Computing local invariants of quantum-bit systems

Markus Grassl,* Martin Rötteler,† and Thomas Beth‡
Institut für Algorithmen und Kognitive Systeme, Universität Karlsruhe, Am Fasanengarten 5, D-76 128 Karlsruhe, Germany
(Received 18 December 1997; revised manuscript received 29 May 1998)

We investigate means to describe the nonlocal properties of quantum systems and to test if two quantum systems are locally equivalent. For this we consider quantum systems that consist of several subsystems, especially multiple quantum bits, i.e., systems consisting of subsystems of dimension 2. We compute invariant polynomials, i.e., polynomial functions of the entries of the density operator that are invariant under local unitary operations. As an example, we consider a system of two quantum bits. We compute the Molien series for the corresponding representation, which gives information about the number of linearly independent invariants. Furthermore, we present a set of polynomials that generate all invariants (at least) up to degree 23. Finally, the use of invariants to check whether two density operators are locally equivalent is demonstrated. [S1050-2947(98)10609-1]

PACS number(s): 03.67.−a, 02.20.Hj

I. INTRODUCTION

Nonlocality is one of the astonishing phenomena in quantum mechanics. Well-known examples are EPR pairs [1] and the GHZ state [2]. States of quantum codes contradict local realism, too [3]. One common feature of these states is that the nonlocal properties do not change under local transformations, i.e., unitary operations acting independently on each of the subsystems. Thus, any function invariant under local unitary transformations (LUT) can be used to describe these nonlocal properties [4,5]. Here we study polynomials that are invariant under local unitary transformations. Among these, there are, e.g., the coefficients of the characteristic polynomial of a density operator or of the reduced density operators. The paper extends the work of Rains [6], in which he showed how, in principle, all polynomial invariants can be computed. We present further reductions of complexity that make the computation of polynomial invariants feasible at least for small systems.

The paper is organized as follows. In Sec. II we consider the linear action and the action by conjugation of matrix groups on polynomials. Then we establish a connection between invariant polynomials and the algebra of matrices commuting with all elements of the group. A physical interpretation of the invariant polynomials is given by relating them to some observables. Mainly classical results for these algebras are recalled in Sec. III. In Sec. IV a method to construct a vector space basis of these algebras is presented for the case of two-dimensional subsystems. Furthermore, we present results that imply a further reduction of the complexity to compute all invariants. The special situation of pure states and subspaces is considered in Sec. V. In Sec. VI we compute the Molien series and a set of invariants for a two-quantum-bit system. We conclude in Sec. VII with examples for the application of these invariants.

*Electronic address: grassl@ira.uka.de
†Electronic address: roettele@ira.uka.de
‡Electronic address: EISS_Office@ira.uka.de

II. POLYNOMIAL INVARIANTS

A. Operation on polynomials

The group $GL(n,\mathbb{F})$ of invertible $n\times n$ matrices over the field $\mathbb{F}$ operates on the polynomials $p(x_1,\ldots,x_n)\in\mathbb{F}[x_1,\ldots,x_n]$ in the following manner:

$$p^g(x_1,\ldots,x_n):=p(\tilde{x}_1,\ldots,\tilde{x}_n),$$

$$\text{where}\quad(\tilde{x}_1,\ldots,\tilde{x}_n):=(x_1,\ldots,x_n)^g, \tag{1}$$

i.e., each variable is replaced by the linear combination obtained by multiplying the vector of variables by the group element $g\in GL(n,\mathbb{F})$.

On $n\times n$ matrices the group $GL(n,\mathbb{F})$ acts by conjugation. Hence polynomials $f(\rho_{ij})=f(\rho_{11},\ldots,\rho_{nn})$ in the entries ρ_{ij} of an $n\times n$ density operator ρ are then acted upon by conjugation, i.e.,

$$f^g(\rho_{ij})=f(\tilde{\rho}_{ij}),\quad\text{where}\ \tilde{\rho}:=\rho^g=g^{-1}\cdot\rho\cdot g. \tag{2}$$

Given a subgroup $G\leqslant GL(n,\mathbb{F})$, we are interested in polynomials that are fixed by all elements of G under the action defined by either Eqs. (1) or (2). These invariant polynomials (just called *invariants*) form an algebra over the field $\mathbb{F}$ since any linear combination and any product of invariants is invariant under the action of the group, too. It is sufficient to study homogeneous polynomials as each homogeneous polynomial of degree k remains homogeneous of the same degree under the operation of G and every polynomial can be decomposed additively into its homogeneous components.

For the class of so-called *reductive* groups (e.g., finite groups, unitary groups) the invariant ring is finitely generated (cf. [7]), i.e., every invariant can be expressed in terms of some algebra generators. These so-called *fundamental invariants* can be chosen to be homogeneous polynomials of a small degree. Under this assertion the task is to find a system of fundamental invariants such that any other invariant can be expressed as a polynomial of these. In what follows we focus on this task for invariants under the action of tensor products of unitary groups on density operators by conjugation given by Eq. (2).

B. Invariant matrices

Instead of studying the invariant polynomials directly, we use the relation between homogeneous polynomials in the entries of a density operator ρ and constant matrices.

