DOI 10.1007/s10958-017-3409-1
Journal of Mathematical Sciences, Vol. 224, No. 2, July, 2017

ON THE RING OF LOCAL UNITARY INVARIANTS FOR MIXED X-STATES OF TWO QUBITS

V. Gerdt,[*] **A. Khvedelidze,**[†] **and Yu. Palii**[‡]

UDC 512.714, 530.145

Entangling properties of a mixed two-qubit system can be described by local homogeneous unitary invariant polynomials in the elements of the density matrix. The structure of the corresponding ring of invariant polynomials for a special subclass of states, the so-called mixed X-states, is established. It is shown that for the X-states there is an injective ring homomorphism of the quotient ring of $SU(2) \times SU(2)$-invariant polynomials modulo its syzygy ideal to the $SO(2) \times SO(2)$-invariant ring freely generated by five homogeneous polynomials of degrees $1, 1, 1, 2, 2$. *Bibliography:* 18 *titles.*

1. Introduction

• **Motivation** • In this paper, we consider a bipartite quantum system composed of two qubits, whose state space $\mathfrak{P}_X$ is a special 7-dimensional family of so-called X-states [1]. Our interest to this subspace of a generic two-qubit space $\mathfrak{P}$ is due to the fact that many well-known states, e.g., Bell states [2], Werner states [3], isotropic states [4], and maximally entangled mixed states [5, 6], are particular subsets of X-states. Since their introduction in [1], many interesting properties of X-states have been established. In particular, it was shown that for a fixed set of eigenvalues, the states of maximal concurrence, negativity, or relative entropy of entanglement are X-states.[1]

• **Content** • Here we pose the question of studying the algebraic structure of the algebra of local unitary polynomial invariants corresponding to the X-states. More precisely, the fate of the ring of generic $SU(2) \times SU(2)$-invariant polynomials [8–11] under the restriction of the total two-qubit state space $\mathfrak{P}$ to its subspace $\mathfrak{P}_X$ will be discussed. The quotient structure of the ring obtained as the result of this restriction will be determined. Furthermore, we establish an injective homomorphism between this ring and the invariant ring $\mathbb{R}[\mathfrak{P}_X]^{SO(2)\times SO(2)}$ of local unitary invariant polynomials for two-qubit X-states. In doing so, we show that the latter ring is *freely* generated by five homogeneous invariants of degrees 1, 1, 1, 2, 2.

2. Framework and settings

In this section, a collection of main algebraic structures associated with a finite-dimensional quantum system is given.

2.1. General algebraic settings and conventions.

Hereafter, we use the standard notation $\mathbb{R}[x_1, \dots, x_n]$ for the ring of polynomials in n variables $x_1, \dots, x_n$ with coefficients in $\mathbb{R}$. Given a polynomial set

$$F := \{ f_1, \dots, f_m \} \in \mathbb{R}[x_1, \dots, x_n], \tag{1}$$

[*] Laboratory of Information Technologies, Joint Institute for Nuclear Research; University "Dubna," Dubna, Russia, e-mail: gerdt@jinr.ru.

[†] Institute of Quantum Physics and Engineering Technologies, Georgian Technical University; A. Razmadze Mathematical Institute, Iv. Javakhishvili Tbilisi State University, Tbilisi, Georgia; National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Moscow, Russia, e-mail: akhved@jinr.ru.

[‡] Institute of Applied Physics, Chisinau, Republic of Moldova, e-mail: palii@jinr.ru.

[1] For a detailed review of X-states and their applications, we refer to the recent article [7].

Published in *Zapiski Nauchnykh Seminarov POMI*, Vol. 448, 2016, pp. 107–123. Original article submitted September 16, 2016.

generating the subring

$$\mathbb{R}[F] := \mathbb{R}[f_1, \dots, f_m] \subset \mathbb{R}[x_1, \dots, x_n], \tag{2}$$

we will consider the polynomial ring $\mathbb{R}[y_1, \dots, y_m]$ associated with $\mathbb{R}[F]$, where $y_1, \dots, y_m$ are variables (indeterminates).

Note that $\mathbb{R}[F]$ differs from the *ideal* $I_F = \langle F \rangle \subseteq \mathbb{R}[x_1, \dots, x_n]$ generated by F:

$$I_F = \left\{ \sum_{i=1}^{m} h_i f_i \mid h_1, \dots, h_m \in \mathbb{R}[x_1, \dots, x_n] \right\}. \tag{3}$$

The polynomial set F determines a real affine variety $V \subset \mathbb{R}^m$. The radical $I(V) := \sqrt{I_F}$ of I_F, i.e., the ideal such that $f \in \sqrt{I_F}$ if and only if $f^m \in I_F$ for some positive integer m, yields the *coordinate ring* of V as the quotient ring

$$\mathbb{R}[x_1, \dots, x_n]/I(V). \tag{4}$$

A nonzero polynomial $g(y_1, \dots, y_m) \in \mathbb{R}[y_1, \dots, y_m]$ such that

$$g(f_1, \dots, f_m) = 0$$

in $\mathbb{R}[x_1, \dots, x_n]$ is called a *syzygy*, or a *nontrivial algebraic relation* among $f_1, \dots, f_m$. The set of all syzygies forms the *syzygy ideal*

$$I_F := \{ s \in \mathbb{R}[y_1, \dots, y_m] \mid s = 0 \text{ in } \mathbb{R}[x_1, \dots, x_n] \}.$$

The following ring isomorphism holds (cf. [12, Chap. 7, Proposition 2]):

$$\mathbb{R}[F] \cong \mathbb{R}[y_1, \dots, y_m]/I_F. \tag{5}$$

Given an ideal I_F in (3), a subset $\mathfrak{X} \subseteq \{ x_1, \dots, x_n \}$ of indeterminates is called *independent modulo* I_F if $I_F \cap \mathbb{R}[\mathfrak{X}] = \{ \}$. Otherwise $\mathfrak{X}$ is called *dependent modulo* I_F. The *affine dimension* of I_F, denoted by $\dim(I_F)$, is defined to be the cardinality of a largest subset independent modulo I_F. If $I_F = \mathbb{R}[x_1, \dots, x_n] = \langle 1 \rangle$, then the affine dimension of I_F is defined to be -1.

