Entanglement measures under symmetry

K. G. H. Vollbrecht* and R. F. Werner†
Institut für Mathematische Physik, TU Braunschweig, Mendelssohnstrasse 3, 38106 Braunschweig, Germany
(Received 15 January 2001; published 14 November 2001)

We show how to simplify the computation of the entanglement of formation and the relative entropy of entanglement for states, which are invariant under a group of local symmetries. For several examples of groups we characterize the state spaces, which are invariant under these groups. For specific examples we calculate the entanglement measures. In particular, we derive an explicit formula for the entanglement of formation for $(U\otimes U)$-invariant states, and we find a counterexample of the additivity conjecture for the relative entropy of entanglement.

DOI: 10.1103/PhysRevA.64.062307 PACS number(s): 03.67.−a, 03.65.Ta, 03.65.Ca, 89.70.+c

I. INTRODUCTION

One of the reasons the general theory of entanglement has proved to be so difficult is the rapid growth of dimension of the state spaces. For bipartite entanglement between d_1- and d_2-dimensional Hilbert spaces, entanglement is a geometric structure in the $(d_1^2 d_2^2 - 1)$-dimensional state space. Hence, even in the simplest nontrivial case ($d_1 = d_2 = 2$; 15 dimensions), naive geometric intuitions can be misleading. On the other hand, the rapid growth of dimensions is partly responsible for the potential of quantum computing. Hence, exploring this complexity is an important challenge for quantum information theory.

Model studies have been an important tool for developing and testing new concepts and relations in entanglement theory, both qualitative and quantitative. In this paper we explore a method for arriving at a large class of models, which are equally simple, and yet show some of the interesting features of the full structure.

The basic idea of, namely, looking at sets of states that are invariant under a group of local unitary operators is not new, and goes back to the first studies of entanglement [1,2] in the modern sense. Two classes, in particular, have been considered frequently: the so-called *Werner states* (after [1]), which are invariant under all unitary operators of the form $U\otimes U$, and the so-called *isotropic states* [3], which are invariant under all $U\otimes U^*$, where U^* is the complex conjugate of U in some basis. Symmetry has also been used in this way to study tripartite entanglement [4,5]. A recent paper of Rains [6] discusses distillable entanglement under symmetry, so we have eliminated the pertinent remarks from this paper.

Several of the ingredients of our general theory, for example, the role of the twirl projection and the commutant, have been noted in these special cases and can be considered to be well known. The computation of the relative entropy of entanglement [7] was known [8] for Werner states. The first study in which symmetry is exploited to compute the entanglement of formation [9] beyond the Wootters formula [10] is Ref. [12], where the case of isotropic states is investigated. Our theory of entanglement of formation can be viewed as an abstract version of arguments from that paper.

What is new in the present paper is, first, the generality. We regard our theory as a toolkit for constructing examples adapted to specific problems, and we have tried to present it in a self-contained way, facilitating such applications. Exploring all the possibilities would have been too much for a single paper but, of course, we also have some new results in specific examples.

Our most striking specific result is perhaps a counterexample of the conjecture that the relative entropy of formation should be additive. The evidence in favor of this conjecture had been partly numerical, but it was perhaps clear that a random search for counterexamples was not very strong evidence to begin with: the relative entropy of entanglement is defined by a variational formula in a very high dimensional space, whose solution is itself not easy to do reliably. In addition, the additivity conjecture is true on a large set in the state space, so unless one has a specific idea where to look, a random search may well produce misleading evidence. The second strong point in favor of the additivity conjecture had been a theorem by Rains (Theorems 4 and 5 in Ref. [13]) implying a host of nontrivial additivity statements. However, our counterexample satisfies the assumptions of the Rains' theorem, so that theorem is, unfortunately, false.

Further specific results in our paper are the formulas for entanglement of formation and relative entropy of entanglement for Werner states.

The paper is organized as follows: In Sec. II we review the essential techniques for the investigation of symmetric states and describe how the partial transposition fit in this context. Section II D presents a zoo of different symmetry groups. Some of these are used later, others are only presented as briefly, to illustrate special properties possible in this setup. We hope that this list will prove useful for finding the right tradeoff between high symmetry, making an example manageable, and richness of the symmetric state space, which may be needed to see the phenomenon under investigation. In Sec. III we briefly recapitulate the definitions of the entanglement of formation and the relative entropy of entanglement and the additivity problem. In Sec. IV we turn to the entanglement of formation. We show first how the computation may be simplified using local symmetry. These ideas are then applied to the basic symmetry groups UU and UU*, arriving at an explicit formula in both cases

*Electronic address: k.vollbrecht@tu-bs.de
†Electronic address: R.Werner@tu-bs.de

(the results for UU* are merely cited here for completeness from work of the first author with Terhal [12]). For the group OO of orthogonal symmetries, which unifies and extends these two examples, we find formulas in large sections of the state space. Section V deals with the relative entropy of entanglement. Again we begin by showing how the computation is simplified under symmetry. We then present the counterexample of additivity mentioned in this section. Some possible extensions are mentioned in the concluding remarks.

II. SYMMETRIES AND PARTIAL TRANSPOSES

From the beginning of the theory of entanglement the study of special subclasses of symmetric states has played an important role. In this section we give a unified treatment of the mathematical structure underlying all these studies. For simplicity we restrict attention to the bipartite finite dimensional case, although some of the generalizations to more than two subsystems [4] and infinite dimension are straightforward. So throughout we will consider a composite quantum system with Hilbert space $\mathcal{H}=\mathcal{H}_1\otimes\mathcal{H}_2$, with $\dim\mathcal{H}_i=d_i<\infty$. We denote the space of states (=density operators) on $\mathcal{H}$ as $\mathcal{S}(\mathcal{H})$, or simply by $\mathcal{S}$. The space of all separable states (explained in Sec. II B) is denoted as $\mathcal{D}$.

A. Local symmetry groups

Two states ρ,ρ' are regarded as "equally entangled" if they differ only by a choice of basis in $\mathcal{H}_1$ and $\mathcal{H}_2$ or, equivalently, if there are unitary operators U_i acting on H_i such that $\rho'=(U_1\otimes U_2)\rho(U_1\otimes U_2)^\dagger$. If in this equation $\rho'=\rho$, we call $U=(U_1\otimes U_2)$ a (local) symmetry of the entangled state ρ. Clearly, the set of symmetries forms a closed group of unitary operators on $\mathcal{H}_1\otimes\mathcal{H}_2$. We will now turn this around, i.e., we fix the symmetry group and study the set of states left invariant by it.

So from now on, let G be a closed group of unitary operators of the form $U=(U_1\otimes U_2)$. As a closed subgroup of the unitary group, G is compact, hence carries a unique measure that is normalized and invariant under right and left group translation. Integrals with respect to this *Haar measure* will just be denoted by "$\int dU$," and should be considered as averages over the group. In particular, when G is a finite group, we have $\int dU\, f(U)=|G|^{-1}\Sigma_{U\in G}f(U)$. An important ingredient of our theory is the projection

$$\mathbf{P}(A)=\int dU\, UAU^\dagger, \tag{1}$$

for any operator A on $\mathcal{H}_1\otimes\mathcal{H}_2$, which is sometimes referred to as the *twirl* operation. It is a completely positive operator, and is *doubly stochastic* in the sense that it takes density operators to density operators and the identity operator to itself. Using the invariance of the Haar measure it is immediately clear that "$\mathbf{P}A=A$" is equivalent to "$[U,A]=0$ for all $U\in G$." The set of all A with this property is called the *commutant* of G. We will denote it by G', which is the standard notation for commutants in the theory of von Neumann algebras. It will be important later on that G' is always an algebra (closed under the operator product), although in general $\mathbf{P}(AB)\neq(\mathbf{P}A)(\mathbf{P}B)$. Computing the commutant is always the first step in applying our theory. Typically, one tries to pick a large symmetry group G from the outset, so the commutant becomes a low-dimensional space, spanned by just a few operators.

Our main interest does not lie in the set G' of G-invariant observables, but dually, in the G-invariant density operators ρ with $\mathbf{P}\rho=\rho$. As for observables, this set is the projection $\mathbf{P}\mathcal{S}$ of the full state space under twirling. The relation between invariant observables and states is contained in the equation

$$\mathrm{tr}[\mathbf{P}(\rho)A]=\mathrm{tr}[\rho\mathbf{P}(A)], \tag{2}$$

which follows easily by substituting $U\mapsto U^\dagger=U^{-1}$ in the integral (1), and moving one factor U under the trace. Due to this equation, we do not need to know the expectations $\mathrm{tr}(\rho A)$ for all observables A in order to characterize a G-invariant ρ, but only for the invariant elements $\mathbf{P}(A)\in G'$. Indeed, if we have a linear functional $f:G'\to\mathbb{C}$, which is positive on positive operators, and normalized to $f(\mathbb{I})=1$, that is, a *state* on the algebra G' in C*-algebraic terminology, the equation $\mathrm{tr}(\rho A)=f(\mathbf{P}(A))$ uniquely defines a G-invariant density operator ρ, because $\mathbf{P}$ preserves positivity and $\mathbf{P}(\mathbb{I})=\mathbb{I}$. Under this identification of G-invariant density operators and states on G' it becomes easy to compute the image of a general density operator ρ under twirling. Using again Eq. (2) we find that $\mathbf{P}\rho$ is determined simply by computing its expectation values for $A\in G'$, i.e., its *restriction* to G'.

To characterize the invariant state space we always choose a basis in G' of k Hermitian operators A_α, where k denotes the dimension of G'. The state space of invariant states is then identified with the k tuples of expectation values $\langle A_\alpha\rangle=\mathrm{tr}(A_\alpha\rho)$. As a simplification we will always choose one operator to be the identity. Due to the normalization of the states, this expectation value has to be equal to 1 and we are left with $(k-1)$ parameters.

Let us demonstrate this in the two basic examples of twirling.

Example 1: The group UU *(Werner states*).

We take the Hilbert spaces of Alice and Bob to be the same ($\mathcal{H}=\mathcal{H}_1\otimes\mathcal{H}_1$), and choose for G the group of all unitary operators of the form $U\otimes U$, where U is a unitary operator on $\mathcal{H}_1$. As an abstract topological group this is the same as the unitary group on $\mathcal{H}_1$, so the Haar measure on G is just invariant integration with respect to U. It is a well-known result of group representation theory, going back to Weyl [14] or further, that the commutant of G is spanned by the permutation operators of the factors, in this case the identity $\mathbb{I}$ and the *flip* defined by $\mathbb{F}(\phi\otimes\psi)=\psi\otimes\phi$, or in a basis $|i\rangle$ of $\mathcal{H}_1$, with $|ij\rangle=|i\rangle\otimes|j\rangle$,

$$\mathbb{F}=\sum_{i,j}|ij\rangle\langle ji|. \tag{3}$$

Hence the algebra G' consists of all operators of the form $A=\alpha\mathbb{I}+\beta\mathbb{F}$ and we can take $\{\mathbb{I},\mathbb{F}\}$ as a basis for the commutant. As an abstract * algebra with identity G' is characterized by the relations $\mathbb{F}^2=\mathbb{I}$ and $\mathbb{F}^*=\mathbb{F}$. Thus G-invariant states can be parametrized in terms of the single parameter $\langle\mathbb{F}\rangle=\mathrm{tr}(\rho\mathbb{F})$, which ranges from -1 to 1. Note that every invariant density operator can be written as $\rho=a\mathbb{I}+bF$ with suitable $a,b\in\mathbb{R}$. But as we will see, the parameters a,b are less natural to use, and more dimension-dependent than $\mathrm{tr}(\rho\mathbb{F})$.