Lemma 1. For every homogeneous polynomial f of degree k in the entries of the density operator ρ there exists a matrix F such that

$$f(\rho_{ij})=f_F(\rho_{ij})=\mathrm{tr}(F\cdot\rho^{\otimes k}). \tag{3}$$

Proof. This follows directly from the fact that the matrix $\rho^{\otimes k}$ contains all monomials in the variables ρ_{ij} of degree k.

Next, we characterize invariant polynomials in terms of the corresponding matrices.

Theorem 2. A homogeneous polynomial f of degree k in the entries of the density operator ρ is invariant under the operation of a compact group $G\leqslant GL(n,\mathbb{F})$ by conjugation if and only if $f=f_F$ for a matrix F that is invariant under conjugation by $(g^{-1})^{\otimes k}$ (equivalently, if and only if the matrix F commutes with $g^{\otimes k}$) for all $g\in G$.

Proof. Conjugation of ρ by g corresponds to conjugation of F by $(g^{-1})^{\otimes k}$ as shown by the following calculation:

$$\begin{aligned} f_F\Big((g^{-1}\cdot\rho\cdot g)_{ij}\Big) &= \mathrm{tr}\Big(F\cdot(g^{-1}\cdot\rho\cdot g)^{\otimes k}\Big)\\ &= \mathrm{tr}\Big(F\cdot(g^{-1})^{\otimes k}\cdot\rho^{\otimes k}\cdot g^{\otimes k}\Big)\\ &= \mathrm{tr}(\underbrace{g^{\otimes k}\cdot F\cdot(g^{-1})^{\otimes k}}_{\tilde F}\cdot\rho^{\otimes k})\\ &= f_{\tilde F}(\rho_{ij}). \end{aligned}$$

If F commutes with $g^{\otimes k}$, then the equality of $\tilde F$ and F implies $f_F((g^{-1}\rho g)_{ij})=f_F(\rho_{ij})$.

If on the other hand f is invariant under the operation of G, for any matrix F with $f=f_F$, we have $f_F((g^{-1}\rho g)_{ij})=f_F(\rho_{ij})$. Since the group G is compact, we can average over the group (cf. [8]) and obtain the matrix

$$\bar F=\int_{g\in G}(g^{\otimes k}\cdot F\cdot(g^{-1})^{\otimes k})d\mu_G(g). \tag{4}$$

By construction, $\bar F$ is invariant under conjugation by $(g^{-1})^{\otimes k}$ and furthermore $f=f_{\bar F}$.

Using this theorem and lemma 1, we are in principle able to compute invariants of the group G starting from any matrix F and computing a matrix $\bar F$ that commutes with $g^{\otimes k}$ for all $g\in G$. But in practice, the integration (4) is very difficult to perform. In Sec. III we will present a method to calculate the matrices F directly without integration.

C. Physical interpretation of the polynomial invariants

Although we do not have full insight into the physical interpretation of the polynomial invariants yet, we will relate them to some observables.

Recall from Eq. (3) that all polynomial invariants of degree k can be written as $f_F(\rho_{ij})=\mathrm{tr}(F\cdot\rho^{\otimes k})$. From F we construct two Hermitian operators

$$M_1:=F+F^\dagger \quad\text{and}\quad M_2:=iF-iF^\dagger.$$

Both M_1 and M_2 commute with $g^{\otimes k}$ for all $g=U_1\otimes\cdots\otimes U_N\in U(n)^{\otimes N}$ since F (and thus $F^\dagger$) commutes with $g^{\otimes k}$ (cf. theorem 2). Hence, the (real) mean values

$$\langle M_1\rangle:=\mathrm{tr}(M_1\cdot\rho^{\otimes k})\quad\text{and}\quad\langle M_2\rangle:=\mathrm{tr}(M_2\cdot\rho^{\otimes k})$$

are also invariant under local unitary transformation. In principle they can be obtained by joint measurements of k copies of the quantum system with density operator ρ.

III. INVARIANT ALGEBRAS

In order to compute all homogeneous invariants of degree k it is sufficient to know the algebra of matrices that commute with $g^{\otimes k}$ for all $g\in G$. Such algebras have been studied, e.g., by Brauer for many classes of groups (cf. [9]). For the unitary group and tensor products of unitary groups, we have the following theorems and corollaries.

Theorem 3 (Brauer). The matrix algebra $\mathcal{A}_{n,k}$ of matrices that commute with any matrix $U^{\otimes k}$ for $U\in U(n)$ is generated by the representation $T_{n,k}:S_k\to GL(n^k,\mathbb{C})$ of the symmetric group S_k that operates on the tensor product space $(\mathbb{C}^n)^{\otimes k}=V_1\otimes\cdots\otimes V_k$ by permuting the k spaces V_i of dimension n.

This result extends to tensor products of unitary groups.

Corollary 4. The algebra of matrices that commute with any matrix $U_1^{\otimes k}\otimes\cdots\otimes U_N^{\otimes k}$ for $U_i\in U(n_i)$ is given by the tensor product of the algebras $\mathcal{A}_{n_i,k}$.

To obtain the ''natural'' ordering of the tensor factors, we have to conjugate the matrices by a permutation matrix.

