

Properties of entanglement monotones for three-qubit pure states

R. M. Gingrich

California Institute of Technology, Pasadena, California 91125

(Received 3 July 2001; published 15 April 2002)

Various parametrizations for the orbits under local unitary transformations of three-qubit pure states are analyzed. The interconvertibility, symmetry properties, parameter ranges, calculability, and behavior under measurement are looked at. It is shown that the entanglement monotones of any multipartite pure state uniquely determine the orbit of that state under local unitary transformations. It follows that there must be an entanglement monotone for three-qubit pure states which depends on the Kempe invariant defined in Phys. Rev. A **60**, 910 (1999). A form for such an entanglement monotone is proposed. A theorem is proved that significantly reduces the number of entanglement monotones that must be looked at to find the maximal probability of transforming one multipartite state to another.

DOI: 10.1103/PhysRevA.65.052302

PACS number(s): 03.67.-a, 03.65.Ud, 03.65.Ta

I. INTRODUCTION

Entanglement is at the heart of the studies of quantum computation and quantum information theory. It is what separates these studies from their classical counterparts. If we are to understand what different phenomena occur when we look at the true quantum mechanical description of nature as opposed to the approximations of classical mechanics, then we must understand how the quantum mechanical description differs from the classical description. Entanglement is a measure of this difference. While entanglement between two parties is quite well understood [2–5], the entanglement within a quantum algorithm or in a state shared between many parties involves multipartite entanglement, which is just beginning to be understood [6–8].

An integral part of the study of entanglement is determining the probability of transforming one pure state into another by local operations and classical communication (LOCC). For two-part systems this problem was solved, or at least reduced to the problem of finding the eigenvalues of a Hermitian matrix, by [4,5]. For an $N \times M$ pure state the Schmidt decomposition tells us that we can write

$$|\psi\rangle = \sum_{i=1}^n \sqrt{\lambda_i^\uparrow} |i\rangle |i'\rangle, \quad (1)$$

where the λ_i^\uparrow are in increasing order, $\sum_i \lambda_i^\uparrow = 1$, the $|i\rangle$ and $|i'\rangle$ are an orthonormal set of vectors in spaces A and B , respectively, and $n = \min(N, M)$. If we define

$$E_k(|\psi\rangle) = \sum_{i=1}^k \lambda_i^\uparrow, \quad k = 1, \dots, n-1, \quad (2)$$

then the highest attainable probability of transforming $|\psi\rangle$ to $|\phi\rangle$, $P(|\psi\rangle \rightarrow |\phi\rangle)$, is given by [5]

$$P(|\psi\rangle \rightarrow |\phi\rangle) = \min \left\{ \frac{E_k(|\psi\rangle)}{E_k(|\phi\rangle)}, 1 \right\},$$

$$k = 1, \dots, n-1. \quad (3)$$

The proof of this theorem is constructive so we can actually write down the transformation that gives us $|\phi\rangle$ from $|\psi\rangle$. For pure states of more than two parts no such nice theorem is known. The question of whether two three-qubit pure states can be transformed into each other with nonzero probability by LOCC has been solved by Dür *et al.* [9], but just getting a reasonable upper bound on that probability when it is nonzero is unsolved. In this paper I attempt to make some progress toward solving this problem for three-qubit pure states and hopefully shed some light on how we might solve it for larger dimensional spaces and more parts.

One way to find $P(|\psi\rangle \rightarrow |\phi\rangle)$ is to look at the entanglement monotones $E(|\psi\rangle)$ for the two states. For the duration of this paper “state” will refer to a pure state unless explicitly called a mixed state. An entanglement monotone (EM) is defined as a function that goes from states to positive real numbers and does not increase under LOCC. As a convention the value of any EM for a separable state is 0. For mixed and pure states of any dimension and number of parts the following theorem holds [10]:

$$P(\rho \rightarrow \rho') = \min_E \frac{E(\rho)}{E(\rho')}, \quad (4)$$

where the minimization is taken over the set of all EMs [10]. This can be seen by considering $P(\rho \rightarrow \rho')$ as an EM for ρ . The problem is that this minimization is difficult to take since there is no known way to characterize all the entanglement monotones for multipartite states. We would like a “minimal set” of EMs similar to the E_k for the bipartite case in order to take the minimization.

The situation for three or more parts is somewhat different than for bipartite pure states. First, generic $M \times M$ bipartite states have a stabilizer (i.e., the set of unitaries that takes a state to itself) of dimension $M-1$ isomorphic to $U(1)^{\otimes M-1}$ while pure states with more parts generically have a discrete stabilizer. States whose parts are not of the same dimension may have larger stabilizers but bipartite states are the only ones that always have a continuous stabilizer. Secondly, the generalized Schmidt decomposition, however you choose to generalize it [11,12], has complex coefficients for pure states

with three or more parts. This implies that generally these states are not locally unitarily equivalent to their complex conjugate states (i.e., the state with each of its coefficients complex conjugated). Also, for bipartite pure states all the local unitary (LU) invariants can be calculated from the eigenvalues of the reduced density matrices but this does not hold for more parts. I will go into more detail about LU invariants in the next section.

