(s\,t\,q)}$.

Following the construction suggested in [32], consider the following set of invariants:[5]

- 3 invariants of second degree,

$$C^{(002)} = c_{ij}c_{ij}, \quad C^{(200)} = a_i a_i, \quad C^{(020)} = b_i b_i; \tag{29}$$

- 2 invariants of third degree,

$$C^{(003)} = \frac{1}{3!}\epsilon_{ijk}\epsilon_{\alpha\beta\gamma}c_{i\alpha}c_{j\beta}c_{k\gamma}, \quad C^{(111)} = a_i c_{ij} b_j; \tag{30}$$

- 4 invariants of fourth degree,

$$C^{(004)} = c_{i\alpha}c_{i\beta}c_{j\alpha}c_{j\beta}, \tag{31}$$
$$C^{(202)} = a_i a_j c_{i\alpha}c_{j\alpha}, \tag{32}$$
$$C^{(022)} = b_\alpha b_\beta c_{i\alpha}c_{i\beta}, \tag{33}$$
$$C^{(112)} = \epsilon_{ijk}\epsilon_{\alpha\beta\gamma}a_i b_\alpha c_{j\beta}c_{k\gamma}; \tag{34}$$

- 1 invariant of fifth degree,

$$C^{(113)} = a_i c_{i\alpha}c_{\beta\alpha}c_{\beta j}b_j; \tag{35}$$

- 4 invariants of sixth degree,

$$C^{(123)} = \epsilon_{ijk}b_i c_{\alpha j}a_\alpha c_{\beta k}c_{\beta l}b_l, \tag{36}$$
$$C^{(204)} = a_i c_{i\alpha}c_{j\alpha}c_{j\beta}c_{k\beta}a_k, \tag{37}$$
$$C^{(024)} = b_i c_{\alpha i}c_{\alpha j}c_{\beta j}c_{\beta,k}b_k, \tag{38}$$
$$C^{(213)} = \epsilon_{\alpha\beta\gamma}a_\alpha c_{\beta i}b_i c_{\gamma j}c_{\delta j}a_\delta; \tag{39}$$

[5] In the expressions below, we always assume that the summation is over all repeated indices from one to three.

• 2 invariants of seventh degree,

$$C^{(214)} = \epsilon_{ijk} b_i c_{\alpha j} a_\alpha c_{\beta k} c_{\beta l} c_{\gamma l} a_l, \tag{40}$$

$$C^{(124)} = \epsilon_{\alpha\beta\gamma} a_\alpha c_{\beta j} b_j c_{\gamma k} c_{\delta k} c_{\delta l} b_l; \tag{41}$$

• 2 invariants of eighth degree,

$$C^{(125)} = \epsilon_{ijk} b_i c_{\alpha j} c_{\alpha l} b_l c_{\beta k} c_{\beta m} c_{\gamma m} a_\gamma, \tag{42}$$

$$C^{(215)} = \epsilon_{\alpha\beta\gamma} a_\alpha c_{\beta i} c_{\delta i} a_\delta c_{\gamma k} c_{\varrho k} c_{\varrho l} b_l; \tag{43}$$

• 2 invariants of ninth degree,

$$C^{(306)} = \epsilon_{\alpha\beta\gamma} a_\alpha c_{\beta i} c_{\delta i} a_\delta c_{\gamma j} c_{\varrho j} c_{\varrho k} c_{\sigma k} a_\sigma, \tag{44}$$

$$C^{(036)} = \epsilon_{ijk} b_i c_{\alpha j} c_{\alpha l} b_l c_{\beta k} c_{\beta m} c_{\gamma m} c_{\gamma s} b_s. \tag{45}$$

From these invariants a basis of $\mathbb{C}[\mathfrak{P}_+]^{\mathrm{SU}(2)\otimes\mathrm{SU}(2)}$ can be build. As a criterion for its construction, we choose the principle of using a basis with the minimum number of elements involved in the definition of $\mathfrak{P}_+$. Having in mind this rule and noting that the space $\mathfrak{P}_+$ is defined in terms of the Casimir operators (19)–(21) of the group SU(4), we expand $\mathfrak{C}_2, \mathfrak{C}_3, \mathfrak{C}_4$ in terms of the local invariants (29)–(31) introduced above:

$$\mathfrak{C}_2 = \frac{1}{3}\,(C^{(200)} + C^{(020)} + C^{(002)}), \tag{46}$$

$$\mathfrak{C}_3 = C^{(111)} - C^{(003)}, \tag{47}$$

$$\mathfrak{C}_4 = \frac{1}{6}\,[2(C^{(200)}C^{(020)} + C^{(202)} + C^{(022)} - C^{(112)}) + (C^{(002)})^2 - C^{(004)}]. \tag{48}$$

From Eqs. (46)–(48) it follows that one can consider the Casimir operators $\mathfrak{C}_2, \mathfrak{C}_3, \mathfrak{C}_4$ as basis elements instead of the scalars $C^{(002)}, C^{(003)}$, and $C^{(112)}$.