Another usual way to write such an invariant density operator is in terms of the minimal projections

$$\rho_{\pm}=\frac{1}{d(d\pm1)}(\mathbb{I}\pm\mathbb{F}) \tag{4}$$

and a single positive parameter p, which ranges from 0 to 1. Here d denotes the dimension of the Hilbert space $\mathcal{H}_1$. With these parameters ρ is given by $\rho=p\rho_-+(1-p)\rho_+$. The parameter p is simply connected with the flip expectation value via $p=(\langle\mathbb{F}\rangle+1)/2$.

Example 2: The group UU (isotropic states*).

Again we take both Hilbert spaces to be the same, and moreover, we fix some basis in this space. The group G now consists of all unitary operators of the form $U\otimes U^*$, where U is a unitary operator on $\mathcal{H}_1$, and U^* denotes the matrix element-wise complex conjugate of U with respect to the chosen basis. One readily checks that the maximally entangled vector $\Phi=\Sigma_i|ii\rangle$ is invariant under such unitary operators, and indeed the commutant is now spanned by $\mathbb{I}$ and the rank one operator

$$\hat{\mathbb{F}}=|\Phi\rangle\langle\Phi|=\sum_{i,j}|ii\rangle\langle jj|. \tag{5}$$

This operator is positive with norm $d=\|\Phi\|^2=\dim\mathcal{H}_1$, so the invariant states are parametrized by the expectation value $\langle\hat{\mathbb{F}}\rangle$, which ranges in the interval $[0,d]$. Every invariant state can be written as $\rho=a\mathbb{I}+b\hat{\mathbb{F}}$ with suitable $a,b\in\mathbb{R}$ or in terms of a convex combination of the two minimal projections $\rho_1=\hat{\mathbb{F}}/d$ and $\rho_2=[1/(d^2-1)](\mathbb{I}-\rho_1)$. We want to use the expectation value $\langle\hat{\mathbb{F}}\rangle=\mathrm{tr}(\rho\hat{\mathbb{F}})$ as parameter for these states. This choice for the parameter is motivated by the results in Sec. II C, where we show that these examples can be obtained from the first example by the method of partial transposition.

It is perhaps helpful to note that there are not so many functions $U\mapsto\tilde{U}$, taking unitary operators on $\mathcal{H}_1$ to unitary operators on the same space $\mathcal{H}_1$, such that the operators of the form $U\otimes\tilde{U}$ again form a group. For this it is necessary that $U\mapsto\tilde{U}$ is a homomorphism, so, for example, $\tilde{U}=U^\dagger$ does not work. Inner homomorphisms, i.e., those of the form $\tilde{U}=VUV^\dagger$ are equivalent to Example 1 by a trivial basis change in the second factor, given by V. Similarly, functions differing only by a scalar phase factor give the same transformations on operators, and should thus be considered equivalent. Then (up to base changes and phase factors) all functions $U\mapsto\tilde{U}$ not equivalent to the identity are equivalent to Example 2, i.e., the above list is in some sense complete. However, many interesting examples arise, when the Hilbert spaces are not of the same dimension, or the group of operators in the first factor is not the full unitary group.

Computing $\mathbf{P}\mathcal{S}$ in Examples 1 and 2 is very simple, because it is just an interval. We will encounter more complicated cases below, in most of which, however, the algebra G' is Abelian. When G' has dimension, say, k, it is then generated by k minimal projections, which correspond precisely to the extreme points of $\mathbf{P}\mathcal{S}$. Therefore, the state space is a *simplex* (generalized tetrahedron).

B. How to compute the separable states $\mathbf{P}\mathcal{D}$

For the study of entanglement of symmetric states it is fundamental to know which of the states in $\mathbf{P}\mathcal{S}$ are *separable* or ''classically correlated'' [1], i.e., convex combinations

$$\rho=\sum_\alpha \lambda_\alpha\rho_1^{(\alpha)}\otimes\rho_2^{(\alpha)} \tag{6}$$

of product-density operators. We denote this set of states by $\mathcal{D}$. Because we assume the group G to consist of local unitaries, it is clear that for a separable state ρ the integrand of $\mathbf{P}\rho$ consists entirely of separable states, hence $\mathbf{P}\rho$ is separable. Hence $\mathbf{P}\mathcal{D}\subset(\mathcal{D}\cap\mathbf{P}\mathcal{S})$. But here we even have equality, because any state in $(\mathcal{D}\cap\mathbf{P}\mathcal{S})$ is its own projection. Hence

$$\mathcal{D}\cap\mathbf{P}\mathcal{S}=\mathbf{P}\mathcal{D}. \tag{7}$$

In order to determine this set, recall that by decomposing $\rho_{1,2}^{(\alpha)}$ in Eq. (6) into pure states, we may even assume the $\rho_{1,2}^{(\alpha)}$ in Eq. (6) to be pure. If we compute $\mathbf{P}\rho$ termwise, we find that each $\rho\in\mathbf{P}\mathcal{D}$ is a convex combination of states $\mathbf{P}(\sigma_1\otimes\sigma_2)$ with pure $\sigma_i=|\phi_i\rangle\langle\phi_i|$. Thus we can compute $\mathbf{P}\mathcal{D}$ in two stages:

Choose a basis in G', consisting of, say, k Hermitian operators A_α and compute the expectations of these operators in arbitrary pure product states,

$$a_\alpha=\langle\phi_1\otimes\phi_2|A_\alpha|\phi_1\otimes\phi_2\rangle,$$

this determines the projections $\mathbf{P}(\sigma_1\otimes\sigma_2)$.

Determine the set of real k tuples $(a_1,\ldots,a_k)$ obtained in this way, as the ϕ_i range over all normalized vectors.

Compute the convex hull of this set.

Two simplifications can be made in this procedure: first, we always have $\mathbb{I}\in G'$, so by choosing $A_k=\mathbb{I}$, it suffices to work with the $(k-1)$-tuples $(a_1,\ldots,a_{k-1})$. Second, the vectors $\phi_1\otimes\phi_2$ and $U(\phi_1\otimes\phi_2)$ with $U\in G$ give the same expectations, so when determining the range one can make special choices, as long as one vector is chosen from each orbit of product vectors under G.

Let us illustrate this procedure in the two basic examples above: In Example 1 we only need to compute

$$\langle\phi\otimes\psi|\mathbb{F}|\phi\otimes\psi\rangle=|\langle\phi|\psi\rangle|^2. \tag{8}$$

Clearly, this quantity ranges over the interval $[0,1]$, and a UU-invariant state ρ is separable if $\mathrm{tr}(\rho\mathbb{F})\geqslant 0$ [1]. Similarly, in Example 2,

$$\langle\phi\otimes\psi|\hat{\mathbb{F}}|\phi\otimes\psi\rangle=\left|\sum_i \phi_i\psi_i\right|^2=|\langle\phi|\psi^*\rangle|^2, \tag{9}$$

which again ranges over the interval $[0,1]$. Note, however, that the state space in this case is the interval $[0,d]$. The fact that the two state-space intervals $[-1,1]$ for UU and $[0,d]$ for UU* intersect precisely in the separable subset $[0,1]$ is an instance of the Peres-Horodecki criterion for separablility, as we now proceed to show.

C. Partial transposition

The partial transpose of an operator on $\mathcal{H}_1\otimes\mathcal{H}_2$ is defined in a product basis by transposing only the indices belonging to the basis of $\mathcal{H}_2$, and not those pertaining to $\mathcal{H}_1$. Equivalently, we can define this operation as

$$\Theta_2(A\otimes B)=A\otimes\Theta(B), \tag{10}$$

where $\Theta(B)$ denotes the ordinary matrix transpose of B. This also depends on the choice of basis in $\mathcal{H}_2$, so from now on we assume a basis of $\mathcal{H}_2$ to be fixed. This equation suffices to define Θ_2, because all operators on $\mathcal{H}_1\otimes\mathcal{H}_2$ can be expanded in terms of product operators. The partial transpose operation has become a standard tool in entanglement theory with the realization that the partial transpose of a separable density operator is again positive. This is evident from Eqs. (6) and (10), and the observation that the transpose of a positive operator is positive. In $2\otimes 2$ and $2\otimes 3$ Hilbert-space dimensions, this criterion, known as the Peres-Horodecki criterion, is even sufficient for separability [15]. For all higher dimensions sufficiency fails in general. States with positive partial transpose (PPT states) are known not to be *distillable*, i.e., even when many copies of such a state are provided, it is not possible to extract any highly entangled states by local quantum operations and classical communication alone.

For special classes of states on higher-dimensional Hilbert spaces the PPT property may still be sufficient for separability. Pure states are a case in point, and so are some of the spaces of symmetric states studied in this paper. Let us check how the action of a product unitary operator is modified by partial transposition. If U_i, A_i are operators on $\mathcal{H}_i$ $(i=1,2)$, we find

$$\begin{aligned}
&\Theta_2((U_1\otimes U_2)(A_1\otimes A_2)(U_1^\dagger\otimes U_2^\dagger))\\
&\quad=\Theta_2((U_1A_1U_1^\dagger)\otimes(U_2A_2U_2^\dagger))\\
&\quad=(U_1A_1U_1^\dagger)\otimes(\Theta(U_2^\dagger)\Theta(A_2)\Theta(U_2))\\
&\quad=(U_1\otimes U^*{}_2)\Theta_2(A_1\otimes A_2)(U_1\otimes U^*{}_2)^\dagger.
\end{aligned}$$

Note that by linearity we can replace in this equation $A_1\otimes A_2$ by any other operator on $\mathcal{H}_1\otimes\mathcal{H}_2$. This computation motivates the following definition: For any group G of product unitary operators, we denote by $\tilde{G}$ the group of unitary operators $U_1\otimes U^*{}_2$, where $U_1\otimes U_2\in G$. For example, for $G=\mathrm{UU}$ of Example 1 we get $\tilde{G}=\mathrm{UU}^*$, and vice versa.

There is a slightly tricky point in this definition, because the map $U_1\otimes U_2\mapsto U_1\otimes U^*{}_2$ is not well defined: If we multiply U_1 by a phase and U_2 with the inverse phase, the operator $U_1\otimes U_2$ does not change, but $U_1\otimes U^*{}_2$ picks up twice the phase. What the definition therefore requires is to take in $\tilde{G}$ *all* operators arising in this way. Repeating the "tilde" operation may thus fail to lead back to G, but instead leads to G enlarged by the group of phases. It is therefore convenient to assume that all groups under consideration contain the group of phases. We may do so without loss of generality, since the phases act trivially on operators anyhow, and hence the twirling projection $\mathbf{P}$ is unchanged.

If we integrate the above computation with respect to a group G of local unitary operators, and introduce $\tilde{\mathbf{P}}$ for the twirling projection associated with $\tilde{G}$, we get the fundamental relation

$$\Theta_2\mathbf{P}=\tilde{\mathbf{P}}\Theta_2. \tag{11}$$

Since Θ_2 is a linear bijection on the space of all operators on $\mathcal{H}_1\otimes\mathcal{H}_2$, we immediately find the relations between the ranges of $\mathbf{P}$ and $\tilde{\mathbf{P}}$,

$$\Theta_2(G')=\tilde{G}', \tag{12}$$

i.e., the operators invariant under $\tilde{G}$ are precisely the partial transposes of those invariant under G. This has a surprising consequence: taking the partial transposes of an algebra of operators in general has little chance of producing again an algebra of operators, since Θ_2 is definitely not a homomorphism. That is, in general, one would not expect that the operator product of two partial transposes is again the partial transpose of an element of the original algebra. If the algebra arises as the commutant of a group of *local* unitary operators, however, we get again a commutant, hence an algebra.

The first application of Eq. (12) is the computation of the commutant in Example 2: With $G=\mathrm{UU}$ we find the partial transposes of the operators in G', i.e., the operators $\Theta_2(\alpha\mathbb{I}+\beta\mathbb{F})=\alpha\mathbb{I}+\beta\hat{\mathbb{F}}$, since $\Theta_2(\mathbb{F})=\hat{\mathbb{F}}$.

