Measuring polynomial invariants of multiparty quantum states

M. S. Leifer* and N. Linden
Department of Mathematics, University of Bristol, University Walk, Bristol, BS8 1TW, United Kingdom

A. Winter†
Department of Computer Science, University of Bristol, Merchant Venturers Building, Woodland Road, Bristol, BS8 1UB, United Kingdom

(Received 15 August 2003; published 7 May 2004)

We present networks for directly estimating the polynomial invariants of multiparty quantum states under local transformations. The structure of these networks is closely related to the structure of the invariants themselves and this lends a physical interpretation to these otherwise abstract mathematical quantities. Specifically, our networks estimate the invariants under local unitary (LU) transformations and under stochastic local operations and classical communication (SLOCC). Our networks can estimate the LU invariants for multiparty states, where each party can have a Hilbert space of arbitrary dimension and the SLOCC invariants for multiqubit states. We analyze the statistical efficiency of our networks compared to methods based on estimating the state coefficients and calculating the invariants.

DOI: 10.1103/PhysRevA.69.052304 PACS number(s): 03.67.Mn, 03.65.Ud, 03.65.Ta

I. INTRODUCTION

Entanglement is a key resource in quantum information and computation since it can be used to perform tasks such as teleportation, superdense coding, and key distribution. Therefore, it is important to find ways of classifying and quantifying the entanglement properties of quantum states. Central to this is the idea that locally invariant quantities can be used to characterize entanglement. Invariants under local unitary (LU) and more general transformations, such as, stochastic local operations and classical communication (SLOCC), have been extensively studied in this context [1–13].

However, invariants are rather abstract mathematical objects and it is natural to ask whether any physical meaning can be given to them. One way of doing this is to investigate how these quantities might be measured given a number of copies of an unknown state. This could be done by simply measuring the coefficients of the state and then calculating the invariants. However, finding procedures to measure the invariants directly may be more efficient and also lends the invariants a physical interpretation as "collective observables" of the state.

For bipartite pure states, the Schmidt coefficients are a complete set of LU invariants and optimal protocols for measuring them were given in Ref. [14]. Also, in Ref. [15] a method was given for estimating the polynomial SLOCC invariants of a general two-qubit state.

In this paper we present networks for estimating two classes of polynomial invariants for multiparty states: the LU invariants for multiparty states with arbitrary local Hilbert-space dimension and the SLOCC invariants for multiqubit states. In both cases, the protocol works for both pure and mixed states. In particular, the structure of the networks reflects the structure of the invariants in a very simple way.

In Sec. II, we review the construction of local invariants under LU transformations. We merely sketch the theory of polynomial invariants here and no proofs of the results are given. The interested reader can find the mathematical details in Refs. [16,17]. In Sec. III, the networks for measuring these invariants are presented. We then turn to invariants under SLOCC transformations, reviewing their construction in Sec. IV and presenting networks to measure them in Sec. V. In order to construct the networks for SLOCC invariants we make use of the structural physical approximation (SPA) to nonphysical maps introduced in Ref. [18]. The relevant details of this are presented in Sec. VI. Finally, in Sec. VII we evaluate estimation protocols based on our networks by comparing them to simple techniques based on estimating the state coefficients.

II. POLYNOMIAL INVARIANTS UNDER LU TRANSFORMATIONS

A. Pure states

Two n-party pure states $|\psi\rangle, |\psi'\rangle \in \otimes_{j=1}^{n} \mathbb{C}^{d_j}$ are equivalent under LU transformations if

$$|\psi'\rangle = U_1 \otimes U_2 \otimes \cdots \otimes U_n |\psi\rangle, \tag{1}$$

where $U_j \in U(d_j)$ is a unitary operation acting on the Hilbert space of the jth party. States on the same orbit under this action have the same entanglement properties. Given a particular state, we might be interested in determining which orbit it belongs to. This can be done by establishing a canonical point on each orbit, such as the Schmidt form for bipartite states. However, canonical forms rapidly be-

*Present address: Perimeter Institute for Theoretical Physics, 35 King Street North, Waterloo, Ontario, N2J 2W9, Canada. Email address: mleifer@perimeterinstitute.ca

†Present address: Department of Mathematics, University of Bristol, University Walk, Bristol, BS8 1TW, United Kingdom.

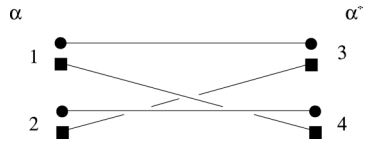

FIG. 1. Diagrammatic representation of the quartic two-qubit LU invariant J, given in Eq. (4). The first index of each term is represented by a circle and the second by a square. A line joins indices that are contracted with a δ.

come more complicated as the number of parties is increased. Alternatively, we can construct polynomial functions of the state coefficients that are invariant on each orbit. Theorems from invariant theory guarantee that a finite set of such polynomials is enough to distinguish the generic orbits under this action. We now review the construction of such a set.

1. One party

Consider the state $|\psi\rangle=\Sigma_{i=1}^{d}\alpha^i|i\rangle$ in a single party Hilbert space $\mathbb{C}^d$, where $\{|i\rangle\}$ is an orthonormal basis. The only independent invariant under unitary transformations of this state is the norm $\langle\psi|\psi\rangle$. This may be written as

$$\langle\psi|\psi\rangle=\sum_i \alpha^i\alpha_i^*=\sum_{i,j}\alpha^i\delta_i^j\alpha_j^*, \tag{2}$$

where δ_i^j is the Kronecker delta. δ_i^j is the $U(d)$ invariant tensor and invariants for larger numbers of parties are formed by similar contractions of the state coefficients with their complex conjugates.

