Parts of quantum states

Nick S. Jones* and Noah Linden†
Department of Mathematics, University of Bristol, University Walk, Bristol BS8 1TW, United Kingdom
(Received 25 August 2004; published 18 January 2005)

It is shown that generic N-party pure quantum states (with equidimensional subsystems) are uniquely determined by their reduced states of just over half the parties; in other words, all the information in almost all N-party pure states is in the set of reduced states of just over half the parties. For N even, the reduced states in fewer than $N/2$ parties are shown to be an insufficient description of almost all states (similar results hold when N is odd). It is noted that real algebraic geometry is a natural framework for any analysis of parts of quantum states: two simple polynomials, a quadratic and a cubic, contain all of their structure. Algorithmic techniques are described which can provide conditions for sets of reduced states to belong to pure or mixed states.

DOI: 10.1103/PhysRevA.71.012324 PACS number(s): 03.67.Mn, 03.65.Ud, 03.65.Ta, 02.70.Wz

I. INTRODUCTION

Given parts of pure, multiparty, quantum states, where the parts are reduced states in subsets of the parties, what does one know about the whole? One might have expected that the parts leave something out: that most pure states contain higher-order correlations that are independent of the lower-order ones. This is not the case.

In fact, knowing the reduced states in appropriate subsets of the parties specifies the state completely [1,2]; the only state, pure or mixed, consistent with these reduced states is the original state itself. Thus all the information in most pure multiparty states resides in these reduced states.

In [2] upper and lower bounds were found on the size of the subsets whose reduced states determine the full pure states. It was shown that reduced states in no more than two-thirds of the parties are sufficient (generically). The upper bound was independent of the local dimension, but the lower bound in [2] was dimension dependent, varying from about 18.9% for qubits ($d=2$) and increasing monotonically to one-half for large local dimension. A main result of this paper is to improve both bounds to close to one-half.

Specifically we show that, considering the m-party reduced states of an N-party pure state (each party having equidimensional Hilbert spaces), a small, interesting (see Fig. 1) set of reduced states in $m=\lceil N/2\rceil+1$ parties (where $\lceil\ \rceil$ and $\lfloor\ \rfloor$ indicate rounding up and down to the nearest integer) almost always forms a unique description of the state. We also prove the lower bound that the $\lfloor N/2\rfloor$-party reduced states of pure states do not uniquely distinguish them from other pure or mixed states.

A question, closely related to the above, is, given a set of reduced states, under what circumstances are they compatible with *any* states (not necessarily unique or pure) of the full system. One can think of reduced states as jigsaw puzzle pieces and the question is whether there exist one, or more, jigsaw puzzles of which these are some of the pieces. In [1] examples were given which show this can be a complicated issue and a number of authors [3–6] have made partial progress. In Sec. IV, by giving a particular characterization of quantum states, we describe how real algebraic geometry (RAG)—the geometric study of real roots of polynomials [7]—provides a unified mathematical description for these quantum jigsaw puzzles. Methods from RAG provide systematic algorithms for tasks like finding conditions that sets of reduced states must satisfy in order to be compatible with a quantum state of the full system. While future developments in algorithmic RAG may well make it a useful tool for questions of this sort, these tasks appear to be hard in a technical sense. Despite this, given the simplicity of the equations involved, a sphere and cubic surface [Eq. (22)], there is hope that analytic progress can be made.

Section II provides the proof of the upper bound that reduced states in $\geqslant\lceil N/2\rceil+1$ parties generically uniquely characterize the state. Section III proves the lower bound. Section IV reveals how real algebraic geometry provides a framework for understanding questions about parts of quantum states. We conclude with some open questions.

II. UPPER BOUND

We consider a pure quantum state of N parties, each of which has a d-dimensional Hilbert space. In the first instance

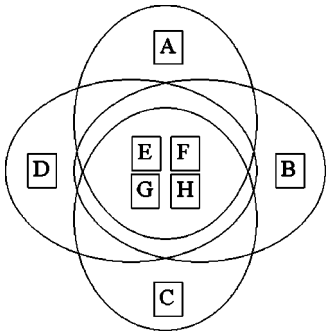

FIG. 1. The four overlapping, five-party reduced states ρ_{AEFGH}, ρ_{BEFGH}, ρ_{CEFGH}, ρ_{DEFGH} are almost always a sufficient description of the eight-party pure state $|\phi\rangle_{ABCDEFGH}$.

