Quantum Information and Computation, Vol. 0, No. 0 (2003) 000–000

Local invariants for multi-partite entangled states allowing for a simple entanglement criterion

Hans Aschauer[1], John Calsamiglia[2], Marc Hein[1,2], and Hans J. Briegel[1,2,3]
[1] *Sektion Physik, Ludwig-Maximilians-Universität München*
Theresienstr. 37, D-80333 München, Germany
[2] *Institut für Theoretische Physik, Universität Innsbruck,*
A-6020 Innsbruck, Austria.
[3] *Institut für Quantenoptik und Quanteninformation der Österreichischen Akademie der Wissenschaften*
A-6020 Innsbruck, Austria.

Received (received date)
Revised (revised date)

We present local invariants of multi-partite pure or mixed states, which can be easily calculated and have a straight-forward physical meaning. As an application, we derive a new entanglement criterion for arbitrary mixed states of n parties. The new criterion is weaker than the partial transposition criterion but offers advantages for the study of multipartite systems. A straightforward generalization of these invariants allows for the construction of a complete set of observable polynomial invariants.

Keywords: Entanglement, local invariants
Communicated by:

1 Introduction

Quantum mechanical states have a complex description in terms of their density matrix, which comprises all information available about a system under a given experimental situation. Different density matrices correspond to different states of a system, and allow for different predictions on its future behavior. For many purposes, however, we are only interested in properties of the state (such as its entropy or purity) which are invariant under unitary transformations.

For systems composed of several parts, or subsystems, there exists a natural tensor product structure underlying the state space. For such composite systems, the superposition principle gives rise to the phenomenon of entanglement which manifests itself in peculiar "quantum" correlations between results of measurements on its different parts [1, 2, 3]. To capture the essential features of this entanglement, we look for properties of the density matrix that are invariant under *local unitary transformations*, corresponding to a local change of basis in the Hilbert spaces of the individual subsystems. Such local invariants have attracted the attention of people working on the foundation of quantum mechanics and, more recently, in quantum information theory [4, 5, 6, 7, 8], where entanglement is perceived as a resource for tasks in quantum communication and computation.

In this paper, we present a family of local invariants of a multi-partite quantum system. These invariants are derived from an invariant decomposition of the state space of the system,

regarded as a real vector space of hermitian operators with a scalar product. They have a natural geometric interpretation in terms of the length of projections of vectors onto invariant subspaces. Such subspaces contain all information either about one local subsystem *or* about correlations between a given set of subsystems. Beyond their straight-forward geometric interpretation, these invariants have a number of merits. They can easily be calculated – even analytically – for many states, and they are directly connected to measurement data [9, 10].

The representation of the density matrix as an element in the real (metric) vector space of hermitian matrices is well known, and a number of researchers have used a similar approach before [11, 12, 4, 13, 14, 15]. Nevertheless, our results go beyond existing work in at least two respects. First, the explicit decomposition of the state space into a direct sum of invariant sub-spaces makes the identification of invariants quite transparent — it allowed us in fact to find a family of new invariants. Second, from the *convexity* of the set of separable states, we are able to derive constraints on the invariants of separable states and propose a new entanglement criterion. Here, we will discuss some of its strengths and limitations and apply it to a wide class of multi-qubit states.

Moreover, for each state the obtained invariants are homogeneous polynomials of degree 2 in the coefficients of a basis decompositions of the density operator into hermitian operators. We show how considering polynomials of higher degree one can extend the set of local invariants and make it complete [6].

2 State tomography

It is a well known fact that the four Pauli spin matrices $\sigma_0 = \mathbf{1}, \sigma_1 = \sigma_x, \sigma_2 = \sigma_y, \sigma_3 = \sigma_z$ form a real basis of the vector space of the hermitian operators which act on one qubit. With respect to the scalar product $\langle A, B\rangle = \mathrm{tr}(AB)$, the basis vectors are orthogonal. More generally, for a d-dimensional quantum system, there exists a set of d^2-1 traceless hermitian generators of the $SU(d)$, which we call $\sigma_1, \ldots \sigma_{d^2-1}$. One specific choice of these generators is the so-called Cartan-Weyl-construction (see, e. g. [4]). Combined with the unit operator $\mathbf{1} \equiv \sigma_0$, they form a real non-normalized orthogonal basis of the vector space of hermitian operators in d dimensions,

$$\langle \sigma_i, \sigma_j \rangle = \mathrm{tr}(\sigma_i \sigma_j) = \delta_{i,j} d \tag{1}$$

Let $P = \{1, 2, \ldots, n\}$ be a set of parties and $\mathcal{V}$ the vector space of hermitian operators acting on the n-partite Hilbert space $\mathcal{H}^{(1)} \otimes \mathcal{H}^{(2)} \otimes \cdots \otimes \mathcal{H}^{(n)}$, where $\mathcal{H}^{(a)}$ is a Hilbert space of the (finite) dimension d_a. Clearly, the tensor products of the basis operators form a basis

$$\mathcal{B} = \{\sigma_{i_1}^{(1)} \sigma_{i_2}^{(2)} \cdots \sigma_{i_n}^{(n)} | 0 \leq i_a \leq d_a^2 - 1 \text{ for all } a \in P\} \tag{2}$$

of $\mathcal{V}$.