2. Two qubits

As an example, consider a two-qubit state $|\psi\rangle=\Sigma_{i,j=0}^{1}\alpha^{ij}|ij\rangle$. There is only one independent quadratic invariant, which is simply the norm of the state. However, at quartic order we find the following invariant, which is algebraically independent of the norm,

$$J=\sum \alpha^{i_1j_1}\alpha^{i_2j_2}\delta_{i_1}^{i_3}\delta_{i_2}^{i_4}\delta_{j_1}^{j_4}\delta_{j_2}^{j_3}\alpha_{i_3j_3}^*\alpha_{i_4j_4}^*=\sum \alpha^{i_1j_1}\alpha^{i_2j_2}\alpha_{i_1j_2}^*\alpha_{i_2j_1}^*. \tag{3}$$

For two qubits, we know that this is the only other independent invariant because every state has a canonical Schmidt form $|\psi\rangle=\sqrt{p}|00\rangle+\sqrt{1-p}|11\rangle$, with $1/2\leqslant p\leqslant 1$ and $J=2(p^2-p)+1$ determines p uniquely.

Another useful way of representing the invariant is to define two permutations σ,τ on the set $\{1,2\}$ where σ is the identity permutation and $\tau(1)=2,\tau(2)=1$. Then

$$J_{(\sigma,\tau)}=\sum \alpha^{i_1j_1}\alpha^{i_2j_2}\alpha_{i_{\sigma(1)}j_{\tau(1)}}^*\alpha_{i_{\sigma(2)}j_{\tau(2)}}^*. \tag{4}$$

This also suggests a diagrammatic way of representing the invariant (see Fig. 1).

3. General case

A multipartite pure state can be written in terms of an orthonormal basis as follows:

$$|\psi\rangle=\sum_{i,j,k\ldots}\alpha^{ijk\cdots}|ijk\cdots\rangle. \tag{5}$$

A general polynomial function of the state coefficients and their complex conjugates can be written as

$$\sum c_{i_1j_1k_1\ldots i_2j_2k_2\ldots}^{i_rj_rk_r\cdots}\alpha^{i_1j_1k_1\cdots}\alpha^{i_2j_2k_2\cdots}\cdots\alpha_{i_rj_rk_r\ldots}^*\cdots. \tag{6}$$

If the polynomial (6) has equal numbers of α's and α^*'s and all the indices of the α's are contracted using the invariant tensor δ with those of the α^*'s, each index being contracted with an index corresponding to the same party then the polynomial is manifestly invariant under LU transformations.

Such polynomials can be written in terms of permutations on the indices. Let r be the degree of the polynomial in α (and hence also the degree in α^*). Let $\sigma,\tau,\mu\ldots$ be permutations acting on the set $\{1,2,\ldots,r\}$ and let $\vec{\sigma}=(\sigma,\tau,\mu,\ldots)$. Then the invariants can be written as

$$J_{\vec{\sigma}}=\sum \alpha^{i_1j_1k_1\cdots}\alpha^{i_2j_2k_2\cdots}\cdots\alpha_{i_{\sigma(1)}j_{\tau(1)}k_{\mu(1)}\cdots}^*\alpha_{i_{\sigma(2)}j_{\tau(2)}k_{\mu(2)}\cdots}^*\cdots. \tag{7}$$

In fact, σ can always be chosen to be the identity permutation by permuting the α terms in this expression, provided the remaining permutations are redefined appropriately. Additionally, each $J_{\vec{\sigma}}$ can be associated with a diagram constructed in the same way as Fig. 1.

The invariants $J_{\vec{\sigma}}$ are enough to completely distinguish the generic orbits under LU transformations. In fact, invariant theory guarantees that only a finite collection of them are needed to do this. However, except in a few simple cases, it is unknown which $J_{\vec{\sigma}}$ invariants form minimal complete sets.

B. Mixed states

Two mixed states ρ,ρ' are equivalent under LU transformations if

$$\rho'=U_1\otimes U_2\otimes\cdots\otimes U_n\rho U_1^\dagger\otimes U_2^\dagger\otimes\cdots\otimes U_n^\dagger. \tag{8}$$

The LU invariants for mixed states can be derived by rewriting the pure state invariants (7) in terms of the density matrix $\rho=|\psi\rangle\langle\psi|$ and noting that the resulting expressions are still invariant under LU transformations for general density matrices. This can be done by noting that terms such as $\alpha^{i_1j_1\cdots}\alpha_{i_2j_2\cdots}^*$ are elements of the density matrix. A general density matrix may be written in terms of an orthonormal basis as

$$\rho=\sum \rho_{mnp\ldots}^{ijk\cdots}|ijk\cdots\rangle\langle mnp\cdots|, \tag{9}$$

and the corresponding expression for an LU invariant is

$$J_{\vec{\sigma}}=\sum \rho_{i_{\sigma(1)}j_{\tau(1)}k_{\mu(1)}\ldots}^{i_1j_1k_{1\cdots}}\rho_{i_{\sigma(2)}j_{\tau(2)}k_{\mu(2)}\cdots}^{i_2j_2k_{2\cdots}}\cdots\rho_{i_{\sigma(r)}j_{\tau(r)}k_{\mu(r)}\cdots}^{i_rj_rk_{r\cdots}}. \tag{10}$$

III. MEASURING INVARIANTS UNDER LU TRANSFORMATIONS

Network construction

The general construction of the network used to measure the LU invariants is shown in Fig. 2. It generalizes networks