The ring of elements in $\mathbb{R}[x_1, \dots, x_n]$ invariant under the action of a group G on $\{ x_1, \dots, x_n \}$ will be denoted by $\mathbb{R}[x_1, \dots, x_n]^G$.

2.2. Settings for quantum systems. The mathematical structures associated with finite-dimensional quantum systems, in particular, with multi-qubit systems, can be described as follows.

• The quantum state space • Introducing the space of $n \times n$ Hermitian matrices H_n, one can identify the density operators of an individual qubit and of a pair of qubits with a certain variety of H_2 and H_4, respectively. In general, for an n-dimensional quantum system, this variety, the *state space* $\mathfrak{P}(H_n)$, is the subset of elements from H_n that satisfy the semipositivity and unit trace conditions:

$$\mathfrak{P}(H_n) := \{ \varrho \in H_n \mid \varrho \geq 0, \ \operatorname{tr} \varrho = 1 \}.$$

• The unitary symmetry of the state space • The traditional guiding philosophy in the study of physical models is based on the symmetry principle. In the case of quantum theory, the basic symmetry is realized in the form of the adjoint action of the unitary group $U(n)$ on H_n:

$$(g, \varrho) \to g \varrho g^\dagger , \qquad g \in U(n), \quad \varrho \in H_n. \tag{6}$$

Owing to this *global unitary symmetry*, the correspondence between states and physically relevant configurations is not one-to-one. All density matrices along the unitary orbit

$$\mathcal{O}_\varrho = \{ g \varrho g^\dagger, \ g \in SU(n) \}$$

represent one and the same physical state. The symmetry transformations (6) establish the equivalence relation $\varrho \sim g \varrho g^\dagger$ on the state space $\mathfrak{P}(H_n)$. This equivalence defines the quotient space $\mathfrak{P}(H_n)/\sim$ and allows one to "reduce" the above outlined "redundant" description of a quantum system by passing to the *global unitary orbit space* $\mathfrak{P}(H_n)/U(n)$. The global unitary orbit space accumulates all physically relevant information about the system as a whole. Characteristics of $\mathfrak{P}(H_n)/U(n)$ as an algebraic variety are encoded in the center of the universal enveloping algebra $\mathfrak{U}(\mathfrak{su}(n))$, and can be described in terms of the algebra of real $SU(n)$-invariant polynomials in $\mathfrak{P}(H_n)$.

• Composite quantum systems • If the space H_n is associated with a composite quantum system, then another symmetry comes into play, the so-called *local unitary group*. Restricting ourselves to the case of a two-qubit system, the local unitary group is identified with the subgroup $G = SU(2) \times SU(2) \subset SU(4)$ of the global unitary group $SU(4)$. In contrast to the global unitary symmetry, the local unitary group establishes an equivalence between states of a composite system that have one and the same entangling properties. The algebra of corresponding *local unitary* G-invariant polynomials can be used for quantitative characterization of entanglement. Having in mind the application to a two-qubit system, it is convenient to introduce a $\mathbb{Z}^3$-grading in this algebra of local unitary G-invariant polynomials. This can be achieved by considering the algebra $\imath\mathfrak{su}(4)$ from elements of H_4:

$$\varrho = \frac{1}{4}\left[I_4 + \imath\mathfrak{su}(4)\right], \qquad I_4 \text{ is the identity } 4 \times 4 \text{ matrix,}$$

and decomposing the latter into the direct sum of three real spaces

$$V_1 = \imath\mathfrak{su}(2) \otimes I_2, \qquad V_2 = I_2 \otimes \imath\mathfrak{su}(2), \qquad V_3 = \imath\mathfrak{su}(2) \otimes \imath\mathfrak{su}(2), \tag{7}$$

each representing a G-invariant subspace. Note that if a basis for the algebra $\mathfrak{su}(2)$ in each subspace V is chosen using the Pauli matrices $\boldsymbol{\sigma} = (\sigma_1, \sigma_2, \sigma_3)$, the above G-invariant $\mathbb{Z}^3$-grading gives

$$\varrho = \frac{1}{4}\left[I_2 \otimes I_2 + \sum_{i=1}^{3} a_i \sigma_i \otimes I_2 + \sum_{i=1}^{3} b_i I_2 \otimes \sigma_i + \sum_{i,j=1}^{3} c_{ij} \sigma_i \otimes \sigma_j\right]. \tag{8}$$

This representation of a two-qubit state is known as the Fano decomposition [13]. The real parameters a_i, b_i, and c_{ij}, $i, j = 1, 2, 3$, are subject to constraints coming from the semipositivity condition imposed on the density matrix:

$$\varrho \geq 0. \tag{9}$$

Explicitly, the semipositivity condition (9) reads as a set of polynomial inequalities in the fifteen variables a_i, b_i, and c_{ij} (see, e.g., [11] and references therein).

3. Applying invariant theory

The entangling properties of composite quantum systems admit a description within the general framework of the classical theory of invariants (see [14, 15] and references therein).

As mentioned above, for a two-qubit system, the local unitary group is $G = SU(2) \times SU(2)$. The adjoint action (6) of this group on the two-qubit density matrix ρ induces transformations on the space W defined by the 15 real Fano variables[2] (8):

$$W := \{\, (a_i, b_j, c_{kl}) \in \mathbb{R}^{15} \mid i, j, k, l = 1, 2, 3 \,\}; \tag{10}$$

and the corresponding G-invariant polynomials accumulate all relevant information on the two-qubit entanglement.

