IOPscience iopscience.iop.org

Home Search Collections Journals About Contact us My IOPscience

Monotones and invariants for multi-particle quantum states

This article has been downloaded from IOPscience. Please scroll down to see the full text article.

2001 J. Phys. A: Math. Gen. 34 6787

(http://iopscience.iop.org/0305-4470/34/35/305)

View the table of contents for this issue, or go to the journal homepage for more

Download details:
IP Address: 171.66.16.97
The article was downloaded on 02/06/2010 at 09:12

Please note that terms and conditions apply.

INSTITUTE OF PHYSICS PUBLISHING JOURNAL OF PHYSICS A: MATHEMATICAL AND GENERAL

J. Phys. A: Math. Gen. **34** (2001) 6787–6805 PII: S0305-4470(01)26366-5

Monotones and invariants for multi-particle quantum states

H Barnum[1] **and N Linden**[2]

[1] Department of Computer Science, University of Bristol, Merchant Venturers Building, Bristol BS8 1UB, UK
[2] School of Mathematics, University of Bristol, University Walk, Bristol BS8 1TW, UK

Received 2 July 2001
Published 24 August 2001
Online at stacks.iop.org/JPhysA/34/6787

Abstract
We introduce new entanglement monotones which generalize, to the case of many parties, those which give rise to the majorization-based partial ordering of bipartite states' entanglement. We give some examples of restrictions they impose on deterministic and probabilistic conversion between multipartite states via local actions and classical communication. These include restrictions which do not follow from any bipartite considerations. We derive supermultiplicativity relations between each state's monotones and the monotones for collective processing when the parties share several states. We also investigate polynomial invariants under local unitary transformations, and show that a large class of these are invariant under collective unitary processing and also multiplicative, putting restrictions, for example, on the exact conversion of multiple copies of one state to multiple copies of another.

PACS numbers: 03.65.Ud, 03.65.Ta, 03.67-a

1. Introduction

A key goal of quantum information theory is to understand the local inter-convertibility of quantum states. That is, given two states, $|\psi_1\rangle$ and $|\psi_2\rangle$, we wish to find conditions on $|\psi_1\rangle$ and $|\psi_2\rangle$ for one to be converted into the other by local transformations. Understanding this issue is part of the more general question of characterizing what the truly different types of entangled quantum states are.

While much is known about the entanglement of bipartite quantum states, multipartite entanglement appears to have a considerably more complex structure. Many aspects of bipartite entanglement have been fully understood in terms of a relation known as majorization. This relation gives necessary and sufficient conditions for turning one pure state into another via local operations and classical communication and, when extended to mixed states via a standard 'concave roof' construction, gives necessary and sufficient conditions for converting pure bipartite states into mixed ones or ensembles of mixed ones, and

necessary conditions for general mixed-state conversion. Motivated in part by the importance of multipartite entanglement to quantum computation, in this paper we generalize these monotones to multipartite systems, implying necessary conditions on multiparty LOCC state transformations.

We also investigate aspects of polynomial invariants under local unitary transformations, in particular their relevance to collective processing by the relevant parties of several multipartite states at once.

2. Background: invariants and monotones

A state is entangled if it cannot be prepared by initially independent parties (each acting on one of the subsystems, or, as we say, acting *locally*), even if these parties may communicate classically. (We use the standard acronym LOCC for 'local operations and classical communication'.) More generally, we may say one state is more entangled than another if it cannot be prepared from the second state via LOCC. Two states are equivalent to one another, in terms of entanglement, if the two states may be reversibly interconverted by LOCC. One might wonder if there exists a single measure of entanglement: a function from states to the reals, such that a state may be converted, by LOCC, into any state with an equal or lower value of the function, but not to any state with a higher value of the function. The answer is no: no single measure of entanglement exists. There are, however, many functions with the property that no state may be converted to a state with a higher value of the function—Vidal [1] has dubbed these *entanglement monotones*. Convertibility via LOCC is obviously a partial order on the entangled states; any proposed measure of entanglement must be compatible with this partial ordering. In particular, such a monotone must be an *invariant* under local unitary transformations of the state. The theory of *polynomial* invariants[3] under actions of a group is particularly interesting, and although such invariants are not (at least not *prima facie*) guaranteed to be entanglement monotones, the close connection between local unitary invariance and entanglement, and the mathematical importance of polynomial invariants, suggest that much may be learned about entanglement by studying the equivalence classes of states having fixed values of the polynomial invariants [2]. For example, any bipartite entanglement monotone must be, on pure states $|\psi^{12}\rangle$, a function solely of the eigenvalues λ_i of the reduced density operator $\rho := \mathrm{tr}_2\, |\psi^{12}\rangle\langle\psi^{12}|$, these being invariant under local unitaries. And these eigenvalues may be recovered as the solutions of the system of d polynomial equations in the variables λ_i, $i = 1, \ldots, d$:

$$\sum_{i=1}^{d} \lambda_i^k = X_k \qquad k = 1, \ldots, d \tag{1}$$

where $X_k := \mathrm{tr}\, \rho^k$ are d polynomial invariants, each homogeneous of degree k.

Some of the polynomial invariants are themselves entanglement monotones. In fact, the d polynomial invariants just defined are increasing entanglement monotones: they increase or stay constant under LOCC. This may be proved using example II.3.5(iii) in [3]. These are not, however, complete (by complete, we mean that their nondecrease is a necessary and sufficient condition for pure-state to pure-state transitions with certainty). To see this, consider for example states $|\psi_1\rangle$ with reduced density matrix eigenvalues 0.5, 0.3, 0.2, and $|\psi_2\rangle$ with reduced density matrix eigenvalues 0.51, 0.28, 0.21. These have $(X_1, X_2, X_3) = (1, 0.38, 0.16)$ and $(1, 0.3826, 0.163\,864)$, respectively, so these invariants are nondecreasing as $|\psi_1\rangle \to |\psi_2\rangle$. This is necessary for $|\psi_1\rangle \to |\psi_2\rangle$ with certainty via LOCC, and if it were

[3] That is, polynomial functions of the quantum state.

sufficient, that transition would be possible. However, the vector (0.51, 0.28, 0.21) does not majorize (0.5, 0.3, 0.2), and this majorization is known to be necessary (cf below) for the transition in question.

Also, the elementary symmetric polynomials S_k in the eigenvalues of the reduced density matrix, as well as the ratios S_k/S_{k-1} of them, are (increasing) entanglement monotones (the proof uses example II.3.16 and exercise II.3.19 in [3]).

In quantum mechanics any measure of how mixed a density operator is can be converted into a candidate measure of how entangled a pure bipartite state is. The mixedness of the reduced density operator might be thought to measure the entanglement of the state. For example, the reduced density matrix entropy is one common measure [4]; another is the trace of the square of the reduced density matrix. Alberti and Uhlmann [5], as well as Wehrl [6, 7] and others, have extensively studied a partial ordering $\succeq$ of density matrices: $\rho \succeq \sigma$, means 'ρ is more mixed than σ', if ρ is a convex combination of unitary transforms of σ:

$$\rho = \sum_i p_i U_i \sigma U_i^\dagger. \tag{2}$$

This can be shown to be equivalent to the statement that the vector $\lambda(\rho)$, whose components are ρ's eigenvalues arranged in decreasing order, is majorized by the vector of σ's decreasingly ordered eigenvalues. An important fact about majorization is that, if a vector λ majorizes a vector μ, μ may be obtained by multiplying λ by a doubly stochastic matrix (one whose rows and columns sum to unity). Birkhoff and von Neumann showed that any doubly stochastic matrix is a convex combination of permutation matrices.

It is therefore natural to require that any reasonable measure of entanglement be compatible with the partial ordering '$\geqslant$' on pure states, defined by

$$|\psi^{12}\rangle \geqslant |\phi^{12}\rangle := \rho^1_\psi \succeq \rho^1_\phi. \tag{3}$$

(Here ρ^1_ψ and ρ^1_ϕ are the reduced density matrices of the states.) Any reasonable measure of entanglement should also satisfy that it does not increase under LOCC. If all such measures must be compatible with the above partial ordering, then it must be impossible, by LOCC, to go from one pure bipartite state to another more entangled than it is according to the ordering (3). Indeed, since the ordering (2) appears to be the whole story about whether one density operator is more mixed than another, it was also natural to conjecture that the ordering (3) is the full story with respect to whether one pure bipartite state is more entangled than another. In operational terms, this means that the condition $|\psi^{12}\rangle \geqslant |\phi^{12}\rangle$ is not only necessary, but also sufficient for converting the $|\psi^{12}\rangle$ to $|\phi^{12}\rangle$ by LOCC, and that there should be a protocol to do this conversion by making use of the Birkhoff–von Neumann decomposition in some simple way. This conjecture was proved by Nielsen [8]. While Nielsen's protocol and Hardy's [9] version of it are clearly closely related to the Birkhoff–von Neumann decomposition, Jensen and Schack's version [10] uses it most directly.