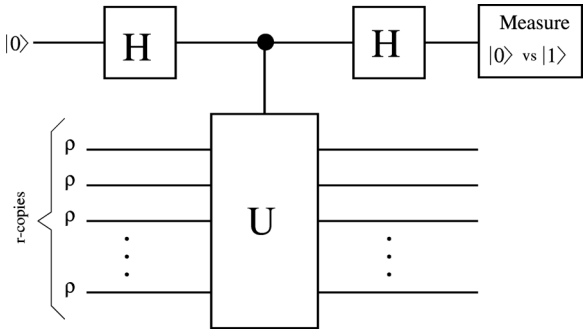

FIG. 2. General construction of network to measure polynomial LU invariants.

for estimating functionals of bipartite states given in Refs. [15,19,20]. To measure an LU invariant of degree r in α (and also degree r in α^*) we take r copies of the unknown state ρ. In addition, we take a single qubit in the state $|0\rangle$ and apply a Hadamard rotation H to transform the state to $(1/\sqrt{2})(|0\rangle + |1\rangle)$. In the next step, we apply a unitary operation U on the r copies of ρ controlled by the Hadamard rotated qubit. Finally we perform a measurement on the single qubit in the $\{|0\rangle, |1\rangle\}$ basis. The expectation value of this measurement will be

$$\langle Z\rangle = \mathrm{Re}[\mathrm{Tr}(U\rho^{\otimes r})]. \tag{11}$$

When $\rho = |\psi\rangle\langle\psi|$ is a pure state then this is equivalent to

$$\langle Z\rangle = \mathrm{Re}\langle\psi|^{\otimes r} U |\psi\rangle^{\otimes r}. \tag{12}$$

In order to determine networks for measuring the LU invariants, it only remains to show that there is a U such that the invariants can be expressed in the form (11).

To do this for pure states, we have to express polynomials of the form (7) in the form of Eq. (12). First, we note that $\alpha^{ijk\cdots} = \langle ijk\cdots|\psi\rangle$, $\alpha^*_{ijk\cdots} = \langle\psi|ijk\cdots\rangle$, and to each permutation σ in Eq. (7) we associate a permutation matrix

$$P_\sigma = \sum_{i_1,i_2,\ldots,i_r=1}^{d} |i_{\sigma(1)} i_{\sigma(2)\cdots} i_{\sigma(r)}\rangle\langle i_1 i_2 \cdots i_r|, \tag{13}$$

where P_σ acts on the Hilbert space of the same party for each of the r copies of the state $|\psi\rangle$. Then to each $\vec{\sigma}$ we associate the permutation matrix

$$P_{\vec{\sigma}} = P_\sigma \otimes P_\tau \otimes P_\mu \otimes \cdots, \tag{14}$$

where $P_\sigma, P_\tau, P_\mu, \ldots$ act on the Hilbert space of the same party as $\sigma, \tau, \mu, \ldots$ in Eq. (7) on each of the r copies of the state. Then Eq. (7) can be written as

$$J_{\vec{\sigma}} = \langle\psi|^{\otimes r} P_{\vec{\sigma}} |\psi\rangle^{\otimes r}. \tag{15}$$

Note that the tensor product that appears in this equation is different from that of Eq. (14). Each component of the product in Eq. (14) acts on the Hilbert space of a single party across all the r copies of the state in Eq. (15). Since $P_{\vec{\sigma}}$ is unitary these invariants can be estimated with the network in Fig. 2 by setting $U = P_{\vec{\sigma}}$ to obtain the real part and $U = iP_{\vec{\sigma}}$ to obtain the imaginary part. For the specific example of the two-qubit invariant (3) we have

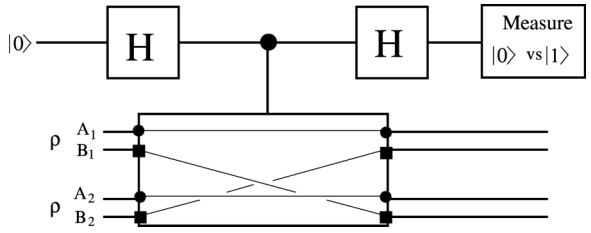

FIG. 3. Network for measuring the two-qubit quartic invariant.

$$J_{(\sigma,\tau)} = \langle\psi|_{A_1B_1}\langle\psi|_{A_2B_2} I_{A_1A_2} \otimes \mathrm{SWAP}_{B_1B_2} |\psi\rangle_{A_1B_1} |\psi\rangle_{A_2B_2}. \tag{16}$$

Note also that the physical construction of $P_{\vec{\sigma}}$ is closely related to the diagram associated with $J_{\vec{\sigma}}$ (compare Figs. 1 and 3, for example).

Finally, note that if ρ is a mixed state then applying the same procedure without modification will give the invariants of Eq. (10).

It has previously been noted [6] that all homogeneous polynomial LU invariants are determined by the expectation values of two observables on r copies of a state. Here, we have given an explicit network for measuring these observables. Also, similar constructions can be made to estimate other polynomial functionals of quantum states [20] and these can be modified to enable the estimation to proceed by local operations and classical communication (LOCC) [21], i.e., with no collective operations over the n parties. A similar modification would enable the LU invariants to be estimated by LOCC, but this would affect the efficiency of the estimation discussed in Sec. VII B.

IV. POLYNOMIAL INVARIANTS UNDER SLOCC

When attempting to classify entanglement, it is often useful to consider invariants under local transformations that are more general than unitary transformations. An important class of transformations, SLOCC was introduced in Ref. [22]; and invariants under SLOCC were studied in Refs. [7–13]. In Sec. V we construct a network to measure the modulus squared of these invariants for the case where each party has a single qubit [i.e., the Hilbert space is $(\mathbb{C}^2)^{\otimes n}$].