*Email address: n.s.jones@bristol.ac.uk
†Email address: n.linden@bristol.ac.uk

we will consider the case that N is even. We will show that almost every such quantum state is completely determined by its reduced states of $N/2+1$ parties: for almost every pure state of N parties, the unique state, pure or mixed, consistent with these reduced states is the original state.

There are $\binom{N}{N/2+1}$ reduced states of $(N/2+1)$ parties. In fact, we will show that knowledge of only $N/2$ of them is sufficient, generically, to uniquely specify an N-party pure state consistent with them. The set of $N/2$ reduced states may be described as follows. Select $N/2$ parties (for convenience and without loss of generality we take these to be parties $N/2+1, N/2+2, \ldots, N$); then form $(N/2+1)$-party reduced states by combining these $N/2$ parties with one further party. Since there are $N/2$ choices for this last party we have a set of $N/2$ $(N/2+1)$-party reduced states—this is illustrated in Fig. 1 for $N=8$. We will write the original pure state as

$$|\phi\rangle_N = \sum_{i_1,\ldots,i_N}^{d} a_{i_1,i_2,\ldots,i_N} |i_1, \ldots, i_N\rangle. \tag{1}$$

Let us consider one of these reduced states obtained by tracing out parties $2,3,\ldots,N/2$ and call it ρ^1:

$$\rho^1 = \sum_{\substack{i_1,\ldots,i_N,\\ j_1,j_{N/2+1},\ldots,j_N}}^{d} a_{i_1,\ldots,i_N} a^*_{j_1,i_2,\ldots,i_{N/2}j_{N/2+1},\ldots,j_N} |i_1, i_{N/2+1}, \ldots, i_N\rangle\langle j_1, j_{N/2+1}, \ldots, j_N|. \tag{2}$$

The most general state of N parties, for which this is a reduced state, will typically be mixed. To allow for this possibility, we consider an environment E with which the system might be entangled in such a way that the whole system is in a pure state $|\psi\rangle$. The most general pure state of system plus environment, consistent with ρ^1, is

$$|\psi^1\rangle = \sum_{i_1,\ldots,i_N}^{d} a_{i_1,\ldots,i_N} |i_1, i_{N/2+1}, \ldots, i_N\rangle |E^1_{i_2,i_3,\ldots,i_{N/2}}\rangle, \tag{3}$$

where the states $|E^1_{i_2,\ldots,i_{N/2}}\rangle$ are states of parties 2,3, up to $N/2$, plus the environment. The $d^{N/2-1}$ vectors $|E^1_{i_2,i_3,\ldots,i_{N/2}}\rangle$ must satisfy

$$\langle E^1_{i_2,\ldots,i_{N/2}} | E^1_{j_2,\ldots,j_{N/2}}\rangle = \delta_{i_2 j_2}, \ldots, \delta_{i_{N/2} j_{N/2}} \tag{4}$$

to ensure that the state $|\psi^1\rangle$, when reduced to parties $(1, N/2+1, \ldots, N)$, yields ρ^1. In fact we will not need to use Eq. (4) to prove our result that the $(N/2+1)$-party reduced states uniquely specify a pure quantum state of N parties.

It will be convenient to rewrite each state $|E^1_{i_2,i_3,\ldots,i_{N/2}}\rangle$ explicitly as an entangled state of system plus environment:

$$|E^1_{i_2,i_3,\ldots,i_{N/2}}\rangle = \sum_{j_2,\ldots,j_{N/2}}^{d} |j_2, \ldots, j_{N/2}\rangle |e^1_{i_2,\ldots,i_{N/2};j_2,\ldots,j_{N/2}}\rangle, \tag{5}$$

where $|e^1_{i_2,\ldots,i_{N/2};j_2,\ldots,j_{N/2}}\rangle$ are states of the environment which need not be normalized or orthogonal, but must only be such that (4) holds. The upper index on the vectors $|e\rangle$ denotes the fact that these are the states of the environment arising from purifications of ρ^1.