Corollary 5. The algebra $\mathcal{A}_{n,k}^{(N)}$ of matrices that commute with any matrix $(U_1\otimes\cdots\otimes U_N)^{\otimes k}$ for $U_i\in U(n)$ is conjugated to the N-fold tensor product of the algebra $\mathcal{A}_{n,k}$, i.e.,

$$\mathcal{A}_{n,k}^{(N)}=\sigma(\mathcal{A}_{n,k})^{\otimes N}\sigma^{-1},\quad \sigma:=T_{n,kN}(\tau). \tag{5}$$

Here τ is the permutation that exchanges the macrocoordinates and microcoordinates according to the isomorphism between the tensor product spaces,

$$(V^{\otimes N})^{\otimes k}\quad\text{and}\quad(V^{\otimes k})^{\otimes N}\quad(\text{where } V=\mathbb{C}^n).$$

As a permutation on $\{1,\dots,k\cdot N\}$, τ maps $ak+b+1$ to $bN+a+1$ (for $a=0,\dots,N-1$, $b=0,\dots,k-1$).

(The reader familiar with the theory of fast Fourier transformations will recognize the similarity to the ''bit reversal permutation'' [10].)

For the special situation of quantum-bit systems, i.e., the group $U(2)$, the dimension of the algebra is given by the following theorem.

Theorem 6. The vector space dimension of the algebra $\mathcal{A}_{2,k}$ is given by the Catalan number [11]

$$C(k)=\frac{1}{k+1}\binom{2k}{k}.$$

Proof. This result is derived in [12] from a theorem of Weyl [8].

Note that the algebra $\mathcal{A}_{2,k}$ was defined by the $k!$ matrices $T_{2,k}(\pi)$ for $\pi\in S_k$. As an algebra, $\mathcal{A}_{2,k}$ is generated by the

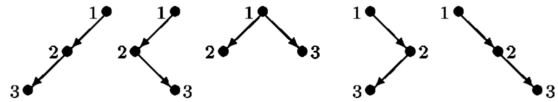

FIG. 1. The five distinct ordered binary trees with three nodes.

image of the generators of S_k, i.e., by only two matrices. Theorem 6 states that, even as a vector space, fewer than $k!$ matrices are sufficient.

IV. BINARY TREES, PERMUTATIONS, AND ALGEBRAS

A. One quantum bit

The mapping (3) from invariant matrices to invariant homogeneous polynomials is a vector space homomorphism. Thus, in order to compute all linearly independent homogeneous invariants of degree k for tensor products of the group $U(2)$, it is sufficient to consider a vector space basis of the algebra $\mathcal{A}_{2,k}$. Such a basis can be constructed starting from binary trees with k nodes, mapping them to permutations of k letters, and finally obtaining matrices via the representation $T_{2,k}$. The construction resembles some of the many beautiful combinatorial properties of Catalan numbers (cf. [11,13]).

Let B_k denote a labeled ordered binary tree with k nodes, i.e., each node in the tree but the root has a father, and each node in the tree has at most one left and at most one right son. The labeling of the k nodes of the tree with the numbers $\{1,\ldots,k\}$ is obtained by traversing the nodes in the order root, left subtree, right subtree. Figure 1 shows all distinct binary trees with three nodes labeled in that manner.

A *maximal right path* in the binary tree B_k is a sequence of nodes $(r_0,r_1,\ldots,r_j)$ such that each of the nodes r_{i+1} is the right son of the node r_i, r_0 is not the right son of any node, and r_j has no right son.

Given the set $\mathcal{R}(B_k)$ of all maximal right paths of a binary tree B_k we define a permutation $\pi(B_k)\in S_k$ by the product of cycles

$$\pi(B_k)=\prod_{(r_0,r_1,\ldots,r_{j_i})\in\mathcal{R}(B_k)}(r_0r_1\cdots r_{j_i}). \tag{6}$$

For example, for the trees of Fig. 1 we get the five permutations (1)(2)(3), (1)(2 3), (1 3)(2), (1 2)(3), and (1 2 3).

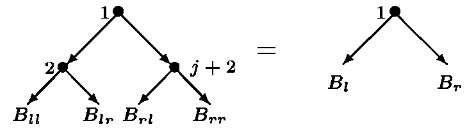

FIG. 2. General form of a tree in the class $\mathcal{B}_{k,j}$. The subtrees B_{ll}, B_{lr}, B_{rl}, and B_{rr} might be empty. Furthermore, for $j=0$ (or $j=k-1$) the left subtree B_l (or the right subtree B_r) is empty.

Let $\mathcal{B}_k$ denote the set of all distinct ordered binary trees with k nodes labeled in the manner described before, and $\mathcal{P}_k=\pi(\mathcal{B}_k)$ be the set of permutations obtained by the mapping π. Using this notation, we can formulate the following theorem.

Theorem 7. The set of matrices $\mathcal{M}_k:=T_{2,k}(\mathcal{P}_k)=\{T_{2,k}(\pi(B)):B\in\mathcal{B}_k\}$ forms a vector space basis of the algebra $\mathcal{A}_{2,k}$.

Proof. For $k=0$ and $k=1$ the statement is obviously true.

For $k>1$, we partition the set $\mathcal{B}_k$ of binary trees with k nodes into k classes $\mathcal{B}_{k,j}$ $(j=0,\ldots,k-1)$. The class $\mathcal{B}_{k,j}$ consists of all trees with j nodes in the left subtree of the root. The general form of a tree in the class $\mathcal{B}_{k,j}$ is shown in Fig. 2.