Nielsen's result implies that, for pure states on the tensor product $\boldsymbol{C}^d \otimes \boldsymbol{C}^d$, the d quantities:

$$E_k(|\psi^{12}\rangle) := \sum_{i=1}^{k} \lambda_i^{\downarrow}(\rho^1) \tag{4}$$

are *entanglement monotones*. For these quantities cannot decrease under LOCC.

The term *entanglement monotone* is sometimes reserved for quantities which cannot increase under LOCC; here we allow either nonincreasing, or nondecreasing, monotones; they are equally useful, as it is trivial to obtain one of one type from one of the other. For convenience, we will call a monotone which cannot decrease under LOCC an *increasing* entanglement monotone, and one which cannot increase under LOCC a *decreasing* entanglement monotone.

In the remainder of this paper, we will investigate some generalizations of the majorization-derived monotones, and of some polynomial invariants under local unitaries, to multipartite systems. In particular, we will examine multiplicativity of such quantities when a given set of parties has several, independent, shared states upon which they may operate. While the generalizations of the majorization monotones will be supermultiplicative (their multiplicativity remaining an open question), some cases for which multiplicativity holds will be investigated. A large class of the polynomial invariants will, on the other hand, be shown to be multiplicative. Multiplicativity is an important property in investigating transformations between many copies of a given state, both for a finite number of copies and in the asymptotic limit in which the rate of conversion of multiple copies of one state into another is of interest.

3. Multipartite monotones

3.1. Definition of the monotones

How might we generalize the majorization-derived monotones to multipartite systems? There is a well known variational characterization [11] of the sums Σ_k of the k largest eigenvalues of an operator as $\Sigma_k(\rho) = \max_{\text{rank-}k \text{ projectors } P} \operatorname{tr} P\rho$. We may use this to characterize the bipartite quantities E_k by

$$E_k(|\psi^{12}\rangle) \equiv \max_{\text{rank-}k \text{ projectors } P} ||I \otimes P|\psi^{12}\rangle||^2. \tag{5}$$

We propose to generalize this definition of the bipartite quantities to multipartite systems, in the following way.

Definition 1. *For an N-partite quantum system in a (not necessarily normalized) pure state $|\psi^{123\ldots N}\rangle$, define*

$$E_{k_1,k_2,\ldots,k_N}(|\psi^{123\ldots N}\rangle) := \max_{\Gamma_1,\ldots,\Gamma_N} ||\Gamma_1 \otimes \cdots \Gamma_N|\psi^{123\ldots N}\rangle||^2 \tag{6}$$

where each of Γ_i is a k_i-dimensional projector in system i.

This is the squared norm of the maximal projection of the state onto a tensor product of local subspaces having dimensions $k_1, \ldots, k_N$. The integers k_i may range from 1 to d_i, the dimension of the ith party's Hilbert space. To reduce clutter we will sometimes write the 'multi-index' $\mathbf{k}$ for $k_1, \ldots, k_N$. For every $E_{\mathbf{k}}$, its maximal value on the set of pure states with squared norm equal to X is just X; thus the maximal value for normalized states is 1, and is attained on pure product states. Note that some non-product states may also have $E_{\mathbf{k}} = 1$ for some $\mathbf{k}$. However, only product states can have $E_{111\ldots1} = 1$.

Observation 2. *$E_{k_1,\ldots,k_N}(|\psi^{1,\ldots,N}\rangle)$ are invariant under local unitary transformations of $|\psi^{1,\ldots,N}\rangle)$.*

This is immediate from (6). Explicitly

$$\begin{aligned} &E_{k_1,\ldots,k_N}(U_1 \otimes \cdots \otimes U_N|\psi^{123\ldots N}\rangle) \\ &\quad = \max_{\Gamma_1,\ldots,\Gamma_N} \langle\psi^{123\ldots N}|U_1^\dagger \otimes \cdots \otimes U_N^\dagger(\Gamma_1 \otimes \cdots \Gamma_N)U_1 \otimes \cdots \otimes U_N|\psi^{123\ldots N}\rangle \\ &\quad = \max_{\Gamma_1,\ldots,\Gamma_N} \langle\psi^{123\ldots N}|(U_1^\dagger\Gamma_1 U_1 \otimes \cdots \otimes U_N^\dagger\Gamma_N U_N)|\psi^{123\ldots N}\rangle. \end{aligned} \tag{7}$$

For any set of Γ_i and initial state $|\psi\rangle$ the same value of the maximand will be achieved with the local unitarily transformed state and the projectors transformed by the inverse; these are also projectors of the same rank, so the maximum over all local projectors is the same for both initial states.

One might consider the analogous definition, but with Γ_i replaced by rank-k_i partial isometries. A rank-k partial isometry may be written as ΓU, where U is unitary and Γ is a rank-k projector. Therefore this would define the same quantities, by the same argument just used for unitary invariance. Explicitly, this definition would be

$$\tilde{E}_{k_1,k_2,\ldots,k_N} := \max_{R_1,\ldots,R_N} ||R_1 \otimes \cdots R_N|\psi^{123\ldots N}\rangle||^2 \tag{8}$$

where R_i are partial isometries with ranks k_i.

We extend these monotones to mixed states via the usual 'concave roof' device of defining the mixed state quantity to be the maximum of the average of the pure state quantity, over ensembles of pure states for the mixed state in question:

$$E_{k_1,\ldots,k_N}(\rho) := \max_{\{|\psi_i\rangle\}_i:\sum_i |\psi_i\rangle\langle\psi_i|=\rho} \sum_i E_{k_1,\ldots,k_N}(|\psi_i\rangle). \tag{9}$$

For normalized mixed states, the maximum of $E_{\mathbf{k}}$ is achieved at separable states, with $E_{\mathbf{k}} = 1$. Again, while some entangled states may have some $E_{\mathbf{k}} = 1$, only separable states can have $E_{111\ldots11} = 1$.

Extend each monotone $E_{\mathbf{k}}$ to *ensembles* $\{p_i, \rho_i\}_i$ of states via $E_{\mathbf{k}}(\{p_i, \rho_i\}_i) := \sum_i p_i E_{\mathbf{k}}(\rho_i)$. Note that the monotones are linearly homogeneous in the density operators:

$$E_{\mathbf{k}}(\lambda\rho) = \lambda E_{\mathbf{k}}(\rho). \tag{10}$$

This has the consequence that we may represent an ensemble $\{p_i, \rho_i\}_i$ by the subnormalized operators $\tilde{\rho}_i$, with $\mathrm{tr}\,\tilde{\rho}_i = p_i$, and then the ensemble average of the monotone is just $\sum_i E_{\mathbf{k}}(\tilde{\rho}_i)$. This representation of ensembles by sequences of unnormalized density operators is useful because the arguments we use will often involve successively finegraining an ensemble, in which case it is slightly cumbersome to renormalize and keep track of the probabilities introduced at each step.

Throughout the paper we use a notation in which sets or ensembles may be referred to by expressions with curly braces around them, such as $\{|\psi_{ij}\rangle\}_i$. Some indices in the expression within braces (i, in our example) also appear as subscripts of the right-hand brace: this indicates that the set consists of all the values taken by the expression within the braces as these indices vary. If there are also 'free' indices (like j in our example) in the expression within the braces, which do not appear as subscripts of the right-hand brace, the overall expression including braces and subscripts ranges over *different* sets or ensembles as these free indices vary. Thus $\{|\psi_{ij}\rangle\}_i$ refers to the jth ensemble of some set of ensembles indexed by j. Each of these ensembles consists of the states $|\psi_{ij}\rangle$ for all values of i. When we view this as an ensemble, we take the probability for each state to be given by its squared norm $|||\psi_{ij}\rangle||^2$. The point of this notation is just to make it clear, when we are considering many ensembles at once, which indices identify the ensemble, and which identify the states within each ensemble. (A similar notation is sometimes used by mathematicians to specify matrices by their matrix elements or tensors by their components, to distinguish indices specifying which component of a tensor from indices specifying which tensor.)

The following observation partly explains the terminology 'concave roof'.