$|\psi^1\rangle$, the most general pure state of system and environment consistent with ρ^1, is then

$$|\psi^1\rangle = \sum_{\substack{i_1,\ldots,i_N,\\ j_2,\ldots,j_{N/2}}}^{d} a_{i_1,j_2,\ldots,j_{N/2},i_{N/2+1},\ldots,i_N} |i_1, \ldots, i_N\rangle |e^1_{j_2,\ldots,j_{N/2};i_2,\ldots,i_{N/2}}\rangle. \tag{6}$$

If ρ^2 is the reduced state of parties $(2, N/2+1, N/2+2, \ldots, N)$ arising from the original state $|\phi\rangle_N$ then $|\psi^2\rangle$, the most general state of system plus environment consistent with ρ^2, is

$$|\psi^2\rangle = \sum_{\substack{i_1,\ldots,i_N,\\ j_1,j_3\ldots j_{N/2}}}^{d} a_{j_1,i_2,j_3,\ldots,j_{N/2},i_{N/2+1},\ldots,i_N} |i_1, \ldots, i_N\rangle |e^2_{j_1,j_3,\ldots,j_{N/2};i_1,i_3,\ldots,i_{N/2}}\rangle. \tag{7}$$

ρ^1 and ρ^2 are both $(N/2+1)$-party reduced states of the original pure state $|\phi\rangle_N$. ρ^1 and ρ^2 have parties $N/2,\ldots,N$ in common: ρ^1 is a state of party 1 and parties $(N/2+1),\ldots,N$ and ρ^2, party 2 and parties $(N/2+1),\ldots,N$. There are analogous states $|\psi^3\rangle,\ldots,|\psi^{N/2}\rangle$ arising from the reduced states $\rho^3,\ldots,\rho^{N/2}$. For there to exist one or more pure states which have $\rho^1,\ldots,\rho^{N/2}$ as their reduced states, these states $|\psi^1\rangle,\ldots,|\psi^{N/2}\rangle$ must be equal.

We will show below that this requirement leads to

$$|e^1_{j_2,\ldots,j_{N/2};i_2,\ldots,i_{N/2}}\rangle = \delta_{j_2 i_2}\delta_{j_3 i_3},\ldots,\delta_{j_{N/2} i_{N/2}}|e^1_{11,\ldots,1;11,\ldots,1}\rangle; \tag{8}$$

all environment states are multiples of a fixed state $|e^1_{11,\ldots,1;11,\ldots,1}\rangle$ so that $|\psi^1\rangle=|\phi\rangle_N|e^1_{11,\ldots,1;11,\ldots,1}\rangle$. $|\psi^1\rangle$ is a product state of the original pure state with a state of the environment. Hence, the unique state of the system consistent with the reduced states is $|\phi\rangle_N$, the original state.

We now prove this result. We first deduce conditions on the states of the environment imposed by requiring $|\psi^1\rangle=|\psi^2\rangle$. From Eqs. (6) and (7) and comparing terms,

$$\sum_{j_2,\ldots,j_{N/2}}^{d} a_{i_1,j_2,\ldots,j_{N/2},i_{N/2+1},\ldots,i_N}|e^1_{j_2,\ldots,j_{N/2};i_2,\ldots,i_{N/2}}\rangle = \sum_{j_1,j_3,\ldots,j_{N/2}}^{d} a_{j_1,i_2,j_3,\ldots,j_{N/2},i_{N/2+1},\ldots,i_N}|e^2_{j_1,j_3,\ldots,j_{N/2};i_1,i_3,\ldots,i_{N/2}}\rangle, \tag{9}$$

for all $(i_1,\ldots,i_N)$. Writing $\mathbf{u}=i_{N/2+1},\ldots,i_N$ $\mathbf{v}=i_3,\ldots,i_{N/2}$, $\mathbf{v}'=j_3,\ldots,j_{N/2}$ the above becomes

$$\sum_{j_2,\mathbf{v}'} a_{i_1,j_2,\mathbf{v}',\mathbf{u}}|e^1_{j_2,\mathbf{v}';i_2,\mathbf{v}}\rangle = \sum_{j_1,\mathbf{v}'} a_{j_1,i_2,\mathbf{v}',\mathbf{u}}|e^2_{j_1,\mathbf{v}';i_1,\mathbf{v}}\rangle, \tag{10}$$