Another application is the determination of the set of PPT states. One might think that a special form for ρ, entailed by its G invariance, is not necessarily helpful for getting spectral information about $\Theta_2\rho$. However, since Θ_2G' is an algebra, and often enough an Abelian one, $\Theta_2\rho$ is, in fact, easily diagonalized.

A good way to represent this connection is to draw the state spaces of G and $\tilde{G}$ (i.e., $\mathbf{P}\mathcal{S}$ and $\tilde{\mathbf{P}}\mathcal{S}$) in the same diagram. Since, in general, G' and $\tilde{G}'$ need not intersect except in the multiples of the identity (see Examples 1 and 2), the projected state spaces $\mathbf{P}\mathcal{S}$ and $\tilde{\mathbf{P}}\mathcal{S}$ in general have only the trace state in common. Hence they do not fit naturally in the same diagram. However, the partial transposes of $\tilde{\mathbf{P}}\mathcal{S}$ lie in G', more precisely in the hyperplane of Hermitian elements with trace 1. The same hyperplane contains $\mathbf{P}\mathcal{S}$. In the pair of Examples 1 and 2, we get Fig. 1.

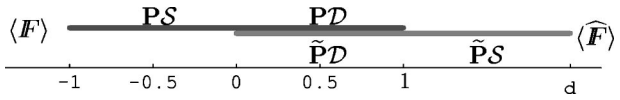

FIG. 1. The state spaces for Werner and isotropic states are just intervals. Drawn together in one diagram, the intersection gives us the space of PPT states, which is in this case equivalent to the separable space.

Note that by exchanging the roles of G and $\tilde{G}$, we get exactly the same diagram, up to maybe an affine transformation due to a different choice of coordinates: the two diagrams are simply related by taking partial transposes. When G and $\tilde{G}$ are swapped in this way, the picture of $\mathbf{P}\mathcal{D}$ remains correct: since $\Theta_2\mathcal{D}=\mathcal{D}$, it suffices to compute the projection of the separable subset for G. By definition, the intersection of $\mathbf{P}\mathcal{S}$ and $\Theta_2\tilde{\mathbf{P}}\mathcal{S}$ is the convex set of G-invariant PPT states. It always contains $\mathbf{P}\mathcal{D}$, but this inclusion may be strict. In the simple case of Fig. 1 $\mathbf{P}\mathcal{D}=\mathbf{P}\mathcal{S}\cap\Theta_2\tilde{\mathbf{P}}\mathcal{S}$, which is the same as saying that the Peres-Horodecki criterion is valid for states invariant under either G or $\tilde{G}$.

D. Further examples of symmetry groups

Example 3: Orthogonal groups: $G=OO$.

The two basic examples can be combined into one by taking the *intersection* of the two groups: $G=\mathrm{UU}\cap\mathrm{UU}^*$ this is the same as the subgroup of unitary operators $U\otimes U$ such that $U^*=U$, i.e., such that U is a real orthogonal matrix. Clearly, both the UU-invariant states and the UU*-invariant states will be G invariant, so we know that G' is at least[1] the algebra generated by UU' and $\mathrm{UU}^{*\prime}$, i.e., it contains $\mathbb{I},\mathbb{F}$, and $\hat{\mathbb{F}}$. Since $\mathbb{F}\hat{\mathbb{F}}=\hat{\mathbb{F}}\mathbb{F}=\hat{\mathbb{F}}$, the linear span of these three is already an algebra, and is spanned by the minimal projections

$$p_0=\frac{1}{d}\hat{\mathbb{F}} \tag{13}$$

$$p_1=\frac{1}{2}(\mathbb{I}-\mathbb{F}) \tag{14}$$

$$p_2=\frac{1}{2}(\mathbb{I}+\mathbb{F})-\frac{1}{d}\hat{\mathbb{F}}, \tag{15}$$

[1]In general, the commutant $(G\cap H)'$ may be suitably larger than the algebra $G'\vee H'$ generated by G' and H'. The equation $(\mathcal{A}\cap\mathcal{B})'=\mathcal{A}'\vee\mathcal{B}'$ is valid only for algebras, and follows readily from the equation $(\mathcal{A}'\vee\mathcal{B}')'=(\mathcal{A}''\cap\mathcal{B}'')$, and the bicommutant theorem [17], which characterizes M'' as the algebra generated by M. However, the algebras G'' and H'' may have an intersection, which is suitably larger than the algebra generated by their intersection. For example, for any irreducible represented group G'' is the algebra of all operators, but two such groups may intersect just in the identity. Hence some caution has to be exercised when computing $(G\cap H)'$ for general groups.

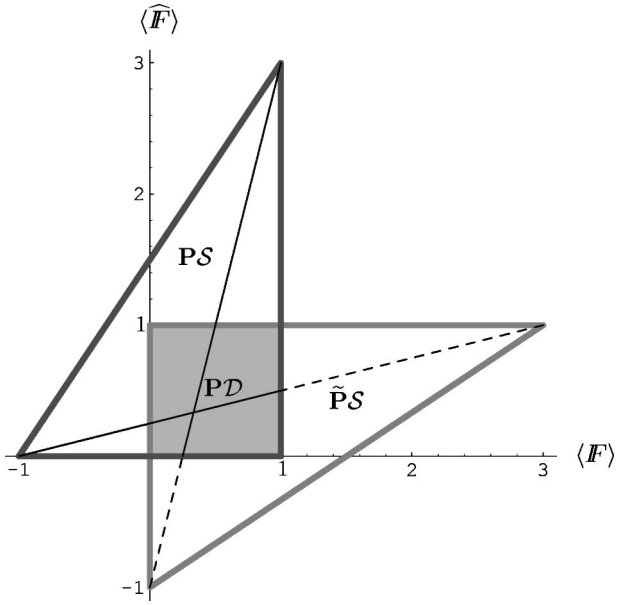

FIG. 2. State spaces for OO and $\mathrm{O}\overline{\mathrm{O}}$ invariant states plotted for $d=3$. The UU and UU* invariant states are drawn as thin lines.

which corresponds precisely to the decomposition of a general (3×3)-matrix into a multiple of the identity, antisymmetric part, and symmetric traceless part. This decomposition of tensor operators with respect to the orthogonal group is well known, so we have identified G'.

The extremal G-invariant states corresponding to these three minimal projections are plotted in Fig. 2 in a coordinate system whose axes represent the expectations of $\mathbb{F}$ and $\hat{\mathbb{F}}$, respectively. The plane of this drawing should be considered as the Hermitian G-invariant operators of trace one. This plane is mapped into itself by partial transposition (since $G=\tilde{G}$), and the coordinates are chosen such that partial transposition is simply the reflection along the main diagonal.

The intersection of $\mathbf{P}\mathcal{S}$ and $\tilde{\mathbf{P}}\mathcal{S}$ is the square $[0,1]\times[0,1]$. Is the Peres-Horodecki criterion valid for these states? All we have to do to check this is to try to get some pure product states, whose expectations of $\mathbb{F}$ and $\hat{\mathbb{F}}$ fall on the corners of this square. For a product vector $\phi\otimes\psi$ we get the pair of expectations

$$(|\langle\phi|\psi\rangle|^2,|\langle\phi|\psi^*\rangle|^2).$$

Here ψ^* denotes the complex conjugate of ψ in a basis in which the representation is real. Now, the point (1,1) in the square is obtained whenever $\phi=\psi$ is real, the point (0,0) is obtained when ϕ and ψ are real and orthogonal, and the point (1,0) is obtained when $\psi=\phi$, and $\langle\phi|\phi^*\rangle=0$, for example, $\phi=(1,i,0)/\sqrt{2}$. Symmetrically, we get (0,1) with the same ϕ and $\psi=\phi^*$. Hence all four corners are in $\mathbf{P}\mathcal{D}$, and as this is a convex set we must have $\mathbf{P}\mathcal{D}=\mathbf{P}\mathcal{S}\cap\Theta_2(\tilde{\mathbf{P}}\mathcal{S})$.

Example 4: SU_2 representations.

A class of examples, in which arbitrary dimensions of $\mathcal{H}_1$ and $\mathcal{H}_2$ can occur is the following. Let $u\mapsto\mathcal{D}^j_u$ denote the spin j irreducible representation of SU_2. Then we can take

$$G=\{\mathcal{D}_u^{j_1}\otimes\mathcal{D}_u^{j_2}|u\in \mathrm{SU}_2\}, \tag{16}$$

where $(2j_k+1)$ is the dimension of $\mathcal{H}_k$ $(k=1,2)$. Since j_k also take half-integer values, these dimensions can be any natural number $\geqslant 1$. It is known from just about any quantum mechanics course (under the key word "addition of angular momenta") that the tensor product representation $\mathcal{D}^{j_1}\otimes\mathcal{D}^{j_2}$ is decomposed into the direct sum of the irreducible representations $\mathcal{D}^s$ with $s=|j_1-j_2|,|j_1-j_2|+1,\ldots,(j_1+j_2)$, each of these representations appearing with multiplicity 1. Therefore, the commutant of G is spanned by the projections onto these subspaces, and is an Abelian algebra.

Note that since the spin-1 representation of SU_2 is the orthogonal group in three dimensions, the case $j_1=j_2=1$ corresponds precisely to the previous example with $d=3$. We have no general expression for the separable subsets, nor even for the partially transposed sets in these examples. We believe, however, that this class of examples deserves further investigation.

Example 5: Bell diagonal states.

In this example we show that the group G can also be Abelian, and we make contact with a well-investigated structure of the two-qubit system. So let $\mathcal{H}_1=\mathcal{H}_2=\mathbb{C}^2$, and let σ_k, $k=1,2,3$ be the Pauli matrices, and $\sigma_0=\mathbb{I}$. Then the set

$$G=\{\mathbb{I},-\sigma_1\otimes\sigma_1,-\sigma_2\otimes\sigma_2,-\sigma_3\otimes\sigma_3\} \tag{17}$$

forms a group, which is isomorphic to the Klein four-group, and Abelian $(G\subset G')$. It is even maximally Abelian, i.e, the algebra G'' generated by G is equal to, and not just contained in G'. The minimal projections in G' are $|\Psi_k\rangle\langle\Psi_k|$, $k=0,1,2,3$, where the Ψ_k are the magical *Bell basis* [9,16]: $\Psi_0=(|11\rangle+|22\rangle)/\sqrt{2}$, and $\Psi_k=i(\mathbb{I}\otimes\sigma_k)\Psi_0$ for $k=1,2,3$. In this basis the group elements and their negatives are the diagonal operators with diagonal elements ± 1, of which an even number are -1. Hence the G-invariant states are the tetrahedron of density operators that are diagonal in Bell basis.

The partial transpose is easy to compute: only σ_2 changes sign under transposition. Hence if we draw the state space in a coordinate system, whose three axes are the expectations of the group elements $-\sigma_k\otimes\sigma_k$ $(k=1,2,3)$, the Bell states are the corners $(1,1,1)$, $(1,-1,-1)$, $(-1,-1,1)$, and $(-1,1,-1)$ of the unit cube, from which their partial transposes are obtained by mirror reflection $x_2\mapsto -x_2$. That is, the partially transposed states occupy the remaining four corners of the unit cube. The PPT subset, which is equal to the separable subset since we are in $2\otimes 2$ dimensions, is hence the intersection of two tetrahedra, and is easily seen to be an octahedron (see Fig. 3)

Example 6: Finite Weyl systems.

In the examples so far the groups G and $\tilde{G}$ were isomorphic or even equal. In this example, which extends the previous one, we see that the two groups and their commutants can be very different.