Any n-partite density operator $\rho \in \mathcal{V}$ can thus be expanded in the product basis

$$\rho = \frac{1}{d} \sum_{i_1, i_2, \ldots, i_n} c_{i_1 i_2 \ldots i_n} \sigma_{i_1}^{(1)} \sigma_{i_2}^{(2)} \cdots \sigma_{i_n}^{(n)}, \tag{3}$$

where $d = \prod_{a=1}^{n} d_a$, and

$$c_{i_1 i_2 \ldots i_n} = \mathrm{tr}\left(\rho\, \sigma_{i_1}^{(1)} \sigma_{i_2}^{(2)} \cdots \sigma_{i_n}^{(n)}\right) = \left\langle \sigma_{i_1}^{(1)} \sigma_{i_2}^{(2)} \cdots \sigma_{i_n}^{(n)} \right\rangle_\rho . \tag{4}$$

In other words, the expansion coefficients $c_{i_1 i_2 \ldots i_n}$ are expectation values of products of hermitian operators. Since these expectation values can, in principle, be measured by local measurements (given a sufficiently large ensemble of copies of ρ), one can use this method in order to determine an unknown n-partite quantum state with the help of local measurements and classical communication (quantum state tomography).

3 Invariant decomposition of the state space

Let $\sigma = \sigma_{i_1}^{(1)} \sigma_{i_2}^{(2)} \cdots \sigma_{i_n}^{(n)}$ be an arbitrary element of the product basis $\mathcal{B}$, and $S = \{a | i_a \neq 0\}$ the set of parties, where σ acts non-trivially. Using this definition, we call σ a S-correlation operator, and the set of all S-correlation operators $\mathcal{B}_S$. It is clear that $\mathcal{B}$ can be written as the union of the (disjoint) sets of S-correlation operators, i. e.

$$\mathcal{B} = \bigcup_{S \subset P} \mathcal{B}_S. \tag{5}$$

Example: In the case of three qubits, we have eight such sets (with $a, b \in \{1, 2, 3\}$): $\mathcal{B}_{\{\}} = \{\mathbf{1}\}$, $\mathcal{B}_{\{a\}} = \{\sigma_i^{(a)} | i = 1, 2, 3\}$, $\mathcal{B}_{\{a,b\}} = \{\sigma_i^{(a)} \sigma_j^{(b)} | i, j = 1, 2, 3\}$, and $\mathcal{B}_{\{1,2,3\}} = \{\sigma_i^{(1)} \sigma_j^{(2)} \sigma_k^{(3)} | i, j, k = 1, 2, 3\}$.

Theorem 1 *For each set S of parties, the vector space $\mathcal{V}_S = \mathrm{span}(\mathcal{B}_S)$ is invariant under local unitary transformations, which act as isometries on $\mathcal{V}_S$.*

Proof. Let $U^{(a)}$ be a unitary operation which acts on party a. If $a \notin S$, all elements of $\mathcal{B}_S$ remain unchanged under the action of $U^{(a)}$. If, on the other hand, $a \in S$, then the orthogonal set of traceless generators $\sigma_i^{(a)}$ $(i > 0)$ is transformed into a different set of orthogonal traceless generators, i. e. for $1 \leq i \leq d_a^2 - 1$,

$$\sigma_i^{(a)} \to \tilde{\sigma}_i^{(a)} = \sum_k \left(O(U^{(a)}) \right)_{ik} \sigma_k^{(a)}$$

with an orthogonal matrix $O(U^{(a)}) \in SO(d_a^2 - 1)$ [11, 4]. Obviously, both sets of generators span the same set of *all* traceless operators. □.

Given a density operator ρ and a set S of parties, the projection of ρ onto the subspace $\mathcal{V}_S$ is given by

$$\xi_S(\rho) = \frac{1}{d} \sum_{\sigma \in \mathcal{B}_S} \langle \rho, \sigma \rangle \, \sigma = \frac{1}{d} \sum_{\sigma \in \mathcal{B}_S} \langle \sigma \rangle_\rho \, \sigma. \tag{6}$$

For simplicity, we will often denote the above projection by ξ_S, where the dependence on the state ρ in question will be understood.

The reduced density operator ρ_S corresponding to the set of parties S can be read off,

$$\tilde{\rho}_S \equiv \rho_S \otimes \frac{\mathbf{1}_{\bar{S}}}{d_{\bar{S}}} = \sum_{S' \subset S} \xi_{S'}(\rho), \tag{7}$$

where $\bar{S} = P \backslash S$ denotes the complement of set S.

By direct substitution into the previous equation one readily checks that the following relation between the projection of ρ onto $\mathcal{V}_S$ and its reductions holds

$$\xi_S(\rho) = \sum_{S' \subset S} (-1)^{|S| - |S'|} \tilde{\rho}_{S'}. \tag{8}$$

Due to Theorem 1, local unitary operations rotate a projection ξ_S only within the subspace $\mathcal{V}_S$. Ignoring the normalization constant $1/d$ leads us to

Corollary 1 *For each set S of parties, the squared length of the projection of a state ρ onto the span $\mathcal{V}_S$ of $\mathcal{B}_S$,*

$$L_S(\rho) = \sum_{\sigma\in\mathcal{B}_S} \langle\sigma\rangle_\rho^2 = d\,\mathrm{tr}(\xi_S(\rho)^2) \tag{9}$$

is invariant under local unitary transformations. We call $L_S(\rho)$ the S-correlation strength of ρ.

From Eq.(8) we find that S-correlation strength depends solely on the purities of the reductions of ρ_S,

$$\begin{aligned} L_S(\rho) &= d\,\mathrm{tr}(\xi_S\xi_S) = d\,\mathrm{tr}(\xi_S\rho) = d\sum_{S'\subset S}(-1)^{|S|-|S'|}\,\mathrm{tr}(\rho_{S'}\otimes\frac{\mathbf{1}_{\bar S}}{d_{\bar S}}\rho) \\ &= \sum_{S'\subset S}(-1)^{|S|-|S'|}\frac{d}{d_{\bar S}}\,\mathrm{tr}\left[\rho_{S'}\,\mathrm{tr}_{\bar S}\,(\rho)\right] = \sum_{S'\subset S}(-1)^{|S|-|S'|}d_{S'}\,\mathrm{tr}(\rho_{S'}^2)\;, \end{aligned} \tag{10}$$

where $d_{S'} = \prod_{a\in S'} d_a$ and we have made use of $\mathrm{tr}(\xi_S\xi_{S'}) = d_S\delta_{S,S'}$. We notice that the S-correlation depends only on the reduced density matrix of the set of parties S, $L_S(\rho) = L_S(\rho_S)$. Thus, the only invariant which contains information about the total state is $L_P(\rho)$.