Observation 3 (Concave roofs are concave). *Let*

$$R(\rho) := \max_{\{|\psi_i\rangle\}_i:\sum_i |\psi_i\rangle\langle\psi_i|=\rho} \sum_i Q(|\psi_i\rangle). \tag{11}$$

Then $R(\rho)$ is concave in ρ, i.e.

$$\sum_k R(\rho_k) \leqslant R\left(\sum_k \rho_k\right). \tag{12}$$

Proof. Define Q on pure-state ensembles by $Q(\{|\psi_i\rangle\}_i) := \sum_i Q(|\psi_i\rangle)$. We do the case $k \in \{1, 2\}$; the general case follows by a trivial induction or by the same proof with wider-ranging indices. Consider states ρ_1, ρ_2, and pure-state ensembles $\Upsilon_1 = \{|\psi_i^1\rangle\}_i$ and $\Upsilon_2 = \{|\psi_i^2\rangle\}_i$ for ρ_1, ρ_2, respectively. The ensemble made from the states of both ensembles, $\Upsilon := \{|\psi_i^k\rangle\}_{k,i}$, is a pure-state ensemble for $\rho_1 + \rho_2$. Now, $Q(\Upsilon) = Q(\Upsilon_1) + Q(\Upsilon_2)$ from the definition, so if Υ_1 and Υ_2 achieve the maximum in (11), then $Q(\Upsilon) := R(\rho_1) + R(\rho_2)$. But as Υ is a pure-state ensemble for $\rho := \rho_1 + \rho_2$, by (11) $R(\rho)$ cannot be less than $Q(\Upsilon)$. □

To help the reader get used to our notation for ensembles, using unnormalized states, we record for comparison the more standard way of writing concavity, with ensembles of normalized states and explicit probabilities:

$$\sum_i p_i R(\hat{\rho}_i) \leqslant R\left(\sum_i p_i \hat{\rho}_i\right). \tag{13}$$

It follows from observation 3 that $E_{k_1,\ldots,k_N}$ are concave. $E_{k_1,\ldots,k_N}$ are candidates for (increasing) multipartite entanglement monotones. They generalize the bipartite case.

Proposition 4. *For a bipartite system, pure states $|\psi^{12}\rangle$ satisfy*

$$E_{k_1,k_2}(|\psi^{12}\rangle) = E_{k_2,k_1}(|\psi^{12}\rangle) = \sum_{i=1}^{\min(k_1,k_2)} \lambda_i(\rho_1). \tag{14}$$

(Recall that $\lambda_i(\rho)$ is the ith decreasingly ordered eigenvalue of ρ.) The proof makes interesting use of some tools which are useful in many places in quantum information theory; to avoid interrupting the flow of our exposition, it appears in an appendix.

3.2. Demonstrating monotonicity

Vidal [12] gave succinct necessary and sufficient conditions for a quantity to be an increasing entanglement monotone. Such a quantity must be *concave*, and *increasing under unilocal operations*. Concavity means that if we throw away information about which state of the ensemble we have, the expected entanglement decreases (the monotone increases):

$$M(\{|\psi_{ij}\rangle\}_{ij}) \leqslant \sum_i M\left(\left\{\sum_j |\psi_{ij}\rangle\langle\psi_{ij}|\right\}_i\right). \tag{15}$$

Increase under unilocal operations means that under any set of quantum operations $\mathcal{A}_m$ on one subsystem which sum to a trace-nonincreasing operation $\mathcal{A} = \sum_m \mathcal{A}_m$, we have

$$M(\rho) \leqslant \sum_m M(\mathcal{A}_m(\rho)). \tag{16}$$

(Each of the $\mathcal{A}_m$ is assumed to act nontrivially on the *same* party's subsystem, and only on that subsystem.) We have already shown, in observation 3, that $E_{k_1,\ldots,k_N}$ are concave. They are also increasing under unilocal operations:

Proposition 5. *$E_{k_1,\ldots,k_N}$ increases or remains constant under unilocal quantum operations.*

Proof. The most general objects on which our monotones E are defined are ensembles of (possibly mixed) states. Consider an ensemble of unnormalized states ρ_i; then $E_{\mathbf{k}}(\{\rho_i\}_i) := \sum_i E_{\mathbf{k}}(\rho_i)$. To show that this increases under unilocal operations, it suffices to show that $E_{\mathbf{k}}(\rho_i)$ does so for each i. We therefore suppress the index i and consider a single mixed input

state ρ. Let $\{\mathcal{A}_m\}_m$ be a unilocal set of operations, which we take WLOG to be on system N. We wish to show that

$$E_{\mathbf{k}}(\rho) \leqslant \sum_m E_{\mathbf{k}}(\mathcal{A}_m(\rho)). \tag{17}$$

Each $\mathcal{A}_m$ has a Hellwig–Kraus decomposition A_{ms} with s taking a finite number of values, so that $\mathcal{A}_m(\rho) = \sum_s A_{ms}\rho A_{ms}^\dagger$. By concavity,

$$\sum_{ms} E_{\mathbf{k}}(A_{ms}\rho A_{ms}^\dagger) \leqslant \sum_m E_{\mathbf{k}}\left(\sum_s A_{ms}\rho A_{ms}^\dagger\right). \tag{18}$$

Therefore, we will show monotonicity under sets $\{\mathcal{A}_j\}_j$ of 'one-operator' unilocal operations, for which each $\mathcal{A}_j$ corresponds to a single operator A_j. For, taking j to be the double index ms in (18), monotonicity under sets of general unilocal operations will follow from monotonicity under sets of one-operator unilocal operations and (18). To show monotonicity under one-operator sets of unilocal operations, let $\{|\psi_i^{\max}\rangle\}_i$ be a pure-state ensemble for ρ which achieves the maximum in the convex roof expression

$$E_{k_1,\ldots,k_N}(\rho) := \max_{\{|\psi_i\rangle\}_i:\sum_i |\psi_i\rangle\langle\psi_i|=\rho} \sum_i E_{k_1,\ldots,k_N}(|\psi_i\rangle). \tag{19}$$

Under unilocal operations $\mathcal{A}_j$, each with one Hellwig–Kraus operator A_j on the Nth system, we have

$$\rho \to \{A_j\rho A_j^\dagger\}_j =: \{\rho_j\}_j. \tag{20}$$

Suppose that $\hat{\Gamma}_1^i, \ldots, \hat{\Gamma}_N^i$ achieves the maximum, for the initial state $|\psi_i^{\max}\rangle$, in the definition (6) of $E_{\mathbf{k}}$. Define

$$|\tilde{\psi}_i\rangle := \hat{\Gamma}_1^i \otimes \hat{\Gamma}_2^i \otimes \cdots \hat{\Gamma}_{N-1}^i |\psi_i^{\max}\rangle. \tag{21}$$

Then

$$E_{k_1,\ldots,k_N}(|\tilde{\psi}_i\rangle) = \max_{\Gamma_N^i} \left|\Gamma_N^i|\tilde{\psi}_i\rangle\right|^2 = E_{k_N}(|\tilde{\psi}_i'\rangle) \tag{22}$$

where $|\tilde{\psi}_i'\rangle$ is $|\tilde{\psi}_i\rangle$ considered as the state of a bipartite system in which systems $1, \ldots, N-1$ are viewed as a single quantum system, tensored with system N. By the definition (21) of $|\tilde{\psi}_i\rangle$

$$E_{\mathbf{k}}(\rho) = \sum_i E_{k_1,\ldots,k_N}(|\tilde{\psi}_i\rangle). \tag{23}$$

By (22), this is equal to

$$\sum_i E_{k_N}(|\tilde{\psi}_i'\rangle) \leqslant \sum_{ij} E_{k_N}(A_j|\tilde{\psi}_i'\rangle) \tag{24}$$

where the inequality is due to the monotonicity of the bipartite monotones E_k [13]. Inserting the definition of these bipartite monotones, the right-hand side is

$$\sum_{ij} \max_{\Gamma_N^{ij}} \left|\Gamma_N^{ij} A_j|\tilde{\psi}_i'\rangle\right|^2. \tag{25}$$

Using the definitions of $|\tilde{\psi}_i'\rangle$ and $|\tilde{\psi}_i\rangle$ gives

$$\sum_{ij} \max_{\Gamma_N^{ij}} \left|\hat{\Gamma}_1^i \otimes \cdots \otimes \hat{\Gamma}_{N-1}^i \otimes \Gamma_N^{ij} A_j|\psi_i^{\max}\rangle\right|^2 \tag{26}$$

which is less than or equal to

$$\sum_{ij} \max_{\Gamma_1^{ij},\ldots,\Gamma_N^{ij}} \left|\Gamma_1^{ij} \otimes \cdots \otimes \Gamma_{N-1}^{ij} \otimes \Gamma_N^{ij} A_j|\psi_i^{\max}\rangle\right|^2$$

(with Γ^{ij} constrained to have the ranks k_i) since we have just widened the domain of maximization. By the definition of $E_{\mathbf{k}}$, this is equal to

$$\sum_{ij} E_{\mathbf{k}}(A_j|\psi_i^{\max}\rangle) = E_{\mathbf{k}}(\{A_j|\psi_i^{\max}\rangle\}_{ij}). \tag{27}$$

We now note that $\{A_j|\psi_i^{\max}\rangle\}_i$ (for fixed j) is an ensemble for ρ_j, hence by the concavity of $E_{\mathbf{k}}$

$$E_{\mathbf{k}}(\{A_j|\psi_i^{\max}\rangle\}_{ij}) \leqslant E_{\mathbf{k}}(\{\rho_j\}_j) \tag{28}$$

as required. □

The conjunction of proposition 5 and the concavity of $E_{\mathbf{k}}$ gives

Theorem 6. *$E_{\mathbf{k}}$ are entanglement monotones.*

When analysing particular multipartite states, we should remember that this definition of monotones gives us not only the monotones explicitly mentioned in definition 6, but also all the monotones given by the same definition, but with some subsets of the set of systems grouped and considered as single systems, and definition 6 applied to this 'coarsegrained' party structure. These are also monotones under LOCC with respect to the finegrained party structure, since operations local with respect to the finegrained structure are also local with respect to the coarser one. (Some obvious inequalities therefore hold between monotones and the coarse-grainings of them.) An example of this construction is the frequent practice of grouping the parties into two disjoint sets, and applying bipartite monotones to the resulting bipartite structure, when studying multipartite states. Note, however, that while our multipartite monotones include all such bipartite monotones based on majorization of the reduced density matrix of some set of parties, they also include, as we will show in section 6, irreducibly multipartite monotones giving us information not provided by the majorization-based monotones studied by Nielsen and Vidal.