The structure of the paper is as follows. In Sec. II the interconvertibility, behavior under measurement, symmetry properties, parameter ranges, and calculability of two generalizations of the Schmidt decomposition of Eq. (1) and the polynomial invariants (defined below) are looked at. In Sec. III it is shown that the entanglement monotones uniquely determine the orbit of multipartite pure states and this is used to show that there must be an EM algebraically independent of the known EMs. A form for this EM is proposed and studied. Section IV discusses other monotones that must exist and their properties. Lastly, in Sec. V a theorem is proved that significantly reduces the number of EMs that must be minimized over to get $P(\rho \rightarrow \rho')$ of Eq. (4).

II. DECOMPOSITIONS AND INVARIANTS OF THREE-QUBIT PURE STATES

Let $|\psi\rangle$ be a multipartite state in $\mathcal{H}_1 \otimes \mathcal{H}_2 \cdots \otimes \mathcal{H}_n$ and let $A_k^{(i)}: \mathcal{H}_i \rightarrow \mathcal{H}_i'$ be Krauss operators for an operation on the Hilbert space \mathcal{H}_i with $\sum_k A_k^{(i)\dagger} A_k^{(i)} = \mathcal{I}_i$ and \mathcal{I}_i the identity acting on \mathcal{H}_i . A (nonincreasing) EM is a real valued function $E(|\psi\rangle)$ such that

$$E(|\psi\rangle) \geq \sum_k p_k E\left(\frac{I_1 \otimes \cdots \otimes A_k^{(i)} \otimes \cdots \otimes I_n |\psi\rangle}{\sqrt{p_k}}\right) \quad (5)$$

for any state $|\psi\rangle$, operation $A_k^{(i)}$, and space i where

$$p_k = \|I_1 \otimes \cdots \otimes A_k^{(i)} \otimes \cdots \otimes I_n |\psi\rangle\|^2. \quad (6)$$

This definition for pure states is taken from the definition for a general state in [10]. One can always transform a state into product states and a product state cannot be transformed into anything but another product state so the value of an EM for a product state is chosen to be zero and all other states must have a non-negative value for the EM. Since $A_k^{(i)}$ can be a unitary operator or the inverse of that operator, Eq. (5) implies that all EMs must be invariant under LU. Hence, a first step to understanding the EMs is to look at the LU invariants that parametrize the set of orbits.

There are many ways to find LU invariants for three-qubit states [13,12,14,11,6,15,16] some of which can be generalized to more parts and larger spaces, but for now I will concentrate on the three-qubit case. The three sets of invariants I will look at in this section are the polynomial invariants [13], what I will call the diagonalization decomposition [12], and what I will call the maximization decomposition [11].

A. The polynomial invariants

A general polynomial invariant $P_{\sigma,\tau}(|\psi\rangle)$ for a three-qubit state of the form

$$|\psi\rangle = \sum_{i,j,k=0}^1 t_{ijk} |ijk\rangle \quad (7)$$

is written as

$$P_{\sigma,\tau}(|\psi\rangle) = \sum t_{i_1 j_1 k_1} \cdots t_{i_n j_n k_n} \bar{t}_{i_1 j_{\sigma(1)} k_{\tau(1)}} \cdots \bar{t}_{i_n j_{\sigma(n)} k_{\tau(n)}} \quad (8)$$

where σ and τ are permutations on n elements, repeated indices are summed, and \bar{t} stands for the complex conjugate of t [13]. If one applies a unitary to any of the qubits in $|\psi\rangle$ and explicitly writes out $P_{\sigma,\tau}(|\psi\rangle)$ again it becomes apparent that $P_{\sigma,\tau}(|\psi\rangle)$ is invariant. Of course, any polynomial in terms of the polynomial invariants $P_{\sigma,\tau}(|\psi\rangle)$ is another polynomial invariant. In fact, it can be shown that all the polynomial invariants are of this form.

We know from [11] that the number of independent polynomial invariants is given by

$$\dim[\mathcal{C}^2 \otimes \mathcal{C}^2 \otimes \mathcal{C}^2] - 3 \dim[\text{SU}(2)] - \dim[\text{U}(1)] - 1 = 5, \quad (9)$$

where the last -1 is due to the fact that we are using normalized states. The five independent continuous invariants are

$$\begin{aligned} I_1 &= P_{e,(12)}, \\ I_2 &= P_{(12),e}, \\ I_3 &= P_{(12),(12)}, \\ I_4 &= P_{(123),(132)}, \end{aligned} \quad (10)$$

$$\begin{aligned} I_5 &= \left| \sum t_{i_1 j_1 k_1} t_{i_2 j_2 k_2} t_{i_3 j_3 k_3} t_{i_4 j_4 k_4} \right. \\ &\quad \left. \times \epsilon_{i_1 i_2} \epsilon_{i_3 i_4} \epsilon_{j_1 j_2} \epsilon_{j_3 j_4} \epsilon_{k_1 k_3} \epsilon_{k_2 i_4} \right|^2, \end{aligned}$$

where $\epsilon_{00} = \epsilon_{11} = 0$, $\epsilon_{01} = -\epsilon_{10} = 1$, and again repeated indices are summed. I_4 is the Kempe invariant [1]. If one writes out I_5 and uses the identity $\epsilon_{ij} \epsilon_{rs} = \delta_{ir} \delta_{js} - \delta_{is} \delta_{jr}$ it can be shown that I_5 is just the sum and difference of 64 polynomials of the form in Eq. (8). With one more discrete invariant