For $j<k-1$ in each of the trees, $B\in\mathcal{B}_{k,j}$, $j+2$ is a right son of 1, and thus $\pi(B)$ maps 1 to $j+2$. For $j=k-1$, the root 1 has no right son and thus $\pi(B)$ fixes 1. To combine these two cases, we identify $k+1$ and 1. Hence $T_{2,k}(\pi(B))$ maps $|\boldsymbol{e}_1\rangle$ to $|\boldsymbol{e}_{j+2}\rangle$, where $|\boldsymbol{e}_i\rangle=|0\rangle^{\otimes i-1}|1\rangle|0\rangle^{\otimes k-i}$. This shows that for $B\in\mathcal{B}_{k,j}$

$$\mathrm{tr}(|\boldsymbol{e}_1\rangle\langle\boldsymbol{e}_{j'+2}|T_{2,k}(\pi(B)))=\delta_{j,j'}.$$

Therefore, for $j\neq j'$ the matrices in the sets $T_{2,k}(\pi(\mathcal{B}_{k,j}))$ and $T_{2,k}(\pi(\mathcal{B}_{k,j'}))$ are mutually linearly independent.

For fixed j, each permutation $\pi(B)$ for a tree $B\in\mathcal{B}_{k,j}$ with left and right subtrees B_l and B_r (see Fig. 2) can be written in the form

$$\pi(B)=(1j+2)\cdot\pi(B_l)\cdot\pi(B_r),$$

where the permutations $\pi_l=\pi(B_l)$ and $\pi_r=\pi(B_r)$ operate on the sets $\{2,\ldots,j+1\}$ and $\{j+2,\ldots,k\}$, respectively. The corresponding representations are "shifted" tensor products, i.e.,

$$T_{2,k}(\pi(B))$$
$$=T_{2,k}((1j+2))\cdot(\mathbb{1}_{2^{j+1}}\otimes T_{2,k-j-1}(\pi_r'))\cdot(\mathbb{1}_{2^1}\otimes T_{2,j}(\pi_l')\otimes\mathbb{1}_{2^{k-j-1}})=T_{2,k}((1j+2))\cdot(\mathbb{1}_{2^1}\otimes T_{2,j}(\pi_l')\otimes T_{2,k-j-1}(\pi_r')),$$

where $\pi_l'\in S_j$ and $\pi_r'\in S_{k-j-1}$ are obtained by relabeling. By the induction hypothesis, the matrices corresponding to the subtrees B_l and B_r are linearly independent for different trees. Thus we have shown that the matrices in $\mathcal{M}_k$ are linearly independent. It remains to show that they form a basis of $\mathcal{A}_{2,k}$. But this follows from theorem 6 together with the fact that there are exactly $C(k)$ different ordered binary trees with k nodes (cf. [14], p. 389).

B. Multiple quantum bits

In order to compute a basis of the algebra $\mathcal{A}_{n,k}^{(N)}$ for an N-particle system, we define the following representation $T_{n,k}^{(N)}:(S_k)^N\rightarrow GL(n^{kN},\mathbb{C})$ of the N-fold direct product of the symmetric group S_k:

$$(\pi_1,\ldots,\pi_N)\mapsto\sigma\cdot(T_{n,k}(\pi_1)\otimes\cdots\otimes T_{n,k}(\pi_N))\cdot\sigma^{-1}$$

TABLE I. Number of pairs $(\pi_1,\pi_2)\in(S_k)^2$ to be considered for the construction of invariants using the different theorems.

k	$(k!)^2$	$C(k)^2$	Th. 9	Th. 10	Th. 9 Th. 10	Th. 9 Th. 10 Th. 11
1	1	1	1	1	1	1
2	4	4	4	3	3	2
3	36	25	10	15	6	3
4	576	196	36	97	20	10
5	14 400	1 764	114	733	60	22
6	518 400	17 424	496	6 147	291	100
7	25 401 600	184 041	2 142	55 541	1 310	361
8	1 625 702 400	2 044 900	10 758	530 773	6 975	1 717

[where the matrix σ is given by Eq. (5)].

In the special case of N quantum bits (i.e., $n=2$) combining theorem 7 and corollary 5 we obtain the following.

Corollary 8. The set of matrices $T_{2,k}^{(N)}(\mathcal{P}_k^N)$ is a vector space basis of the algebra $\mathcal{A}_{2,k}^{(N)}$.

So far, we are able to compute a vector space basis for $\mathcal{A}_{2,k}^{(N)}$ as follows: (i) Generate the set $\mathcal{B}_k$ of all different binary trees; (ii) generate the set of permutations $\mathcal{P}_k$ obtained by construction (6); and (iii) for each N-tuple of permutations $(\pi_1,\ldots,\pi_N)$ apply the representation $T_{2,k}^{(N)}$, i.e., compute the tensor product of the representations $T_{2,k}(\pi_\nu)$.

Instead of computing a matrix for each of the $(k!)^N$ tuples of permutations in $(S_k)^N$, it is sufficient to consider only the $C(k)^N$ permutations, implying a complexity reduction from $O(k^{kN})$ to $O(4^{kN})$.

Using Eq. (3), we get a set of polynomials invariant under local transformations spanning the vector space of homogeneous polynomial invariants of degree k.