A. Pure states

Two n-party pure states $|\psi\rangle$ and $|\psi'\rangle$ are equivalent under SLOCC if it is possible to obtain $|\psi'\rangle$ with nonzero probability via a sequence of LOCC starting from a single copy of $|\psi\rangle$ and vice versa. In Ref. [23], this criterion was shown to be equivalent to

$$|\psi'\rangle = M_1 \otimes M_2 \otimes \cdots \otimes M_n |\psi\rangle, \tag{17}$$

where $M_j \in \mathrm{GL}(d_j)$ is an invertible linear transformation acting on the d_j-dimensional Hilbert space of the jth party.

In what follows, we find polynomial invariants for the special case where $M_j \in \mathrm{SL}(2)$, i.e., the transformation has unit determinant and each party has a single qubit. Networks to determine the modulus squared of these invariants will be given in Sec. V. Note that it is not possible to measure the $\mathrm{SL}(2)^n$ invariants directly because they are not invariant under global phase transformations $|\psi\rangle \to e^{i\theta}|\psi\rangle$, which have no physical significance. It is for this reason that we instead measure the modulus squared, which is invariant under these phase transformations.

Under general $\mathrm{GL}(2)^n$ transformations, the polynomial $\mathrm{SL}(2)^n$ invariants are still invariant up to a multiplicative factor, which is just some power of the determinant of $M_1 \otimes M_2 \otimes \cdots \otimes M_n$. Thus, ratios of appropriate powers of these polynomials will be invariants under $\mathrm{GL}(2)^n$.

1. Two qubits

In order to illustrate the polynomial invariants under $\mathrm{SL}(2)^n$, first consider the case where $n=2$. Two states $|\psi\rangle = \sum_{j,k=1}^{2} \alpha^{jk}|jk\rangle$ and $|\psi'\rangle = \sum_{j,k=1}^{2} \alpha'^{jk}|jk\rangle$ satisfy Eq. (17) if

$$\alpha' = M_1 \alpha M_2^T. \tag{18}$$

This means that $\det(\alpha) = \det(\alpha')$ is an $\mathrm{SL}(2) \times \mathrm{SL}(2)$ invariant, since $\det(M_1) = \det(M_2) = 1$. This may be written as

$$\det \alpha = \sum \epsilon_{i_1 i_2} \epsilon_{j_1 j_2} \alpha^{i_1 j_1} \alpha^{i_2 j_2}, \tag{19}$$

where the totally antisymmetric tensor ϵ_{ij} is the SL(2) invariant tensor. For two-qubit pure states, all other $\mathrm{SL}(2) \times \mathrm{SL}(2)$ invariants that can be constructed are algebraically dependent on this one.

2. General case

The $\mathrm{SL}(2)^n$ invariants can be constructed in a similar way to the LU invariants except the invariant tensor is now ϵ_{ij}, and we contract α's with α's instead of α^*'s. Thus, polynomials of the form

$$K_{\vec{\sigma}} = \sum_{1}^{2} \epsilon_{i_1 i_2} \epsilon_{j_1 j_2} \epsilon_{k_1 k_2} \cdots \epsilon_{i_{r-1} i_r} \epsilon_{j_{r-1} j_r} \epsilon_{k_{r-1} k_r} \alpha^{i_{\sigma(1)} j_{\tau(1)} k_{\mu(1)} \cdots} \times \alpha^{i_{\sigma(2)} j_{\tau(2)} k_{\mu(2)} \cdots} \cdots \alpha^{i_{\sigma(r)} j_{\tau(r)} k_{\mu(r)} \cdots} \tag{20}$$

are manifestly invariant and all other invariants are algebraically dependent on these [16]. Note that it is straightforward to generalize this construction to the case where each party has a d-dimensional Hilbert space by contracting with the $\mathrm{SL}(d)^n$ invariant tensor $\epsilon_{i_1 i_2 \ldots i_d}$ instead of ϵ_{ij}. However, it is not yet clear how to measure these invariants because the effect of the higher rank ϵ tensors cannot be physically implemented by linear transformations on states.

B. Mixed states

In general, two mixed states ρ, ρ' are equivalent under SLOCC if there exists two completely positive maps $\mathcal{E}_1, \mathcal{E}_2$ which are implementable via LOCC with nonzero probability of success such that $\rho' = \mathcal{E}_1(\rho)$ and $\rho = \mathcal{E}_2(\rho')$. In order to derive invariants using the expressions from the preceding section, we will restrict to the case where ρ and ρ' are related by

$$\rho' = M_1 \otimes M_2 \otimes \cdots \otimes M_n \rho M_1^\dagger \otimes M_2^\dagger \otimes \cdots \otimes M_n^\dagger \tag{21}$$

with $M_j \in \mathrm{SL}(2)$. The resulting expressions may not be invariant under more general SLOCC transformations, but are related to important quantities in entanglement theory as described in Sec. IV C

Unlike the LU invariants, it is clear that Eq. (20) cannot be written simply in terms of the coefficients of the density matrix $\rho = |\psi\rangle\langle\psi|$. However, $|K_{\vec{\sigma}}|^2$ can be written as follows:

$$|K_{\vec{\sigma}}|^2 = \sum_{1}^{2} \epsilon_{i_1 i_2} \epsilon_{j_1 j_2} \epsilon_{k_1 k_2} \cdots \epsilon_{i_{r-1} i_r} \epsilon_{j_{r-1} j_r} \epsilon_{k_{r-1} k_r} \times \epsilon^{m_1 m_2} \epsilon^{n_1 n_2} \epsilon^{p_1 p_2} \cdots \epsilon^{m_{r-1} m_r} \epsilon^{n_{r-1} n_r} \epsilon^{p_{r-1} p_r} \times \rho^{i_{\sigma(1)} j_{\tau(1)} k_{\mu(1)} \cdots}_{m_{\sigma(1)} n_{\tau(1)} p_{\mu(1)} \cdots} \rho^{i_{\sigma(2)} j_{\tau(2)} k_{\mu(2)} \cdots}_{m_{\sigma(2)} n_{\tau(2)} p_{\mu(2)} \cdots} \cdots \rho^{i_{\sigma(r)} j_{\tau(r)} k_{\mu(r)} \cdots}_{m_{\sigma(r)} n_{\tau(r)} p_{\mu(r)} \cdots} \tag{22}$$

and these will also be $\mathrm{SL}(2)^n$ invariants for mixed states.