For pure product states (i.e. $\mathrm{tr}(\rho_S^2) = 1\ \forall S$) we find

$$L_S^{\mathrm{pure}} = \sum_{S'\subset S}(-1)^{|S|-|S'|}\prod_{a\in S'} d_a = \prod_{a\in S}(d_a - 1), \tag{11}$$

which further simplifies to $L_S^{\mathrm{pure}} = 1$ for n-qubit systems.

The idea of local-invariant spaces and correlation strength can be easily extended to a scenario where parties can form coalitions, giving rise to different *partitions* of the set of parties. We allow the parties $a_1\ldots a_k$ in a coalition to apply joint operations, or equivalently, we treat them as a single super-party acting on higher-dimensional quantum system b. One can obtain the required traceless generators for the new party b as products of the generators of the old parties $a_1\ldots a_k$,

$$\tilde\sigma^{(b)}_{i_1\ldots i_k} = \sigma^{(a_1)}_{i_1}\sigma^{(a_2)}_{i_2}\cdots\sigma^{(a_k)}_{i_k}, \tag{12}$$

with $(i_1,\ldots,i_k)\neq(0,\ldots,0)$.

Any partitioning can be realized by iteratively joining parties pairwise, say $a_1, a_2 \to b = \{a_1, a_2\}$. Using Eq. (12), one can easily verify that the correlation strength for a set $S = \{b\}\cup S' = \{b\}\cup\{a_\mu, a_\nu, \ldots\}$ of parties, is given by

$$L_{\{b\}\cup S'} = L_{\{a_1\}\cup S'} + L_{\{a_2\}\cup S'} + L_{\{a_1,a_2\}\cup S'}, \tag{13}$$

which means that the correlation strengths for coarse partitions are functions of the correlations strengths of the finest partition.

A special partition is obtained if we allow *all* parties to operate jointly as a super-party $b = P = \{a_1,\ldots,a_n\}$. $L_{\{b\}}$ is then invariant under *all* unitary operations, and thus describes a global property of the state. Indeed, we have

$$L_{\{P\}}(\rho) = \sum_{\sigma\in\mathcal{B}}\langle\sigma\rangle_\rho^2 - \langle\mathbf{1}\rangle_\rho = d\,\mathrm{tr}\left(\rho^2\right) - 1, \tag{14}$$

so that $L_{\{P\}}$ is a measure for the purity of the state ρ.

Using Eq. 5 and 9, we can re-write the left-hand side of Eq. 14 as the sum of all S-correlation strengths,

$$\sum_{\{\}\neq S\subset P} L_S = d\,\mathrm{tr}\left(\rho^2\right) - 1, \tag{15}$$

which allows us to state

Corollary 2 *For any state ρ, the sum of all correlation strengths is given by the purity of the state. This implies, in particular, that for states with the same purity, there is a trade-off between local and the different non-local correlations.*

For a pure state $\rho = |\psi\rangle\langle\psi|$, we have $\mathrm{tr}(\rho^2) = \mathrm{tr}(\rho) = 1$, so that Corollary 2 can be regarded as a quantitative expression of the folklore saying that in entangled states, the information about the state is contained in its correlations rather than its local properties.

It is a useful fact that the convex structure of the space $\mathcal{V}$ of states is obeyed by the subspaces $\mathcal{V}_S$ separately, in the following sense: If a state is given by a convex sum of states ρ_l, i. e. $\rho = \sum_l p_l\rho_l$ with $p_l > 0$ for all l and $\sum_l p_l = 1$, then the projection of ρ onto each of the subspaces $\mathcal{V}_S$ is the convex sum of the projections of the states ρ_l onto $\mathcal{V}_S$. If ρ is a separable state, it can be written as a convex sum of pure product states. In this case, the projection of ρ onto each of the subspaces $\mathcal{V}_S$ is a convex sum of vectors with the squared length L_S^{pure}, so that the squared length $L_S(\rho)$ cannot exceed L_S^{pure}. This allows us to formulate the following entanglement criterion:

Theorem 2 *Given a multi-partite state ρ, if there exists a subset S of parties such that the S-correlation strength is greater than L_S^{pure}, then ρ is entangled.*

Corollary 2 then implies that all pure multi-partite entanglement will be detected by this criterion.

It is interesting to note that the strongest entanglement criterion is obtained for the finest partition, in the following sense: Let $b = \{a_1, a_2\}$ be a coarsening as in Eq. (13), and $L_S(\rho) < L_S^{\mathrm{pure}}$ for all $S \subset \{b_1, b_2\} \cup S' \subset P$. Using (13) for the state ρ and for product states, we find

$$\begin{aligned} L_{\{b\}\cup S'} &= L_{\{a_1\}\cup S'} + L_{\{a_2\}\cup S'} + L_{\{a_1,a_2\}\cup S'} \\ &\leq L^{\mathrm{pure}}_{\{a_1\}\cup S'} + L^{\mathrm{pure}}_{\{a_2\}\cup S'} + L^{\mathrm{pure}}_{\{a_1,a_2\}\cup S'} \\ &= L^{\mathrm{pure}}_{\{b\}\cup S'}. \end{aligned} \tag{16}$$

This means that we do not detect entanglement in any coarse partition, if we do not detect it in the finest partition.

The correlation-strength L_S defined here can be understood as special case of 'g-purity' defined by Barnum *et al.*[16] (see also [17]) as the purity relative to a restricted subset of observables g. They use this definition to give a 'generalized notion of entanglement': given a subset of observables g (not necessarily related to a sub-system), a pure state is 'unentangled' iff the g-purity is maximal. Other than using the standard convex roof extension of such criterion —for which no closed form is known—, their criterion is limited to pure states.