For any N-tuple $\pi=(\pi_1,\ldots,\pi_N)\in(S_k)^N$ of permutations we obtain a homogeneous invariant of degree k given by

$$f_{\pi_1,\ldots,\pi_N}(\rho_{i,j}):=\mathrm{tr}(T_{2,k}^{(N)}(\pi_1,\ldots,\pi_N)\cdot\rho^{\otimes k}). \tag{7}$$

Clearly, there exist relations between the invariant polynomials obtained from the tuple of permutations $(\pi_1,\ldots,\pi_N)\in(S_k)^N$ (also with varying k). Some of these relations can be expressed in terms of the permutations. This allows a further reduction of the number of tuples of permutations that have to be considered to compute all invariants.

Theorem 9. If $(\pi_1,\ldots,\pi_N)$ and $(\pi'_1,\ldots,\pi'_N)$ are ‘‘simultaneously’’ conjugated, i.e., there exists $\tau\in S_k$ such that $\pi'_\nu=\tau^{-1}\pi_\nu\tau$ for all $\nu\in\{1,\ldots,N\}$, then $f_{\pi_1,\ldots,\pi_N}(\rho_{ij})=f_{\pi'_1,\ldots,\pi'_N}(\rho_{ij})$.

Proof. Simultaneous conjugation of the permutations π_ν by τ corresponds to permuting the tensor factors in $\rho^{\otimes k}$ by τ, keeping $\rho^{\otimes k}$ fixed as a whole. Thus $f_{\pi_1,\ldots,\pi_N}(\rho_{ij})$ does not change.

Next we give a condition on the permutations when an invariant can be written as a product of invariants.

Theorem 10. If the subgroup $H\leqslant S_k$ generated by $\pi_1,\ldots,\pi_N$ is not transitive, then the homogeneous invariant $f_{\pi_1,\ldots,\pi_N}(\rho_{ij})$ of degree k is a product of invariants of smaller degree.

Proof. If H is not transitive, it defines a nontrivial partition of the set $\{1,\ldots,k\}$ into orbits. By simultaneous conjugation using theorem 9, we can assume that the partition $\{1,\ldots,k_1\}$ and $\{k_1+1,\ldots,k\}$ respects the orbits. Thus, for $\nu=1,\ldots,N$ each permutation π_ν can be written as a product $\pi_\nu=\pi'_\nu\cdot\pi''_\nu$ with $\pi'_\nu\in S_{k_1}$ operating on $\{1,\ldots,k_1\}$ and $\pi''_\nu\in S_{k_2}$ operating on $\{k_1+1,\ldots,k\}$ $(k_1+k_2=k)$. Furthermore,

$$\begin{aligned}
f_{\pi_1,\ldots,\pi_N}(\rho_{ij})&=\mathrm{tr}(T_{2,k}^{(N)}(\pi_1,\ldots,\pi_N)\cdot\rho^{\otimes k})\\
&=\mathrm{tr}((T_{2,k_1}^{(N)}(\pi'_1,\ldots,\pi'_N)\\
&\quad\otimes T_{2,k_2}^{(N)}(\pi''_1,\ldots,\pi''_N))\cdot\rho^{\otimes k})\\
&=\mathrm{tr}(T_{2,k_1}^{(N)}(\pi'_1,\ldots,\pi'_N)\cdot\rho^{\otimes k_1})\\
&\quad\times\mathrm{tr}(T_{2,k_2}^{(N)}(\pi''_1,\ldots,\pi''_N)\cdot\rho^{\otimes k_2})\\
&=f_{\pi'_1,\ldots,\pi'_N}(\rho_{ij})\cdot f_{\pi''_1,\ldots,\pi''_N}(\rho_{ij}).
\end{aligned}$$

For the case of two quantum bits, Table I shows the reduction of the number of pairs of permutations to be considered using the construction of permutations from binary trees, theorem 9, theorem 10, both theorems 9 and 10, and finally the combination of theorems 9, 10, 11.

V. PURE STATES AND SUBSPACES

The technique to compute polynomials invariant under the action of tensor products of unitary groups does not only apply to density operators of mixed states, but also to subspaces and pure states. To study nonlocal properties of subspaces with basis $|\psi_i\rangle$ (e.g., quantum error-correcting codes), one can use the invariants of the corresponding projection operator $P=\Sigma_i|\psi_i\rangle\langle\psi_i|$. Pure states $|\phi\rangle$ can be considered as a one-dimensional subspace with projection operator $P=|\phi\rangle\langle\phi|$, or equivalently as a mixed state with density operator $\rho=|\phi\rangle\langle\phi|$.

In that situation, we have the additional relation $P^2=P$ $(\rho^2=\rho)$ which can be used for a further reduction of the number of permutations to be considered. The following theorem is quoted from [6], adding an explicit proof.

Theorem 11. Let P be a projection operator. If for $(\pi_1,\ldots,\pi_N)\in(S_k)^N$ there exist different numbers l and m such that for each permutation π_ν we have $\pi_\nu(l)=m$, then the invariant $f_{\pi_1,\ldots,\pi_N}(P_{ij})=f_{\pi'_1,\ldots,\pi'_N}(P_{ij})$ where the permutations $\pi'_\nu\in S_{k-1}$ are obtained by identifying the points l and m followed by a relabeling.