Now we will give some known results on the structure of the ring of G-invariant polynomials. It is worth noting that most of these results are applicable to linear actions of compact groups

[2] More precisely, in correspondence with the above-mentioned $\mathbb{Z}^3$-grading, W is the space of irreducible representations of the form $D_1 \times D_0$, $D_0 \times D_1$, and $D_1 \times D_1$ of $SU(2) \times SU(2)$, respectively.

on linear spaces and thus cannot be directly used for a description of quantum systems, due to the semipositivity of the density matrix (9). However, for a moment we relax the semipositivity constraints on the Fano parameters and identify the space W with $\mathbb{R}^{15}$. The positivity of density matrices can be written in a G-invariant form and, therefore, can be taken into account later.

• **The ring of G-invariant polynomials** • Let $\mathbb{R}[W] := \mathbb{R}[x_1, x_2, \ldots, x_{15}]$ be the coordinate ring of W (with the ideal $I(W) = \{0\}$ in (4)), and let $R := \mathbb{R}[W]^G \subset \mathbb{R}[W]$ be the subring of polynomials invariant under the above-mentioned transformations on W. The ring of invariant polynomials R has the following important properties [10,15].

- The ring R is a graded algebra over $\mathbb{R}$, and, according to the classical Hilbert theorem, there is a finite set of homogeneous *fundamental invariants* generating R as an $\mathbb{R}$-algebra.
- The invariant ring R is Cohen–Macaulay, that is, R is a finitely generated free module over $\mathbb{R}[F_p]$ (Hironaka decomposition):
$$R = \bigoplus_{f_k \in F_s} f_k \, \mathbb{R}[F_p],$$
where F_p is a set of algebraically independent *primary invariants*, or *homogeneous system of parameters* [15], sometimes called an *integrity basis*, and F_s is a set of linearly independent *secondary invariants.* Here $1 \in F_s$, and the set $F_p \cup F_s$ generates R.
- Let R_k be the subspace spanned by all homogeneous invariants in R of degree k. If this subspace has dimension d_k, then the corresponding Molien series
$$M(q) = \sum_{k=0}^{\infty} d_k q^k \qquad (11)$$
generated by the Molien function $M(q)$ contains information on the number of primary and secondary invariants and their degrees (see formula (12) in the next section).
- Orbit separation: for any $u, v \in W$ such that $G \cdot u \neq G \cdot v$ there exists $p \in R$ such that $p(u) \neq p(v)$.

Because of the G-invariance of polynomials in R, their orbit separation property, and the Noetherianity of R, the use of fundamental invariants is natural in the description of the orbit space of a linear action of a compact Lie group and, in particular, of the G-invariant entanglement space of two-qubit states.

• **Computational aspects** • Constructive methods and algorithms for computing homogeneous generators of invariant rings are the main research objects of computational invariant theory [15,16]. There are various algorithms known in the literature and implemented in computer algebra software, e.g., Maple, Singular, Magma (see [15, Chaps. 3 and 4] and [17]). But, unfortunately, constructing a basis of invariants for $SU(2) \times SU(2)$ is too hard computationally for all those algorithms oriented to some rather wide classes of algebraic groups, and an integrity basis together with a set of secondary invariants for this group have been constructed (see [10] and references therein) by methods exploiting its special properties. We will use this basis in the next sections. Moreover, even our attempts to verify the algebraic independence of the primary invariants, that is, to check that the variety in $\mathbb{C}$ defined by the polynomial set F_p is 0, by using the standard Gröbner basis technique for algebraic elimination failed because of too large computer resources required.

3.1. A basis of the ring of $SU(2) \times SU(2)$-invariants. For two qubits, a basis of the polynomial ring $\mathbb{R}[W]^{SU(2)\times SU(2)}$ was constructed in [10]. An explicit form of its elements will be presented below.

As mentioned above, the space of polynomials in the fifteen variables (10) is decomposed into irreducible representations of $SO(3) \times SO(3)$. Furthermore, it inherits the $\mathbb{Z}^3$-grading from H_4, since the space of homogeneous polynomials of degree s, t, q in a_i, b_i, c_{ij} $(i, j = 1, 2, 3)$, respectively, is invariant under the action of $SU(2) \times SU(2)$. All such invariants C can be classified according to their degrees s, t, q of homogeneity in a_i, b_i, c_{ij}. Following Quesne's construction [8], we will denote them by $C^{(s\,t\,q)}$. The degrees of homogeneous polynomials can be controlled from the knowledge of the Molien function. The Molien function for mixed states of two qubits (see [8–10]),

$$M(q) = \frac{1 + q^4 + q^5 + 3q^6 + 2q^7 + 2q^8 + 3q^9 + q^{10} + q^{11} + q^{15}}{(1-q)(1-q^2)^3(1-q^3)^2(1-q^4)^3(1-q^6)}, \tag{12}$$

shows that an integrity basis of the invariant ring consists of 10 primary invariants of degrees $1, 2, 2, 2, 3, 3, 4, 4, 4, 6$, and there are 15 secondary invariants, whose degrees are $4, 5, 6, 6, 6, 7, 7, 8, 8, 9, 9, 9, 10, 11, 15$. Quesne's invariants represent the source of such primary and secondary invariants. Explicitly, Quesne's invariants are as follows:

3 invariants of the second degree

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

2 invariants of the third degree

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

4 invariants of the fourth degree

$$\begin{aligned} C^{(004)} &= c_{i\alpha}c_{i\beta}c_{j\alpha}c_{j\beta}, \\ C^{(202)} &= a_i a_j c_{i\alpha}c_{j\alpha}, \\ C^{(022)} &= b_\alpha b_\beta c_{i\alpha}c_{i\beta}, \\ C^{(112)} &= \frac{1}{2}\,\epsilon_{ijk}\epsilon_{\alpha\beta\gamma}a_i b_\alpha c_{j\beta}c_{k\gamma}, \end{aligned}$$