We let d be an integer, and introduce on $\mathbb{C}^d$ the *Weyl operators*, given by

$$W(x,y)|z\rangle=\omega^{xz}|z-y\rangle, \tag{18}$$

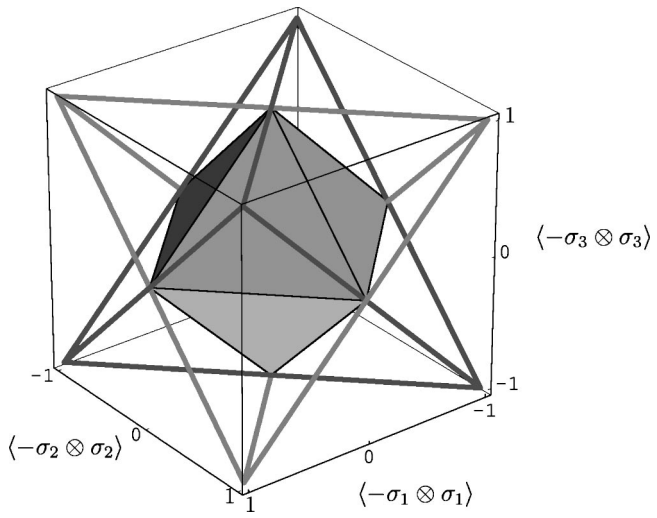

FIG. 3. State spaces for Bell diagonal states.

where $\omega=\exp(2\pi i/p)$. These are unitary, and satisfy the "Weyl relations"

$$W(x_1,y_1)W(x_2,y_2)=\omega^{-x_1y_2}W(x_1+x_2,y_1+y_2). \tag{19}$$

Hence these operators, together with the pth roots of unity form a group. On $\mathbb{C}^d\otimes\mathbb{C}^d$ we introduce the operators $W(x_1,y_1,x_2,y_2)\equiv W(x_1,y_1)\otimes W(x_2,y_2)$, and take

$$G=\{\omega^z W(x,y,x,y)|x,y,z=0,\ldots,d-1\}. \tag{20}$$

The commutant is readily computed from the Weyl relations to be

$$G'=\mathrm{span}\{W(x,y,-x,-y)|x,y=0,\ldots,d-1\}. \tag{21}$$

The Weyl operators in G' satisfy Weyl relations with ω replaced by ω^2. If d is odd, such relations are equivalent to the Weyl relations (19) for a d-dimensional system, and hence G' is isomorphic to the $d\times d$ matrices.

On the other hand, complex conjugation of $W(x,y)$ just inverts the sign of x, so $\tilde{G}$ contains the Weyl operators $W(x,y,-x,y)$. But this time, rather than getting twice the Weyl phase, the phases cancel, and $\tilde{G}$ is *Abelian*. One also verifies that

$$\tilde{G}'=\mathrm{span}\{W(x,y,-x,y)|x,y=0,\ldots,d-1\} \tag{22}$$

is spanned by $\tilde{G}$, so this algebra is even maximally Abelian: it contains d^2 one-dimensional projections, which thus form the extreme points of $\tilde{\mathbf{P}}\mathcal{S}$. Hence we get the following picture: the set $\mathbf{P}\mathcal{S}$ of G-invariant states is isomorphic to the space of $d\times d$ density operators, and the G-invariant operators with positive partial transpose are a simplex spanned by 9 extreme points, which are mapped into each other by the action of a $d\times d$ Weyl system. The intersection $\mathbf{P}\mathcal{S}\cap\Theta_2(\tilde{\mathbf{P}}\mathcal{S})$ is a rather complicated object. We do not know yet whether it differs from $\mathbf{P}\mathcal{D}$.

Example 7: Tensor products.

Additivity problems for entanglement (see Sec. III C for a brief survey) concern tensor products of bipartite states, which are taken in such a way as to preserve the splitting between Alice and Bob. Thus in the simplest case we have four subsystems, described in Hilbert spaces $\mathcal{H}_i, \mathcal{K}_i$, $i=1,2$, such that systems $\mathcal{H}_1$ and $\mathcal{K}_1$ belong to Alice, systems $\mathcal{H}_2$ and $\mathcal{K}_2$ belong to Bob, and such that the systems in $\mathcal{H}_i$ are prepared together according to a density matrix ρ on $\mathcal{H}_1 \otimes \mathcal{H}_2$ and, similarly, the remaining systems are prepared according to σ, a density operator on $\mathcal{K}_1 \otimes \mathcal{K}_2$. We wish to study the entanglement properties of $\rho \otimes \sigma$, when both these density matrices are assumed to be invariant under suitable groups of local unitaries.

Let us denote by G (H) the group of local unitary operators on $\mathcal{H}_1 \otimes \mathcal{H}_2$ (by $\mathcal{K}_1 \otimes \mathcal{K}_2$), and assume ρ and σ to be invariant under the respective group. Then, clearly, $\rho \otimes \sigma$ is invariant under all unitary operators $U_1 \otimes U_2 \otimes V_1 \otimes V_2$, where $U_1 \otimes U_2 \in G$ and $V_1 \otimes V_2 \in H$. These again form a group of local unitaries, denoted by $G \otimes H$, where ''local'' is understood in the sense of the Alice-Bob splitting of the system, i.e., the unitary $U_1 \otimes V_1$ acts on Alice's side and $U_2 \otimes V_2$ on Bob's. In this sense the product state is invariant under the group $G \otimes H$ of local unitaries, and we can apply the methods developed below to compute various entanglement measures for it.

Computing the commutant $(G \otimes H)'$ is easy, because we do not have to look at the Alice-Bob splitting of the Hilbert space. In fact, we can invoke the ''commutation theorem'' for von Neumann algebras to get

$$(G \otimes H)' = G' \otimes H', \tag{23}$$

where the notation on the right-hand side is the tensor product of algebras, i.e., this is the set of all linear combinations of elements of the form $A \otimes B$ where $A \in G'$ acts on the first two and $B \in H'$ acts on the second two factors of $\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \mathcal{K}_1 \otimes \mathcal{K}_2$. In particular, if G' and H' are Abelian, so is $G' \otimes H'$, and we can readily compute the minimal projections, which correspond to the extremal invariant states: if p_α are the minimal projections of G' and q_β are those of H', then the minimal projections of $G' \otimes H'$ are all $p_\alpha \otimes q_\beta$.

Partial transposition also behaves naturally with respect to tensor products, which implies that $(G \otimes H)^\sim = \tilde{G} \otimes \tilde{H}$, and allows us to compute in a simple way the $(G \otimes H)$-invariant states with positive partial transpose from the corresponding data of G and H. However, for the determination of $\mathbf{P}\mathcal{D}$ no such shortcut exists.

We illustrate this in the example, which we will also use for the counterexample to additivity of the relative entropy of entanglement discussed in the Introduction. For this we take $G = H = \mathrm{UU}$, with a one-particle space $\mathcal{H}_1 = \mathcal{H}_2 = \mathcal{K}_1 = \mathcal{K}_2 = \mathbb{C}^d$, for any dimension $d < \infty$. The extreme points of the state space of G' are given by the normalized projections

$$\rho_\pm = \frac{1}{d(d \pm 1)} (\mathbb{I} \pm \mathbb{F}). \tag{24}$$

Hence the state space of the Abelian algebra $(G' \otimes H')$ is spanned by the four states $\rho_{s_1} \otimes \rho_{s_2}$, $s_1, s_2 = \pm$ and is a tetrahedron. A convenient coordinate system is given by the expectations of the three operators

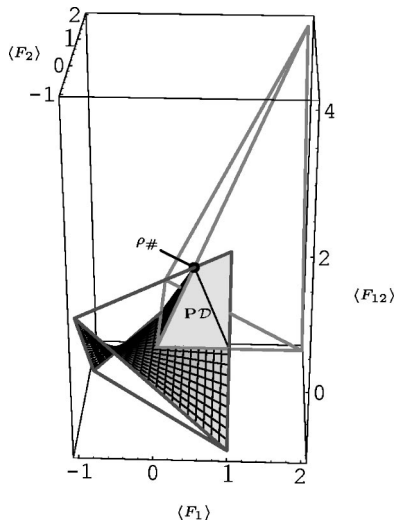

FIG. 4. State space for UUVV-invariant states plotted for dimension $d=3$.

$$F_1 = \mathbb{F} \otimes \mathbb{I} \tag{25}$$

$$F_2 = \mathbb{I} \otimes \mathbb{F} \tag{26}$$

$$F_{12} = \mathbb{F} \otimes \mathbb{F}. \tag{27}$$

The four extreme points are then on the edges of the unit cube: $\rho_{s_1} \otimes \rho_{s_2}$ has expectation triple $(s_1, s_2, s_1 s_2)$. This is drawn in Fig. 4.

The extreme points are special instances of product states: when ρ, σ are UU-invariant states with flip expectations f_1 and f_2, respectively, the product state $\rho \otimes \sigma$ has coordinates $(f_1, f_2, f_1 f_2)$. Hence the manifold of product states is embedded in the state space as a piece of hyperboloid. Partial transposition turns the flip operators (25) into their counterparts using $\hat{\mathbb{F}}$ instead of $\mathbb{F}$. Hence the operators with positive partial transposes are represented in the diagram by a tetrahedron with vertices $(0,0,0)$, $(0,d,0)$, $(d,0,0)$, and (d,d,d^2). The intersection, i.e., the set of states with trace equal to one and positive partial transpose (represented in Fig. 4 as a solid) is a polytope with the five extreme points $(0,0,0)$, $(0,1,0)$, $(1,0,0)$, $(1,1,1)$, and, on the line connecting the origin to the point (d,d,d^2), the point $(1/d, 1/d, 1)$. The density operator corresponding to this last point is

$$\rho_\# = \frac{d+1}{2d} \rho_+ \otimes \rho_+ + \frac{d-1}{2d} \rho_- \otimes \rho_- . \tag{28}$$

It turns out that $\rho_\#$ is separable: Let $\Phi = d^{-1/2} \Sigma_k |kk\rangle$ be a maximally entangled vector, and consider a pure state with vector $\Psi = \Phi_{\mathrm{Alice}} \otimes \Phi_{\mathrm{Bob}}$. Note that this is a tensor product with respect to the Alice-Bob splitting, i.e., $13|24$ rather than the splitting between pair 1 and pair 2, i.e., $12|34$. We claim that upon twirling this pure state becomes $\rho_\#$. For this we only need to evaluate the expectations of the three operators (25), and compare with those of $\rho_\#$. Clearly, Ψ is a symmet-

ric product (Bose-) vector with respect to the total flip F_{12}, hence this operator has expectation 1. The expectations of F_1 and F_2 are equal to

$$\langle\Psi|F_1\Psi\rangle=\frac{1}{d^2}\sum\langle ijij|(\mathbb{F}\otimes\mathbb{I})|k\ell k\ell\rangle$$

$$=\frac{1}{d^2}\sum_{i,j,k,\ell}\langle ijij|\ell kk\ell\rangle=\frac{1}{d}.$$

Since the other four extreme points are separable as tensor products of separable states, we conclude that all PPT states are separable in this example, so the solid in Fig. 4 also represents the separable subset.

Example 8: Tripartite symmetry: $U\otimes(U\otimes U)$.

The idea of symmetry can also be used to study multipartite entanglement. A natural choice of symmetry group is the group of all unitary operators of the form $U\otimes U\otimes U$. The resulting five-dimensional state space has been studied in great detail in Ref. [4]. This study also has a bipartite chapter, where this group is considered as a group of local unitary operators $U\otimes(U\otimes U)$ in the sense of the present paper. The set of separable states is strictly smaller than the set of states with positive partial transposes. However, if we enlarge the group to include the unitary operator $\mathbb{I}\otimes\mathbb{F}$, the two once again coincide, forming a tetrahedron.