Proof. By theorem 9, we can assume without loss of generality that $l=1$ and $m=2$, i.e., $\pi_\nu(1)=2$ for all permutations π_ν. We will show that in the summation (7) there are entries of P^2 that can be replaced by those of P. The entries of $P^{\otimes k}$ are of the form

$$(P^{\otimes k})_{(i^{(1)},\ldots,i^{(k)}),(j^{(1)},\ldots,j^{(k)})}=P_{i^{(1)},j^{(1)}}\cdots P_{i^{(k)},j^{(k)}}.$$

Here the indices $i^{(\mu)}$ are N-tuples $(i_1^{(\mu)},\ldots,i_N^{(\mu)})$ (for a system with N particles). The subscript of $i_\nu^{(\mu)}$ corresponds to the νth particle, whereas the superscript corresponds to the

μth copy of the whole system. Left-multiplication by $T_{n,k}^{(N)}(\pi_1,\ldots,\pi_2)$ permutes the rows of $P^{\otimes k}$ yielding the matrix M with entries

$$M_{(i^{(1)},\ldots,i^{(k)}),(j^{(1)},\ldots,j^{(k)})}=P_{i^{(\pi(1))},j^{(1)}}\cdots P_{i^{(\pi(k))},j^{(k)}}.$$

The operation of $\pi=(\pi_1,\ldots,\pi_N)$ on the indices is given by $i^{(\pi(\mu))}=(i_1^{(\pi_1(\mu))},\ldots,i_N^{(\pi_N(\mu))})$. Since $\pi_\nu(1)=2$ we have

$$M_{(i^{(1)},\ldots,i^{(k)}),(j^{(1)},\ldots,j^{(k)})}=P_{i^{(2)},j^{(1)}}\cdot P_{i^{(\pi(2))},j^{(2)}}\cdots P_{i^{(\pi(k))},j^{(k)}}.$$

Now taking the trace results in

$$\sum_{j^{(1)},\ldots,j^{(k)}} M_{(j^{(1)},\ldots,j^{(k)}),(j^{(1)},\ldots,j^{(k)})} = \sum_{j^{(1)},\ldots,j^{(k)}} P_{j^{(2)},j^{(1)}}\cdot P_{j^{(\pi(2))},j^{(2)}}\cdot\ldots\cdot P_{j^{(\pi(k))},j^{(k)}}. \tag{8}$$

Considering the summation over $j^{(2)}$ separately and using $P^2=P$, we get

$$\sum_{j^{(2)}} P_{j^{(\pi(2))},j^{(2)}}P_{j^{(2)},j^{(1)}}=P_{j^{(\pi(2))},j^{(1)}}. \tag{9}$$

Combining Eqs. (8) and (9) yields

$$\sum_{j^{(1)},\ldots,j^{(k)}} M_{(j^{(1)},\ldots,i^{(k)}),(j^{(1)},\ldots,j^{(k)})} = \sum_{j^{(1)},j^{(3)},\ldots,j^{(k)}} P_{j^{(\pi(2))},j^{(1)}}\cdot P_{j^{(\pi(3))},j^{(3)}}\cdots P_{j^{(\pi(k))},j^{(k)}}.$$

Now the result follows immediately if we identify the points 1 and 2.

VI. THE INVARIANT RING OF A TWO QUANTUM-BIT SYSTEM

To illustrate the results, we consider the smallest nontrivial example, a system of two quantum bits. Using our algorithm, we are able to compute homogeneous invariants for each degree. As stated before, the homogeneous invariants of a fixed degree form a vector space. Therefore it is sufficient to compute a basis for that vector space, e.g., a maximal linearly independent set of homogeneous invariants. In order to know how many invariants we need, we address the problem of determining the dimension d_k of the vector space of invariants of degree k. Information about these dimensions is encoded in a formal power series, the Molien series (cf. [15])

$$P(z):=\sum_{k\geq 0} d_k z^k\in\mathbb{Z}[[z]].$$

In case of a finitely generated algebra the Molien series turns out to be a rational function (see, e.g., [16]). Thus it can be expressed in a closed form with a finite number of terms. In principle, the Molien series for the linear action (1) of a compact group G on polynomials can be computed by means of the following averaging formula:

$$P(z)=\int_{g\in G}\frac{d\mu_G(g)}{\det(id-zg)}, \tag{10}$$

where μ_G is the normalized Haar measure of G.

In this paper, however, we are concerned with the action of $G=SU(2)\times SU(2)$ on matrices by conjugation (2), for which the formula (10) does not apply directly. Since the operation on ρ given by

$$\rho\mapsto(U_1\otimes U_2)\cdot\rho\cdot(U_1\otimes U_2)^\dagger \quad \text{for } U_1,U_2\in SU(2)$$

is linear, we write ρ as a vector $\vec{\rho}$ of length n^2 and obtain the representation

$$\vec{\rho}\mapsto(U_1\otimes U_2\otimes\overline{U_1}\otimes\overline{U_2})\vec{\rho},$$

where $\overline{U_i}$ denotes the complex conjugate of the matrix U_i.