Bearing in mind this observation and using the results of [14], where the ring $\mathbb{C}[\mathbb{R}^{16}]^{\mathrm{SU}(2)\otimes\mathrm{SU}(2)}$ was described, we define the following set consisting of 10 *primary invariants*, including the Casimir operators $\mathfrak{C}_2, \mathfrak{C}_3$:

$$\deg = 1, \quad K_1 = 1, \tag{49}$$

$$\deg = 2, \quad K_2 = \mathfrak{C}_2, \qquad K_3 = C^{(200)}, \quad K_4 = C^{(020)}, \tag{50}$$

$$\deg = 3, \quad K_5 = \mathfrak{C}_3, \qquad K_6 = C^{(111)}, \tag{51}$$

$$\deg = 4, \quad K_7 = C^{(004)}, \qquad K_8 = C^{(202)}, \quad K_9 = C^{(022)}, \tag{52}$$

$$\deg = 6, \quad K_{10} = C^{(204)} + C^{(024)}, \tag{53}$$

and 15 *secondary invariants*, including the Casimir operator $\mathfrak{C}_4$,

$$\deg = 4, \quad J_1 = \mathfrak{C}_4, \tag{54}$$

$$\deg = 5, \quad J_2 = C^{(113)}, \tag{55}$$

$$\deg = 6, \quad J_3 = C^{(204)} - C^{(024)}, \quad J_8 = C^{(123)}, \quad J_9 = C^{(213)}, \tag{56}$$

$$\deg = 7, \quad J_{10} = C^{(214)}, \qquad J_{11} = C^{(124)}, \tag{57}$$

$$\deg = 8, \quad J_{12} = C^{(215)}, \qquad J_{13} = C^{(125)}, \tag{58}$$

$$\deg = 9, \quad J_4 = J_1 J_2, \qquad J_{14} = C^{(306)}, \quad J_{15} = C^{(036)}, \tag{59}$$

$$\deg = 10, \quad J_5 = J_1 J_3, \tag{60}$$

$$\deg = 11, \quad J_6 = J_2 J_3, \tag{61}$$

$$\deg = 15, \quad J_7 = J_1 J_2 J_3. \tag{62}$$

We conclude that the set of homogeneous invariants (49)–(62) is a basis for the ring $\mathbb{C}[\mathfrak{P}]^{\mathrm{SU}(2)\otimes\mathrm{SU}(2)}$:

$$\mathbb{C}[\mathfrak{P}_+]^{\mathrm{SU}(2)\otimes\mathrm{SU}(2)} = \bigoplus_{k=0}^{15} J_k\, \mathbb{C}[K_1, K_2, \ldots, K_{10}], \tag{63}$$

under the condition that two primary invariants K_2, K_5 and one secondary invariant J_1 satisfy inequalities (22).

6. Conclusion

An important problem of the quantum theory of information is qualitative and quantitative characterization of purely quantum correlations caused by the entanglement of quantum states. The theory of classical invariants provides tools for the study of the corresponding entanglement space, i.e., the orbit space of the action of the group of local transformations on the space of states of composite systems. For the case we are interested in, the system of two qubits in a mixed state, the local transformations of density matrices form the group $\mathrm{SU}(2)\otimes\mathrm{SU}(2)$. Its adjoint action, on the space of Hermitian unit-trace matrices identified with $\mathbb{R}^{15}$, determines the principal orbit space

$$\mathcal{O} := \frac{\mathbb{R}^{15}}{\mathrm{SU}(2)\otimes\mathrm{SU}(2)},$$

of dimension

$$\dim \mathcal{O} = 15 - 2\times 3 = 9.$$

However, the orbit space defined in this way is not the entanglement space $\mathcal{E}_2$. Due to the nonnegativity of density matrices, the space of physical states is $\mathfrak{P}_+ \subset \mathbb{R}^{15}$. In the present article, we suggest a description of $\mathfrak{P}_+$ based on polynomial inequalities in the Casimir operators of the enveloping algebra su(4). Furthermore, we show how these restrictions can be effectively taken into account when constructing a basis for the ring $\mathbb{C}[\mathfrak{P}_+]^{\mathrm{SU}(2)\otimes\mathrm{SU}(2)}$ in which only two primary invariants of degree 2, 3 and one secondary invariant of degree 4 in the Hironaka decomposition are constrained by the polynomial inequalities (22).

In conclusion, it is important to emphasize that without inequalities (22), the usage of local invariants for "coordinatization" of the entanglement space $\mathcal{E}_2$ is not correct. We leave the analysis of consequences imposed by these constraints on the geometry of $\mathcal{E}_2 \subset \mathcal{O}$ for future publications.

Acknowledgments

This work was supported in part by the Georgian National Science Foundation research grant GNSF/ST08/4-405, by the Russian Foundation for Basic Research grant No. 10-01-00200, and by the Ministry of Education and Science of the Russian Federation grant No. 3810.2010.2.

Translated by A. Khvedelidze.