for all $(i_1,i_2,\mathbf{u},\mathbf{v})$. It is convenient to rewrite this as

$$\sum_{j_2\neq i_2,\mathbf{v}'} a_{i_1,j_2,\mathbf{v}',\mathbf{u}}|e^1_{j_2,\mathbf{v}';i_2,\mathbf{v}}\rangle - \sum_{j_1\neq i_1,\mathbf{v}'} a_{j_1,i_2,\mathbf{v}',\mathbf{u}}|e^2_{j_1,\mathbf{v}';i_1,\mathbf{v}}\rangle + \sum_{\mathbf{v}'} a_{i_1,i_2,\mathbf{v}',\mathbf{u}}[|e^1_{i_2,\mathbf{v}';i_2,\mathbf{v}}\rangle - |e^2_{i_1,\mathbf{v}',i_1,\mathbf{v}}\rangle] = 0 \tag{11}$$

for all $(i_1,i_2,\mathbf{u},\mathbf{v})$. Note that the index $\mathbf{u}$ takes $d^{N/2}$ values. Let us set $(i_1,i_2,\mathbf{v})=(c_1,c_2,c_\mathbf{v})$ for some constant integers $c_1,c_2,c_\mathbf{v}$. We will consider sets of $d^{N/2}$ equations in which $\mathbf{u}$ varies and the other indices are fixed. The above equation becomes

$$\sum_{j_2\neq c_2,\mathbf{v}'} a_{c_1,j_2,\mathbf{v}',\mathbf{u}}|e^1_{j_2,\mathbf{v}';c_2,c_\mathbf{v}}\rangle - \sum_{j_1\neq c_1,\mathbf{v}'} a_{j_1,c_2,\mathbf{v}',\mathbf{u}}|e^2_{j_1,\mathbf{v}';c_1,c_\mathbf{v}}\rangle + \sum_{\mathbf{v}'} a_{c_1,c_2,\mathbf{v}',\mathbf{u}}[|e^1_{c_2,\mathbf{v}';c_2,c_\mathbf{v}}\rangle - |e^2_{c_1,\mathbf{v}',c_1,c_\mathbf{v}}\rangle] = 0. \tag{12}$$

For a given $\mathbf{u}$, the terms in $|e^1_{j_2,\mathbf{v}';c_2,c_\mathbf{v}}\rangle$ $(j_2\neq c_2)$, $|e^2_{j_1,\mathbf{v}';c_1,c_\mathbf{v}}\rangle$ $(j_1\neq c_1)$, and $[|e^1_{c_2,\mathbf{v}';c_2,c_\mathbf{v}}\rangle-|e^2_{c_1,\mathbf{v}',c_1,c_\mathbf{v}}\rangle]$ all have different coefficients for all $j_1,j_2,\mathbf{v}'$ values. Similarly, on comparing any two equations with different $\mathbf{u}$ values one notes that the coefficients of $|e^1_{j_2,\mathbf{v}';c_2,c_\mathbf{v}}\rangle$, $|e^2_{j_1,\mathbf{v}';c_1,c_\mathbf{v}}\rangle$ and $[|e^1_{c_2,\mathbf{v}';c_2,c_\mathbf{v}}\rangle-|e^2_{c_1,\mathbf{v}',c_1,c_\mathbf{v}}\rangle]$ are all indexed by $\mathbf{u}$—so between equations with different $\mathbf{u}$ values, the coefficients will differ. Let us treat $|e^1_{j_2,\mathbf{v}';c_2,c_\mathbf{v}}\rangle, |e^2_{j_1,\mathbf{v}';c_1,c_\mathbf{v}}\rangle$ and $[|e^1_{c_2,\mathbf{v}';c_2,c_\mathbf{v}}\rangle - |e^2_{c_1,\mathbf{v}',c_1,c_\mathbf{v}}\rangle]$ for all $\mathbf{v}'$, $j_1\neq c_1$, $j_2\neq c_2$, as the variables in a set of $d^{N/2}$ homogeneous equations indexed by $\mathbf{u}$. There are $2d^{N/2-1}-d^{N/2-2}$ of these variables [recall that $(c_1,c_2,c_\mathbf{v})$ are fixed]. Since we know that all of the coefficients of the variables are distinct, and generically there is no relationship between them, we can pick a subset of $2d^{N/2-1}-d^{N/2-2}$ equations from the $d^{N/2}$ and solve to show $|e^1_{j_2,\mathbf{v}';c_2,c_\mathbf{v}}\rangle=0$ for all $\mathbf{v}', j_2\neq c_2$, $|e^2_{j_1,\mathbf{v}';c_1,c_\mathbf{v}}\rangle=0$ for all $\mathbf{v}', j_1\neq c_1$, and $|e^1_{c_2,\mathbf{v}';c_2,c_\mathbf{v}}\rangle = |e^2_{c_1,\mathbf{v}',c_1,c_\mathbf{v}}\rangle$ for all $\mathbf{v}'$. By repeating the above procedure for different c_2 and $c_\mathbf{v}$ values we find $|e^1_{j_2,\mathbf{v}';i_2,\mathbf{v}}\rangle=\delta_{j_2 i_2}|e^1_{1,\mathbf{v}';1,\mathbf{v}}\rangle$.