The correlation strength criterion is also stronger than the criterion that results from the 'global' entanglement measure proposed by Meyer and Wallach[18]. The latter has in fact

been proven [19] to be equivalent to the criterion proposed in [16] applied to multi-partite systems.

For multi-qubit systems, the generalized Bell-inequalities [20, 14] —criterion for the existence of a local-realistic description of a set of correlation measurements on a given state—provides a weaker entanglement criterion than the correlation strengths. Indeed, if there exists a set of local dichotomic measurements on a state ρ such that a Bell-inequality is violated, than it follows that there is a local coordinate system $\{x, y\}$ such that $\sum_{i_1,\ldots i_N=1}^{2} c^2_{i_1\ldots i_N} > 1$ (Eq. (15) in [14]). Since this is precisely the sum in Eq.(9) excluding the terms with $i_k = 3$, one arrives at $L_P(\rho) > 1$.

However, as one might have guessed by the fact that our criterion only depends on the mixedness of ρ and its reductions, the criterion fails to detect a variety of mixed entangled states. This will be seen in the next section where some important classes of multi-qubit states will be studied. In fact, it turns out [21] that the proposed criterion is weaker than the well known positive partial transposition (PPT) bipartite separability criteria [22]: i. e. any state for which a given correlation strength $L_S(\rho) > 1$, will have a bipartite split $\{A, \bar{A}\}$ such that the corresponding partial transposition results in a non-positive operator $\rho^{T_A} \ngeq 0$.

4 Correlation strengths for multi-qubit systems

In this section we will compute the local invariants and check the entanglement criterion for different classes of relevant n-qubit states. We will see that for most examples the correlation strengths can be computed even for large values of n.

4.1 Dicke-States

Dicke states $|n, m\rangle$ are n-qubit symmetric pure states with m excitations (or qubits in state $|0\rangle$),

$$|n, m\rangle \propto \sum_i \Pi_i |1, \overset{m}{\ldots}, 1, 0, \ldots 0\rangle \tag{17}$$

with $\{\Pi_i\}$ being the group of all permutation matrices. We denote $\rho^m = |n, m\rangle\langle n, m|$. Obviously, the states $|n, m\rangle$ and $|n, n - m\rangle$ will have the same entanglement properties.

Dicke states appear naturally in quantum optical and condensed matter systems, and have also received attention within the field of quantum information (see for example [23],[24]). Due to the large symmetry of these states, the purity of their reduced density matrices can be readily computed in the excitation-basis leading to,

$$L_S(\rho^m) = \sum_{k=0}^{|S|} 2^k \binom{|S|}{k} \sum_{n=0}^{\min(k,m)} \left(\binom{n}{m}^{-1} \binom{k}{n} \binom{n-k}{m-n} \right)^2 \tag{18}$$

which depends only on the size $|S|$ of the set of parties.

For $m = 1$, which corresponds to W states [24], we obtain a S-correlation strength $L_S(\rho^{m=1}) = \frac{1}{n^2}(n^2 + 8|S|^2 - 4(n + 1)|S|)$. The maximum value is achieved for the correlation strength involving all parties $L_P(\rho^{m=1}) = 5 - \frac{4}{n}$. Entanglement in such states is know to be extremely robust to particle loss, exhibiting entanglement even when all but two particles are lost. However, we see that using our criterion, entanglement is only detected for sets S with more than $|S| > \frac{n+1}{2}$ parties. Similarly, for other m values we obtain maximum

values that converge as $\frac{1}{n}$ for increasing n and also exhibit a threshold for the minimal size of the sets of parties to detect entanglement.

4.2 Graph and Graph-diagonal states

Graph-states [25, 26] form a new and very wide class of multi-partite entangled states that have been shown to play an important role in quantum information processing: they occur in some error correcting codes [26], provide a universal resource for quantum computation [27], improve frequency standards [28], and allow for secret sharing [29]. Something particularly interesting in the context of studying multi-partite entanglement is that they count with an efficient description. Given a graph $G = (V, E)$ —i. e. a set of n vertices V connected by edges E that specify the neighborhood relation between vertices—graph-states can be conveniently defined through the set of commuting observables $\{K_G^a\}_{a=1}^n$,

$$K_G^a = \sigma_x^{(a)} \prod_{b \in N_a} \sigma_z^{(b)} \quad \text{for } a = 1, \ldots, n \tag{19}$$

where N_a denotes the set of neighboring vertices of vertex a ($\{b : \{a, b\} \in E\}$). The common eigenvectors of this set of observables form a complete orthonormal basis of graph-states corresponding to the graph G,

$$K_G^i |\psi_{\vec{\mu}}\rangle = (-1)^{\mu_i} |\psi_{\vec{\mu}}\rangle \text{ for } i = 1, \ldots, n \tag{20}$$

where the n-dimensional binary array $\vec{\mu}$ labels each of the 2^n graph basis states.

These basis vectors are related by a local unitary $|\psi_{\vec{\mu}}\rangle = \sigma_z^{\vec{\mu}} |\psi_{\vec{0}}\rangle$, where $\sigma_z^{\vec{\mu}}$ denotes the action of σ_z on the parties i specified by $\mu_i = 1$.

The stabilizer S_G of a graph-state is the finite group generated by $\{K_G^a\}_{a=1}^n$. Every element in S_G will be a Pauli operator that can be labeled by a binary array $\vec{\nu}$: $\sigma_{\vec{\nu}} = \prod_{a=1}^n (K_G^{(a)})^{\nu_a}$.