The integral (10) is simplified by means of the integral formula of Weyl (cf. [17], Sec. 26.2), which allows one to perform an integration over the whole group in two steps. The first step involves an integration over a maximal torus T of the group G and the second an integration on the residue classes G/T. Next, the integral is transformed into a complex path integral that can be solved by the theorem of residues. Finally, we end up with the Molien series

TABLE II. The invariants $f_{\pi_1,\pi_2}(\rho_{ij})$ corresponding to these permutations (listed together with the degree and the number of terms of the invariants) generate the polynomial invariants of a two-quantum-bit system (at least) up to degree 23.

degree	π_1	π_2	number of terms
1	id	id	4
2	id	(12)	10
2	(12)	id	10
2	(12)	(12)	10
3	(123)	(12)	52
3	(123)	(123)	24
4	(1234)	(13)	110
4	(1234)	(123)	144
4	(1234)	(1234)	70
4	(1234)	(12)(34)	98
5	(123)(45)	(12345)	456
6	(123456)	(1235)	1 334
6	(123)(45)	(12456)	1 586
6	(123)(45)	(123456)	1 542
6	(123)(45)	(1234)(56)	1 464
7	(1234)(567)	(124567)	4 156
7	(1234)(567)	(1267)(35)	4 576
8	(12345)(678)	(1235678)	10 414
8	(12345)(678)	(12378)(46)	11 340
9	(12345)(678)	(1236789)(45)	24 780
9	(12345)(6789)	(1235678)	24 168

$$
\begin{aligned}
P(z)=&\frac{z^{10}-z^8-z^7+2z^6+2z^5+2z^4-z^3-z^2+1}{(z-1)^{10}(z+1)^6(z^2+1)^2(z^2+z+1)^3}\\
=&1+z+4z^2+6z^3+16z^4+23z^5+52z^6+77z^7+150z^8\\
&+224z^9+396z^{10}+583z^{11}+964z^{12}+1395z^{13}\\
&+2180z^{14}+3100z^{15}+4639z^{16}+6466z^{17}+9344z^{18}\\
&+12\,785z^{19}+17\,936z^{20}+24\,121z^{21}+33\,008z^{22}\\
&+43\,674z^{23}+O(z^{24}).
\end{aligned}
$$

The information about the dimensions of the vector spaces can now be used to compute all invariants degree by degree. Having computed an algebra basis for all invariants of degree less than k, homogeneous invariants of degree k are obtained by multiplying invariants of smaller degrees that sum up to k. By computing the vector space dimension of these invariants and comparing it to the dimension given by the Molien series, we know how many linearly independent invariants are missing. Next, these missing invariants are constructed from pairs of permutations $\pi_\nu\in S_k$. It is sufficient to draw randomly from the pairs of permutation remaining after theorem 9 and theorem 10 until the vector space dimension given by the Molien series.

Using the computer algebra system MAGMA [18] we found 21 invariants corresponding to the permutations shown in Table II. Furthermore, we were able to show that these invariants generate all invariants up to degree 23. We conjecture that any polynomial invariant of a two-quantum-bit system can be expressed in terms of these 21 invariants. It should be noted that there are 43 674 linearly independent invariants of degree 23 and that the invariants of degree 9 have more than 24 000 terms.

The Molien series provides also information about the maximal number of algebraically independent invariants. This number is given by the order of the pole $z=1$ of the Molien series [15]. For the two-quantum-bit system, there are 10 algebraically independent invariants. Thus any 11 invariants fulfill a polynomial equation, i.e., given numerical values for 10 algebraically independent invariants, the values of the remaining invariants are some roots of polynomials. But these values are not unique since none of the 21 invariants is a polynomial function of the others.

VII. EXAMPLES

A. Characteristic polynomials

As stated in the Introduction, the coefficients of the characteristic polynomial $\chi_\rho(X)$ of a density operator ρ and of the reduced density operators are invariant under local unitary transformation. They can be expressed in terms of the invariants f_{π_1,π_2} presented in Table II as follows:

$$
\begin{aligned}
\chi_\rho(X)=&X^4-f_{id,id}X^3+\left(\frac{1}{2}f_{id,id}^2-\frac{1}{2}f_{(1\,2),(1\,2)}\right)X^2\\
&+\left(-\frac{1}{6}f_{id,id}^3+\frac{1}{2}f_{id,id}f_{(1\,2),(1\,2)}-\frac{1}{3}f_{(1\,2\,3),(1\,2\,3)}\right)X\\
&+\frac{1}{24}f_{id,id}^4-\frac{1}{4}f_{id,id}^2f_{(1\,2),(1\,2)}+\frac{1}{3}f_{id,id}f_{(1\,2\,3),(1\,2\,3)}\\
&+\frac{1}{8}f_{(1\,2),(1\,2)}^2-\frac{1}{4}f_{(1\,2\,3\,4),(1\,2\,3\,4)}.
\end{aligned}
$$

Here, the coefficient of X^3 in χ_ρ is a linear invariant polynomial that equals the negative trace of ρ, and the constant coefficient of χ_ρ is an invariant of degree 4 that equals the determinant of ρ.