C. Examples of $\mathrm{SL}(2)^n$ invariants

The $K_{\vec{\sigma}}$ invariants are especially interesting in entanglement theory because many important entanglement measures can be easily calculated from them. For example, in the case of two qubits, the concurrence [24] is defined as a simple function of the eigenvalues of $\rho\tilde{\rho}$, where

$$\tilde{\rho} = \sigma_y \otimes \sigma_y \rho^T \sigma_y \otimes \sigma_y, \tag{23}$$

and ^{T} stands for transpose in the computational basis. These eigenvalues can be calculated from $\mathrm{Tr}[(\rho\tilde{\rho})^m]$ for $m = 1,2,3,4$, which are simply the moduli squared of $K_{\vec{\sigma}}$ invariants. In Ref. [15], networks were constructed to estimate these invariants for two qubits and we will generalize this construction to $K_{\vec{\sigma}}$ invariants for larger number of parties.

Another interesting example is the 3-tangle [25,26], which is defined for pure states as the modulus of the following three-qubit $K_{\vec{\sigma}}$ invariant.

$$\tau_3 = \sum_{1}^{2} \alpha^{i_1 j_1 k_1} \alpha^{i_2 j_2 k_2} \epsilon_{i_1 i_3} \epsilon_{j_1 j_3} \epsilon_{k_1 k_4} \epsilon_{i_2 i_4} \epsilon_{j_2 j_4} \epsilon_{k_2 k_3} \alpha^{i_3 j_3 k_3} \alpha^{i_4 j_4 k_4}. \tag{24}$$

The 3-tangle gives information about the genuine three-party entanglement between the qubits.

Finally, note that the $K_{\vec{\sigma}}$ invariants can be given similar diagrammatic representations to the $J_{\vec{\sigma}}$ invariants. This is illustrated for the 3-tangle in Fig. 4.

V. MEASURING SLOCC INVARIANTS

The modulus squared of the SLOCC invariants can be measured using a network similar to Fig. 2 except that the unknown states ρ must be preprocessed prior to the

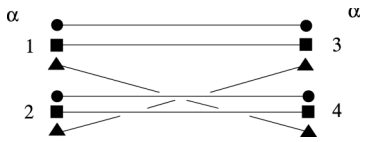

FIG. 4. Diagrammatic representation of the 3-tangle. The first index of each term is represented by a circle, the second by a square, and the third by a triangle. A line joins indices that are contracted with an ϵ.

controlled-U operation. If $K_{\vec{\sigma}}$ is of degree r in α then we will need r copies of ρ. The preprocessing stage will consist of collective unitary operations and completely positive maps that act on the entire Hilbert space of the r copies of ρ. The resulting state ρ', will yield the expectation value

$$\langle Z\rangle = \mathrm{Re}[\mathrm{Tr}(U\rho')] \tag{25}$$

for the measurement at the end of the network. In this section, we describe the preprocessing operations and unitary operations U that enable the modulus squared of the SLOCC invariants to be written in this form.

First, we apply the inverse of the permutation matrix associated with $\vec{\sigma}$ to the r copies of ρ to obtain $P_{\vec{\sigma}}^{\dagger}\rho^{\otimes r}P_{\vec{\sigma}}$.

The second, and final, part of the preprocessing stage is to apply a completely positive map $\overline{\Lambda}$ to the state. To describe Λ we first define the multiparty analog of Eq. (23):

$$\tilde{\rho} = \sigma_y \otimes \sigma_y \otimes \cdots \otimes \sigma_y \rho^T \sigma_y \otimes \sigma_y \otimes \cdots \otimes \sigma_y. \tag{26}$$

Next, we define a map Λ that acts on a product of r states by applying the tilde operation to the even numbered states as follows:

$$\Lambda(\rho_1 \otimes \rho_2 \otimes \cdots \otimes \rho_r) = \rho_1 \otimes \tilde{\rho}_2 \otimes \rho_3 \otimes \cdots \otimes \tilde{\rho}_r, \tag{27}$$

where each ρ_j is an n-party state.

Unfortunately, Λ cannot be physically implemented, since it is not a completely positive map. This can be dealt with by using the SPA to Λ, which we will call $\overline{\Lambda}$. $\overline{\Lambda}$ is the "closest" physical map to Λ. This is discussed in Sec. VI, but for now we construct the network as if Λ could be implemented perfectly.

The final preprocessed state ρ' will be

$$\rho' = \Lambda(P_{\vec{\sigma}}^{\dagger}\rho^{\otimes r}P_{\vec{\sigma}}). \tag{28}$$

Next, the controlled U operation in our network must be chosen such that $\langle Z\rangle = |K|_{\vec{\sigma}}^2$ when ρ' is used as the input. One can easily verify that the pairwise SWAP gate, defined by

$$\begin{aligned} U|\phi_1\rangle \otimes |\phi_2\rangle \otimes \cdots \otimes |\phi_{r-1}\rangle \otimes |\phi_r\rangle \\ = |\phi_2\rangle \otimes |\phi_1\rangle \otimes \cdots \otimes |\phi_r\rangle \otimes |\phi_{r-1}\rangle, \end{aligned} \tag{29}$$

where $|\phi_j\rangle$ is an n-party state fulfills this condition.