1 invariant of the fifth degree

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

4 invariats of the sixth degree

$$\begin{aligned} C^{(123)} &= \epsilon_{ijk}b_i c_{\alpha j}a_\alpha c_{\beta k}c_{\beta l}b_l, \\ C^{(204)} &= a_i c_{i\alpha}c_{j\alpha}c_{j\beta}c_{k\beta}a_k, \\ C^{(024)} &= b_i c_{\alpha i}c_{\alpha j}c_{\beta j}c_{\beta,k}b_k, \\ C^{(213)} &= \epsilon_{\alpha\beta\gamma}a_\alpha c_{\beta i}b_i c_{\gamma j}c_{\delta j}a_\delta, \end{aligned}$$

2 invariants of the seventh degree

$$\begin{aligned} C^{(214)} &= \epsilon_{ijk}b_i c_{\alpha j}a_\alpha c_{\beta k}c_{\beta l}c_{\gamma l}a_l, \\ C^{(124)} &= \epsilon_{\alpha\beta\gamma}a_\alpha c_{\beta j}b_j c_{\gamma k}c_{\delta k}c_{\delta l}b_l, \end{aligned}$$

2 invariants of the eighth degree

$$\begin{aligned} C^{(125)} &= \epsilon_{ijk}b_i c_{\alpha j}c_{\alpha l}b_l c_{\beta k}c_{\beta m}c_{\gamma m}a_\gamma, \\ C^{(215)} &= \epsilon_{\alpha\beta\gamma}a_\alpha c_{\beta i}c_{\delta i}a_\delta c_{\gamma k}c_{\varrho k}c_{\varrho l}b_l, \end{aligned}$$

2 invariants of the ninth degree

$$C^{(306)} = \epsilon_{\alpha\beta\gamma} a_\alpha c_{\beta i} c_{\delta i} a_\delta c_{\gamma j} c_{\varrho j} c_{\varrho k} c_{\sigma k} a_\sigma,$$
$$C^{(036)} = \epsilon_{ijk} b_i c_{\alpha j} c_{\alpha l} b_l c_{\beta k} c_{\beta m} c_{\gamma m} c_{\gamma s} b_s.$$

In the above formulas, summation over all repeated indices from one to three is assumed.

4. Constructing the ring of invariant polynomials for X-states

Now we will discuss the fate of the ring of $SU(2) \times SU(2)$-invariant polynomials when the state space of two qubits is restricted to the subspace of X-states. We start with a very brief description of characteristics of X-states.

4.1. X-states. Consider the subspace $\mathfrak{P}_X \subset \mathfrak{P}(\mathbb{R}^{15})$ of X-states. Their name is due to the visual similarity of the density matrix, whose nonzero entries lie only on the main and minor (secondary) diagonals, with the Latin letter "X":

$$\varrho_X := \begin{pmatrix} \varrho_{11} & 0 & 0 & \varrho_{14} \\ 0 & \varrho_{22} & \varrho_{23} & 0 \\ 0 & \varrho_{32} & \varrho_{33} & 0 \\ \varrho_{41} & 0 & 0 & \varrho_{44} \end{pmatrix}. \tag{13}$$

In (13), the diagonal entries are real numbers, while the elements of the minor diagonal are pairwise complex conjugate, $\varrho_{14} = \overline{\varrho}_{14}$ and $\varrho_{23} = \overline{\varrho}_{32}$.

Comparing this with the Fano decomposition (8), one can see that X-states belong to the 7-dimensional subspace W_X of the vector space W from (10) defined as

$$W_X := \{ w \in W \mid c_{13} = c_{23} = c_{31} = c_{32} = 0, \quad a_i = b_i = 0, \quad i = 1, 2 \}.$$

X-matrices represent density operators that do not mix the subspaces corresponding to the matrix entries with indices $1, 4$ and $2, 3$ of elements of the Hilbert space $\mathcal{H}_4$. This can easily be verified by using the permutation matrix

$$P_\pi = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

that corresponds to the permutation

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}.$$

X-states can be transformed into the 2×2 block-diagonal form:

$$\varrho_X = P_\pi \begin{pmatrix} \varrho_{11} & \varrho_{14} & 0 & 0 \\ \varrho_{41} & \varrho_{44} & 0 & 0 \\ 0 & 0 & \varrho_{33} & \varrho_{32} \\ 0 & 0 & \varrho_{23} & \varrho_{22}. \end{pmatrix} P_\pi. \tag{14}$$

4.2. The restriction of Quesne's invariants to the subspace of X-states. Now we consider the restriction of Quesne's fundamental invariants $C^{(s\,t\,q)}$ introduced above to the subspace W_X. A straightforward evaluation shows that the set of fundamental invariants restricted to W_X reduces to 12 nonzero invariants:

$$\mathcal{P} = \{ C^{200}, C^{020}, C^{002}, C^{111}, C^{003}, C^{202}, C^{022}, C^{004}, C^{112}, C^{113}, C^{204}, C^{024} \}. \tag{15}$$