$$I_6 = \text{sgn}[\text{Im}(P_{(34)(56),(13524)})], \quad (11)$$

the LU orbit of a three-qubit state is determined uniquely [12,17]. In this paper I will define $\text{sgn}[x]$ as 1 for non-negative numbers and -1 otherwise. The polynomial invariants have the advantage of being easy to compute for any state and the four previously known independent EMs [6] are the following simple functions of I_1 , I_2 , I_3 , and I_5 :

$$\begin{aligned}
 \tau_{(AB)C} &= 2(1 - I_1), \\
 \tau_{(AC)B} &= 2(1 - I_2), \\
 \tau_{(BC)A} &= 2(1 - I_3), \\
 \tau_{ABC} &= 2\sqrt{I_5}.
 \end{aligned} \tag{12}$$

B. The diagonalization decomposition

The diagonalization decomposition (DD) introduced by Acin *et al.* [12] is accomplished by first defining matrices $(T_0)_{j,k} = t_{0jk}$ and $(T_1)_{j,k} = t_{1jk}$, where the t_{ijk} are given by Eq. (7). Next find a unitary operation on space A that makes T_0 singular and unitaries on spaces B and C that make T_0 diagonal. Use the remaining phase freedom to get rid of as many phases as possible. What is left is a state of the form

$$\begin{aligned}
 |\psi_{\text{DD}}\rangle &= \sqrt{\mu_0}|000\rangle + \sqrt{\mu_1}e^{i\phi}|100\rangle + \sqrt{\mu_2}|101\rangle + \sqrt{\mu_3}|110\rangle \\
 &\quad + \sqrt{\mu_4}|111\rangle,
 \end{aligned} \tag{13}$$

where $\mu_i \geq 0$, $\mu_0 + \mu_1 + \mu_2 + \mu_3 + \mu_4 = 1$, and $0 \leq \phi \leq \pi$. Note that generically there are two unitaries that will make T_0 singular but it can be shown that only one will lead to ϕ between 0 and π . If there is another solution, with ϕ between π and 2π exclusive, it is referred to as the dual state of $|\psi_{\text{DD}}\rangle$. Some nice properties of DD are that there is a one to one correspondence with the orbits and there are a set of invertible functions between the parameters of the decomposition and the set of polynomial invariants given above; namely,

$$\begin{aligned}
 I_1 &= 1 - 2\mu_0(\mu_2 + \mu_4) - 2\Delta, \\
 I_2 &= 1 - 2\mu_0(\mu_3 + \mu_4) - 2\Delta, \\
 I_3 &= 1 - 2\mu_0(\mu_2 + \mu_3 + \mu_4), \\
 I_4 &= 1 - 3[(\mu_2 + \mu_3)(\mu_0 - \mu_4) + \mu_4(1 - \mu_4) - \mu_2\mu_3\mu_0 \\
 &\quad + (1 - \mu_0)(\Delta - \mu_1\mu_4)], \\
 I_5 &= 4\mu_0^2\mu_4^2, \\
 I_6 &= \text{sgn}\{\sin(\phi)\mu_0^2\sqrt{\mu_1\mu_2\mu_3\mu_4} \\
 &\quad \times [\Delta - \mu_4(1 - 2\mu_0 + \mu_1) - \mu_2\mu_3]\},
 \end{aligned} \tag{14}$$

where $\Delta = \mu_1\mu_4 + \mu_2\mu_3 - 2\sqrt{\mu_1\mu_2\mu_3\mu_4}\cos(\phi)$. If we define

$$\begin{aligned}
 J_1 &= \frac{1}{4}(1 - I_1 - I_2 + I_3 - 2\sqrt{I_5}), \\
 J_2 &= \frac{1}{4}(1 - I_1 + I_2 - I_3 - 2\sqrt{I_5}), \\
 J_3 &= \frac{1}{4}(1 + I_1 - I_2 - I_3 - 2\sqrt{I_5}),
 \end{aligned} \tag{15}$$

$$J_4 = \sqrt{I_5},$$

$$J_5 = \frac{1}{4}\left(\frac{5}{3} - I_1 - I_2 - I_3 + \frac{4}{3}I_4 - 2\sqrt{I_5}\right),$$

then the coefficients are given by

$$\begin{aligned}
 \mu_0^\pm &= \frac{J_4 + 5 \pm \sqrt{Y}}{2(J_1 + J_4)}, \\
 \mu_i^\pm &= \frac{J_i}{\mu_0^\pm}, \quad i = 2, 3, 4, \\
 \mu_1^\pm &= 1 - \mu_0^\pm - \frac{J_2 + J_3 + J_4}{\mu_0^\pm}, \\
 \cos(\phi^\pm) &= \frac{\mu_1^\pm\mu_4^\pm + \mu_2^\pm\mu_3^\pm - J_1}{2\sqrt{\mu_1^\pm\mu_2^\pm\mu_3^\pm\mu_4^\pm}},
 \end{aligned} \tag{16}$$

$$\begin{aligned}
 \text{sgn}[(\sin(\phi^\pm))] &= I_6 \text{sgn}(\sqrt{\mu_1^\pm\mu_2^\pm\mu_3^\pm\mu_4^\pm}\{J_1 - J_2J_3 - J_4 \\
 &\quad \times [J_2 + J_3 + J_4 - (\mu_0^\pm)^2]\}),
 \end{aligned}$$

where $Y = (J_4 + J_5)^2 - 4(J_1 + J_4)(J_2 + J_4)(J_3 + J_4) \geq 0$. The + and - solutions for the coefficients correspond to $|\psi_{\text{DD}}\rangle$ and its dual state. The inversion of the equations for I_i was done independently in [17]. Note that their definition of I_4 is different from the one in this paper.