III. ENTANGLEMENT MEASURES AND ADDITIVITY

A. Entanglement of formation and the convex hull construction for functions

The entanglement of a pure state is well described by the von Neumann entropy of its restricted density operator. Thus for a pure state $\rho=|\Psi\rangle\langle\Psi|$ such that Ψ is expressed in Schmidt form as $\Psi=\Sigma_k\sqrt{c_k}e_k\otimes e'_k$, we have

$$E(\rho)=\sum_k\eta(c_k)\quad\text{with}\tag{29}$$

$$\eta(t)=-t\ln(t).\tag{30}$$

The *entanglement of formation* is a specific extension of this function to mixed states. The extension method is a general one, known as the *convex hull* construction for functions, and since we will need this construction for stating our main result, we will briefly review it.

So let K be a compact convex set, let $M\subset K$ be an arbitrary subset, and let $f:M\to\mathbb{R}\cup\{+\infty\}$. We then define a function $\mathrm{co}f:K\to\mathbb{R}\cup\{+\infty\}$ by

$$\mathrm{co}f(x)=\inf\left\{\sum_i\lambda_i f(s_i)\,\middle|\,s_i\in M,\sum_i\lambda_i s_i=x\right\},\tag{31}$$

where the infimum is over all convex combinations with $\lambda_i\geqslant 0$, $\Sigma_i\lambda_i=1$, and by convention the infimum over an empty set is $+\infty$. The name "convex hull" of this function is due to the property that co$f$ is the largest convex function, which is $\leqslant f$ at all points, where f is defined. Another way of putting this is to say that the "supergraph" of co$f$, i.e., $\{(x,r)\in K\times\mathbb{R}|r\geqslant\mathrm{co}f(x)\}$, is the convex hull (as a subset of $K\times\mathbb{R}$) of $\{(x,r)\in K\times\mathbb{R}|x\in M,r\geqslant f(x)\}$.

In this notation, the usual definition [9] of entanglement of formation is then

$$E_F(\rho)=(\mathrm{co}E)(\rho),\tag{32}$$

where on the right-hand side E is understood as the function (29) defined only on the submanifold $M\subset\mathcal{S}(\mathcal{H}_1\otimes\mathcal{H}_2)$ of pure states.

B. Relative entropy of entanglement

Another measure of entanglement, originally proposed in Ref. [7] is based on the idea that entanglement should be zero for separable density operators [see Eq. (6)], and should increase as we move away from $\mathcal{D}$. Such a function might be viewed as measuring some kind of distance of the state to the set $\mathcal{D}$ of separable states. If one takes this idea literally, and uses the relative entropy [19]

$$\mathrm{S}(\rho,\sigma)=\mathrm{tr}\,\rho(\ln\rho-\ln\sigma)\tag{33}$$

to measure the "distance," one arrives at the *relative entropy of entanglement*

$$E_{\mathrm{RE}}(\rho)=\inf\{\mathrm{S}(\rho,\sigma)|\sigma\in\mathcal{D}\}.\tag{34}$$

Initially, other distance functions have also been used to define measures of entanglement. However, the one based on the relative entropy is the only proposal, which coincides with pure states with the "canonical" choice described in Eq. (29). Since E_{RE} is easily shown to be convex, it must be smaller than the largest convex function with this property, namely E_F. Another reason to prefer relative entropy over other distancelike functionals is that it has good additivity properties. The hope that E_{RE} might be additive was borne out by initial explorations, and has become a folk conjecture in the field. However, we will give a counterexample below.

C. Additivity

A key problem in the current discussion of entanglement measures is the question, which of these are "additive" in the following sense: if ρ,σ are bipartite states on the Hilbert spaces $\mathcal{H}_1\otimes\mathcal{H}_2$ and $\mathcal{K}_1\otimes\mathcal{K}_2$, then $\rho\otimes\sigma$ is a state on $\mathcal{H}_1\otimes\mathcal{H}_2\otimes\mathcal{K}_1\otimes\mathcal{K}_2$. After sorting the factors in this tensor product into spaces $\mathcal{H}_1,\mathcal{K}_1$ belonging to Alice and $\mathcal{H}_2,\mathcal{K}_2$ belonging to Bob, we can consider $\rho\otimes\sigma$ as a bipartite state on $(\mathcal{H}_1\otimes\mathcal{K}_1)\otimes(\mathcal{H}_2\otimes\mathcal{K}_2)$. This corresponds precisely to the situation of a source distributing particles to Alice and Bob, $\rho\otimes\sigma$, and similar larger tensor products, being interpreted as the state obtained by letting Alice and Bob *collect* their respective particles. Additivity of an entanglement measure E is then the equation

$$E(\rho\otimes\sigma)=E(\rho)+E(\sigma).\tag{35}$$

We speak of *subadditivity* if "$\leqslant$" holds instead of equality here. Both E_{RE} and E_F are defined as infima, and for a prod-

uct we can insert tensor products of convex decompositions or closest separable points into these infima, and use the additivity properties of entropy to get subadditivity in both cases. It is the converse inequality, which presents all the difficulties, i.e., the statement that in these minimization problems the tensor product solutions (and not some entangled options) are already the best.

Additivity of an entanglement functional is a strong expression of the *resource character* of entanglement. According to an additive functional, sharing two particles from the same preparing device is exactly ''twice as useful'' to Alice and Bob as having just one. Here preparing two pairs means preparing *independent* pairs, expressed by the tensor product in Eq. (35). It is interesting to investigate the influence of correlations and entanglement between the different pairs. On the one hand, Alice and Bob might not be aware of such correlations, and use the pairs as if they were independent. On the other hand, they might make use of the exact form of the state, including all correlations. Is the second possibility always preferable? Entanglement functionals answering this question with ''yes'' have a property stronger than additivity, called *strong superadditivity*. It is written as

$$E(\rho)\geqslant E(\rho_{\mathcal{H}})+E(\rho_{\mathcal{K}}), \tag{36}$$

where ρ is a density operator for two pairs (four particles altogether), and $\rho_{\mathcal{H}}$ and $\rho_{\mathcal{K}}$ are the restrictions to the first and second pair. An entanglement functional satisfying this as well as subadditivity is clearly additive. Since additivity is already difficult to decide, it is clear that strong superadditivity is not known for any of the standard measures of entanglement.

One case of strong superadditivity is satisfied both for E_F and E_{RE}, and we establish this property here in order to get a more focused search for counterexamples later on: We claim that Eq. (36) holds, whenever $\rho_{\mathcal{K}}$ is separable, in which case, of course, the second term on the right vanishes (as a special case of additivity, when $\rho_{\mathcal{K}}$ is even a product, this was noted recently in Ref. [18]). We will show this by establishing another property, called *monotonicity*: for both $E=E_F$ and $E=E_{\mathrm{RE}}$, we claim

$$E(\rho)\geqslant E(\rho_{\mathcal{H}}). \tag{37}$$

Monotonicity for E_{RE} follows readily from a similar property of the relative entropy: if $\rho_{\mathcal{H}},\sigma_{\mathcal{H}}$ denote the restrictions of states ρ,σ to the same subsystem, then $\mathrm{S}(\rho_{\mathcal{H}},\sigma_{\mathcal{H}})\leqslant\mathrm{S}(\rho,\sigma)$. But if σ is separable in Eq. (34), then so is its restriction $\sigma_{\mathcal{H}}$. The infimum over *all* separable states on $\mathcal{H}_1\otimes\mathcal{H}_2$ is still smaller, hence monotonicity holds.

Monotonicity for E_F is similar: We may do the reduction in stages, i.e., first reduce Alice's and then Bob's system, and because E_F is symmetric with respect to the exchange of Alice and Bob, it suffices to consider the case of a reduction on only one side, i.e., the restriction from $\mathcal{H}_1\otimes(\mathcal{H}_2\otimes\mathcal{K}_2)$ to $\mathcal{H}_1\otimes\mathcal{H}_2$.

Let ρ be a state on $\mathcal{H}_1\otimes(\mathcal{H}_2\otimes\mathcal{K}_2)$ and ρ' its restriction to $\mathcal{H}_1\otimes\mathcal{H}_2$.

Consider the states s_i on the larger space appearing in the minimizing convex decomposition of ρ, and let s_i' denote their restrictions to $\mathcal{H}_1\otimes\mathcal{H}_2$. Of course, both s_i and s_i' have the same restriction to the first factor $\mathcal{H}_1$. Hence

$$E_F(\rho)=\sum_i \lambda_i f(s_i'), \tag{38}$$

where $f(\sigma)$ denotes the von Neumann entropy of the restriction of a state σ to $\mathcal{H}_1$, and $\Sigma_i\lambda_i s_i'=\rho'$. Because the entropy of the restriction is a concave function, the value of the sum (38) can be made smaller by replacing each s_i' with a decomposition into pure states on $\mathcal{H}_1\otimes\mathcal{H}_2$. Minimizing over all such decompositions of ρ' yields $E_F(\rho')$, which is hence smaller than $E_F(\rho)$.

IV. ENTANGLEMENT OF FORMATION

A. Simplified computation

Our method for computing the entanglement of formation can also be explained in the general setting of the convex hull construction in Sec. III A, and this is perhaps the best way to see the geometrical content. So in an addition to a subset $M\subset K$ of a compact convex set and a function $f:M\rightarrow\mathbb{R}\cup\{+\infty\}$, consider a compact group G of symmetries acting on K by transformations $\alpha_U:K\rightarrow K$, which preserve convex combinations. We also assume that $\alpha_U M\subset M$, and $f(\alpha_U s)=f(s)$ for $s\in M$. All this is readily verified for $\alpha_U(A)=UAU^\dagger$ and f the entanglement defined on the subset $M\subset K$ of pure bipartite states. Our task is to compute $\mathrm{co}f(x)$ for all G-invariant $x\in K$, i.e., those with $\alpha_U(x)=x$ for all $U\in G$.

Since the integral with respect to the Haar measure is itself a convex combination, we can define, as before, the projection $\mathbf{P}:K\rightarrow K$ by $\mathbf{P}x=\int dU\,\alpha_U(x)$. The set of projected points $\mathbf{P}x$ will be denoted by $\mathbf{P}K$. Usually, this will be a much lower dimensional object than K, so we will try to reduce the computation of the infimum (31), which involves a variation over all convex decompositions of x in the high-dimensional set K to a computation, which can be done entirely in $\mathbf{P}K$. To this end, we define the function $\varepsilon:\mathbf{P}K\rightarrow\mathbb{R}\cup\{+\infty\}$ by

$$\varepsilon(x)=\inf\{f(s)\,|\,s\in M,\mathbf{P}s=x\}, \tag{39}$$

again with the convention that the infimum over the empty set is $+\infty$. Then the main result of this subsection is that, for $x\in\mathbf{P}K$,

$$\mathrm{co}f(x)=\mathrm{co}\epsilon(x), \tag{40}$$

where the convex hull on the left is defined by Eq. (31), but the convex hull on the right is now to be computed in the convex subset $\mathbf{P}K$.

We thus arrive at the following recipe for computing the entanglement of formation of G-invariant states:

- Find, for every state $\rho\in\mathbf{P}\mathcal{S}$, the set M_ρ of pure states σ such that $\mathbf{P}\sigma=\rho$.
- Compute

$$\varepsilon(\rho) := \inf\{E(\sigma) \,|\, \sigma \in M_\rho\}. \tag{41}$$

• For later use try to get a good understanding of the pure states achieving this minimum.

• Compute the convex hull of the function (41).

The following simplifications are sometimes possible: first of all, all pure states in an orbit of G give the same value of E, hence we may replace M_ρ by a suitably parametrized subset containing at least one element from every orbit. At this stage it is sometimes already possible to discard further states, in favor of others "obviously" giving a smaller value of E. The final stage is sometimes carried out by showing that the function ε is convex to begin with, but, as we will see, this is not always the case.