VI. THE STRUCTURAL PHYSICAL APPROXIMATION

The Λ operation encountered in the preceding section is an example of a positive, but not completely positive map. These cannot be implemented exactly, but instead we can apply an approximation.

$$\overline{\Lambda}(\rho) = \alpha I + \beta\Lambda(\rho), \tag{30}$$

where I is the identity operator and α, β are real positive constants chosen such that $\overline{\Lambda}$ is completely positive. If we fix α and β such that $\overline{\Lambda}$ is trace preserving and β is maximized, then the results of Ref. [18] imply that

$$\overline{\Lambda}(\rho) = \frac{2^{(3/2)nr}}{2^{(3/2)nr}+1}\frac{I}{2^{nr}} + \frac{1}{2^{(3/2)nr}+1}\Lambda(\rho), \tag{31}$$

where n is the number of qubits in each copy of the state and r is the degree of the $K_{\vec{\sigma}}$ for which we are estimating the modulus squared.

On replacing Λ with $\overline{\Lambda}$ in our network the expectation value of the Z measurement still allows the modulus squared of the $K_{\vec{\sigma}}$ invariant to be determined via

$$|K_{\vec{\sigma}}|^2 = (2^{(3/2)nr}+1)\langle Z\rangle - 2^{nr}. \tag{32}$$

However, the SPA does affect the accuracy to which the invariant is determined. This is discussed further in the following section. Additionally, in Ref. [21], it is shown that this sort of SPA can be implemented by LOCC. Thus, the SLOCC invariants could also be estimated by LOCC, but the efficiency discussed in Sec. VII B would be affected.

VII. EVALUATION

The main aim of the protocols presented in Secs. III and V is to provide a physical interpretation for the polynomial invariants. However, we have not yet addressed the question of how efficient these measurement protocols are. In this section, we compare the efficiency of our protocols to protocols based on simply measuring the state coefficients and calculating the invariants. We use unbiased estimators based on counting [27–29]. Also, we perform the analysis in the limit where a large number of copies of the state have been measured, so that the variances of the estimates are small and can be treated to first order in all subsequent calculations. We note that more sophisticated estimation procedures are also possible [30], but our purpose here is to compare the networks to methods that are easily accessible experimentally.

Measuring the state coefficients would clearly be a more straightforward procedure to perform experimentally than using our network. Although more parameters have to be determined, this does not necessarily mean that it is a less efficient method for estimating the invariants than using our networks. There are several quite general reasons why this might be the case.

First, suppose that we are interested in measuring a complete set of polynomial LU invariants for some unknown state of n parties, where each party has a d-dimensional Hilbert space. In general, we do not know how many we would need to measure, but parameter counting arguments [1–3] show that the number of local degrees of freedom is linear in

n whereas the total number of degrees of freedom is exponential in n. Thus, for large n almost all the degrees of freedom are nonlocal. Even for moderately sized n, there are nearly as many algebraically independent invariants as there are state coefficients [35]. In addition, the invariants are typically highly nonlinear functions of the state coefficients. For these reasons, we expect that measuring a complete set of invariants directly will generally not be more efficient than measuring the state coefficients for large n. Similar considerations also apply to the SLOCC invariants.

Despite these considerations, it may be the case that our networks are more efficient if we are only interested in measuring a small incomplete subset of the invariants. Also, they may be more efficient for estimating complete sets when n is small. For this reason, and for simplicity, we concentrate on estimating two-qubit invariants in this section.

There are also other reasons why our protocols may not be efficient. For example, our protocols only employ a two-outcome measurement for each r copies of the state whereas estimating the state coefficients uses a two-outcome measurement on each copy. Also, for the $K_{\vec{\sigma}}$ invariants, we will see that using the SPA introduces a lot of noise into the measurement. Nonetheless, there are still some cases where using our networks is more efficient than estimating the state coefficients.

A. Statistical analysis of the network

For a particular setup in our network we make repeated measurements of an observable Z, with expectation value $F = \mathrm{Tr}(U\rho')$. Z is a random variable [36] with distribution

$$p(Z = +1) = \tfrac{1}{2}(1+F),$$

$$p(Z = -1) = \tfrac{1}{2}(1-F). \tag{33}$$

If we define the event $Z=+1$ as a success and set $p = P(Z=+1)$ then repeating the network N times is equivalent to performing N Bernoulli trials. The number of successes N_s is a random variable with a binomial distribution and its expectation value is $\langle N_s\rangle = Np = (N/2)(1+F)$. In an actual experiment, the observed number of successes $\hat{N}_s$ can be used to compute an unbiased estimator for F, given by

$$\hat{F} = 2\frac{\hat{N}_s}{N} - 1 \tag{34}$$

with variance

$$\mathrm{var}(\hat{F}) = \frac{1}{N}(1-F^2). \tag{35}$$

We are interested in determining how many trials are needed in order for the estimate $\hat{F}$ to be reasonably accurate. Specifically, we would like to quantify how many trials are needed to make the variance of $\mathrm{var}(\hat{F}) \leqslant \epsilon$ for some $\epsilon > 0$. In an experimental situation, we would not be able to calculate $\mathrm{var}(\hat{F})$ from our data, so we would have to estimate it using the sample variance, $\hat{\mathrm{var}}(\hat{F})$. However, in the limit $N \to \infty$ we can use the fact that $\mathrm{var}(\hat{F}) = O(N^{-1})$ and $\mathrm{var}[\hat{\mathrm{var}}(\hat{F})] = O(N^{-4})$, i.e., $\hat{\mathrm{var}}(\hat{F})$ converges to the true variance much faster than $\hat{F}$ converges to F so $\hat{\mathrm{var}}(\hat{F}) \approx \mathrm{var}(\hat{F})$. Thus, in this limit we have that