Another nice property of the DD is that we can perform an arbitrary measurement on it in space A and stay in the DD form. Since any measurement can be broken into a series of two outcome measurements [18], we can look at the two outcome measurement A_1 and A_2 where $A_1^\dagger A_1 + A_2^\dagger A_2 = I$. Using the singular value decomposition we can write $A_i = U_i D_i V$ where V does not depend on i because the two positive Hermitian operators $A_1^\dagger A_1$ and $A_2^\dagger A_2$ sum to the identity and therefore must be simultaneously diagonalizable. The diagonal matrices D_i can be written as

$$D_1 = \begin{bmatrix} x & 0 \\ 0 & y \end{bmatrix}, \quad D_2 = \begin{bmatrix} \sqrt{1-x^2} & 0 \\ 0 & \sqrt{1-y^2} \end{bmatrix}, \tag{17}$$

where $0 \leq x, y \leq 1$ [9]. Since we are only concerned with what orbit the outcomes are in we may choose the U_i transformation. Also, matrices of the form

$$\begin{bmatrix} e^{i\psi_1} & 0 \\ 0 & e^{i\psi_2} \end{bmatrix}, \tag{18}$$

where ψ_1 and ψ_2 are real numbers, commute with the D_i matrices so the most general V can be written as

$$\begin{bmatrix} \alpha & \sqrt{1-\alpha^2}e^{i\theta} \\ -\sqrt{1-\alpha^2}e^{-i\theta} & \alpha \end{bmatrix}, \tag{19}$$

where $0 \leq \alpha \leq 1$ and θ is real. If we choose

$$U_1 = \frac{1}{\sqrt{\gamma}} \begin{bmatrix} y\alpha & -x\sqrt{1-\alpha^2}e^{i\theta} \\ x\sqrt{1-\alpha^2}e^{-i\theta} & y\alpha \end{bmatrix},$$

$$\gamma = y^2\alpha^2 + x^2(1-\alpha^2), \quad (20)$$

and similarly for U_2 with (x,y) replaced by $(\sqrt{1-x^2}, \sqrt{1-y^2})$, then in going from $|\psi_{\text{DD}}\rangle$ to $A_1|\psi_{\text{DD}}\rangle$ the DD coefficients undergo the following transformations:

$$\mu_0 \rightarrow \frac{x^2 y^2 \mu_0}{\gamma},$$

$$\mu_1 \rightarrow \frac{1}{\gamma} |e^{-i\theta}(x^2 - y^2)\alpha\sqrt{\mu_0(1-\alpha^2)} + e^{i\phi}\gamma\sqrt{\mu_1}|^2, \quad (21)$$

$$\mu_i \rightarrow \mu_i \gamma, \quad i=2,3,4,$$

$$\phi \rightarrow \arg[e^{-i\theta}(x^2 - y^2)\alpha\sqrt{\mu_0(1-\alpha^2)} + e^{i\phi}\gamma\sqrt{\mu_1}],$$

and again similarly for $A_2|\psi_{\text{DD}}\rangle$. Things become more complicated when ϕ becomes larger than π and we have a dual solution. In this case we need to transform to the dual state, which can be quite tedious. It should also be noted that if we want to put this last form for the DD coefficients into Eqs. (14) the normalization must be taken into account. The normalization will just be the sum of the forms (21) for μ_0 through μ_4 .

C. The maximization decomposition

The maximization decomposition (MD) [11] has a somewhat different way of decomposing the three-qubit states. First we find the states $|\phi_A\rangle$, $|\phi_B\rangle$, and $|\phi_C\rangle$, each defined up to an overall phase, that maximize

$$g(|\phi_A\rangle, |\phi_B\rangle, |\phi_C\rangle) = \|\langle\psi|\phi_A\rangle|\phi_B\rangle|\phi_C\rangle\|^2 \quad (22)$$

and apply a unitary such that $|\phi_A\rangle|\phi_B\rangle|\phi_C\rangle$ becomes $|000\rangle$. Defining $|1\rangle$, up to an overall phase, as the vector perpendicular to $|0\rangle$, then the derivative of g along $|1\rangle$ at the point $|000\rangle$,

$$\lim_{\epsilon \rightarrow 0} \frac{g(|0\rangle + \epsilon|1\rangle, |0\rangle, |0\rangle) - g(|0\rangle, |0\rangle, |0\rangle)}{\epsilon}$$

$$= 2 \operatorname{Re}[\langle\psi|100\rangle\langle 000|\psi\rangle] \quad (23)$$

must be zero because $g(|0\rangle, |0\rangle, |0\rangle)$ is a maximum. Since we still have phase freedom in $|0\rangle$ and $|1\rangle$ this implies that $\langle\psi|100\rangle = 0$ and similarly for $\langle\psi|010\rangle$ and $\langle\psi|001\rangle$. Using the remaining phase freedom in the choice of $|0\rangle$ and $|1\rangle$ we can eliminate all but one phase, leaving us with