The remainder of this subsection is devoted to the proof of Eq. (40). We will proceed by showing that both sides are equal to

$$Z = \inf\left\{ \sum_i \lambda_i f(s_i) \,\middle|\, s_i \in M, \sum_i \lambda_i \mathbf{P} s_i = x \right\}. \tag{42}$$

Indeed, the only difference between Eqs. (42) and (31) is that in Eq. (42) a weaker condition is demanded on the s_i. Hence more s_i are admissible, and this infimum is smaller, $Z \leqslant \mathrm{co}f(x)$. On the other hand, if s_i satisfying the constraint for Z are given, inserting the definition of $\mathbf{P}$ produces a convex combination giving x, namely, the combination of the states $\alpha_U(s_i)$, labeled by the pair (i,U), and weighted with $\Sigma_i \lambda_i \int dU$. This convex combination is admissible for the infimum defining $\mathrm{co}f$, and gives the value $\Sigma_i \lambda_i \int dU\, f(\alpha_U(s_i)) = \Sigma_i \lambda_i \int dU\, f(s_i) = \Sigma_i \lambda_i f(s_i)$, where we have used the invariance property of f and the normalization of the Haar measure. Hence all numbers arising in the infimum (42) also appear in the infimum (31), which proves that $Z \leqslant \mathrm{co}f(x)$, hence $Z = \mathrm{co}f(x)$. In order to prove the equality $Z = \mathrm{co}\epsilon(x)$ just note that in the infimum (42) the constraint is only in terms of $\mathbf{P}s_i$, whereas the functional to be minimized involves $f(s_i)$. Therefore, we can compute the infimum (42) in stages, by first fixing all $\mathbf{P}s_i$ and minimizing each $f(s_i)$ under this constraint, which amounts to replacing f by ε, and then varying over the $\mathbf{P}s_i$, which is the infimum defining $\mathrm{co}\epsilon$. Hence $\mathrm{co}\epsilon(x) = Z = \mathrm{co}f(x)$.

B. Extending the computation to some nonsymmetric states

It is a basic feature of the convex hull that whenever the infimum in Eq. (31) is found at a nontrivial convex combination, there is a "flat piece" in the graph of $\mathrm{co}f$, i.e., $\mathrm{co}f$ is also known on the convex hull of the minimizing s_i [11]. The geometrical meaning of this elementary observation is immediately clear from low-dimensional pictures. It is also easy to prove in general, as described below.

Suppose that $\Sigma_i \lambda_i s_i = x$ is a convex decomposition of x (with $\lambda_i > 0$) minimizing $\Sigma_i \lambda_i f(s_i)$, and let $x' = \Sigma_i \lambda_i' s_i$ be another convex combination of the same points s_i. We claim that this convex combination solves the minimization problem for $\mathrm{co}f(x')$, i.e.,

$$\mathrm{co}f(x') = \sum_i \lambda_i' f(s_i). \tag{43}$$

Indeed, let $x' = \Sigma_j \mu_j t_j$ be any convex combination with $t_j \in M$. Then we can find a small number $\varepsilon > 0$ such that $(\lambda_i - \varepsilon \lambda_i') \geqslant 0$ for all i. Hence

$$x = \sum_i (\lambda_i - \varepsilon \lambda_i') s_i + \sum_j \varepsilon \mu_j t_j$$

is a convex combination of elements from M representing x. But since the decomposition using only the s_i is optimal, we have

$$\sum_i (\lambda_i - \varepsilon \lambda_i') f(s_i) + \sum_j \varepsilon \mu_j f(t_j) \geqslant \sum_i \lambda_i f(s_i).$$

From this we immediately get the claimed optimality of $x' = \Sigma_j \lambda_j' s_j$.

These remarks are especially useful for the case of entanglement of formation, for any mixed state the optimizing convex decomposition necessarily involves several terms. Hence any computation of an entanglement of formation immediately extends to a larger class of states. Therefore, it is of great interest not only to get the value of the entanglement of formation for a given mixed state, but also to find the set of pure states solving the variational problem defining E_F.

The symmetric situation studied in this paper is extreme in this regard: The minimizing sets are always complete orbits of the symmetry group. Therefore, we get a fairly large set of nonsymmetric mixed states for which the computations below also give the exact value of E_F.

C. Results for $G = \mathbf{U}\mathbf{U}$

In this subsection we will apply the general method to computing the entanglement of formation for the states of Example 1.

In the first step we have to determine the set M_f of vectors $\Phi \in \mathcal{H} \otimes \mathcal{H}$ such that $\langle \Phi | \mathbb{F} \Phi \rangle = f$. In terms of the vector components Φ_{ij} we get

$$\langle \psi | \mathbb{F} \psi \rangle = \sum_{ij} \Phi_{ij} \Phi_{ji}^*. \tag{44}$$

On the other hand, the reduced density operator has components $\rho_{ij} = \Sigma_k \Phi_{ik} \Phi^*_{jk}$ or, in matrix notation, $\rho = \Phi \Phi^\dagger$. Here we may introduce a simplification due to $U \otimes U$ symmetry, by choosing ρ diagonal. Note, however, that we *cannot* choose the restriction to the second system, i.e., $\Phi^T \overline{\Phi}$ to be diagonal at the same time without loss of generality. In any case, the eigenvalues of ρ become $\rho_{ii} = \Sigma_k |\Phi_{ik}|^2$. Hence the pure-state entanglement of Φ, which by Eq. (29) is the entropy of ρ is

$$E(|\Phi\rangle\langle\Phi|) = \sum_i \eta\left(\sum_k |\Phi_{ik}|^2 \right), \tag{45}$$

where η is the entropy function from Eq. (30).

For analyzing the variational problem it is useful to consider the contributions of each pair of variables Φ_{ij} and Φ_{ji}, and of each diagonal element Φ_{ii} separately. The weights of these contributions are

$$\lambda_{ij}=|\Phi_{ij}|^2+|\Phi_{ji}|^2, \quad \text{for } i<j \tag{46}$$

$$\lambda_{ii}=|\Phi_{ij}|^2. \tag{47}$$

The normalized contribution of one such pair or diagonal element to f is

$$f_{ij}=\lambda_{ij}^{-1}2\,\mathrm{Re}(\Phi_{ij}\Phi_{ji}^*), \quad \text{for } i<j \tag{48}$$

$$f_{ii}=1, \quad \text{so that} \tag{49}$$

$$f=\sum_{i\leqslant j}\lambda_{ij}f_{ij}. \tag{50}$$

Similarly, we can write the probability distribution $\rho_{11},\ldots,\rho_{dd}$ as a convex combination of probability distributions with respective entropies

$$s_{ij}=H_2(\lambda_{ij}^{-1}|\Phi_{ij}|^2), \quad \text{for } i<j \tag{51}$$

$$s_{ii}=0, \tag{52}$$

where we have used the abbreviation $H_2(p)=\eta(p)+\eta(1-p)$ for the entropy of a two-point probability distribution $(p,1-p)$. By concavity of the entropy we have

$$E(|\Phi\rangle\langle\Phi|)\geqslant\sum_{i\leqslant j}\lambda_{ij}s_{ij}. \tag{53}$$

To find the lower bound on s_{ij} given f_{ij} is just another instance of the variational problem we are solving, albeit with the considerable simplification that only one off-diagonal pair of components of Φ is nonzero. This leaves the following problem:

Given two complex variables x,y with the constraint $|x|^2+|y|^2=1$, with $2\,\mathrm{Re}(xy^*)=f$, minimize $s=H_2(|x|^2)$.

Since s is monotonically increasing in $|x|^2$ from 0 to 1/2, this is equivalent to minimizing $|x|^2$, given f. The pairs $(|x|^2,f)$ compatible with the constraints form the convex set

$$\{(\lambda,f)\,|\,|f|\leqslant 2\sqrt{\lambda(1-\lambda)};0\leqslant\lambda\leqslant 1\}.$$

From this we get the minimal admissible $|x|^2=(1-\sqrt{1-f^2})/2$ in the above two-variable variational problem. Hence

$$s_{ij}\geqslant\varepsilon_2(f_{ij})=H_2[\tfrac{1}{2}(1-\sqrt{1-f_{ij}^2})]. \tag{54}$$

This function ε_2 can be shown to be convex by explicitly computing the second derivative and expanding logarithms in a power series. Combining the bounds (53), (52), and (54) with the convexity of ε_2, we get

$$\begin{aligned}E(|\Phi\rangle\langle\Phi|)&\geqslant\sum_{i<j}\lambda_{ij}\varepsilon_2(f_{ij})\\&\geqslant\varepsilon_2\left(\sum_{i<j}\lambda_{ij}f_{ij}\right)\\&=\varepsilon_2\left(f-\sum_i\lambda_{ii}\right).\end{aligned}$$

Now suppose that $f\geqslant 0$. Then we can choose just a single diagonal entry Φ_{ii} to be nonzero, and find $E(|\Phi\rangle\langle\Phi|)=0$, which is clearly the minimum. However, if $f<0$ them the last equation shows that letting any diagonal entry $\Phi_{ii}\neq 0$ decreases the argument of ε_2 further in a range where this function is monotonically decreasing. Hence the optimum is choosing all $\Phi_{ii}=0$, and allowing only two nonzero components Φ_{ij} and Φ_{ji} for some $i\neq j$. This concludes the computation of E_F for UU-invariant states (see summary below).

However, as noted in Sec. IV B, knowledge of the minimizers for ε automatically leads to an extension of the computation to some noninvariant states. Let x,y be a solution of the two-variable variational problem with $f=\mathrm{tr}(\rho\mathbb{F})$. Then the minimizing vector is of the form

$$x|12\rangle+y|21\rangle=(x\mathbb{I}+y\mathbb{F})|12\rangle. \tag{55}$$

All $U\otimes U$ translates of this vector will do just as well and appear in the minimizing decomposition of the UU-invariant state. Hence all convex combinations of the density operators

$$(x\mathbb{I}+y\mathbb{F})(U\otimes U)|12\rangle\langle 12|(U\otimes U)^\dagger(x\mathbb{I}+y\mathbb{F})^\dagger$$

with fixed x,y, and arbitrary U, have the same E_F. For determining these convex combinations we can drop the outer factors, and afterwards shift the operators found with $(x\mathbb{I}+y\mathbb{F})\in G'$. Let

$$\mathcal{F}=\mathrm{co}\{(U\otimes U)|12\rangle\langle 12|(U\otimes U)^\dagger\,|\,U\text{ unitary}\}. \tag{56}$$

Clearly, every operator in $\mathcal{F}$ is a separable density operator with flip expectation zero. Conversely, any operator $\tilde{\rho}$ with these properties may be decomposed into pure product states $|\phi\otimes\psi\rangle\langle\phi\otimes\psi|$. These must also have flip expectation zero, which means that $\phi\perp\psi$, so that there is a unitary operator U with $\phi\otimes\psi=(U\otimes U)|12\rangle$. Consequently, $\tilde{\rho}\in\mathcal{F}$.

Hence in order to determine whether for a given ρ we can compute $E_F(\rho)$, we transform it to $\tilde{\rho}$ by the appropriate $(x\mathbb{I}+y\mathbb{F})^{-1}$, and then test the separability of $\tilde{\rho}$ (Fig. 5).

Let us summarize:

- For the $(U\otimes U)$-invariant state ρ with $\mathrm{tr}(\rho\mathbb{F})=f\leqslant 0$, we have

$$E_F(\rho)=H_2[\tfrac{1}{2}(1-\sqrt{1-f^2})], \tag{57}$$

independently of the dimension d of the underlying Hilbert space. When $f\geqslant 0$, the state ρ is separable, and $E_F(\rho)=0$.