4. Collective processing and multiplicativity

Suppose we have two multiparty states, $|\psi^X\rangle$ and $|\chi^Y\rangle$, on Hilbert spaces X and Y each composed of subsystems $1, \ldots, N$ held by N different parties. Thus $X = X^1 \otimes X^2 \otimes \cdots \otimes X^N$, and similarly for Y, but there is no assumption that X^i and Y^i are isomorphic. For the purposes of multipartite LOCC protocols, party i may operate on his part of both the X and the Y systems; in other words, *arbitrary* operations by i on $X^i \odot Y^i$ are considered local operations in this framework[4]. We will refer to such operations, and their obvious generalization to more than two states shared by the same set of parties, as *collective* processing of the states (of $|\psi^X\rangle$ and $|\chi^Y\rangle$, in the two-state case).

The question of collective processing is important for a number of reasons. Firstly it is known that collective processing is needed, in general, to distill entanglement from quantum states. Specifically, given a quantum state, one may wish to perform (LOCC) operations on it so that there is some probability that one of the outcomes of the measurements has more entanglement than the initial state (of course one cannot increase the average entanglement of the outcomes). It has been shown, however, [14] that, in general, entanglement distillation is not possible if one only has one copy of a qubit state, even though with collective processing of more than one copy of the same state, distillation is possible. Secondly, in order to extract

[4] If we have two states ρ_1 and ρ_2 we will denote their tensor product $\rho_1 \odot \rho_2$; the aim of this notation is to reinforce the fact that this is not the tensor product of the Hilbert spaces of the parties (for which we will use the usual notation $\otimes$).

the maximum possible entanglement from a pure bipartite state (i.e. the local entropy of one of the parties) one needs collective processing [15].

When using monotones or invariants to investigate collective processing, it is important to know about the behaviour of the quantities in question under the tensor product $\odot$ of different states of the same parties. If the quantities are additive or multiplicative, this makes their application to collective processing much simpler, as they may be evaluated for the individual states, and from this one obtains their values for many copies of the same state, or for the combination of several copies of each of several different types of state.

The monotones $E_{k_1,\ldots,k_N}$ are supermultiplicative in the sense given by the following proposition.

Proposition 7 (Supermultiplicativity).

$$E_{k_1,\ldots,k_N}(|\psi^X\rangle)E_{l_1,\ldots,l_N}(|\chi^Y\rangle) \leqslant E_{k_1l_1,\ldots,k_Nl_N}(|\psi^X\rangle \odot |\chi^Y\rangle). \tag{29}$$

The proof of this proposition is immediate from the definition of these monotones: one need only note that the product of a rank-k_i projector $P_{k_i}^{X_i}$ on X^i and a rank-l_i projector $Q_{l_i}^{Y_i}$ on Y^i is a rank-k_il_i projector on $X^i \odot Y^i$, and therefore the value $E_{k_1,\ldots,k_N}(|\psi^X\rangle)E_{l_1,\ldots,l_N}(|\chi^Y\rangle)$ is achievable in the maximization defining $E_{k_1l_1,\ldots,k_Nl_N}(|\psi^X\rangle \odot |\chi^Y\rangle)$. It is far from obvious, however, that the two quantities in the above proposition are equal, i.e. that multiplicativity holds. It may be that projectors which do not have a product structure with respect to the $X \odot Y$ tensor factorization can achieve a higher projection. (Werner and coworkers, however, have numerically investigated some cases of the maximum modulus-squared inner product with a pure product (with respect to the party structure) state, in other words, cases of $E_{1,1,\ldots,1}$, and have not found violations of multiplicativity [16].)

In some special cases, it is easy to show multiplicativity.

Proposition 8. *For monotones $E_{k_1,\ldots,k_N}$ and states $|\psi\rangle$ and $|\chi\rangle$ for which the reduced density matrix of each state onto the systems with less-than-full-rank k_i is maximally mixed, we* do *have multiplicativity, i.e. equality in (29).*

Proposition 9. *When we tensor an entangled state of all parties with a product state $|\nu\rangle$ of all parties, the optimal projector may be decomposed as $Q_{k_1} \otimes \cdots \otimes Q_{k_N} = |\nu\rangle\langle\nu| \odot P_{k_1} \otimes \cdots \otimes P_{k_N}$. This implies that the value of our monotones is unchanged by tensoring with a product pure state.*

This proposition must hold for any entanglement monotone, as the operations of adjoining or discarding $|\nu\rangle$ are both LOCC. In the case of our monotones, we can also use proposition 7 and the fact that the monotones are equal to 1 on separable states, plus just the fact that adjoining $|\nu\rangle$ is LOCC.

5. Applications of the monotones

It seems likely that for each multipartite Hilbert space (each number of parties N and set of dimensions $d_1, \ldots, d_N$), there exist many fundamentally distinct types of entanglement. This statement may be taken in various senses. For example, one case in which we might wish to say that two states have fundamentally different types of entanglement is when neither one can be transformed into the other with certainty via LOCC. We say they are incommensurable under deterministic LOCC (DLOCC, for short). If neither one can be transformed into the other with finite probability (i.e., the parties are not guaranteed to succeed, but there is a finite probability of success and they know when they have succeeded), this is a stronger sense in

which the states exhibit fundamentally different types of entanglement: we will say they are incommensurable under SLOCC (the S is for stochastic). Dür *et al* [17] define two states to be equivalent under SLOCC when there is nonzero probability for a transition in both directions (this is an equivalence relation). (Note, however, that the relation of incommensurability under SLOCC defined above need not be an equivalence relation; while symmetric, it is not obviously transitive. Nor, of course, is it the complement of Dür *et al*'s SLOCC equivalence.) Another sense, stronger still, is if there is no nonzero asymptotic rate R at which C_1 copies of one state $|\psi\rangle$ ($|\chi\rangle$) can be LOCC-transformed into C_2 copies of the other state $|\chi\rangle(|\psi\rangle)$, in the limit in which $C_1, C_2 \to \infty$, $C_1/C_2 \to R$, and the fidelity of the transformed state to the target state $|\chi\rangle^{\otimes C_2}$ ($|\psi\rangle^{\otimes C_1}$) approaches one. The monotones $E_{\mathbf{k}}$ give direct information on the first two questions, and if their multiplicativity properties discussed in section 4 can be understood, or at least controlled for some examples as $C_1, C_2 \to \infty$, then they may yield information on the third as well.

To this end, one would like to calculate the monotones for interesting multipartite states, hoping to find examples of pairs of states ranked in the reverse order by two of the $E_{\mathbf{k}}$. This implies they are DLOCC-incommensurable. SLOCC may be investigated using the following observation.

Proposition 10.

$$\mathrm{prob}(|\psi\rangle \to |\chi\rangle) \leqslant \frac{1 - E_{\mathbf{k}}(|\psi\rangle)}{1 - E_{\mathbf{k}}(|\chi\rangle)}. \tag{30}$$

Proof. Suppose $|\psi\rangle \to |\chi\rangle$ via LOCC with probability p. Then $|\psi\rangle$ goes to some ensemble Υ containing the state $\sqrt{p}|\chi\rangle$. $E_{\mathbf{k}}(|\psi\rangle) \leqslant E_{\mathbf{k}}(\Upsilon) \leqslant (1-p) + pE_{\mathbf{k}}(|\chi\rangle)$ (the first inequality is from the fact that E is a monotone, and the second is from the fact that the largest value of E for an ensemble containing $|\chi\rangle$ with probability p occurs where all the other states are separable). Algebra gives the proposition. □

This is the same argument already used by Vidal for bipartite monotones. Note that $1 - E_{\mathbf{k}}$ are *decreasing* entanglement monotones. Also, the RHS of (30) can be greater than 1 for some monotones and states. This is not a problem, it merely means that the monotone in question imposes no restriction on SLOCC transformations of the states in question. (Other monotones may, however.)