$$N \gtrsim \frac{1}{\epsilon}(1-F^2). \tag{36}$$

Recall that for the LU invariants, the real and imaginary parts of the invariant are estimated independently and that each use of the network requires r copies of the state, where r is the degree of the invariant in α. If we use the same number of samples for estimating both the real and imaginary parts then the total number of copies required is

$$M \gtrsim \frac{r}{\epsilon}(2 - |J_{\vec{\sigma}}|^2). \tag{37}$$

In some cases, we know *a priori* that the invariant is always real or always imaginary. If this is the case, then we can achieve the same accuracy with

$$M \gtrsim \frac{r}{\epsilon}(1 - |J_{\vec{\sigma}}|^2). \tag{38}$$

For the SLOCC invariants, each use of the network requires r copies of the state, where r is the degree of the invariant in α. Also the estimate of the invariant must take into account the use of the SPA via Eq. (32). In this case, the total number of copies required is

$$M \gtrsim \frac{r}{\epsilon}[(2^{(3/2)nr}+1)^2 - (|K_{\vec{\sigma}}|^2 + 2^{nr})^2]. \tag{39}$$

Notice that the 2^{3nr} term will dominate the term in the square bracket for large n and r. This is due to the noise introduced into the measurement by the SPA.

B. Comparison to methods based on state estimation

In order to evaluate our protocols, we compare them to methods based on estimating the density matrix of the state and then calculating the invariants. We do this by estimating each state coefficient using observations on single copies of the state. This is known as homodyne tomography (see Ref. [30] for an overview and also Refs. [27–29]). This is not the optimal way of reconstructing the state in general [31], but it will greatly simplify the analysis.

1. Example: Two-qubit LU invariants

A general two-qubit density matrix can be written as

$$\rho = \frac{1}{4}\left(I_2 \otimes I_2 + \sum_j a_j \sigma_j \otimes I_2 + \sum_j b_j I_2 \otimes \sigma_j + \sum_{j,k} R_{jk}\sigma_j \otimes \sigma_k\right). \tag{40}$$

The two-qubit LU invariant (3) can be written in terms of these coefficients as

$$J = \mathrm{Tr}(\rho_B^2) = \frac{1}{2}\left(1 + \sum_j b_j^2\right). \tag{41}$$

Each b_j can be determined by simply performing a σ_j measurement on N_j copies of Bob's half of the state. The probability distributions of the associated random variables are given by

$$p(\sigma_j = +1) = \tfrac{1}{2}(1 + b_j),$$

$$p(\sigma_j = -1) = \tfrac{1}{2}(1 - b_j). \tag{42}$$

Thus, each b_j can be estimated in the same way as F in Eq. (34) and we have that

$$\mathrm{var}(\hat{b}_j) = \frac{1 - b_j^2}{N_j}. \tag{43}$$

We can then construct an estimator for J given by

$$\hat{J} = \frac{1}{2}\left(1 + \sum_j \hat{b}_j{}^2\right), \tag{44}$$

which will be biased, but in the large N_j limit

$$\mathrm{var}(\hat{J}) \approx \sum_j b_j^2 \left(\frac{1 - b_j^2}{N_j}\right) \tag{45}$$

to first order in $\mathrm{var}(b_j)$.

If we make the additional restriction that each observable σ_j is sampled the same number of times (i.e., $N_j = N/3$) then we must take

$$N \gtrsim \frac{3}{\epsilon} \sum_j b_j^2 (1 - b_j^2) \tag{46}$$

for our estimate to have variance $\lessapprox \epsilon$.

One way to compare this to the result for our network is to take an average over all pure states. If we assume that all pure states are equally likely, i.e., integrate (Sec. VII B) and Eq. (46) using Haar measure (for details see Ref. [32]), then we find that on average we will need $3/2$ times as many copies of the state if we use the coefficient estimation method. This is half of what one might expect from parameter counting alone, since three times as many parameters are estimated in the state coefficient method. The factor of two is explained by the fact that each use of our network uses two copies of the state.

However, it is possible to find parameter ranges in which the state coefficient method performs better than our networks. One such range is given by setting $b_1 = b_2 = 0$, $-\sqrt{3/5} < b_3 < \sqrt{3/5}$. This illustrates the fact that parameter counting does not always reflect the statistical efficiency of a given protocol. Any partial information we have available about the type of states being measured might change our judgement of which protocol is more efficient.

2. Example: Two-qubit SLOCC invariants

For the two-qubit SLOCC invariants we take the quadratic invariant (19) as an example. In terms of the decomposition (40) this can be written as

$$|K|^2 = \frac{1}{4}\left[1 - \sum_j (a_j^2 + b_j^2) + \sum_{jk} R_{jk}^2\right]. \tag{47}$$

If we estimate this by measuring all 15 of the state coefficients an equal number of times then by a similar analysis to the LU case we find that we need at least

$$N \gtrsim \frac{15}{4\epsilon}\left[\sum_j [a_j^2(1 - a_j^2) + b_j(1 - b_j^2)] + \sum_{jk} R_{jk}^2 (1 - R_{jk}^2)\right] \tag{48}$$

copies of the state to get a variance $\lessapprox \epsilon$.