$$|\psi_{\text{MD}}\rangle = a e^{i\phi}|000\rangle + b|011\rangle + c|101\rangle + d|110\rangle + f|111\rangle, \quad (24)$$

where $a^2 + b^2 + c^2 + d^2 + f^2 = 1$, $0 \leq \phi \leq 2\pi$, $0 \leq a, b, c, d, f$, and $b, c, d, f \leq a$. Note that $g(|0_A\rangle, |0_B\rangle, |0_C\rangle) = a^2$. Unfortu-

nately, the parameters as they are given above are not in one to one correspondence with the orbits. While the decomposition is generically unique, there are choices of the parameters within the given ranges that are not the result of the decomposition. For example, states with $a^2 = 1/5 + \epsilon$, $b^2 = c^2 = d^2 = f^2 = 1/5 - \epsilon/4$, and any choice of ϕ have

$$g\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right) \geq a^2 \quad (25)$$

for $\epsilon \leq 0.014$. Hence, these choices of the parameters are not a result of the decomposition. The true ranges of the parameters that would give a one to one correspondence with the orbits are as yet unknown.

A nice property of the MD is that it is symmetric in particle exchange. Exchanging the particles is equivalent to exchanging b , c , and d . This makes the permutation properties of the polynomial invariants easier to see when written in terms of the MD coefficients. They take the following forms:

$$I_1 = 1 - 2[(a^2 + d^2)(b^2 + c^2) + a^2 f^2],$$

$$I_2 = 1 - 2[(a^2 + c^2)(b^2 + d^2) + a^2 f^2],$$

$$I_3 = 1 - 2[(a^2 + b^2)(c^2 + d^2) + a^2 f^2], \quad (26)$$

$$I_4 = 1 - 3[a^2(1 - a^2) - (b^2 c^2 + b^2 d^2 + c^2 d^2)(1 - 2a^2) - 2b^2 c^2 d^2 - 2abcd f^2 \cos(\phi)],$$

$$I_5 = a^2 |a f^2 + 4bcde^{i\phi}|^2,$$

$$I_6 = \operatorname{sgn}\{abcd f^2 \sin(\phi)[a^2(1 - 2a^2)(1 - 2a^2 - f^2) - 4b^2 c^2 d^2 - 2abcd f^2 \cos(\phi)]\}.$$

It is apparent from these equations that I_1 , I_2 , and I_3 are symmetric in permutations of particles AB , AC , and BC , respectively, and I_4 , I_5 , and I_6 are symmetric in any permutation of the particles. Unfortunately, the equations in (26) are not as easy to invert as those in (14). In fact, just calculating the MD coefficients for an arbitrary state is not an easy task, as it is in the case of the polynomial invariants and the DD coefficients, since determining the unitaries for the MD involves maximizing over a six-dimensional space with typically many local maxima.

One more interesting fact about the MD is that $1 - a^2$ is a nonincreasing EM. We know this because in [16] it is shown that a function of the form

$$E_{k_A, k_B, k_C}(|\psi\rangle) = \max_{\Gamma_A, \Gamma_B, \Gamma_C} \|\Gamma_A \otimes \Gamma_B \otimes \Gamma_C |\psi\rangle\|^2, \quad (27)$$

where Γ_X is a k_X -dimensional projector on system $X = A, B, C$, is a nondecreasing EM and $E_{1,1,1}(|\psi\rangle) = a^2$. The EM $1 - a^2$ can be shown to be independent of τ from Eq. (12) by looking at the gradient vectors of τ , $1 - a^2$ and $N = a^2 + b^2 + c^2 + d^2 + f^2$, at, for instance, the point $a = 3$, $b, c, d, f = 1$, and $\phi = \pi/2$. Since the gradient vectors

span a six-dimensional space, $1 - a^2$ cannot be written in terms of the τ and N . The problem with using $1 - a^2$ as an EM is that one needs to find the global maximum of a six-dimensional space with many local maxima to calculate it. This is a difficult task for most states.

III. FIFTH INDEPENDENT EM

In Sec. II it was shown that all EMs must be invariant under LU and hence are determined by the orbit of the state. For three-qubit states this means that EMs are a function of only the polynomial invariants, DD coefficients, or MD coefficients. In fact, this determination is unique.

Theorem 1. The set of all EMs for any multipartite pure state $|\psi\rangle$ uniquely determines the orbit of the state.

Proof. Suppose two states $|\psi\rangle$ and $|\phi\rangle$ in $\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \dots \otimes \mathcal{H}_n$ have the same values for the EMs but lie in different orbits. We know by using Eq. (4) that

$$P(|\psi\rangle \rightarrow |\phi\rangle) = P(|\phi\rangle \rightarrow |\psi\rangle) = 1, \quad (28)$$

so $|\psi\rangle$ can be transformed to $|\phi\rangle$ (and vice versa) by n -party LOCC (n -LOCC), with probability 1. Since EMs are nonincreasing with any n -LOCC they must remain constant during the entire transformation from $|\psi\rangle$ to $|\phi\rangle$ (and vice versa). Also, we know that any two-party EM (2-EM $_X$) between a system $X = A, B, \dots$ and the rest of the systems thought of as one [e.g., between B and $(ACD \dots)$] is also an n -party EM. This comes from the fact that the set of n -LOCC is a subset of the 2-LOCCs for any choice of X . Since a 2-EM $_X$ is nonincreasing over 2-LOCC for any value of X then it is also nonincreasing under n -LOCC and hence it is an EM. In particular, the sum of the lowest k eigenvectors of the reduced density matrices,

$$E_k^X(|\psi\rangle) = \sum_{i=1}^k \lambda_i^\downarrow[\rho_X(|\psi\rangle)] \quad (29)$$