Corollary 11. *If $E_{\mathbf{k}}(|\psi\rangle) = 1$ while $E_{\mathbf{k}}(|\chi\rangle) \neq 1$ for some $E_{\mathbf{k}}$, then $|\psi\rangle$ may not be converted into $|\chi\rangle$ via SLOCC.*

6. Examples

As an example of our monotones in action, we consider some simple tripartite states known to have irreducibly tripartite entanglement, the states $|W\rangle := 1/\sqrt{3}(|001\rangle + |100\rangle + |010\rangle$ [17] and $|\mathrm{GHZ}\rangle := 1/\sqrt{2}(|000\rangle + |111\rangle)$. We compare them to states with only bipartite entanglement, such as the tensor product of a Bell state of two parties with a pure state for the third party.

- GHZ state: $E_{2,1,1} = E_{1,2,1} = E_{1,1,2} = 1/2$; $E_{1,1,1} = 1/2$;
  $E_{2,1,1}$ (or any permutation) $= 1/2$.
- Singlet for parties 1 and 2 tensored with a pure state for party 3:
  $E_{2,1,1} = E_{1,2,1} = E_{1,1,2} = 1/2$;
  $E_{1,1,1} = 1/2$; $E_{1,2,2} = E_{2,1,2} = 1/2$; $E_{2,2,1} = 1$.

Even taken together, the values of $E_{2,1,1}$ and permutations, and of $E_{1,1,1}$, do not differentiate between the GHZ and the singlet. Of course, $E_{2,2,1}$ does differentiate between these cases.

Thus, in the case of Bell versus GHZ, the only one of our multipartite monotones which distinguishes the two kinds of state is essentially bipartite in nature. One might worry that the new multipartite monotones never provide any interesting information about state transformations which does not stem from bipartite considerations. This worry would be unjustified, as a comparison of the $|\mathrm{GHZ}\rangle$ and $|W\rangle$ states shows.

We have:

- $|W\rangle$: $E_{2,1,1} = 1/3$; $E_{1,1,1} = 4/9$; $E_{2,2,1}$(or any permutation) $= 2/3$.

$E_{2,2,1}$ tells us that a $|W\rangle$ cannot go to a $|\mathrm{GHZ}\rangle$ via DLOCC. This involves only bipartite considerations. But $E_{1,1,1}$ tells us, in addition, that a $|\mathrm{GHZ}\rangle$ cannot go to a $|W\rangle$. This is not forbidden by bipartite considerations. So, the multipartite monotones we have defined cannot all be just monotonic functions of the bipartite ones. Rather, they give us further, irreducibly multipartite, information about which state transformations are possible via multipartite LOCC. In fact, proposition 30 lets us use the multipartite monotones to bound the probabilities for conversion via SLOCC: $p \leqslant 2/3$ (from $E_{2,2,1}$) for $|W\rangle \to |\mathrm{GHZ}\rangle$, $p \leqslant 3/4$ (from $E_{2,1,1}$) for $|\mathrm{GHZ}\rangle \to |\mathrm{W}\rangle$.

We know from the work of Dür *et al* [17] that neither of these probabilities can be nonzero, so the bounds are not tight. So the nondecrease of these monotones, even considered all together, is not a sufficient condition for multipartite SLOCC. This despite the fact that they generalize, in a way that does give further irreducibly multipartite constraints on SLOCC, a set of bipartite monotones whose nonincrease *is* known to be a necessary and sufficient condition even for SLOCC.

7. Invariants

In the rest of this paper, we introduce polynomial invariants for simultaneous collective processing of more than one quantum state of N parties. In order to explain these invariants, it will be helpful to first recall some information about invariants for processing of single quantum states.

There has been much written about the situation when N parties share a single quantum state $|\psi\rangle$ and the Hilbert space of each party is a qubit. A useful tool for analysing this case is invariant theory [2]. Thus it is known that there is an infinite set of polynomial functions of the state, each of which is invariant under local unitary transformations. If two N-party states have different values of any invariant polynomial, then they are not transformable into each other by local unitary transformations. For comparison with what follows it is useful to give an explicit example here. So consider the case $N = 3$. A general pure state $|\psi\rangle$ may be written as

$$|\psi\rangle = \sum_{i,j,k=1}^{2} \psi_{ijk}|i\rangle|j\rangle|k\rangle. \tag{31}$$

It is useful to think of arranging the set of polynomial invariants in order of increasing degree in the state $|\psi\rangle$. Some of the invariants of low degree are

$$I_2 = \sum_{i,j,k=1}^{2} \psi_{ijk}\psi^*_{ijk} \tag{32}$$

$$I_4^{(1)} = \sum_{i,j,k,m,n,p=1}^{2} \psi_{ijk}\psi^*_{imn}\psi_{pmn}\psi^*_{pjk} \tag{33}$$

$$I_4^{(2)} = \sum_{i,j,k,m,n,p=1}^{2} \psi_{jik}\psi^*_{min}\psi_{mpn}\psi^*_{jpk} \tag{34}$$

$$I_4^{(3)} = \sum_{i,j,k,m,n,p=1}^{2} \psi_{jki}\psi^*_{mni}\psi_{mnp}\psi^*_{jkp} \tag{35}$$

$$I_4^{(4)} = \sum_{i,j,k,m,n,p=1}^{2} \psi_{ijk}\psi^*_{ijk}\psi_{mnp}\psi^*_{mnp} \tag{36}$$

$$I_6 = \sum_{i,j,k,m,n,p=1}^{2} \psi_{ijk}\psi^*_{imn}\psi_{pqn}\psi^*_{pjs}\psi_{rms}\psi^*_{rqk}. \tag{37}$$

The lower index on the invariant indicates the degree in $|\psi\rangle$, the upper index is used to distinguish between invariants of the same degree. Sums and products of invariants are clearly also invariant (the set of polynomial invariants forms a ring).

The above invariants have been constructed by contracting each local index with the invariant tensor δ_{ij} of $U(2)$, in such a way that a ψ index is always contracted with a ψ^* index; e.g. I_2 may be written

$$I_2 = \sum_{i_1,j_1,k_1,i_2,j_2,k_2=1}^{2} \psi_{i_1j_1k_1}\psi^*_{i_2j_2k_2}\delta_{i_1i_2}\delta_{j_1j_2}\delta_{k_1k_2}. \tag{38}$$

When an invariant is written this way, we will say it is *in simple form*. Not all polynomial invariants can be written in simple form; those which can, we will call *simple*. Of course, even simple invariants can also be written in forms which are not simple.

Another interesting invariant is the residual tangle [18]. Its definition is

$$T := 2\left|\sum_{i,j,k,m,n,p,q.i',j',k',m',n',p'} \psi_{ijk}\psi_{i'j'm}\psi_{npk'}\psi_{n'p'm'}\epsilon_{ii'}\epsilon_{jj'}\epsilon_{kk'}\epsilon_{mm'}\epsilon_{nn'}\epsilon_{pp'}\right| \tag{39}$$

where ϵ_{ij} is the antisymmetric invariant tensor of $SU(2)$ (the fact that we take the modulus of the expression means that it is invariant under $U(2)$). T is not a polynomial in ψ and ψ^*. However its square is a polynomial, and it may be written as a sum of simple terms involving the invariant tensor δ. This may be done by using the relation $\epsilon_{ii'}\epsilon_{jj'} = \delta_{ij}\delta_{i'j'} - \delta_{ij'}\delta_{i'j}$. If we pair ϵ from the ψ terms with ϵ from the ψ^* terms (which are absent from within the modulus in (39), but are introduced—along with twelve new indices and the removal of the modulus—when (39) is squared), the expression will (when multiplied out) be a sum of simple invariant terms, as claimed. Explicitly:

$$\begin{aligned} T^2 = 4\sum \psi_{ijk}\psi_{i'j'm}\psi_{npk'}\psi_{n'p'm'}\psi^*_{IJK}\psi^*_{I'J'M}\psi^*_{NPK'}\psi^*_{N'P'M'} \\ \times(\delta_{iI}\delta_{i'I'} - \delta_{iI'}\delta_{i'I})(\delta_{jJ}\delta_{j'J'} - \delta_{jJ'}\delta_{j'J}) \\ \times(\delta_{kK}\delta_{k'K'} - \delta_{kK'}\delta_{k'K})(\delta_{mM}\delta_{m'M'} - \delta_{mM'}\delta_{m'M}) \\ \times(\delta_{nN}\delta_{n'N'} - \delta_{nN'}\delta_{n'N})(\delta_{pP}\delta_{p'P'} - \delta_{pP'}\delta_{p'P}). \end{aligned} \tag{40}$$

(Possibly there are other similar expressions for T^2, which cannot be matched with this one term-by-term by renaming dummy indices, arising through different pairings of ϵ when applying the ϵ–δ identity.)