An explicit form of these invariants as polynomials in seven real variables, coordinates on

$$W_X := \{ \, (\alpha, \beta, \gamma, c_{11}, c_{12}, c_{21}, c_{22}) \in \mathbb{R}^7 \, \}, \tag{16}$$

is given by the following formulas:

$$\begin{aligned}
&\deg = 2, \qquad C^{200} = \alpha^2, \quad C^{020} = \beta^2, \quad C^{002} = c_{11}^2 + c_{12}^2 + c_{21}^2 + c_{22}^2 + \gamma^2,\\
&\deg = 3, \qquad C^{111} = \alpha\beta\gamma, \quad C^{003} = \gamma(c_{11}c_{22} - c_{12}c_{21}),\\
&\deg = 4, \qquad C^{202} = \alpha^2\gamma^2, \quad C^{022} = \beta^2\gamma^2, \quad C^{112} = \alpha\beta(c_{11}c_{22} - c_{12}c_{21}),\\
&\qquad\qquad\;\; C^{004} = \left(c_{11}^2 + c_{12}^2 + c_{21}^2 + c_{22}^2\right)^2 - 2(c_{11}c_{22} - c_{12}c_{21})^2 + \gamma^4,\\
&\deg = 5, \qquad C^{113} = \alpha\beta\gamma^3,\\
&\deg = 6, \qquad C^{204} = \alpha^2\gamma^4, \quad C^{024} = \beta^2\gamma^4.
\end{aligned}$$

Having the set of polynomials $\mathcal{P}$ in (15), one can consider the polynomial ring $\mathbb{R}[\mathcal{P}] \subset \mathbb{R}[W_X]$ generated by $\mathcal{P}$.[3]

4.3. The syzygy ideal in $\mathbb{R}[\mathcal{P}]$. According to the isomorphism (5) mentioned in Sec. 2.1, the subring $\mathbb{R}[\mathcal{P}_1, \dots, \mathcal{P}_{12}]$ can be written in the quotient form

$$\mathbb{R}[\mathcal{P}_1, \dots, \mathcal{P}_{12}] \cong \mathbb{R}[y_1, y_2 \dots y_{12}]/I_{\mathcal{P}}, \tag{17}$$

with the syzygy ideal $I_{\mathcal{P}}$ for $\mathcal{P}$ given by

$$I_{\mathcal{P}} := \{h \in \mathbb{R}[y_1, \dots, y_{12}] \mid h(\mathcal{P}_1, \dots, \mathcal{P}_{12}) = 0 \;\text{ in }\; \mathbb{R}[w_1, \dots, w_7]\}\,.$$

The syzygy ideal can be determined by applying the well-known elimination technique [16]. Following this method, we compute a Gröbner basis of the ideal

$$J_{\mathcal{P}} = \langle \mathcal{P}_1 - y_1, \dots, \mathcal{P}_{12} - y_{12}\rangle \in J_{\mathcal{P}} \subset \mathbb{R}[\omega_1, \dots, \omega_7, y_1, y_{12}]$$

for the lexicographic ordering

$$\begin{aligned}
&c_{11} \succ c_{12} \succ c_{21} \succ c_{22} \succ \alpha \succ \beta \succ \gamma \succ\\
&\succ y_{12} \succ y_{11} \succ y_{10} \succ y_8 \succ y_9 \succ y_7 \succ y_6 \succ y_5 \succ y_4 \succ y_3 \succ y_2 \succ y_1.
\end{aligned}$$

The intersection of the obtained Gröbner basis with $\mathbb{R}[y_1, \dots, y_{12}]$ forms a lexicographic Gröbner basis of the syzygy ideal $I_{\mathcal{P}}$. This basis consists of the following 37 polynomials:

$$\begin{aligned}
I_{\mathcal{P}} =\langle\, & y_2y_6 - y_4^2,\; y_1y_7 - y_4^2,\; -y_1y_2y_5 + y_4y_9,\; -y_1y_4y_5 + y_6y_9,\\
& - y_2y_4y_5 + y_7y_9,\; -y_1y_2y_3^2 + y_1y_2y_8 + 2y_3y_4^2 - 2y_6y_7 + 2y_9^2,\\
& - y_1^2y_3^2y_4 + y_1^2y_4y_8 + 2y_1^2y_5y_9 + 2y_1y_3y_4y_6 - 2y_4y_6^2,\\
& - y_2^2y_3^2y_4 + y_2^2y_4y_8 + 2y_2^2y_5y_9 + 2y_2y_3y_4y_7 - 2y_4y_7^2,\\
& 2y_1^2y_2y_5^2 - y_1y_3^2y_4^2 + y_1y_4^2y_8 + 2y_3y_4^2y_6 - 2y_6^2y_7,\\
& 2y_1y_2^2y_5^2 - y_2y_3^2y_4^2 + y_2y_4^2y_8 + 2y_3y_4^2y_7 - 2y_6y_7^2,\\
& 2y_1y_2y_4^2y_5^2 - y_3^2y_4^4 + 2y_3y_4^2y_6y_7 + y_4^4y_8 - 2y_6^2y_7^2,\\
& 2y_1^3y_5^2 - y_1^2y_3^2y_6 + y_1^2y_6y_8 + 2y_1y_3y_6^2 - 2y_6^3,\\
& 2y_2^3y_5^2 - y_2^2y_3^2y_7 + y_2^2y_7y_8 + 2y_2y_3y_7^2 - 2y_7^3,\\
& y_1y_{10} - y_4y_6, y_{10}y_2 - y_4y_7, \quad y_{10}y_4 - y_6y_7,
\end{aligned}$$

[3] Hereafter, slightly abusing notation, we will write $\mathbb{R}[W]$ and $\mathbb{R}[W_X]$ for the coordinate ring of the variety W in (10) and its subvariety W_X, respectively. To save space, the coordinate ring of W_X will be denoted by $\mathbb{R}[w_1, \dots, w_7] \equiv \mathbb{R}[\alpha, \beta, \gamma, c_{11}, c_{12}, c_{21}, c_{22}]$.