[i.e., the 2-EMs in Eq. (2)] must be EMs. So the $E_k^X(|\psi\rangle)$ must remain unchanged and hence the spectrum of ρ_X is unchanged during the transformation from $|\psi\rangle$ to $|\phi\rangle$. In particular, an operation on space X , given by A_1 and A_2 , must be such that

$$\rho_X \left(\frac{A_i |\psi\rangle}{\sqrt{N}} \right) = U \rho_X(|\psi\rangle) U^\dagger, \quad (30)$$

where N is the normalization. This can always be satisfied with A_i/\sqrt{N} a unitary matrix. Since every operation can be written as a unitary, $|\psi\rangle$ and $|\phi\rangle$ are unitarily equivalent. This contradicts our original supposition. ■

Since we know there are five parameters that determine the orbit of a three-qubit state then by Theorem 1 there must be five independent, continuous EMs. To the best of the author's knowledge the only four known independent continuous EMs that do not require a difficult maximization over a multidimensional space are the four τ EMs defined in Eq. (12). Any candidate for the fifth independent EM must de-

pend on I_4 since the τ are invertible functions of I_1, I_2, I_3 , and I_5 , respectively. The following function fulfills that criterion:

$$\sigma_{ABC} = 3 - (I_1 + I_2 + I_3)I_4, \quad (31)$$

and numerical results suggest that it is an EM. After generating over 300 000 random states and applying a random operation to each of them the inequality in Eq. (5) was never violated by σ_{ABC} . Also, note that σ_{ABC} is symmetric in particle permutations as is τ_{ABC} . For the rest of the paper I will assume that σ_{ABC} is an EM. Indeed, it may be that there is a set of measure zero or perhaps just a very small measure for which σ_{ABC} is not a monotone and my numerical test did not explore this space, but there must exist some function of the polynomial invariants which is independent of the τ 's and is an EM. For it to be useful in improving our upper bound for $P(|\psi\rangle \rightarrow |\phi\rangle)$ there should be pairs of states $|\psi\rangle$ and $|\phi\rangle$ such that

$$\frac{\sigma_{ABC}(|\psi\rangle)}{\sigma_{ABC}(|\phi\rangle)} < \min_{\tau} \frac{\tau(|\psi\rangle)}{\tau(|\phi\rangle)} \quad (32)$$

and I have found such states numerically. The largest value of

$$\frac{\sigma_{ABC}(|\psi\rangle)}{\sigma_{ABC}(|\phi\rangle)} - \min_{\tau} \frac{\tau(|\psi\rangle)}{\tau(|\phi\rangle)} \quad (33)$$

that I found in my limited number of examples of was 0.01. I was able to find examples of states for which $\tau(|\psi\rangle)/\tau(|\phi\rangle)$ is greater than 1 for all τ and $\sigma_{ABC}(|\psi\rangle)/\sigma_{ABC}(|\phi\rangle)$ is less than 1.

IV. OTHER EMS AND THE DISCRETE INVARIANT

The five independent continuous EMs $\tau_{(AB)C}, \tau_{(AC)B}, \tau_{(BC)A}, \tau_{ABC}$, and σ_{ABC} can easily be inverted to find $I_1 - I_5$ but to completely determine the orbit of a state we must also have an EM that will give us the value of the discrete invariant I_6 . This is equivalent to finding an EM that is not the same for a state and its complex conjugate state. Note that I_1, \dots, I_5 and hence τ and σ_{ABC} do not change when a state is conjugated but by looking at any of the sets of LU invariants we can see that generically a state is not LU equivalent to its conjugate. By looking at Eq. (4) we can see that this implies that there must be EMs that are not the same for the generic state and its conjugate. It is also easy to see that for any operation that takes a state $|\psi\rangle$ to its conjugate $|\bar{\psi}\rangle$ with probability p there is an operation that takes $|\bar{\psi}\rangle$ to $|\psi\rangle$ with the same probability. So for a generic state $|\psi\rangle$ there must be an EM that goes down for the operation $|\psi\rangle \rightarrow |\bar{\psi}\rangle$ and a similar one that goes down the same amount for $|\bar{\psi}\rangle \rightarrow |\psi\rangle$. Thus EMs of the following form must exist:

$$v^\pm(|\psi\rangle) = \begin{cases} v + v', & \pm I_6 = 1, \\ v & \text{otherwise,} \end{cases} \quad (34)$$

where v and v' are functions of $\tau_{(AB)C}$, $\tau_{(AC)B}$, $\tau_{(BC)A}$, τ_{ABC} , and σ_{ABC} .