Having considered $|\psi^1\rangle=|\psi^2\rangle$ we now study $|\psi^1\rangle=|\psi^r\rangle$ for all r, $1<r\leq N/2$, and find similarly $|e^1_{j_r,\mathbf{w}';i_r,\mathbf{w}}\rangle = \delta_{j_r i_r}|e^1_{1,\mathbf{w}';1,\mathbf{w}}\rangle$ where $\mathbf{w}=i_2,i_3,\ldots,i_{r-1},i_{r+1},\ldots,i_{N/2}$ and $\mathbf{w}'=j_2,j_3,\ldots,j_{r-1},j_{r+1},\ldots,j_{N/2}$. Combining these results we obtain Eq. (8). A similar analysis can be repeated for N odd. Here a set of $(N-1)/2$ reduced states in $(N+3)/2$ parties, generically, uniquely determines the quantum state.

III. LOWER BOUND

We now derive a lower bound: the reduced states of this fraction of the parties are not sufficient (generically) to allow one to reconstruct a unique state of the full system. Again one starts with a pure state $|\phi\rangle_N$ of N parties. We calculate all m-party reduced states. We then ask whether these $\binom{N}{m}$ m-party reduced states are consistent with a unique starting state (i.e., $|\phi\rangle$) or whether there are other (typically mixed) states of N parties consistent with these $\binom{N}{m}$ m-party reduced states. We show that reduced states of $\lfloor N/2\rfloor$ parties do not contain enough information to reconstruct a unique state.

Consider a starting N-party pure state $|\phi\rangle_N$. Let us calculate from it the reduced state $\rho^{(1)}$ of the first m parties ($m\leq N/2$). This will typically have rank d^m, and we may expand it as

$$\rho^{(1)} = \sum_{a=1}^{d^m} |v^{(1)}_a\rangle\langle v^{(1)}_a|, \tag{13}$$

where $|v^{(1)}_a\rangle$ are non-normalized eigenvectors of $\rho^{(1)}$. The most general state of N parties consistent with this reduced state will be mixed and of rank d^N. It will be convenient to purify this mixed state of N parties to a state $|\psi^{(1)}\rangle$ of N parties plus an environment of dimension d^N. So,

$$|\psi^{(1)}\rangle = \sum_{a=1}^{d^m} |v^{(1)}_a\rangle|F^{(1)}_a\rangle, \tag{14}$$

$$|F^{(1)}_a\rangle = \sum_{i_{m+1},\ldots,i_N}^{d} |i_{m+1},\ldots,i_N\rangle|f^{(1)}_{ai_{m+1},\ldots,i_N}\rangle, \tag{15}$$

$$|\psi^{(1)}\rangle = \sum_{a=1}^{d^m}\sum_{i_{m+1},\ldots,i_N}^{d} |v^{(1)}_a\rangle|i_{m+1},\ldots,i_N\rangle|f^{(1)}_{ai_{m+1},\ldots,i_N}\rangle. \tag{16}$$