Thus, in the Pauli operator basis the representative graph state is given by $|\psi_{\vec{0}}\rangle\langle\psi_{\vec{0}}| = \frac{1}{d} \sum_{\sigma_{\vec{\nu}} \in S_G} \sigma_{\vec{\nu}}$, and the other basis states by $|\psi_{\vec{\mu}}\rangle\langle\psi_{\vec{\mu}}| = \frac{1}{d} \sum_{\sigma_{\vec{\nu}} \in S_G} (-1)^{\vec{\mu}\cdot\vec{\nu}} \sigma_{\vec{\nu}}$. Thus, we notice that the S-correlation strength of a graph states is given by the number of elements of the stabilizer that are S-correlation operators, i. e. $L_S(|G\rangle\langle G|) = |S_G \cap \mathcal{B}_S|$.

By making use of Eq. (10) and the fact that graph states have equally weighted Schmidt coefficients for any bi-partition [25] we can also rewrite the S-correlation length as,

$$L_S(|G\rangle\langle G|) = \sum_{S' \subset S} (-1)^{|S|-|S'|} 2^{|S'|-E^{S'}(G)} \tag{21}$$

where the Schmidt measure $E^{S'}(G)$ in respect to partition $(S', \bar{S}')$ is determined by the Schmidt rank r, $E^{S'}(G) = \log_2(r)$ [25].

An arbitrary n-qubit state can be depolarized by local operations and classical communication to a graph-diagonal [30] state. Specifically, this is done by applying sequentially the mixing maps $\mathcal{D}_i(\rho) = \frac{1}{2}(\rho + K_G^i \rho K_G^i)$ for $i = 1, \ldots, n$. For such a graph-diagonal state ρ_G with weights $\{p_{\vec{\mu}}\}$ the S-correlation strength is given by

$$L_S(\rho_G) = \sum_{\sigma_{\vec{\nu}} \in S_G \cap \mathcal{B}_S} \left(\sum_{\vec{\mu}} (-1)^{\vec{\nu}\cdot\vec{\mu}} p_{\vec{\mu}} \right)^2 = \boldsymbol{p} \cdot M \cdot \boldsymbol{p} \tag{22}$$

with $M_{ij} = \sum_{\sigma_{\vec{\nu}} \in S_G \cap \mathcal{B}_S} (-1)^{\vec{\nu}\cdot(\vec{S}_i + \vec{S}_j)}$

This can be readily computed numerically and in some cases also analytically. Below we discuss the class of GHZ-diagonal states.

GHZ-diagonal states: The generalized GHZ-states [31] correspond to 'star'-graphs [25]. The representative graph state is given by, $|\psi_{\vec{0}}\rangle = \frac{1}{\sqrt{2}}(|0\rangle_z|0\ldots0\rangle_x + |1\rangle_z|1\ldots1\rangle_x)$. The remaining GHZ-basis states are $|\psi_{\vec{\mu}}\rangle$, where the first bit of the binary array $\vec{\mu}$ determines the phase, while the remaining $n-1$ bits correspond to the bit-flips in the $n-1$ last qubits. Here, we will label each graph-state basis vector either by the the binary array $\vec{\mu}$ or by the corresponding integer in the decimal basis $\mu \in [0, 2^n - 1]$.

Since for GHZ-states the Schmidt measure is $E^S(|GHZ\rangle) = 1$ for all partitions with exception of $S = \{\}$ and $S = P$ for which it vanishes, one can readily show that (Eq.22)

$$L_P(GHZ) = 2^{n-1} + \delta_{n,\text{even}} \quad \text{and} \quad L_S(GHZ) = \delta_{|S|,\text{even}} \text{ for } S \subsetneq P. \tag{23}$$

Following the previous notation for the stabilizer group elements, the set of Pauli operators $\sigma_{\vec{\nu}} \in S_G \cap \mathcal{B}_P$ is given by $\mathcal{A}^{\text{odd}} = \{\vec{\nu}\} = \{(1, \vec{x}) | x = 0, \ldots, 2^{n-1} - 1\}$ for n odd, and $\mathcal{A}^{\text{even}} = \mathcal{A}^{\text{odd}} \cup \{(0, 1, \ldots, 1)\}$. The P-correlation strength for GHZ-diagonal states can then be shown to be (Eq.22),

$$L_P(\rho) = 2^{n-1} \sum_{\mu=0}^{2^{n-1}-1} (p_\mu - p_{\mu+2^{n-1}})^2 + \delta_{n,\text{even}} \left(\sum_{\mu=0}^{2^{n-1}-1} (p_\mu + p_{\mu+2^{n-1}})(-1)^{|\vec{\mu}|} \right)^2, \tag{24}$$

where we have used $\sum_{\vec{x}} (-1)^{\vec{x}\cdot\vec{\mu}} = \delta_{\vec{\mu},\vec{0}} 2^n$. According to our chosen convention, the state corresponding to the index-label $\mu + 2^{n-1}$ is the same than that with label μ but with opposite phase ($\pm$). Hence, the weights p_μ and $p_{\mu+2^{n-1}}$ of GHZ states with opposite phase always appear together as a difference (and also as sum in the even n case). Since the reductions of a GHZ are always separable, it is clear that $L_S(\rho) \leq 1$ for $S \subsetneq P$.

These expressions can be further simplified if we restrict to a still very relevant class that can be obtained from a general state by a further local depolarization step [32]. The class is fully specified by 2^{n-1} parameters,

$$p_i = p_{i+2^{n-1}} \text{ for } i \geq 1, \text{ and } \Delta = p_0 - p_{2^{n-1}}. \tag{25}$$

Such states [32] play the role of generalized multi-qubit Werner-states and have the nice property that the positivity of the partial transposition in respect to a subset A is easily checked: $\rho^{T_A} \geq 0 \Leftrightarrow \Delta \leq 2p_\mu$ (where $\vec{\mu}$ is the binary array with $\vec{\mu}_i = 1$ iff $i \in A$).