- Let ρ be a (not necessarily invariant) density operator with $\mathrm{tr}(\rho\mathbb{F})=f$ and $-1<f<0$. Then with suitably chosen $\alpha,\beta\in\mathbb{R}$,

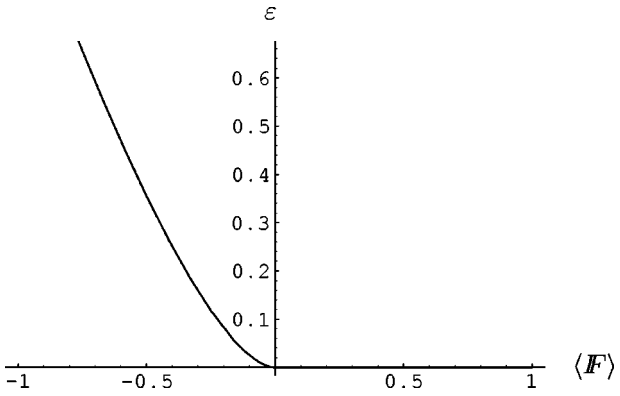

FIG. 5. ε function for UU-invariant states.

$$\tilde{\rho}=(\alpha\mathbb{I}+\beta\mathbb{F})^{\dagger}\rho(\alpha\mathbb{I}+\beta\mathbb{F}) \tag{58}$$

is a density operator with $\mathrm{tr}(\tilde{\rho}\mathbb{F})=0$. Suppose that $\tilde{\rho}$ is separable. Then formula (57) also holds for ρ.

D. Results for $G=UU^*$

The computation of the entanglement of formation for Example 2 is already known [12]. The minimizing pure states are of the form

$$(x\mathbb{I}+y\hat{\mathbb{F}})|11\rangle, \tag{59}$$

with real x,y.

The extension to noninvariant states works in principle similarly to the UU case, but for $d>2$ it is getting a bit more complicated, because the ε function is not convex anymore (Fig. 6).

• For the $(U\otimes U^*)$-invariant state ρ with $\mathrm{tr}(\rho\hat{\mathbb{F}})=f\geqslant 1/d$, we have

$$E_F(\rho)=\mathrm{co}[H_2(\gamma)+(1-\gamma)\ln(d-1)], \tag{60}$$

with $\gamma=(1/d^2)[\sqrt{f}+\sqrt{(d-1)(d-f)}]^2$. For $d>2$ we need also to compute the convex hull. When $f<1/d$, the state ρ is separable, and $E_F(\rho)=0$.

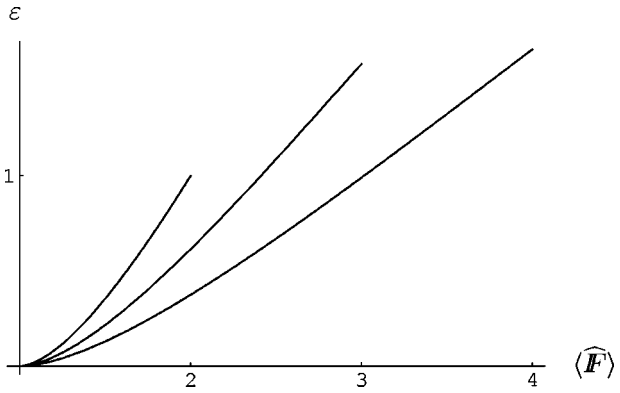

FIG. 6. ε function for UU*-invariant states for $d=2,3,4$. The functions are not convex near the right endpoint for $d\geqslant 3$.

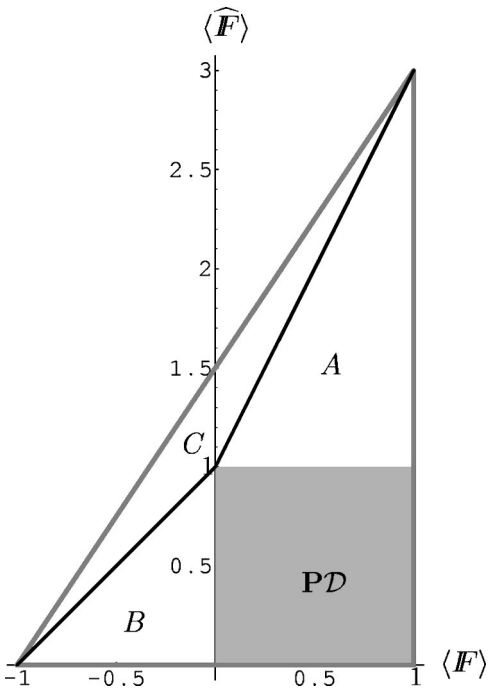

FIG. 7. The state space for OO-invariant states seems to split naturally in four regions. The separable square $\mathbf{P}\mathcal{D}$ and the three triangles *A*, *B*, and *C*.

• Let ρ be a (not necessarily invariant) density operator with $\mathrm{tr}(\rho\hat{\mathbb{F}})=f$, $1<f<d$ and $\mathrm{co}[\varepsilon(f)]=\varepsilon(f)$. Then with suitably chosen $\alpha,\beta\in\mathbb{R}$

$$\tilde{\rho}=(\alpha\mathbb{I}+\beta\hat{\mathbb{F}})^{\dagger}\rho(\alpha\mathbb{I}+\beta\hat{\mathbb{F}}) \tag{61}$$

is a density operator with $\mathrm{tr}(\tilde{\rho}\hat{\mathbb{F}})=1$. Suppose that $\tilde{\rho}$ is separable. Then formula (60) also holds for ρ.

• If f satisfies $\mathrm{co}[\varepsilon(f)]<\varepsilon(f)$, the convex hull has a flat section between $f_1<f<f_2$ where f_1,f_2 are the two end points of the flat piece satisfying $\mathrm{co}[\varepsilon(f_{1/2})]=\varepsilon(f_{1/2})$. We can always find a convex decomposition of ρ in two states with expectation values f_1,f_2. If now the above procedure works for these two states, then we have found an optimal decomposition for ρ and can easily compute the entanglement of formation.

E. Results for OO-invariant states

Here the extension method of Sec. IV B turns out to do much of the work. The state space, plotted in Fig. 7, is separated in four regions: the separable square and the three triangles *A*, *B*, and *C*.

In order to apply the extension method to the UU-invariant states, we have to see which states can be written as $\rho=(x\mathbb{I}+y\mathbb{F})\tilde{\rho}(x\mathbb{I}+y\mathbb{F})^{\dagger}$, with $\tilde{\rho}$ a separable state with flip expectation zero. If we take for $\tilde{\rho}$ any state at the left edge of the separable square, it is clear that we will get an OO-invariant state again. The explicit computation shows that with this method we get $E_F(\rho)$ in the full triangle *B*. Note that by this construction $E_F(\rho)$ depends only on the

expectation $\langle \mathbb{F} \rangle$, and not on $\langle \hat{\mathbb{F}} \rangle$ or the dimension d. Employing similarly the extension method for UU* we find $E_F(\rho)$ in the triangle A, getting a function depending only on $\langle \hat{\mathbb{F}} \rangle$ and the dimension, but not on $\langle \mathbb{F} \rangle$.

F. Results for Bell states

The Bell states were one of the first classes for which entanglement of formation could be calculated [9]. Of course, our method reproduces this result, albeit with a more economical decomposition. This is a feature shared with the Wootters formula [10]. It is a natural question whether the extension method, applied in this basic example, reproduces the Wootters formula. However, it turns out that one gets the result only on state manifolds of lower dimension. We also did not succeed in finding another group of local symmetries, which would give Wootter's formula in full generality.

V. RELATIVE ENTROPY OF ENTANGLEMENT

A. Simplified computation

Symmetry simplifies the computation of the relative entropy of entanglement dramatically: it reduces the variation in Eq. (34) from a variation over all separable states $\sigma \in \mathcal{D}$ to those which are also G invariant. i.e., when $\rho = \mathbf{P}\rho$, we have

$$E_{\mathrm{RE}}(\rho) = \inf\{\mathrm{S}(\rho,\sigma) \,|\, \sigma \in \mathbf{P}\mathcal{D}\}. \tag{62}$$

The only ingredients of the proof are the convexity of $\sigma \mapsto \mathrm{S}(\rho,\sigma)$, the invariance of relative entropy under (local) unitary transformations of both its arguments, and that $\mathcal{D}$ is a convex-set invariant under local unitary operators. Indeed, the properties of $\mathcal{D}$ imply that for any σ in the full variational problem, $\mathbf{P}\sigma \in \mathbf{P}\mathcal{D} \subset \mathcal{D}$, is also a legitimate argument, and the convexity properties of S show that this cannot increase $\mathrm{S}(\rho,\sigma)$. Hence the variation may be restricted as in Eq. (62). We have listed the ingredients of the proof so explicitly, because many variations of E_{RE} may be of interest. For example, the ''distance'' function relative entropy can be replaced by a host of other functions, like norm differences of any kind. The set $\mathcal{D}$, too, may be replaced, for example by the set of PPT states, as suggested by Rains [13], who also made similar use of symmetry.

A second simplification concerns the computation of $\mathrm{S}(\rho,\sigma)$ itself, when both arguments are G invariant. We have seen that G-invariant states can be considered as states on the commutant algebra G'. Now the relative entropy is defined for pairs of states on arbitrary C* algebras [19], and the form (33) involving density matrices is only the special form valid for a full matrix algebra. Since $\mathbf{P}$ is a conditional expectation onto G', the result does not depend [19] on whether we compute the relative entropy via density matrices, or for the corresponding abstract linear functionals on G'. Without going into the details for general algebras G' here, let us see how this helps in the case when G' is Abelian, as in most of our examples.

Suppose p_α, $\alpha = 1, \ldots, N$ are the minimal projections of G', and denote by $\omega_\alpha = (\mathrm{tr}\, p_\alpha)^{-1} p_\alpha$ the extremal density matrices of $\mathbf{P}\mathcal{S}$. Then every $\rho \in \mathbf{P}\mathcal{S}$ has a unique representation as a convex combination

$$\rho = \sum_\alpha \rho_\alpha \omega_\alpha = \sum_\alpha \frac{\rho_\alpha}{\mathrm{tr}\, p_\alpha} p_\alpha, \tag{63}$$

where the second expression is at the same time the spectral resolution of ρ. If we compute the von Neumann entropy $-\mathrm{tr}(\rho \ln \rho)$ from this, we find a dependence of the result not only on the expectations $\rho_\alpha = \mathrm{tr}(\rho p_\alpha)$, but also on the multiplicities $\mathrm{tr}(p_\alpha)$, as is quite familiar from statistical mechanics. On the other hand, the fact that relative entropy can be defined for states on abstract algebras shows that no such dependence can occur for relative entropies. Indeed, the terms involving $\ln \mathrm{tr}(p_\alpha)$ from ρ and σ cancel, and we get

$$\mathrm{S}(\rho,\sigma) = \sum_\alpha \rho_\alpha [\ln(\rho_\alpha) - \ln(\sigma_\alpha)], \tag{64}$$

where ρ_α and σ_α are the respective expectations of p_α.

A typical application is the observation that for UU-invariant states the expression for the relative entropy of entanglement can be written down in terms of the $\mathrm{tr}(\rho F)$, independently of the dimension d of the underlying Hilbert spaces.

For UU- and UU*-invariant states the sets of separable states are just intervals, and the definition of relative entropy of entanglement requires a minimization over this interval. However, due to a general property of the relative entropy, the convexity in both arguments, it is clear that the minimum is, in fact, always obtained at the endpoint: if ρ is the state whose entanglement we want to calculate, and σ is the minimizing separable state, convexity implies

$$\begin{aligned} \mathrm{S}(\rho, \lambda\sigma + (1-\lambda)\rho) &\leqslant \lambda \mathrm{S}(\rho,\sigma) + (1-\lambda)\mathrm{S}(\rho,\rho) \\ &= \lambda \mathrm{S}(\rho,\sigma). \end{aligned}$$

Hence if there were any separable state on the straight-line segment connecting ρ and σ, it would give a strictly lower minimum, contradicting the minimality of σ.