$$\begin{aligned}
&y_1y_3^2y_4-y_1y_4y_8-2y_1y_5y_9-2y_3y_4y_6+2y_{10}y_6,\\
&y_2y_3^2y_4-y_2y_4y_8-2y_2y_5y_9-2y_3y_4y_7+2y_{10}y_7,\quad -y_4^2y_5+y_{10}y_9,\\
&-2y_1y_2y_5^2+y_3^2y_4^2-2y_3y_6y_7-y_4^2y_8+2y_{10}^2,\quad y_1y_{11}-y_6^2, y_{11}y_2-y_6y_7,\\
&y_1y_3^2y_4-y_1y_4y_8-2y_1y_5y_9-2y_3y_4y_6+2y_{11}y_4,\\
&-2y_1^2y_5^2+y_1y_3^2y_6-y_1y_6y_8-2y_3y_6^2+2y_{11}y_6,\\
&-2y_1y_2y_5^2+y_3^2y_4^2-2y_3y_6y_7-y_4^2y_8+2y_{11}y_7,\ -y_4y_5y_6+y_{11}y_9,\\
&y_1y_3^3y_4-y_1y_3y_4y_8-2y_1y_3y_5y_9-2y_1y_4y_5^2-y_3^2y_4y_6-y_4y_6y_8+2y_{10}y_{11},\\
&-2y_1^2y_3y_5^2+y_1y_3^3y_6-y_1y_3y_6y_8-2y_1y_5^2y_6-y_3^2y_6^2-y_6^2y_8+2y_{11}^2,\\
&y_1y_{12}-y_6y_7,\quad y_{12}y_2-y_7^2,\quad y_2y_3^2y_4-y_2y_4y_8-2y_2y_5y_9-2y_3y_4y_7+2y_{12}y_4,\\
&-2y_1y_2y_5^2+y_3^2y_4^2-2y_3y_6y_7-y_4^2y_8+2y_{12}y_6,\\
&-2y_2^2y_5^2+y_2y_3^2y_7-y_2y_7y_8-2y_3y_7^2+2y_{12}y_7,\quad -y_4y_5y_7+y_{12}y_9,\\
&y_2y_3^3y_4-y_2y_3y_4y_8-2y_2y_3y_5y_9-2y_2y_4y_5^2-y_3^2y_4y_7-y_4y_7y_8+2y_{10}y_{12},\\
&-2y_1y_2y_3y_5^2+y_3^3y_4^2-y_3^2y_6y_7-y_3y_4^2y_8-2y_4^2y_5^2-y_6y_7y_8+2y_{11}y_{12},\\
&-2y_2^2y_3y_5^2+y_2y_3^3y_7-y_2y_3y_7y_8-2y_2y_5^2y_7-y_3^2y_7^2-y_7^2y_8+2y_{12}^2\,\rangle.
\end{aligned}$$

Both Maple and Mathematica compute this basis in a few seconds on a PC. The ideal $I_{\mathcal{P}}$ has dimension 5. It can be computed by the command `HilbertDimension` in Maple or using a code available on the Mathematica Stack Exchange web page `http://mathematica.stackexchange.com/questions/37015/`.

If one uses the maximal independent set of variables $\{\,y_1,y_2,y_3,y_4,y_5\,\}$ as parameters, the other variables, due to the above list of algebraic relations, are easily expressible in terms of the five parametric variables by applying the command `Solve` in Maple or Mathematica:

$$\begin{aligned}
&y_6=\frac{y_4^2}{y_2},\quad y_7=\frac{y_4^2}{y_1},\\
&y_8=\frac{2y_1^3y_2^3y_5^2+y_1^2y_2^2y_3^2y_4^2-2y_1y_2y_3y_4^4+2y_4^6}{y_1^2y_2^2y_4^2},\\
&y_9=\frac{y_1y_2y_5}{y_4},\quad y_{10}=\frac{y_4^3}{y_1y_2},\quad y_{11}=\frac{y_4^4}{y_1y_2^2},\quad y_{12}=\frac{y_4^4}{y_1^2y_2}.
\end{aligned}\tag{18}$$

This structure of the ring $\mathbb{R}[y_1,y_2,\ldots,y_{12}]/I_{\mathcal{P}}$ indicates that the polynomial invariants obtained from the rational relations (18) by clearing their denominators form a Gröbner basis of the syzygy ideal $I_{\mathcal{P}}$ in the ring of polynomials in $y_6,\ldots,y_{12}$ over the parametric coefficient field $\mathbb{R}(y_1,\ldots,y_5)$ of rational functions.

The determined properties of the ring $\mathbb{R}[\mathcal{P}_1,\ldots,\mathcal{P}_{12}]$ are in partial agreement with the initial structure of $\mathbb{R}[W]^{SU(2)\times SU(2)}$. Indeed, the five Quesne polynomials $C^{(200)}, C^{(020)}, C^{(002)}, C^{(111)}$, and $C^{(003)}$, which represent a subset of algebraically independent invariants, survive after the restriction to the subspace W_X and correspond to the variables y_1, y_2, y_3, y_4, y_5, which are independent modulo $I_{\mathcal{P}}$. While the restrictions of the other Quesne invariants represent variables that are dependent modulo $I_{\mathcal{P}}$.

4.4. Mapping $\mathbb{R}[\mathcal{P}]$ to a freely generated ring. Now we establish an injective homomorphism between the ring $\mathbb{R}[\mathcal{P}]$ and a certain subring of the coordinate ring $\mathbb{R}[W_X]$ which is freely generated by polynomials of degrees $1, 1, 1, 2, 2$. The latter subring is defined as follows. Consider the following set of polynomials on W_X:

$$f_1 = \gamma, \quad g_1 := x_3 + y_3, \quad g_2 := x_3 - y_3, \quad g_3 := x_1^2 + x_2^2, \quad g_4 := y_1^2 + y_2^2, \tag{19}$$

where the following variables are introduced:

$$\begin{aligned} x_1 &= c_{11} - c_{22}, & y_1 &= c_{11} + c_{22}, \\ x_2 &= c_{12} + c_{21}, & y_2 &= c_{12} - c_{21}, \\ x_3 &= \alpha + \beta, & y_3 &= \beta - \alpha. \end{aligned} \tag{20}$$

It turns out that all twelve Quesne polynomials $\mathcal{P}$ in (15) can be expanded over these five algebraically independent polynomials. An explicit form of these expansions for all nonvanishing Quesne polynomials up to the 6th order is given in Table 1.