For such class of states the P-correlation (Eq. 24) only depends on the parameter Δ (for odd n).

$$L_P(\Delta) = 2^{n-1}\Delta^2 + \delta_{n,\text{even}} \left(2 \sum_{\mu=0}^{2^{n-1}-1} (-1)^{|\vec{x}_i|} p_i + \Delta \right)^2 \tag{26}$$

In the remaining of this section we use the previous results to compare the performance of the correlation strength with other entanglement criteria:

- For noisy GHZ: $p|GHZ\rangle\langle GHZ| + (1-p)\frac{1}{d}\mathbf{1}$ $\begin{cases} L_P(\rho) \rightarrow & p > (2^{n-1} + \delta_{n,\text{even}})^{-\frac{1}{2}} \\ \text{Bell Ineq.} \rightarrow & p > (2^{n-1})^{-\frac{1}{2}} \\ \text{NPPT} \rightarrow & p > (2^{n-1} + 1)^{-1} \end{cases}$

- $L_S(\rho) > 1 \not\Leftrightarrow \langle GHZ|\rho|GHZ\rangle > \frac{1}{2} \Rightarrow$ N-distillability. That is, the correlation strength criterion is neither stronger nor weaker than the MES-overlap criterion.

- The correlation strength criterion is neither stronger nor weaker than realignment criterion [33, 34]. It is known that the realignment method can detect some PPT bound entangled states, while the correlation strength can not. On the other hand, there are simple examples —even in the 2x2 case (see [34])—, where the entanglement is not detected by the realignment criteria, but $L_{\{1,2\}} > 1$.

- It detects NPPT multi-partite 'bound' entanglement[35], $\begin{cases} L_P(\rho) \to & N \geq 8 \\ \text{Bell Ineq.} \to & N \geq 8 \\ \text{NPPT} \to & N \geq 4 \end{cases}$

- If ρ has m or more positive partial transposes $L_P(\rho) < L_P(\Delta_c)$ where $\Delta_c = \frac{1}{m+1}$.

- k-separability: If a GHZ-diagonal state can be written as $\rho = \sum_i p_i \rho_i^1 \otimes \ldots \otimes \rho_i^k$ there will be $m = 2^{k-1} - 1$ PPT, and one arrives to $L_P(\rho) \leq 2^{n-2k+1}$. This coincides with the strongest upper-bound obtained from quadratic Bell-Inequalities [36] in restricted experimental settings [37]. Using the property $L_S(\rho_A \otimes \rho_B) = L(\rho_A)L(\rho_B)$ it is also possible to derive k-separability criteria for general states [21].

5 Towards a complete set of invariants

The local invariants L_S do not form a complete set of invariants, i. e. they do not contain *all* information about the entanglement properties of a given state. However, the formalism used in this paper allows us to identify a larger class of invariants, many of which also have a straight-forward geometrical interpretation.

From the proof of Theorem 1, it follows that the transformation properties of the subspaces $\mathcal{V}_S$ are closely related. In order to show how this can be used for the construction of invariants, we first define the S-correlation tensor C_S, which is composed of the components of the projection ξ_S in (6),

$$C_S = \left(\left\langle \prod_{a \in S} \sigma_{i_a}^{(a)} \right\rangle_\rho \right)_{i_a > 0} . \tag{27}$$

One can easily see that a contraction of two such tensors with respect to a index i_ν at the same position is invariant under local unitary operations, i. e. under orthogonal transformation $\mathcal{O}$ which affect this index:

$$\begin{aligned} \sum_{i_\nu} c_{\ldots i_\nu \ldots} c_{\ldots i_\nu \ldots} &= \sum_{i_\nu, i_\nu''} \delta_{i_\nu, i_\nu''} c_{\ldots i_\nu \ldots} c_{\ldots i_\nu'' \ldots} \\ &= \sum_{i_\nu', i_\nu, i_\nu''} \mathcal{O}_{i_\nu' i_\nu} c_{\ldots i_\nu \ldots} \mathcal{O}_{i_\nu' i_\nu''} c_{\ldots i_\nu'' \ldots} \\ &= \sum_{i_\nu'} \tilde{c}_{\ldots i_\nu' \ldots} \tilde{c}_{\ldots i_\nu' \ldots} \end{aligned} \tag{28}$$

Any complete contraction of correlation tensors, i. e. a polynomial in the expansion coefficients, in which indices are either zero or summed up pairwise, is thus a local invariant. Examples for

such polynomials are $c_{0jk}c_{ij0}c_{i0k}$, $c_{0j00}c_{ij0l}c_{ij'k0}c_{cj'kl}$ (where, as usual, the sum is taken over all indices which occur twice), the correlation strengths L_S, and other objects which can be interpreted as scalar products, such as the scalar product of $\rho_{a_1a_2a_3}$ with the tensor product of $\rho_{\{a_1\}}, \rho_{\{a_2\}}$ and $\rho_{\{a_3\}}$,

$$\langle \rho_{\{a_1\}} \otimes \rho_{\{a_2\}} \otimes \rho_{\{a_3\}}, \rho_{\{a_1a_2a_3\}} \rangle = \sum_{i,j,k>0} c_{i00}c_{0j0}c_{00k}c_{ijk}. \tag{29}$$

Unfortunately, it is not possible to construct a complete set of local invariants using the construction above: already for the case of two qubits, there are seven independent invariants which can be written as contraction of correlation tensors; the two remaining invariants are functions of the determinant and sub-determinants of the correlation tensor [13].