General theorems from invariant theory imply that any polynomial invariant may be written, as we have done with T^2, as a sum of simple invariants. Each simple invariant is a product of equal numbers of ψ and ψ^* with all the local indices for a given party contracted (pairing ψ-indices with ψ^*-indices) using the invariant tensor δ_{ij}; also any such polynomial is invariant (see [2] for further details). It is also known how to calculate a generating function (the

Molien series) for the number of linearly independent invariants of each degree. The simple invariants will turn out to be particularly interesting when we come to consider collective processing of more than one state below. Note, however, that the squared tangle is not written in simple form above. We believe that it cannot be written in simple form, and thus is not simple.

An alternative way of writing the above invariants which will be useful below is using an 'index-free' notation. Let us write $|\psi\rangle\langle\psi|$ as ρ; we also find it helpful now to label the parties A, B, C. Then the above invariants may be written as

$$I_2 = \mathrm{Tr}_{ABC}\,\rho \tag{41}$$

$$I_4^{(1)} = \mathrm{Tr}_{BC}[\mathrm{Tr}_A\,\rho]^2 \tag{42}$$

$$I_4^{(2)} = \mathrm{Tr}_{AC}[\mathrm{Tr}_B\,\rho]^2 \tag{43}$$

$$I_4^{(3)} = \mathrm{Tr}_{AB}[\mathrm{Tr}_C\,\rho]^2 \tag{44}$$

$$I_4^{(4)} = (\mathrm{Tr}_{ABC}\,\rho)^2 \tag{45}$$

$$I_6 = \mathrm{Tr}_{ABC}[1_A \otimes \mathrm{Tr}_A\,\rho][1_B \otimes \mathrm{Tr}_B\,\rho][1_C \otimes \mathrm{Tr}_C\,\rho]. \tag{46}$$

In the expressions above Tr_{AB} denotes the trace over the Hilbert space for the first and second parties and the symbol 1_A means the 2×2 identity operator on the first Hilbert space.

Of course, not all the infinitely many invariants are independent of each other (for example $I_4^{(4)} = (I_2)^2$). The Hilbert basis theorem states that, for any ring of invariants of interest to us, there exists a finite basis of the ring (i.e. any invariant may be written as a sum of products of elements of the basis, and the number of elements in this basis is finite). Thus in checking whether two states are locally equivalent, one only needs to check whether the elements of basis have equal values when evaluated for the two states. Unfortunately there is no simple procedure for calculating the basis for any given example. Thus, while the basis is simple to find for $N = 2$ parties (in fact, for any dimension of local Hilbert space, not just qubits), and a basis for the case $N = 3$ has been reported [19], the basis is not known for more parties, as far as we are aware. Nonetheless, knowing the invariants of low degree can still be very useful in applications (see e.g. [20] and below).

8. Collective processing and multiplicative invariants

We now turn to the case that the N parties share not one quantum state but a number C: $\{|\psi_1\rangle, |\psi_2\rangle, \ldots |\psi_C\rangle\}$, and we increase the types of operation the parties are allowed to do to include unitary processing of all these copies together. A particularly interesting case is when all states are copies of a single state, but most of what we will have to say is applicable to the more general case in which the states are different. We will continue to use the notation $\odot$, introduced in section 4, for the tensor product of different state spaces belonging to the same set of parties, and of states belonging to these different state spaces. Recall that *collective* processing of states refers to the possibility that each party's local operations may be 'nonlocal' with respect to the tensor product structure $\odot$: that is, the different states shared by the same parties may all be processed together, though still locally with respect to the party structure.

In the case of bipartite systems there is a well known function, the local entropy $S(\rho) = -\mathrm{Tr}_B\left[\mathrm{Tr}_A\,[\rho]\log \mathrm{Tr}_A\,[\rho]\right]$ which is invariant under collective processing; it is also additive, namely $S(\rho_1 \odot \rho_2) = S(\rho_1) + S(\rho_2)$. Our aim here is to show that there is a large class of polynomial functions for multi-party systems which are invariant under collective unitary transformations, and which are multiplicative (hence their logarithms, when defined, are additive).

The most general form of collective processing allows general LOCC transformations on multiple copies. As a step towards understanding this general case we will discuss what can be said about processing with collective *unitary* transformations. To be explicit let us first consider qubit states and consider pure states of three parties (extensions to more parties and states of higher-dimensional systems will then follow). The space of states of single copies is $\boldsymbol{C}^2 \otimes \boldsymbol{C}^2 \otimes \boldsymbol{C}^2 = \boldsymbol{C}^8$; the group of local unitary transformations on this space is $U(2) \times U(2) \times U(2)$. Thus the Hilbert space of two states is

$$(\boldsymbol{C}^2 \odot \boldsymbol{C}^2) \otimes (\boldsymbol{C}^2 \odot \boldsymbol{C}^2) \otimes (\boldsymbol{C}^2 \odot \boldsymbol{C}^2) = \boldsymbol{C}^4 \otimes \boldsymbol{C}^4 \otimes \boldsymbol{C}^4. \tag{47}$$

We will be interested in properties of the combined state invariant under $U(4) \times U(4) \times U(4)$.

The sort of question we would like to address is as follows. Kempe [20] has produced an interesting example of two 3-qubit states which are not locally equivalent although they have equal values of their bipartite invariants (or equivalently their local entropies). The non-equivalence was demonstrated by calculating the value of I_6. The two states and the values of the invariants are

$$\begin{aligned} &|\phi_1\rangle = 1/\sqrt{37}(2\sqrt{3}|000\rangle - 5|111\rangle) \\ &|\phi_2\rangle = 1/\sqrt{37}(4\sqrt{2}|000\rangle - 5|{+}{+}{+}\rangle) \\ &I_4^{(j)}(|\phi_1\rangle) = I_4^{(j)}(|\phi_2\rangle) = 769/1369 \qquad (j = 1, 2, 3) \\ &I_6(|\phi_1\rangle) \approx 0.343 \neq I_6(|\phi_2\rangle) \approx 0.242. \end{aligned} \tag{48}$$

Here $|+\rangle := (|0\rangle + |1\rangle)/\sqrt{2}$. Imagine now that one has many copies of $|\phi_1\rangle$; can they be transformed into many copies of $|\phi_2\rangle$ by collectively processing them using unitary transformations? The point is that the group we are going to allow to act is much larger in the collective case than in the case of one copy (the group of local unitary actions in the case of one copy is $U(2) \times U(2) \times U(2)$; in the case of C copies it is $U(2^C) \times U(2^C) \times U(2^C)$). In particular, consider starting with C copies of $|\phi_1\rangle$; the state of these C copies lies inside $\boldsymbol{C}^{2^C} \otimes \boldsymbol{C}^{2^C} \otimes \boldsymbol{C}^{2^C}$ in a particular way. Using collective unitaries we can transform the state $(|\phi_1\rangle)^{\otimes C}$ into other states, some of which may be written as the tensor power of some other state but the way in which the new tensor structure of each of the local Hilbert spaces lies inside $\boldsymbol{C}^{2^C}$ may be quite different from the way the Hilbert space was initially decomposed as a C-fold tensor product. The question is then: does the extra freedom collective processing allows enable us to transform multiple copies of $|\phi_1\rangle$ into multiple copies of $|\phi_2\rangle$?

We now present an infinite family of polynomials which are invariant under collective processing of any number of qubits. The easiest way to describe the family is by an example. Consider then a particular homogeneous polynomial of a single state which is invariant under $U(2) \times U(2) \times U(2)$, namely

$$I_4^{(1)} = \mathrm{Tr}_{B_1 C_1} \left[\mathrm{Tr}_{A_1}\, \rho\right]^2. \tag{49}$$

Here Tr_{A_1} denotes the trace of the operator over the two-dimensional Hilbert space A_1, etc (we will shortly be taking the tensor product of more than one Hilbert space for each party); as before we use ρ to denote the density matrix associated with the pure state $|\psi\rangle\langle\psi|$. This invariant may be easily extended to an invariant under collective processing of two states. Denote by A the four-dimensional Hilbert space of the first party, etc; clearly

$$\mathrm{Tr}_{BC}\, [\mathrm{Tr}_A\, \rho_1 \odot \rho_2]^2 \tag{50}$$

is invariant under local actions of $U(4)$ by each party, since each trace is invariant. Of course (50) is just one of the local invariants of states of three parties, each having a four-level system (see below). Moreover for any operator X on $\boldsymbol{C}^4$, we may write

$$\mathrm{Tr}_A(X) = \mathrm{Tr}_{A_1}\left(\mathrm{Tr}_{A_2}(X)\right) \tag{51}$$

where $\mathcal{H}_A = \mathcal{H}_{A_1} \odot \mathcal{H}_{A_2}$ is the local Hilbert space of party A; A_1 and A_2 label *any* decomposition of the local Hilbert space $\mathcal{H}_A = \boldsymbol{C}^4$ as a tensor product of two copies of $\boldsymbol{C}^2$. If we take the decomposition corresponding to $|\psi_1\rangle$ and $|\psi_2\rangle$ we see that

$$\begin{aligned}\mathrm{Tr}_{BC}[\mathrm{Tr}_A\,\rho]^2 &= \mathrm{Tr}_{BC}[\mathrm{Tr}_{A_1}\,\mathrm{Tr}_{A_2}\,\rho_1 \odot \rho_2]^2 \\ &= \mathrm{Tr}_{BC}[\mathrm{Tr}_{A_1}\,\rho_1 \odot \mathrm{Tr}_{A_2}\,\rho_2]^2 \\ &= \mathrm{Tr}_{BC}[\mathrm{Tr}_{A_1}\,\rho_1]^2 \odot [\mathrm{Tr}_{A_2}\,\rho_2]^2 \\ &= \mathrm{Tr}_{B_1C_1}[\mathrm{Tr}_{A_1}\,\rho_1]^2\,\mathrm{Tr}_{B_2C_2}[\mathrm{Tr}_{A_2}\,\rho_2]^2. \end{aligned} \tag{52}$$

We have used the facts that $(X \odot Y)^2 = X^2 \odot Y^2$ and $\mathrm{Tr}_{A_1A_2}(X \odot Y) = \mathrm{Tr}_{A_1}(X)\,\mathrm{Tr}_{A_2}(Y)$.