Taking averages, one finds that fewer copies are needed in the state coefficient protocol by a factor $\approx 5 \times 10^3$ despite the fact that many more parameters have to be estimated in this protocol than when using our network. This is largely due to the factor 2^{12} that appears in Eq. (39), which arises from the noise introduced by the SPA. This suggests that other estimation and detection protocols based on the SPA [15,19] may be less efficient than parameter counting arguments would imply. In fact, there are no states for which our network performs better than the coefficient estimation method. Even in the best possible case for our network, the state coefficient method requires fewer states by about three orders of magnitude.

VIII. CONCLUSIONS

We have presented networks for measuring the polynomial invariants of quantum states under LU and SLOCC transformations. The structure of these networks is closely related to the structure of the invariants themselves and thus gives the invariants a physical interpretation. Comparison of these networks with methods based on estimating the state coefficients indicate that the networks are of limited practical use for estimating complete sets of invariants. Indeed, our results suggest that any estimation procedure that employs the SPA is statistically inefficient even when the number of parties is small [37].

We know that no procedure for estimating invariants directly can outperform protocols based on estimating the state coefficients as the number of parties is increased. For small number of parties it seems that there can be some increase in efficiency, but the optimal protocol is not known in general.

ACKNOWLEDGMENTS

A.W. was supported by the UK Engineering and Physical Sciences Research Council (EPSRC). We would like to thank the EC for support for this project through the project RESQ.

[1] N. Linden and S. Popescu, Fortschr. Phys. **46**, 567 (1998).
[2] H. Carteret, N. Linden, S. Popescu, and A. Sudbery, Found. Phys. **29**, 527 (1999).
[3] N. Linden, S. Popescu, and A. Sudbery, Phys. Rev. Lett. **83**, 243 (1999).
[4] A. Sudbery, J. Phys. A **34**, 643 (2001).
[5] H. Carteret and A. Sudbery, J. Phys. A **33**, 4981 (2000).
[6] M. Grassl, M. Rötteler, and T. Beth, Phys. Rev. A **58**, 1833 (1998).
[7] F. Verstraete, J. Dehaene, and B. De Moor, e-print quant-ph/0105090.
[8] F. Verstraete, J. Dehaene, and B. De Moor, Phys. Rev. A **65**, 032308 (2002).
[9] F. Verstraete, J. Dehaene, B. De Moor, and H. Verschelde, Phys. Rev. A **65**, 052112 (2002).
[10] G. Jaeger, A. Teodorescu-Frumosu, M. Sergienko, B. A. E. Saleh, and M. C. Teich, Phys. Rev. A **67**, 032307 (2003).
[11] M. Teodorescu-Frumosu and G. Jaeger, Phys. Rev. A **67**, 052305 (2003).
[12] G. Jaeger, A. V. Sergienko, B. E. A. Saleh, and M. C. Teich, Phys. Rev. A **68**, 022318 (2003).
[13] J.-G. Luque and J.-Y. Thibon, Phys. Rev. A **67**, 042303 (2003).
[14] A. Acín, R. Tarrach, and G. Vidal, Phys. Rev. A **61**, 062307 (2000).
[15] P. Horodecki, e-print quant-ph/0111064.
[16] R. Brauer, Ann. Math. **38**, 857 (1937).
[17] E. M. Rains, IEEE Trans. Inf. Theory **46**, 54 (2000).
[18] P. Horodecki, e-print quant-ph/0111036.
[19] P. Horodecki and A. Ekert, Phys. Rev. Lett. **89**, 127902 (2002).
[20] A. K. Ekert *et al.*, Phys. Rev. Lett. **88**, 217901 (2002).
[21] C. M. Alves, P. Horodecki, D. K. L. Oi, L. C. Kwek, and A. K. Ekert, e-print quant-ph/0304123.
[22] C. H. Bennett, S. Popescu, D. Rohrlich, J. A. Smolin, and A. V. Thapliyal, Phys. Rev. A **63**, 012307 (2001).
[23] W. Dür, G. Vidal, and J. I. Cirac, Phys. Rev. A **62**, 062314 (2000).
[24] W. K. Wootters, Phys. Rev. Lett. **80**, 2245 (1998).
[25] W. K. Wootters, Philos. Trans. R. Soc. London **356**, 1717 (1998).
[26] V. Coffman, J. Kundu, and W. K. Wootters, Phys. Rev. A **61**, 052306 (2000).
[27] D. T. Smithey, M. Beck, M. G. Raymer, and A. Faridani, Phys. Rev. Lett. **70**, 1244 (1993).
[28] U. Leonhardt, *Measuring the Quantum State of Light* (Cambridge University Press, Cambridge, 1997).
[29] G. M. d'Ariano, C. Macchiavello, and M. G. A. Paris, Phys. Rev. A **50**, 4298 (1994).
[30] R. Gill and M. I. Guta, e-print quant-ph/0303020.
[31] O. E. Barndorff-Nielsen, R. Gill, and P. E. Jupp, J. R. Stat. Soc. Ser. B. Methodol. **65**, 1 (2003); URL http://www.math.uu.nl/people/gill/Preprints/qiread9statsoc.pdf
[32] V. Bužek *et al.*, Chaos, Solitons Fractals **10**, 981 (1999).
[33] D. R. Cox and D. V. Hinkley, *Theoretical Statistics* (Chapman and Hall, London, 1974).
[34] H. A. Carteret, e-print quant-ph/0309212.
[35] Further invariants are required to specify the full ring of invariants under LU transformations.
[36] The statistical inference theory used in this section can be found in many statistics textbooks, such as Ref. [33].
[37] However, since this work first appeared it has been shown [34] that the SLOCC invariants can be estimated without the need for introducing noise and circuits have been explicitly constructed for the concurrence and 3-tangle. The statistical efficiency of these circuits has not yet been analyzed.