Let us now introduce the ring $\mathbb{R}[f_1, g_1, g_2, g_3, g_4]$, which is generated by the set (19). The relation between the polynomials of $\mathcal{P}$ in the variables (19) and Quesne's invariants, as shown in Table 1, defines a mapping

$$\phi : \ \mathbb{R}[y_1, y_2, \dots, y_{12}]/I_{\mathcal{P}} \longrightarrow \mathbb{R}[f_1, g_1, g_2, g_3, g_4] \tag{21}$$

between the quotient ring of $SU(2) \times SU(2)$-invariant polynomials and $\mathbb{R}[f_1, g_1, g_2, g_3, g_4]$, which is an injective ring homomorphism. Indeed, the mapping (21), obviously, satisfies the relations

$$\phi(p + q) = \phi(p) + \phi(q), \quad \phi(pq) = \phi(p)\phi(q),$$

and

$$\phi(p) - \phi(q) = 0 \quad \text{if and only if} \quad p - q \in I_{\mathcal{P}}.$$

However, (21) is not an isomorphism. The linear invariants f, g_1, g_2 have no preimages in $\mathbb{R}[\mathcal{P}]$, since the polynomial invariants (15) have degrees greater or equal to 2.

Table 1. Expansion of Quesne's invariants for X-states.

deg=2	$C^{200} = \frac{1}{4}\, g_2^2$	$C^{020} = \frac{1}{4}\, g_1^2$	$C^{002} = \frac{1}{2}(g_3 + g_4) + f_1^2$
deg=3	$C^{111} = \frac{1}{4}\, g_1 g_2 f_1$	$C^{003} = \frac{1}{4}\, f_1(g_4 - g_3)$	
deg=4	$C^{202} = \frac{1}{4}\, g_2^2 f_1^2$	$C^{022} = \frac{1}{4}\, g_1^2 f_1^2$	$C^{004} = \frac{1}{8}\,(g_3 + g_4)^2 + \frac{1}{2} g_3 g_4 + f_1^4$ $C^{112} = \frac{1}{16}\, g_1 g_2 (g_4 - g_3)$
deg=5	$C^{113} = \frac{1}{4}\, g_1 g_2 f_1^3$		
deg=6	$C^{204} = \frac{1}{4}\, g_2^2 f_1^4$	$C^{024} = \frac{1}{4}\, g_1^2 f_1^4$	

5. Concluding remarks

We conclude with a group-theoretic explanation of the algebraic results obtained in the previous section. Note that the generic action of the group $SU(4)$ on the subspace $\mathfrak{P}_X \subset \mathfrak{P}$ moves its elements from $\mathfrak{P}_X$. But one can point out a 7-dimensional subgroup $G_X \subset SU(4)$ that preserves the form of X-states.

• **The invariance of X-states** • One can construct a 7-parametric subgroup $G_X \subset SU(4)$ that preserves $\mathfrak{P}_X$, i.e., satisfies

$$G_X \varrho_X G_X^\dagger \in \mathfrak{P}_X.$$

Let us fix the following elements of the algebra[4] $SU(4)$:

$$\begin{aligned}
&e_1 = \sigma_3 \otimes \sigma_3, \\
&e_2 = \sigma_2 \otimes \sigma_1, \qquad e_3 = I \otimes \sigma_3, \quad e_4 = -\sigma_2 \otimes \sigma_2, \\
&e_5 = \sigma_1 \otimes \sigma_2, \qquad e_6 = \sigma_3 \otimes I, \quad e_7 = \sigma_1 \otimes \sigma_1.
\end{aligned}$$

The set of the elements $e_1, e_2, \dots, e_7$ is closed under multiplication, i.e., they form a basis of the subalgebra $\mathfrak{g}_X := \mathfrak{su}(2) \oplus \mathfrak{u}(1) \oplus \mathfrak{su}(2) \in \mathfrak{su}(4)$. The exponentiation of the algebra $\mathfrak{g}_X$ gives the subgroup

$$G_X := \exp(i\mathfrak{g}_X) \in SU(4),$$

which is the invariance group of the space $\mathfrak{P}_X$ of X-states. Writing a generic element of the algebra $\mathfrak{g}_X$ as $i\sum_j^7 \omega_j e_j$, one can verify that an arbitrary element of G_X can be represented in the following block-diagonal form:

$$G_X = P_\pi \left(\begin{array}{c|c} e^{-i\omega_1} SU(2) & 0 \\ \hline 0 & e^{i\omega_1} SU(2)' \end{array} \right) P_\pi, \tag{22}$$

where the two copies of SU(2) are parametrized as follows:

$$\begin{aligned}
SU(2) &= \exp\left[i\left(\omega_4 + \omega_7\right)\sigma_1 + i\left(\omega_2 + \omega_5\right)\sigma_2 + i\left(\omega_3 + \omega_6\right)\sigma_3\right], \\
SU(2)' &= \exp\left[i\left(-\omega_4 + \omega_7\right)\sigma_1 + i\left(-\omega_2 + \omega_5\right)\sigma_2 + i\left(\omega_3 - \omega_6\right)\sigma_3\right].
\end{aligned}$$

Having the representation (22), one can find the transformation laws for elements of X-matrices.