Also, from [9] we know that there are two classes of three-part entangled states (i.e., states with $\tau_{(AB)C}, \tau_{(AC)B}, \tau_{(BC)A} > 0$) that can be converted into each other with some nonzero probability within the class and zero probability between the classes; namely, the GHZ class which contains

$$|\text{GHZ}\rangle \equiv \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \quad (35)$$

and has nonzero τ_{ABC} and the W class which contains

$$|\text{W}\rangle \equiv \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle) \quad (36)$$

and has $\tau_{ABC} = 0$. Looking again at Eq. (4) we see that τ_{ABC} tells us that $P(|\psi_{\text{W}}\rangle \rightarrow |\psi_{\text{GHZ}}\rangle) = 0$ but none of the previously defined EMs tell us that $P(|\psi_{\text{GHZ}}\rangle \rightarrow |\psi_{\text{W}}\rangle) = 0$. Since the only way to get $P(|\psi_{\text{GHZ}}\rangle \rightarrow |\psi_{\text{W}}\rangle) = 0$ is to have an EM that is finite for GHZ-class states and infinite for W-class states or zero for GHZ-class states and nonzero for W-class states, such an EM must exist.

V. FINDING A MINIMAL SET

Since $\tau_{(AB)C}$, $\tau_{(AC)B}$, $\tau_{(BC)A}$, τ_{ABC} , σ_{ABC} , and v^{\pm} determine the orbit of the state all other EMs must depend on them. A fairly general way to create further EMs from known EMs is to use what I will call f -type functions.

Definition 1. A function $f: \mathcal{S} \mathbb{R}^n \rightarrow \mathbb{R}$ is an f -type function if it satisfies the following, (1) $f(\vec{0}) = 0$; (2) if $x_i \geq y_i$ for all $i = 1, 2, \dots, n$ then $f(\vec{x}) \geq f(\vec{y})$ for $\vec{x}, \vec{y} \in \mathcal{S}$; (3) $f(p\vec{x} + (1-p)\vec{y}) \geq pf(\vec{x}) + (1-p)f(\vec{y})$ for any $\vec{x}, \vec{y} \in \mathcal{S}$ and $0 \leq p \leq 1$.

For a set of EMs, $\{E_i\}$, we have

$$E_i(|\psi\rangle) \geq pE_i\left(\frac{A_1|\psi\rangle}{\sqrt{p}}\right) + (1-p)E_i\left(\frac{A_2|\psi\rangle}{\sqrt{1-p}}\right) \quad (37)$$

for any measurement A_1 , A_2 , and any state $|\psi\rangle$. So we have

$$\begin{aligned} f(\vec{E}(|\psi\rangle)) &\geq f\left(p\vec{E}\left(\frac{A_1|\psi\rangle}{\sqrt{p}}\right) + (1-p)\vec{E}\left(\frac{A_2|\psi\rangle}{\sqrt{1-p}}\right)\right) \\ &\geq pf\left(\vec{E}\left(\frac{A_1|\psi\rangle}{\sqrt{p}}\right)\right) + (1-p)f\left(\vec{E}\left(\frac{A_2|\psi\rangle}{\sqrt{1-p}}\right)\right), \end{aligned} \quad (38)$$

where the first inequality comes from property 2 and the second comes from property 3. Hence, $f(E_1, \dots, E_m)$ is also an EM. We can show that any EM $f(E_1, \dots, E_m)$ that is an f -type function of monotones E_1, \dots, E_m does not modify the upper bound on $P(|\psi\rangle \rightarrow |\phi\rangle)$ given by

$$P(|\psi\rangle \rightarrow |\phi\rangle) \leq \min_i \frac{E_i(|\psi\rangle)}{E_i(|\phi\rangle)}; \quad (39)$$

first for the one-dimensional case.

Lemma 1. If $f(x)$ is an f -type function with $n = 1$ then

$$\frac{f(x)}{f(y)} \geq \min\left\{\frac{x}{y}, 1\right\} \quad (40)$$

for any $x, y \in \mathcal{S}$.

Proof.

Case 1. For $x \geq y$ from property 2 we know $f(x) \geq f(y)$ and hence

$$\frac{f(x)}{f(y)} \geq 1. \quad (41)$$

Case 2. For $x < y$ if we choose $p = (x/y) \in [0, 1)$ then we know from properties 1 and 3 that $f(py) \geq pf(y)$ and so

$$\frac{f(x)}{f(y)} \geq \frac{x}{y}. \quad \blacksquare \quad (42)$$

For n dimensions we have the following theorem.

Theorem 2. If $f(x)$ is an f -type function then

$$\frac{f(\vec{x})}{f(\vec{y})} \geq \min\left\{\frac{x_i}{y_i}, 1\right\}, \quad i = 1, 2, \dots, n, \quad (43)$$

for $\vec{x}, \vec{y} \in \mathcal{S}$.

Proof. Let

$$c = \min\left\{\frac{x_i}{y_i}\right\}. \quad (44)$$

Then we have two cases.