Following the ideas of [6] we can can generalize the above constructions in order to obtain a complete set of polynomial invariants in the coordinates $c_{i_1\ldots i_n}$:

Any homogeneous polynomial f of degree k, i.e.

$$f(c_{i_1\ldots i_n}) = \sum_{\substack{i_1^1,\ldots,i_n^1 \\ i_1^2,\ldots,i_n^k}} M_{i_1^1,\ldots,i_n^1,i_1^2,\ldots,i_n^k}\; c_{i_1^1\ldots i_n^1} c_{i_1^2\ldots i_n^2} \cdots c_{i_1^k\ldots i_n^k}, \tag{30}$$

is invariant under local unitary transformation, *iff* the corresponding observable

$$M = \sum_{\substack{i_1^1,\ldots,i_n^1 \\ i_1^2,\ldots,i_n^k}} M_{i_1^1,\ldots,i_n^1,i_1^2,\ldots,i_n^k}\; \sigma^{(1)}_{i_1^1} \ldots \sigma^{(n)}_{i_n^1} \sigma^{(1)}_{i_1^2} \ldots \sigma^{(n)}_{i_n^k} \tag{31}$$

on $\left(\mathcal{H}^{(1)} \otimes \ldots \otimes \mathcal{H}^{(n)}\right)^{\otimes k}$ commutes with all unitaries of the form $(U_1^{(1)} \otimes \ldots \otimes U_n^{(n)})^{\otimes k}$. For example, the proposed invariants L_S are homogeneous polynomials of degree 2 for which the corresponding observable is $M_S = \sum_{\sigma \in \mathcal{B}_S} \sigma \otimes \sigma$. The map is a vector space isomorphism from the algebra of observables M on $\mathcal{H}^{\otimes k}$, with $[M, (U_1^{(1)} \otimes \ldots \otimes U_n^{(n)})^{\otimes k}] = 0$ for all local unitaries, onto the the algebra of invariant homogeneous polynomials of degree k in the coordinates $c_{i_1\ldots i_n}$. A measurement of the observable M on k copies of the state then evaluates the corresponding polynomial invariant M, i.e. $f_M(c_{i_1\ldots i_n}) = \langle M, \rho^{\otimes k} \rangle = \operatorname{tr} M\rho^{\otimes k}$.

Note that the orbits of the compact group of local unitaries can be separated by some polynomial invariants (see [38], p.133). This means that two states ρ_1 and ρ_2 can be transformed into each other by local unitaries if and only if the evaluations of all polynomial invariants f coincide. Moreover, the algebra of invariant polynomials is finitely generated and the generators can be chosen to be homogeneous polynomials. In order to find a complete set of invariants, that generates the whole algebra of polynomial invariants, it is therefore sufficient to find the generators of the algebra of invariant homogeneous polynomials for different degrees k, or equivalently the algebra of hermitian matrices M, that commute with $(U_1^{(1)} \otimes \ldots \otimes U_n^{(n)})^{\otimes k}$ for all local unitaries $U_1^{(1)} \otimes \ldots \otimes U_n^{(n)}$. The proposed set of invariants $\{L_S\}$ are then an example of generating set of homogeneous polynomials of degree $k = 2$.

In [6] the construction of a set of (possibly non-hermitean) generators F can be found. From it, a set of hermitean generators can be obtained by symmetrization: $M_1 = \frac{F+F^\dagger}{2}$ and $M_2 = \frac{F-F^\dagger}{2i}$. For each generator M the coefficients $M_{i_1^1,\ldots,i_n^1,i_1^2,\ldots,i_n^k}$ then can be computed from Eq. (31), which determines a set of generators f_M for the invariant ring of degree k by Eq. (30).

6 Conclusions

In this paper, we have investigated local invariants in terms of correlation operators. The related geometric interpretation of the space of coherence vectors and its LU-invariant subspaces allowed us to explicitly write down a subclass of such invariants. Using a convexity argument, we have given a simple entanglement criterion for multi-partite states.

We have shown that the criterion fails to detect important classes of entangled states —including some NPPT states. Nevertheless, we think that our criterion is of interest. The criterion is simple and with a clear interpretation. It is easily computable even for large number of qubits and some closed forms can be obtained. In particular they are more efficiently computable than the PPT-criteron that involves a matrix diagonalization. This might be especially usefull in the study of entanglement in many-body systems. On the other hand, L_P gives information on all partitions so that one does not need to check the positivity of all $2^{n-1}-1$ possible partial transpositions.

From the experimental point of view our criterion also offers some advantages. Firstly, the proposed criterion are state-independent: it does not require previous knowledge of the state nor optimization over possible experimental-settings, like in the case of Bell-inequalities or general entanglement witnesses. To measure the S-correlation $L_S(\rho)$ efficiently one can measure a single observable $M_S = \sum_{\sigma\in\mathcal{B}_S} \sigma\otimes\sigma$ on two copies $\rho\otimes\rho$ requiring only bi-local operations between equivalent qubits in each of the copies. Alternatively one can opt for a more straightforward approach and measure the correlation functions $\left\langle \sigma_{i_1}^{(1)}\sigma_{i_2}^{(2)}\cdots\sigma_{i_n}^{(n)}\right\rangle_\rho$, as one does in quantum tomography, with the advantage that entanglement might be detected, i. e. L_S becomes larger than one, long before the complete tomography is over.

Finally, it remains an open question whether the values achieved by the correlation strengths are related to the distillability properties of the state.

Acknowledgements

This work has been supported by the Deutsche Forschungsgemeinschaft (Schwerpunkt QIV) and the European Union (IST-2001-38877,-39227).