• **The action of G_X on X-states** • First of all, the group G_X leaves the parameter c_{33} unchanged. Second, according to (22), the adjoint action of the group X induces transformations of the Fano parameters that are unitary equivalent to the following block-diagonal actions of two copies of $SO(3)$ on a pair of three-dimensional vectors in W with coordinates (20):

$$\begin{pmatrix} x_1' \\ x_2' \\ x_3' \\ y_1' \\ y_2' \\ y_3' \end{pmatrix} = \left(\begin{array}{c|c} \mathrm{SO}(3) & \mathrm{O} \\ \hline \mathrm{O} & \mathrm{SO}(3)' \end{array} \right) \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ y_1 \\ y_2 \\ y_3 \end{pmatrix}.$$

Thus we conclude that there are three independent polynomial G_X-invariants:

$$f_1 := c_{33}, \quad f_2 := x_1^2 + x_2^2 + x_3^2, \quad f_3 := y_1^2 + y_2^2 + y_3^2.$$

[4] The choice of such a subgroup is not unique, and there is a 15-fold degeneration: one can consider 15 different sets of seven generators that send X-states to each other, see [18].

Similarly, the local transformations of X-states can be identified, and the corresponding local unitary polynomial invariants can be determined.

- **The local subgroup of** G_X • One can easily verify that the local subgroup of G_X is

$$P_\pi \exp(\imath\,\frac{\varphi_1}{2}\sigma_3) \times \exp(\imath\frac{\varphi_2}{2}\sigma_3)P_\pi \subset G_X.$$

Its action induces two independent $SO(2)$-rotations of two planar vectors, $\boldsymbol{x} := (x_1,\ x_2)$ and $\boldsymbol{y} := (y_1,\ y_2)$, by the angles $\varphi_1 + \varphi_2$ and $\varphi_1 - \varphi_2$, respectively. Therefore, the five polynomials (19), used in the previous section for expanding the $SU(2) \times SU(2)$-invariants, represent algebraically independent local invariants for X-states.

Concluding, our analysis of the two-qubit X-state space shows the existence of two freely generated polynomial rings, one related to the global G_X-invariance,

$$\mathbb{R}[c_{33}, \boldsymbol{x}, \boldsymbol{y}]^{G_X} = \mathbb{R}[f_1, f_2, f_3],$$

and another one corresponding to the local unitary symmetry of X-states,

$$\mathbb{R}[c_{33}, \boldsymbol{x}, \boldsymbol{y}]^{SO(2)\times SO(2)} = \mathbb{R}[f_1, g_1, g_2, g_3, g_4],$$

generated by the linear invariants f_1, g_1, g_2 together with the quadratic invariants g_3, g_4 of two planar vectors under the linear action of the group $SO(2) \times SO(2)$.

Moreover, an injective homomorphism of the ring of local unitary polynomial invariants $\mathbb{R}[W]^{SU(2)\times SU(2)}$ restricted to the subspace of two-qubit X-states to the freely generated invariant ring $\mathbb{R}[W_X]^{SO(2)\times SO(2)}$ introduced above has been established.

Acknowledgments

The authors thank S. Evlakhov for his help in some related computations. The contribution of the first author (V.G.) was partially supported by the Russian Foundation for Basic Research (grant 16-01-00080).

REFERENCES

1. T. Yu and J. H. Eberly, “Evolution from entanglement to decoherence of bipartite mixed “X” states,” — *Quantum Inf. Comput.*, **7**, 459–468 (2007).
2. M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge Univ. Press (2011).
3. R. F. Werner, “Quantum states with Einstein–Podolsky–Rosen correlations admitting a hidden-variable model,” *Phys. Rev. A*, **40**, No. 8, 4277–4281 (1989).
4. M. Horodecki and P. Horodecki, “Reduction criterion of separability and limits for a class of distillation protocols,” *Phys. Rev. A*, **59**, 4206–4216 (1999).
5. S. Ishizaka and T. Hiroshima, “Maximally entangled mixed states under nonlocal unitary operations in two qubits,” *Phys. Rev. A*, **62**, 22310 (2000).
6. F. Verstraete, K. Audenaert, T. D. Bie, and B. D. Moor, “Maximally entangled mixed states of two qubits,” *Phys. Rev. A*, **64**, 012316 (2001).
7. P. Mendonca, M. Marchiolli, and D. Galetti, “Entanglement universality of two-qubit X-states,” *Ann. Phys.*, **351**, 79–103 (2014).
8. C. Quesne, “$SU(2) \times SU(2)$ scalars in the enveloping algebra of SU(4),” *J. Math. Phys.*, **17**, 1452–1467 (1976).
9. M. Grassl, M. Rotteler, T. Beth, “Computing local invariants of qubit quantum systems,” *Phys. Rev. A*, **58**, 1833–1839 (1998).
10. 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).

11. V. Gerdt, A. Khvedelidze, and Yu. Palii, “On the ring of local polynomial invariants for a pair of entangled qubits,” *Zap. Nauchn. Semin. POMI*, **373**, 104–123 (2009).
12. D. Cox, J. Little, and D. O’Shi, *Ideals, Varieties and Algorithms*, 3rd edition, Springer-Verlag, New York (2007).
13. U. Fano, “Description of states in quantum mechanics by density matrix and operator techniques,” *Rev. Modern Phys.*, **29**, 74–93 (1957).
14. V. L. Popov and E. B. Vinberg, “Invariant theory,” in: N. N. Parshin, I. R. Shafarevich (eds.), *Algebraic Geometry* IV, Springer-Verlag, Berlin–Heidelberg (1994), pp. 123–178.
15. H. Derksen and G. Kemper, *Computational Invariant Theory*, 2nd edition, Springer-Verlag, Berlin–Heidelberg (2015).
16. B. Sturmfels, *Algorithms in Invariant Theory*, 2nd edition, Springer, Wien–New York (2008).
17. H. Derksen and G. Kemper, “Computing invariants of algebraic groups in arbitrary characteristic,” *Adv. Math.*, **217**, 2089–2129 (2008).
18. A. R. P. Rau, “Algebraic characterization of X-states in quantum information,” *J. Phys. A*, **42**, 412002 (2009).