For UU the boundary separable state has $\mathrm{tr}(\sigma\mathbb{F}) = 0$, i.e., gives equal weight to the minimal projections. We have to compute the relative entropy with respect to a state with probabilities $(1 \pm f)/2$, i.e., the function

$$e_{\mathrm{RE}}(f) = \ln 2 - S\left(\frac{1+f}{2}, \frac{1-f}{2}\right), \tag{65}$$

where we denote by $S(p_1, \ldots, p_n) = -\Sigma_k p_k \ln p_k$ the entropy of a probability vector $(p_1, \ldots, p_n)$. This function is plotted in Fig. 8, and determines the relative entropy of entanglement of UU-symmetric states ρ via

$$E_{\mathrm{RE}}(\rho) = e_{\mathrm{RE}}[\mathrm{tr}(\rho\mathbb{F})]. \tag{66}$$

Similarly, the boundary point σ of $\mathcal{D}$ for UU* invariant states is given by $\mathrm{tr}(\sigma\hat{\mathbb{F}}) = 1$. For general $\hat{f} = \mathrm{tr}(\rho\hat{\mathbb{F}})$ the minimal projections have weights $\hat{f}/d$ and $(1 - \hat{f}/d)$. Hence for UU*-symmetric ρ, we have $E_{\mathrm{RE}}(\rho) = 0$ for $\hat{f} \leqslant 1$, and

$$\ln d - \left(1 - \frac{\hat{f}}{d}\right)\ln(d-1) - S\left(\frac{\hat{f}}{d}, 1 - \frac{\hat{f}}{d}\right) \tag{67}$$

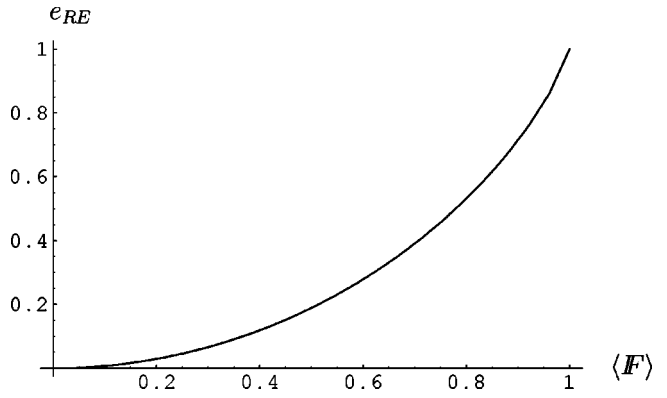

FIG. 8. The relative entropy of entanglement for UU-invariant states.

otherwise. For comparison with the results of Ref. [12], note that $\hat{f}/d$ is the so-called *maximally entangled fraction* of ρ.

Now we look at OO-invariant states. The state space and the separable states are drawn in Fig. 7. First we look at the state with the coordinates (1,3), which is a maximal entangled state. The separable states, that are minimizing the relative entropy for this state, are the states on the whole line connecting the points (0,1) and (1,1). But now we can find the minimizing separable for any state in the whole triangle *A*. We just have to draw the straight line connecting the coordinates of given states with the point (1,3). The intersection with the border of $\mathbf{P}\mathcal{D}$ is then a minimizer for (1,3) and by the properties of the relative entropy of entanglement also the minimizer for all states on the connecting line. The same argumentation works for the edge point $(-1,0)$ and the separable border between (0,0) and (0,1) giving us all minimizers for the triangle *B*. The whole triangle *C* has the same minimizer, namely, (0,1).

B. Counterexample of additivity

To find a counterexample of the additivity of the relative entropy of entanglement, we use the group introduced in Example 7 . We also know that additivity will hold for any state where one of the two independently prepared states is separable. So, in our example, we can restrict to the area where expectation values of both F_1 and F_2 are negative.

For simplicity, we increase the group with $\mathbb{F}_{\text{Alice}}\otimes\mathbb{F}_{\text{Bob}}$ leading us to a smaller commutant only spanned by $\mathbb{I}\otimes\mathbb{I},\mathbb{F}\otimes\mathbb{F},\mathbb{I}\otimes\mathbb{F}+\mathbb{F}\otimes\mathbb{I}$. As coordinate system we use the expectation values of

$$F=\tfrac{1}{2}(\mathbb{I}\otimes\mathbb{F}+\mathbb{F}\otimes\mathbb{I}) \tag{68}$$

$$F_{12}=\mathbb{F}\otimes\mathbb{F}. \tag{69}$$

The state space is drawn in Fig. 9.

It is just the intersection of the state space of the original group (see Fig. 4) with the plane given by $\langle F_1\rangle=\langle F_2\rangle=\langle F\rangle$. The product states, in the sense of additivity, are given by the line $(\langle F\rangle,\langle F\rangle^2)$.

The counterexample we want to look at is the state referring to the coordinates $(-1,1)$, which is given by $\rho_-\otimes\rho_-$

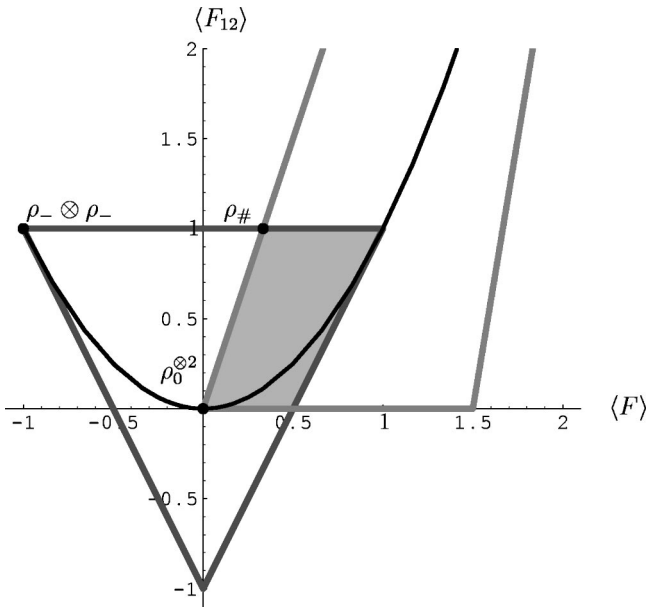

FIG. 9. State space for UUVV and *F*-invariant states for $d=3$.

where ρ_- denotes the normalized projection on the antisymmetric subspace of $\mathbb{C}^d\otimes\mathbb{C}^d$. From Eq. (66) we know the relative entropy of entanglement for ρ_- to be $\ln 2$ independent from the dimension *d*. The minimizing state was the state with flip expectation value equal to zero now denoted as ρ_0. So the expected minimizer for the tensor product would be $\rho_0\otimes\rho_0$ located on the quadratic product line with the expectation values (0,0). This one gives us the expected value of $\ln 4$ for the relative entropy. Now we calculate the relative entropy between $\rho_-^{\otimes 2}=\rho_-\otimes\rho_-$ and $\rho_\#$:

$$\mathrm{S}(\rho_-^{\otimes 2},\rho_\#)=\mathrm{tr}(\rho_-^{\otimes 2}\ln\rho_-^{\otimes 2}-\rho_-^{\otimes 2}\ln\rho_\#) \tag{70}$$

$$=\mathrm{tr}\left(\rho_-^{\otimes 2}\ln\rho_-^{\otimes 2}-\rho_-^{\otimes 2}\ln\frac{d-1}{2d}\rho_-^{\otimes 2}\right) \tag{71}$$

$$=-\ln\frac{d-1}{2d}=\ln 4-\ln\frac{2(d-1)}{d}. \tag{72}$$

Indeed, the minimum must be attained on the line connecting $\rho_0\otimes\rho_0$ and $\rho_\#$, and it can easily be verified that the minimum always is attained on $\rho_\#$. For $d=2$ the whole line gives the same value and although there exits a minimizer that does not belong to the product space, additivity holds. For $d>2$ the expectation values of state $\rho_\#$ given by $(1/d,1)$ shift near to the F_{12} axis and from a geometrical point of view closer to $\rho_-\otimes\rho_-$. Although the relative entropy is not a real kind of geometrical measure this intuition did not fail. In these cases the additivity is violated with an amount of $\ln\{[2(d-1)]/d\}$. For very high dimension *d* we get the really surprising result $E_{RE}(\rho_-\otimes\rho_-)\simeq E_{RE}(\rho_-)$.

VI. CONCLUDING REMARKS

We have concentrated on just two basic entanglement measures. Clearly, there are many more, and for many of

them the computation can be simplified for symmetric states. Among these measures of entanglement are the ''best separable approximation'' of a state [20], the trace norm of the partial transpose [21], the base norm associated with $\mathcal{D}$ (called cross norm in Ref. [22] and absolute robustness in Ref. [23]). For distillable entanglement we refer to the recent paper of Rains [6]. Similarly, there is a lot of work left to be done by carrying out the program outlined in this paper for all the groups of local symmetries listed in, Sec. II A.

ACKNOWLEDGMENTS

Funding by the European Union project EQUIP (contract IST-1999-11053) and financial support from the DFG (Bonn) is gratefully acknowledged.

[1] R.F. Werner, Phys. Rev. A **40**, 4277 (1989).
[2] S. Popescu, Phys. Rev. Lett. **72**, 797 (1994).
[3] M. Horodecki and P. Horodecki, Phys. Rev. A **59**, 4206 (1999).
[4] T. Eggeling and R.F. Werner, e-print quant-ph/0003008.
[5] W. Dr, J.I. Cirac, and R. Tarrach, Phys. Rev. Lett. **83**, 3562 (1999).
[6] E.M. Rains, e-print quant-ph/0008047.
[7] V. Vedral, M.B. Plenio, M.A. Rippin, and P.L. Knight, Phys. Rev. Lett. **78**, 2275 (1997).
[8] V. Vedral and M.B. Plenio, Phys. Rev. A **57**, 1619 (1998).
[9] C.H. Bennett, D.P. DiVincenzo, J.A. Smolin, and W.K. Wootters, Phys. Rev. A **54**, 3824 (1996).
[10] W.K. Wootters, Phys. Rev. Lett. **80**, 2245 (1998).
[11] In the present context this has also been called the roof property of *F*. A. Uhlmann, Open Syst. Inf. Dyn. **5**, 209 (1998).
[12] B. Terhal and K.G.H. Vollbrecht, Phys. Rev. Lett. **85**, 2625 (2000).
[13] E.M. Rains, Phys. Rev. A **60**, 179 (1999).
[14] H. Weyl, *The Classical Groups* (Princeton University, Princeton, NJ, 1946).
[15] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).
[16] K.G.H. Vollbrecht and R.F. Werner, J. Math. Phys. **41**, 6772 (2000).
[17] M. Takesaki, *Theory of Operator Algebras I* (Springer-Verlag, New York, 1979).
[18] F. Benatti and H. Narnhofer, e-print quant-ph/0005126.
[19] M. Ohya and D. Petz, *Quantum Entropy and Its Use* (Springer-Verlag, New York, 1993).
[20] M. Lewenstein and A. Sanpera, Phys. Rev. Lett. **80**, 2261 (1998).
[21] M. Horodecki, P. Horodecki, and Horodecki, Phys. Rev. Lett. **84**, 4260 (2000).
[22] O. Rudolph, J. Phys. A **33**, 3951 (2000).
[23] G. Vidal and R. Tarrach, Phys. Rev. A **59**, 141 (1999).