We have thus shown how to extend the original invariant (49) to one which is invariant under collective processing and also multiplicative (so that its logarithm is additive). We note that it was important the invariant is simple; a sum of invariants will not be multiplicative, in general.

An alternative way of seeing why an object like

$$\mathrm{Tr}_{BC}\,[\mathrm{Tr}_A\,|\psi\rangle\langle\psi|]^2 \tag{53}$$

is invariant under local unitaries and multiplicative under tensor products is to use index notation. We write the invariant as

$$\begin{aligned}&\sum_{\mu,\nu,\rho,\sigma,\tau,\eta=1}^{4} \psi_{\mu\nu\rho}\psi^*_{\mu\sigma\tau}\psi_{\eta\sigma\tau}\psi^*_{\eta\nu\rho} \\ &\qquad = \sum_{1}^{4} \psi_{\mu_1\nu_1\rho_1}\psi^*_{\mu_2\sigma_1\tau_1}\psi_{\eta_1\sigma_2\tau_2}\psi^*_{\eta_2\nu_2\rho_2}\delta_{\mu_1\mu_2}\delta_{\nu_1\nu_2}\delta_{\rho_1\rho_2}\delta_{\sigma_1\sigma_2}\delta_{\tau_1\tau_2}\delta_{\eta_1\eta_2}\end{aligned} \tag{54}$$

where $\psi_{\mu\nu\rho}$, $\mu, \nu, \rho = 1 \ldots 4$ are the components of the state $|\psi\rangle = |\psi_1\rangle \odot |\psi_2\rangle$, and $\delta_{\mu_1\mu_2}$ is the invariant tensor for $U(4)$. Under the decomposition of each local Hilbert space as two copies of $\boldsymbol{C}^2$, each index μ, say, becomes a composite index $a\alpha$; $a, \alpha = 1, 2$. The invariant tensor δ becomes

$$\delta_{\mu_1\mu_2} = \delta_{a_1a_2}\delta_{\alpha_1\alpha_2}. \tag{55}$$

The invariance of the expression (53) follows from the fact that δ is an invariant tensor for $U(4)$. A little algebra reproduces the result that (53) is multiplicative.

The latter method of proof is useful in cases where it is not easy to see how to write a given invariant in an 'index-free' way using traces.

While we have illustrated our point by examples, it should now be clear that any simple polynomial invariant of qubits may be extended to a multiplicative invariant for collective unitary processing of any number of states $|\psi_1\rangle, |\psi_2\rangle, \ldots |\psi_C\rangle$. (Note, however, that if, as we believe, the squared tangle is not simple, this argument does not apply to it.)

The multiplicativity of these invariants, and in particular of I_6, allows us to understand convertibility via collective unitaries for the states Kempe considered. There are no positive integers C_1, C_2 such that C_1 copies of $|\phi_1\rangle$ can be converted to C_2 copies of $|\phi_2\rangle$. The nontrivial but effectively bipartite invariants $I_4^{(j)}$ $(j = 1, \ldots, 3)$, which are all equal, impose the requirement $C_1 = C_2$ in order to maintain equality of the invariants for $|\phi_1\rangle^{\otimes C_1}$ and $|\phi_2\rangle^{\otimes C_2}$. Thus bipartite considerations do not forbid this exact conversion, at a 1 : 1 ratio. But when $C_1 = C_2$, the invariant I_6 will differ for these product states (taking values of approximately 0.343^{C_1} and 0.242^{C_1}, respectively) implying that exact unitary conversion, even collectively, is not possible at any ratio. Most pairs of states will be similarly constrained.

As we mentioned above, the invariants we have been thinking of as multiplicative invariants under collective processing of qubit states are amongst the invariants which arise when

considering local unitary actions on a single copy of an N-party, locally d-level system. The Hilbert space in this latter case is $\odot^N \boldsymbol{C}^d$ and the group of local unitary transformations is $U(d)^N$. In fact, the complete set of local unitary invariants are formed exactly as for qubits: one uses the invariant tensor δ_{RS}, $R, S = 1 \ldots d$ to contract the local indices. General theorems from invariant theory tell us that all polynomial invariants are sums of terms of this form (in fact exactly as for qubits, only the indices run over more values). Thus any polynomial invariant for this case is a polynomial invariant for collective processing of states (where the product of the dimensions of the local Hilbert spaces is d). While sums and products of invariants are invariant, only simple polynomials are multiplicative when thought of as invariants of collective processing of smaller systems.

We now turn to a few remarks about local invariants for density matrices. Reference [21] used a particularly convenient representation of density matrices of qubits, the Bloch decomposition. For example a two-qubit density matrix can be written as

$$\rho = \tfrac{1}{4}\left(1_2 \otimes 1_2 + \alpha_i \sigma_i \otimes 1_2 + \beta_j 1_2 \otimes \sigma_j + R_{ij} \sigma_i \otimes \sigma_j\right) \tag{56}$$

where $i, j = 1 \ldots 3$, σ_i are the Pauli matrices, and α_i, β_j and R_{ij} are real. The action of local unitary transformations becomes the action of $SO(3) \times SO(3)$ on the parameters α, β and R and this allows us to write down invariants and also find simple generating sets for the ring of invariants (see [21] for details). A density matrix of d-level systems can be written in a similar form to (56) with the Pauli matrices replaced by analogous $d \times d$ matrices, and the indices i, j now running from $1 \ldots d^2 - 1$. However it is significant that now the action of the local unitary group on the density matrix induces the action of a subgroup of the orthogonal group on the parameters α, β and R. Thus the full set of invariants is much more complicated when expressed as functions of these parameters. Therefore it is not easy to see how to construct invariants for collective processing using this parametrization for density matrices.

A more fruitful approach is to write invariants in terms of local traces, as was done for pure states above. Indeed, any of the multiplicative invariants we described for pure states are also invariants for density matrices (in the 'index free' form, for example, it is easy to see that any invariant for pure states becomes one for mixed states by simply replacing $|\psi\rangle\langle\psi|$ by a general density matrix ρ). However, there are other invariants, of determinant type, of general density matrices. These arise since the local action on density matrices is essentially an action of the special unitary group rather than full unitary group; the special unitary group has antisymmetric invariant tensors. We will return to the question of the ring of invariants for density matrices in a future publication.

Acknowledgments

HB thanks the EU for support via the QAIP project under IST-1999-11234, and Chris Fuchs for long ago bringing (62) to his attention. NL thanks Bill Wootters for very interesting discussions.