1. A. Einstein, B. Podolsky, and N. Rosen (1935),*Can quantum mechanical description of physical reality be considered complete?*, Phys. Rev. **47**, 777.
2. E. Schrödinger (1935), *The quantum postulate and the recent development of atomic theory*, Naturwissenschaften, vol. 23, pp. 807–812, 823–828, 844–849.
3. J. S. Bell (1964), *On the einstein-podolsky-rosen paradox,* Physics, vol. 1, p. 195. Reprinted in J. S. Bell, *Speakable and unspeakable in quantum mechanics*, Cambidge University Press, 1987.
4. J. Schlienz and G. Mahler (1995), *Description of entanglement* , Phys. Rev. A **52**, 4396 ; G. Mahler, V. A. Weberruß (1995), *Quantum Networks: Dynamics of Open Nanostructures*, Berlin, Springer.
5. N. Linden and S. Popescu (1998), *On multi-particle entanglement,* Fortschr. Physik, vol. 46, p. 567.
6. M. Grassl, M. Rötteler, T. Beth (1998), *Computing local invariants of quantum-bit systems,* Phys. Rev. A, **58**, 1833; E. M. Rains (1997), *Polynomial invariants of quantum codes*, quant-ph/9704042.
7. F. Verstraete, J. Dehaene, and B. D. Moor (2002), *Lorentz singular-value decomposition and its applications to pure states of three qubits,* Phys. Rev. A, **65**, 032308.
8. G. Jaeger, M. Teodorescu-Frumosu, A. Sergienko, B. E. A. Saleh, and M. C. Teich (2003), *Multiphoton stokes-parameter invariant for entangled states,* Phys. Rev. A, **67**, 032307.
9. D. F. V. James, P. G. Kwiat, W. J. Munro, and A. G. White (2001), *Measurement of qubits,* Phys. Rev. A, **64**, 052312.

10. R. T. Thew, K. Nemoto, A. G. White, and W. J. Munro (2002), *Qudit quantum-state tomography,* Phys. Rev. A, **66**, 012303.
11. J. Schwinger (1960), *Unitary operator bases,* Proc. NAS, **46**, no. 4, 570–579.
12. F. T. Hioe and J. H. Eberly (1981), *n-level coherence vector and higher conservation laws in quantum optics and quantum mechanics,* Phys. Rev. Lett. **47**, 838.
13. B.-G. Englert and N. Metwally (2000), *Separability of entangled q-bit pairs,* J. Mod. Opt. **47**, 2221.
14. M. Zukowski and Č. Brukner (2002), *Bell's theorem for general n-qubit states*, Phys. Rev. Lett. **88**, 210401.
15. M. S. Byrd and N. Khaneja (2003), *Characterization of the positivity of the density matrix in terms of the coherence vector representation* , Phys. Rev. A **68**, 062322.
16. H. Barnum, E. Knill, G. Ortiz, R. Somma, L. Viola (2004), *A Subsystem-Independent Generalization of Entanglement*, Phys. Rev. Lett. **92**, 107902.
17. A. A. Klyachko (2002), *Coherent states, entanglement, and geometric invariant theory*, quant-ph/0206012.
18. D. A. Meyer abd N. R. Wallach (2002), *Global entanglement in multiparticle systems* , J. Math. Phys. **43**, 4273.
19. G. K. Brennen (2003), *An observable measure of entanglement for pure states of multi-qubit systems,* Quantum Inf. Comp. **3**, 619.
20. R. F. Werner and M. M. Wolf (2001), *All-multipartite Bell-correlation inequalities for two dichotomic observables per site* , Phys. Rev. A. **64**, 032112.
21. J. Calsamiglia *et al.*, in preparation.
22. A. Peres (1996), *Separability criterion for density matrices,* Phys. Rev. Lett. **77**,1413.
23. J. K. Stockton, J. M. Geremia, A. C. Doherty, H. Mabuchi (2003), *Characterizing the entanglement of symmetric many-particle spin-(1/2) systems* Phys. Rev. A. **67**, 022112.
24. W. Dür, G. Vidal, and J. I. Cirac (2000), *Three qubits can be entangled in two inequivalent ways*, Phys. Rev. A. **62**, 062314.
25. M. Hein, J.Eisert, and H. J. Briegel (2003), *Multi-party entanglement in graph states*, accepted for publication in Phys. Rev. A., quant-ph/0307130.
26. D. Schlingemann and R. F. Werner (2002),*Quantum error-correcting codes associated with graphs,* Phys. Rev. A **65**, 012308.
27. R. Raussendorf and H. J. Briegel (2001), *A One-Way Quantum Computer,* Phys. Rev. Lett. **86**, 5188.
28. S. F. Huelga, C. Macchiavello, T. Pellizzari, A. K. Ekert, M. B. Plenio, and J. I. Cirac (1997), *Improvement of Frequency Standards with Quantum Entanglement*, Phys. Rev. Lett. **79**, 3865.
29. M. Hillery, V. Buzek, A. Berthiaume (1999), *Quantum Secret Sharing*, Phys. Rev. A 59, 1829 ; D. Gottesman (2000), *On the theory of quantum secret sharing*, Phys. Rev. A **61**, 042311.
30. W. Dür, H. Aschauer, and H. J. Briegel (2003), *Multiparticle Entanglement Purification for Graph States,* Phys. Rev. Lett. **91**, 107903.
31. D. M. Greenberger, M. Horne, and A. Zeilinger (1989), *Going beyond bell's theorem* in "Bell's theorem, quantum theory, and conceptions of the universe" (M. Kafatos, ed.), p. 69, Kluwer.
32. W. Dür and J. I. Cirac (2000), *Classification of multiqubit mixed states: Separability and distillability properties*, Phys. Rev. A. **61**, 042314.
33. O. Rudolph (2002), *Further results on the cross norm criterion for separability*, quant-ph/0202121.
34. K. Chen and L.A. Wu (2003), *A matrix realignment method for recognizing entanglement* , Quantum Inf. Comput. **3**, 193.
35. W. Dür (2001), *Multipartite Bound entangled States that Violate Bell's Inequality*, Phys. Rev. Lett. **87**, 230402.
36. J. Uffink (2002), *Quadratic Bell Inequalities as Tests for Multipartite Entanglement*, Phys. Rev. Lett. **88**, 230406.
37. K. Nagata, M. Koashi, N. Imoto (2002), *Configuration of separability and tests for multipartite entanglement in Bell-type experiments,* Phys. Rev. Lett. **89**, 260401.
38. A. Onishchik and E. Vinberg 1990, *Lie Groups and Algebraic Groups*, Heidelberg, Springer.