For the characteristic polynomials of the reduced density operators $\rho^{(1)}:=\mathrm{tr}_2(\rho)$ and $\rho^{(2)}:=\mathrm{tr}_1(\rho)$ we obtain

$$\chi_{\rho^{(1)}}(X)=X^2-f_{id,id}X+\frac{1}{2}(f_{id,id}^2-f_{(1\,2),id})$$

and

$$\chi_{\rho^{(2)}}(X)=X^2-f_{id,id}X+\frac{1}{2}(f_{id,id}^2-f_{id,(1\,2)}).$$

B. Test for local equivalence

Consider the following density operators:

$$\rho_1=\frac{1}{800}\begin{pmatrix}214 & -16-150\,i & -10+8\,i & 3\\ -16+150\,i & 226 & 13 & 10-8\,i\\ -10-8\,i & 13 & 234 & 16+150\,i\\ 3 & 10+8\,i & 16-150\,i & 126\end{pmatrix}$$

and

$$\rho_2=\frac{1}{800}\begin{pmatrix}214 & -16+150\,i & 10+8\,i & -3\\ -16-150\,i & 226 & -13 & -10-8\,i\\ 10-8\,i & -13 & 234 & 16-150\,i\\ -3 & -10+8\,i & 16+150\,i & 126\end{pmatrix}.$$

These density operators are (globally) conjugated to each other, i.e., $\rho_2 = U\rho_1 U^\dagger$, where $U \in U(4)$. Thus they have the same eigenvalues. Furthermore, the reduced density operators are the same. Partial transposition of ρ_1 and ρ_2 yields positive operators $\rho_1^{T_i}$ and $\rho_2^{T_i}$ $(i=1,2)$, thus ρ_1 and ρ_2 are both separable [19]. Again, the eigenvalues and the reduced density operators corresponding to $\rho_1^{T_i}$ and $\rho_2^{T_i}$ are the same. Also, all polynomial invariants up to degree 5 evaluate to the same number for ρ_1 and ρ_2. Hence one might expect that ρ_1 and ρ_2 are locally equivalent.

But we have the following: The values of the invariants of degree 6 corresponding to $\pi_1 = (1\ 2\ 3)(4\ 5)$, $\pi_2 = (1\ 2\ 4\ 5\ 6)$ and $\pi_1 = (1\ 2\ 3)(4\ 5)$, $\pi_2 = (1\ 2\ 3\ 4\ 5\ 6)$ differ showing that ρ_1 and ρ_2 are not locally equivalent. Note that after precomputation of the invariants this can be decided just by evaluating the invariants.

VIII. CONCLUSION

We have established a connection between local polynomial invariants of quantum systems and permutations. The local invariants of an N-particle system can be computed directly from N-tuples of permutations. Theorems 9 and 10 allow a reduction of the number of permutations to be considered. This makes the computation of invariants feasible.

In the particular case of pure states and subspaces, theorem 11 allows a further reduction of complexity. All these theorems apply for subsystems of any dimension.

In the special case of quantum-bit systems, we are able to construct a vector space basis for the matrices directly in terms of permutations derived from binary trees. It has to be investigated if there are similar constructions for subsystems of dimension $n > 2$.

Since our methods are not restricted to density operators, they can also be used to study nonlocal properties of unitary transformations. For example, it can be tested whether two quantum circuits are equivalent with respect to conjugation by single quantum-bit gates.

ACKNOWLEDGMENTS

The authors acknowledge fruitful discussions with Günter Mahler and his co-workers at the University of Stuttgart, and with Jörn Müller-Quade of IAKS, Karlsruhe. Furthermore, we would like to thank Eric Rains for his comments. M. R. is supported by ‘‘Deutsche Forschungsgemeinschaft, Graduiertenkolleg Beherrschbarkeit Komplexer Systeme, Universität Karlsruhe’’ under Contract No. DFG-GRK 209/3-98.

[1] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).
[2] D. M. Greenberger, M. Horne, and A. Zeilinger, *Going Beyond Bell's Theorem*, in *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*, edited by M. Kafatos (Kluwer, Dordrecht, 1989), pp. 73–76.
[3] D. P. DiVincenzo and A. Peres, Phys. Rev. A **55**, 4089 (1997).
[4] J. Schlienz and G. Mahler, Phys. Rev. A **52**, 4396 (1995).
[5] J. Schlienz and G. Mahler, Phys. Lett. A **224**, 39 (1996).
[6] E. M. Rains, e-print quant-ph/9704042 (1997).
[7] T. A. Springer, *Invariant Theory*, Lecture Notes in Mathematics, Vol. 585 (Springer, Berlin, 1977).
[8] H. Weyl, *The Classical Groups* (Princeton University Press, Princeton, 1939).
[9] R. Brauer, Ann. Math. **38**, 857 (1937).
[10] Th. Beth, *Verfahren der schnellen Fourier-Transformation* (Teubner, Stuttgart, 1984).
[11] R. L. Graham, D. E. Knuth, and O. Patashnik, *Concrete Mathematics*, 2nd ed. (Addison-Wesley, Reading, MA, 1994).
[12] M. Rötteler, Diplomarbeit, Universität Karlsruhe (1997).
[13] H. Lüneburg, *Kombinatorik* (Birkhäuser, Stuttgart, 1971).
[14] D. E. Knuth, *The Art of Computer Programming*, 2nd ed. (Addison-Wesley, Reading, MA, 1973), Vol. 1.
[15] B. Sturmfels, *Algorithms in Invariant Theory* (Springer, Wien, 1993).
[16] M. F. Atiyah and I. G. Macdonald, *Introduction to Commutative Algebra* (Addison-Wesley, Reading, MA, 1969).
[17] W. Fulton and J. Harris, *Representation Theory*, Graduate Texts in Mathematics Vol. 129 (Springer, New York, 1991).
[18] W. Bosma, J. J. Cannon, and C. Playoust, J. Symb. Comput. **24**, 235 (1997).
[19] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996).