Appendix. Proof of proposition 4

Consider a pure bipartite state written in a Schmidt decomposition with real coefficients,

$$|\psi^{AB}\rangle = \sum_i \lambda_i^{1/2} |i^A\rangle |i^B\rangle \tag{57}$$

so that $|i^A\rangle$ and $|i^B\rangle$ are orthonormal bases. We may write this as $(I \otimes \rho^{1/2})|\Psi\rangle$, where $|\Psi\rangle := \sum_i |i^A\rangle|i^B\rangle$, an unnormalized vector (note that $|\Psi\rangle$ depends on a choice of local bases

$|i^A\rangle$ for A and $|i^B\rangle$ for B). Thus

$$\begin{aligned}\langle\psi^{AB}|(R\otimes P)|\psi^{AB}\rangle \\ &= \langle\Psi|(I\otimes\rho^{1/2})(I\otimes P)(R\otimes I)(I\otimes\rho^{1/2})|\Psi\rangle \\ &= \langle\Psi|(I\otimes\rho^{1/2})(I\otimes P)(I\otimes\rho^{1/2})(R\otimes I)|\Psi\rangle \\ &= \langle\Psi|(I\otimes\rho^{1/2})(I\otimes P)(I\otimes\rho^{1/2})(I\otimes R^T)|\Psi\rangle \\ &= \langle\Psi|(I\otimes\rho^{1/2}P\rho^{1/2}Q)|\Psi\rangle. \end{aligned} \tag{58}$$

For the second equality, we just commuted operators. The third equality uses the identity (valid for any linear operator X) $(X\otimes I)|\Psi\rangle = (I\otimes X^T)|\Psi\rangle$ where the transpose is done in the local basis $|i^A\rangle$ used to define $|\Psi\rangle$, and the implicit isomorphism between A and B is the one that identifies these local bases $|i^A\rangle$ and $|i^B\rangle$ with each other (for a proof, cf e.g. [22]). The last equality just defines $Q := R^T$ and uses elementary tensor product manipulations. Here, R, P are projectors on spaces A and B respectively, with ranks k_A and k_B; Q is a projector of rank k_A, by the easily checked fact that the transpose of a projector is a projector of the same rank. Maximizing over all projectors of these ranks is the same as holding P, Q fixed and maximizing, over all unitaries U, V on A, B respectively, in the expression:

$$\langle\Psi|(I\otimes\rho^{1/2}VPV^\dagger\rho^{1/2}UQU^\dagger)|\Psi\rangle. \tag{59}$$

Now, this is equal to

$$\operatorname{tr}\rho^{1/2}VPV^\dagger\rho^{1/2}UQU^\dagger \tag{60}$$

and,

$$\max_{U,V}|\operatorname{tr}\rho^{1/2}VPV^\dagger\rho^{1/2}UQU^\dagger| \leqslant \max_{U,V,W,Y}|\operatorname{tr}\rho^{1/2}VPW\rho^{1/2}UQY|. \tag{61}$$

The latter maximization is a special case of a general schema:

$$\max_{U,V,W,Y\ldots Z}|\operatorname{tr}AUBVCW\cdots GZ| = \sum_j \sigma_j(A)\sigma_j(B)\sigma_j(C)\cdots\sigma_j(G) \tag{62}$$

which holds for any finite set of linear operators $A, B, C, \ldots, G$ and unitaries $U, V, W, \ldots, Z$. Here $\sigma_j(X)$ are the decreasingly ordered singular values of X (eigenvalues of $|X| := \sqrt{XX^\dagger}$, which are also the eigenvalues of $\sqrt{X^\dagger X}$ although this is not generally equal to $|X|$).

For the case of two operators and two unitaries, (62) was shown by von Neumann [23]. In the general case, it follows from the facts that

$$\max_{\text{unitary } U}|\operatorname{tr}AU| = \sum_j \sigma_j(A) \tag{63}$$

(cf [11, 22] theorem 7.4.9, p 432),

$$(\eta \preceq_{\mathrm{w}} \mu) \to \lambda\cdot\eta \preceq_{\mathrm{w}} \lambda\cdot\mu \tag{64}$$

and

$$\sigma(AB) \preceq_{\mathrm{w}} \sigma(A)\cdot\sigma(B) \tag{65}$$

(cf [3], equation IV.21, p 94). Here $\sigma(A)$ stands for the vector of the decreasingly ordered singular values of A, and $\preceq_{\mathrm{w}}$ means 'is weakly majorized by', i.e. for all k the sum of the first k components of the RHS vector is greater than or equal to the sum of the first k components of the LHS. λ, μ and η are also assumed to be vectors with decreasingly ordered components, none of which are negative, and notation such as $\lambda\cdot\eta$ does *not* stand for the usual dot product, but rather for the componentwise product of two vectors, whose value is another such vector. (Explicitly, $(\lambda\cdot\eta)_j = \lambda_j\eta_j$.)

The proof that the LHS of (62) is less than or equal to the RHS proceeds inductively as follows. Firstly,

$$\max_{U,V,W,Y\ldots Z} |\operatorname{tr} AUBVCW\cdots GZ| = \sum_j \sigma_j(AUBVC\ldots G) \tag{66}$$

by (63). Then use of (65) gives

$$\sum_j \sigma_j(AUBVC\ldots G) \leqslant \sum_j \sigma_j(AUBVC\ldots F)\sigma_j(G). \tag{67}$$

Now $\sigma(A\ldots F) \preceq_{\mathrm{w}} \sigma(AU\ldots E)\sigma(F)$ by (65), and thus

$$\sigma(A\ldots F)\cdot\sigma(G) \preceq_{\mathrm{w}} \sigma(A\ldots F)\cdot\sigma(F)\cdot\sigma(G). \tag{68}$$

Repeating this step shows that

$$\sigma(A\ldots G) \preceq_{\mathrm{w}} \sigma(A)\cdot\sigma(B)\cdots\sigma(G) \tag{69}$$

and therefore that

$$\max_{U,V,W,Y\ldots Z} |\operatorname{tr} AUBVCW\cdots GZ| = \sum_j \sigma_j(AUBVC\ldots G) \leqslant \sum_j \sigma_j(A)\cdots\sigma_j(G). \tag{70}$$

Finally we note that appropriate choice of the unitaries $U, V, \ldots, Z$ in (62) allows this equality to be reached. Specifically, by the singular value decomposition they may be chosen so as to transform, say, A to $|A|$ and each of $B, C, D\ldots$ to $U|B|U^\dagger$, $V|C|V^\dagger$, $W|D|W^\dagger$, each of which commutes with $|A|$ and has its ordered eigenvalues associated with their common eigenvectors in the same order as $|A|$.

Applying this result to the case at hand, we note that the unitary freedoms on the LHS of (61) are sufficient to achieve this maximum for $A = \rho^{1/2}$, $B = P$, $C = \rho^{1/2}$, $D = Q$. Consequently, the maximal value of (61), which is $E_{k_A,k_B}(|\psi^{AB}\rangle)$, will be the sum of the largest $\min(k_A, k_B)$ eigenvalues of ρ.

References

[1] Vidal G 2000 Entanglement monotones *J. Mod. Opt.* **47** 355

[2] Linden N and Popescu S 1998 On multi-particle entanglement *Fortschr. Phys.* **46** 567–78

[3] Bhatia R 1997 *Matrix Analysis* (New York: Springer)

[4] Bennett C H, DiVincenzo D P, Smolin J A and Wootters W K 1996 Mixed state entanglement and quantum error correction *Phys. Rev.* A **54** 3824

[5] Alberti P M and Uhlmann A 1981 *Stochasticity and Partial Order* (Berlin: VEB Deutscher Verlag Wiss)

[6] Wehrl A 1974 How chaotic is a state of a quantum system? *Rep. Math. Phys.* **6** 15–28

[7] Wehrl A 1978 General properties of entropy *Rev. Mod. Phys.* **50** 221–60

[8] Nielsen M A 1999 Conditions for a class of entanglement transformations *Phys. Rev. Lett.* **83** 436–9

[9] Hardy L 1999 A method of areas for manipulation the entanglement properties of one copy of a two-particle pure entangled state *Preprint* arXiv quant-ph/9903001 v2

[10] Jensen J G and Schack R 2000 A simple algorithm for local conversion of pure states *Preprint* arXiv quant-ph/0006049 v2

[11] Horn R A and Johnson C R 1985 *Matrix Analysis* (Cambridge: Cambridge University Press)

[12] Vidal G, Jonathan D and Nielsen M A 2000 Approximate transformations and robust manipulation of bipartite pure state entanglement *Phys. Rev.* A **62** 012304
(Vidal G, Jonathan D and Nielsen M A 1999 *Preprint* arXiv quant-ph/9910099)

[13] Vidal G 1999 Entanglement of pure states for a single copy *Phys. Rev. Lett.* **83** 1046–9

[14] Linden N, Massar S and Popescu S 1998 Purifying noisy entanglement requires collective measurements *Phys. Rev. Lett.* **81** 3279–82

[15] Bennett C H, Bernstein H J, Popescu S and Schumacher B 1996 Concentrating partial entanglement by local operations *Phys. Rev.* A **53** 2046

[16] Werner R Personal communication

[17] Cirac J I, Dür W and Vidal G 2000 Three qubits can be entangled in two inequivalent ways *Phys. Rev.* A **62** 062314
[18] Coffman V, Kundu J and Wootters W K 1999 Distributed entanglement *Preprint* LANL arXiv.org quant-ph/9907047 v2
[19] Grassl M Personal communication
[20] Kempe J 1999 Multi-particle entanglement and its applications to cryptography *Phys. Rev.* A **60** 910–6
[21] Linden N, Popescu S and Sudbery A 1999 Non-local properties of multi-particle density matrices *Phys. Rev. Lett.* **83** 243–7
[22] Jozsa R 1994 Fidelity for mixed quantum states *J. Mod. Opt.* **41** 2314–23
[23] von Neumann J 1937 Some matrix-inequalities and metrization of matrix-space *Tomsk. Univ. Rev.* **1** 286