REFERENCES

1. A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?" *Phys. Rev.*, **47**, 777–780 (1935).
2. J. Bell, *Speakable and Unspeakable in Quantum Mechanics*, Cambridge Univ. Press, Cambridge (1987).
3. A. Aspect, "Bell's theorem: the naive view of an experimentalist," in: R. A. Bertlmann and A. Zeilinger (eds.), *Quantum [Un]speakables: From Bell to Quantum Information*, Springer-Verlag, Berlin (2002).
4. M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Camridge Univ. Press, Cambridge (2000).
5. V. Vedral, *Introduction to Quantum Information Science*, Oxford Univ. Press, New York (2006).
6. I. Bengtsson and K. Życzkowski, *Geometry of Quantum States. An Introduction to Quantum Entanglement*, Cambridge Univ. Press, Cambridge (2006).
7. R. F. Werner, "Quantum states with Einstein–Podolski–Rosen correlations admitting a hidden-variable model," *Phys. Rev. A*, **40**, 4277–4281 (1989).
8. J. Schlienz and G. Mahler, "Description of entanglement," *Phys. Rev. A*, **52**, 4396–4404 (1995).
9. N. Linden and S. Popescu, "On multi-particle entanglement," *Fortschr. Phys.*, **46**, 567–578 (1998).
10. H. Weyl, *The Classical Groups: Their Invariants and Representations*, Princeton Univ. Press, Princeton (1939).
11. V. L. Popov and E. B. Vinberg, "Invariant theory", in: *Algebraic Geometry IV*, Encycl. Math. Sci., **55**, Springer-Verlag (1994), pp. 123–273.
12. M. Kus and K. Życzkowski, "Geometry of entangled states," *Phys. Rev. A*, **63**, 032307 (2001).
13. M. Grassl, M. Rötteler, and T. Beth, "Computing local invariants of qubit systems," *Phys. Rev. A*, **58**, 1853–1856 (1998).
14. R. C. King, T. A. Welsh, and P. D. Jarvis, "The mixed two-qubit system and the structure of its ring of local invariants," *J. Phys. A*, **40**, 10083–10108 (2007).

15. J. von Neumann, "Warscheinlichtkeitstheoritischer Aufbau der Quantenmechanik," *Nachrichten Göttingen*, 245–272 (1927).
16. L. D. Landau, "Das Dämpfungsproblem in der Wellenmechanik," *Z. f. Physik*, **45**, 430–441 (1927).
17. K. Blum, *Density Matrix. Theory and Applications*, Plenum Press, New York (1981).
18. F. T. Hioe and J. H. Eberly, "N-Level coherence vector and higher conservation laws in quantum optics and quantum mechanics," *Phys. Rev. Lett.*, **47**, 838–841 (1981).
19. U. Fano, "Description of states in quantum mechanics by density matrix and operator techniques," *Rev. Mod. Phys.*, **29**, 74–93 (1957).
20. U. Fano, "Pairs of two-level systems," *Rev. Mod. Phys.*, **55**, 855–874 (1983).
21. J.-G. Luque and J.-Y. Thibon, "The polynomial invariants of four qubits," *Phys. Rev. A*, **63**, 042303 (2003). J.-G. Luque and J.-Y. Thibon, "Algebraic invariants of five qubits," *J. Phys. A*, **39**, 371–377 (2005).
22. A. Miyake, "Classification of multipartite entangled states by multidimensional determinants," *Phys. Rev. A*, **67**, 012108 (2003).
23. B. Sturmfels, *Algorithms in Invariant Theory*, Springer-Verlag, Wien (1993).
24. H. Derksen and G. Kemper, *Computational Invariant Theory*, Encycl. Math. Sci., **130**, Springer-Verlag, Berlin (2002).
25. B. Buchberger, "Gröbner bases – an algorithmic method in polynomial ideal theory," in: N. K. Bose (ed.), *Multidimensional Systems Theory*, D. Reidel, Dordrecht (1985), pp. 184–232.
26. M. Hochster and J. Roberts, "Rings of invariants of reductive groups acting on regular rings are Cohen–Macaulay," *Adv. Math.*, **13**, 125–175 (1974).
27. G Kimura, "The Bloch vector for N-level systems," *Phys. Lett. A*, **314**, 339–349 (2003),
28. M. S. Byrd and N. Khaneja, "Characterization of the positivity of the density matrix in terms of the coherence vector representation," *Phys. Rev. A*, **68**, 062322 (2003).
29. S. Kryszewski and M. Zachcial, "Positivity of the $N \times N$ density matrix expressed in terms of polarization operators," *J. Phys. A*, **39**, 5921–5931 (2006).
30. E. B. Vinberg, *A Course in Algebra* [in Russian], Factorial, Moscow (2002).
31. B. R. Judd, W. Miller Jr., J. Patera, and P. Winternitz, "Complete set of commuting operators and O(3) scalars in the enveloping algebra of $SU(3)$," *J. Math. Phys.*, **15**, 1787–1799 (1974).
32. C. Quesne, "$SU(2) \otimes SU(2)$ scalars in the enveloping algebra of $SU(4)$," *J. Math. Phys.*, **17**, 1452–1467 (1976).