Case 1. If $c \geq 1$ then from property 2 $f(\vec{x}) \geq f(\vec{y})$ and so

$$\frac{f(\vec{x})}{f(\vec{y})} \geq 1. \quad (45)$$

Case 2. If $c < 1$ then define

$$z_i = \frac{x_i}{c}, \quad i = 1, 2, \dots, n, \quad (46)$$

and $g(r) = f(r\vec{z})$. Notice that $g(r)$ is an f -type function with $n = 1$ and hence

$$\frac{g(c)}{g(1)} \geq c, \quad (47)$$

or substituting in f we have

$$\frac{f(\vec{x})}{f(\vec{z})} \geq c. \quad (48)$$

Using $z_i \geq y_i$ and property 2 we have

$$\frac{f(\vec{x})}{f(\vec{y})} \geq c. \quad \blacksquare \quad (49)$$

For three-qubit states if we take the minimum of $E(|\psi\rangle)/E(|\phi\rangle)$ over $\mathcal{E}=\{\tau_{(AB)C}, \tau_{(AC)B}, \tau_{(BC)A}, \tau_{ABC}, \sigma_{ABC}, \nu^\pm\}$ we are actually taking the minimum over the infinite set of all f -type functions of \mathcal{E} . Although from Theorem 1 we know that all EMs must be a function of \mathcal{E} it is possible that there exist EMs that are not f -type functions of \mathcal{E} . These EMs could cause $P(|\psi\rangle \rightarrow |\phi\rangle)$ to be lower than the minimum of $E(|\psi\rangle)/E(|\phi\rangle)$ over \mathcal{E} . The EM mentioned at the end of Sec. IV is an example of such an EM.

VI. CONCLUSIONS AND FURTHER RESEARCH

Theorem 1 along with Theorem 2 implies that there should be a (not necessarily finite) minimal set of EMs M for which all EMs for three-qubit states or similarly for any type of multipartite state are f -type functions of M . I conjecture that such a minimal set should be simple since the f -type functions seem to be a rather general way of creating EMs that are functions of other EMs. The difficult part seems to be finding the EMs that are minimal and showing that they are minimal. Using numerical results it seems that τ may be minimal. I looked at functions of τ that are almost but not quite f type such as $\tau^{1.01}$ and numerically tested whether they are EMs or not. None of them were EMs. I cannot say the same for σ_{ABC} and definitely not for ν^\pm since I do not have an explicit form for ν .

There is further research that may help these problems. If one could invert the equations in (26) to write

a, b, c, d, f , and ϕ in terms of I_1, \dots, I_6 , that would allow us to calculate the EM $1-a^2$ not to mention find the ranges for and calculate the values of a, b, c, d, f , and ϕ . The EM $1-a^2$ could be used to replace σ_{ABC} or perhaps as an addition to \mathcal{E} and may prove more useful than σ_{ABC} . As far as finding the minimal EMs and showing that they are minimal, the arbitrary measurement on the DD at the end of Sec. II B may be useful since it allows us to look at the value of I_1, \dots, I_6 before and after an arbitrary measurement on an arbitrary state with far fewer parameters than if we did not take out the LU freedom. Also, it may be able to tell us the maximal probability of transforming the general complex state $|\psi\rangle$ to its conjugate state $|\bar{\psi}\rangle$ and this is a crucial piece of information that is needed to calculate ν' in Eq. (34). Unfortunately, most of these tasks involve trying to solve nontrivial equations or systems of equations with many variables, which can be difficult or even impossible.

ACKNOWLEDGMENTS

I would like to thank John Preskill for supporting me during this research and for many helpful discussions. I would also like to thank Todd Brun, Sumit Daftuar, Julia Kempe, Michael Nielsen, Federico Spedalieri, Frank Verstraete, Guifre Vidal, Anthony Sudbery, and David Whitehouse for interesting discussions. I thank S. Daftuar and D. Whitehouse in particular for assistance in proving Theorem 2.

-
- [1] J. Kempe, Phys. Rev. A **60**, 910 (1999).
 - [2] S. Hill and W. K. Wootters, Phys. Rev. Lett. **78**, 5022 (1997).
 - [3] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **80**, 5239 (1998).
 - [4] M. A. Nielsen, Phys. Rev. Lett. **83**, 436 (1999).
 - [5] G. Vidal, Phys. Rev. Lett. **83**, 1046 (1999).
 - [6] V. Coffman, J. Kundu, and W. K. Wootters, Phys. Rev. A **61**, 052306 (2000).
 - [7] C. H. Bennett *et al.*, Phys. Rev. A **63**, 012307 (2001).
 - [8] A. Wong and N. Christensen, Phys. Rev. A **63**, 044301 (2001).
 - [9] W. Dür, G. Vidal, and J. I. Cirac, Phys. Rev. A **62**, 062314 (2000).
 - [10] G. Vidal, J. Mod. Opt. **47**, 355 (2000).
 - [11] H. Carteret, A. Higuchi, and A. Sudbery, J. Math. Phys. **41**, 7932 (2000).
 - [12] A. Acin *et al.*, Phys. Rev. Lett. **85**, 1560 (2000).
 - [13] N. Linden and S. Popescu, Fortschr. Phys. **46**, 567 (1998).
 - [14] T. A. Brun and O. Cohen, Phys. Lett. A **281**, 88 (2001).
 - [15] A. Sudbery, J. Phys. A **34**, 643 (2001).
 - [16] H. Barnum and N. Linden, e-print quant-ph/0103155.
 - [17] A. Acin, A. Andrianov, E. Jane, and R. Tarrach, J. Phys. A **34**, 6725 (2001).
 - [18] A. Acin, E. Jane, W. Dür, and G. Vidal, Phys. Rev. Lett. **85**, 4811 (2000).