The $d^m \times d^{N-m} = d^N$ states $|f^{(1)}_{ai_{m+1},\ldots,i_N}\rangle$ of the environment must satisfy

$$\sum_{i_{m+1},\ldots,i_N} \langle f^{(1)}_{ai_{m+1},\ldots,i_N} | f^{(1)}_{bi_{m+1},\ldots,i_N}\rangle = \delta_{ab}, \tag{17}$$

for $|\psi^{(1)}\rangle$ to reduce to $\rho^{(1)}$, the original reduced state of the first m parties. In the following we will group indices, writing $|f^{(1)}_{ai_{m+1}\ldots i_N}\rangle = |f^{(1)}_{\mu}\rangle$, $\mu = 1,\ldots,d^N$. Given a particular purification of a mixed m-party state one can form others by a unitary transformation on the environment alone. Let us fix this freedom by rotating the states $|f^{(1)}_{\mu}\rangle$ so that they are expressed in the following way with respect to a fixed orthonormal basis, $|1\rangle, |2\rangle, \ldots, |d^N\rangle$, of the environment:

$$|f^{(1)}_1\rangle = \alpha^{(1)}_{1,1}|1\rangle,$$

$$|f^{(1)}_2\rangle = \alpha^{(1)}_{2,1}|1\rangle + \alpha^{(1)}_{2,2}|2\rangle,$$

$$|f^{(1)}_3\rangle = \alpha^{(1)}_{3,1}|1\rangle + \alpha^{(1)}_{3,2}|2\rangle + \alpha^{(1)}_{3,3}|3\rangle,$$

$$\vdots$$

$$|f^{(1)}_{d^N}\rangle = \alpha^{(1)}_{d^N,1}|1\rangle + \alpha^{(1)}_{d^N,2}|2\rangle + \cdots + \alpha^{(1)}_{d^N,d^N}|d^N\rangle. \tag{18}$$

We may use the unitary freedom on the environment to arrange for the $\alpha^{(1)}_{\mu,\mu}$ to be real; the remaining coefficients $\alpha^{(1)}_{\mu,\nu}$ $(\nu < \mu)$ will be complex. The total number of real parameters in the states $|f^{(1)}_{\mu}\rangle$ is $d^N \times d^N = d^{2N}$.

Consider a different set of m parties. Again calculate the reduced states of $|\phi\rangle_N$ for these parties and purify it to a pure state $|\psi^{(2)}\rangle$ of the system plus environment using the environment spanned by $|1\rangle, |2\rangle, \ldots, |d^N\rangle$. This will lead to a different set of d^N states of the environment, $|f^{(2)}_{\mu}\rangle$. We will shortly be requiring that $|\psi^{(1)}\rangle = |\psi^{(2)}\rangle$ and therefore the states $|f^{(2)}_{\mu}\rangle$, lie in the span of the fixed basis of $|1\rangle, |2\rangle, \ldots, |d^N\rangle$. The number of real parameters describing the d^N vectors $|f^{(2)}_{\mu}\rangle$ is $2d^{2N}$. Proceeding in this way for each possible set of m parties, we find that the total number of parameters describing the $|f^{(A)}_{\mu}\rangle$ [for $A = 1,\ldots,\binom{N}{m}$] is

$$P = d^{2N} + 2\left[\binom{N}{m} - 1\right] d^{2N} = d^{2N}\left[2\binom{N}{m} - 1\right]. \tag{19}$$

A. Counting constraint equations

There are two types of constraint on the $|f^{(A)}_{\mu}\rangle$. First each set of $|f^{(A)}_{\mu}\rangle$, for fixed A, must satisfy equations like (17) which ensure that the purifications associated with these $|f^{(A)}_{\mu}\rangle$ reduce to the correct m-party reduced state.

The number of constraint equations for each A is d^{2m}, so that the total number of equations of this type is $\binom{N}{m} d^{2m}$ (this is an overestimate since many of these equations will be dependent).

The second set of constraints is that the purifications arising from each set of m parties are equal. The fact that $|\psi^{(1)}\rangle = |\psi^{(2)}\rangle$ leads to $2d^{2N}$ equations. Thus the total number of equations of this type (equating $|\psi^{(1)}\rangle$ to each of the other purifications) is $2d^{2N}\left[\binom{N}{m} - 1\right]$.

It may be that not all the constraints described are independent. An upper bound on the number of independent constraints is thus

$$C = 2d^{2N}\left[\binom{N}{m} - 1\right] + \binom{N}{m} d^{2m}. \tag{20}$$

B. Finding the lower bound on *m*

From above,

$$P - C = d^{2N} - \binom{N}{m} d^{2m}. \tag{21}$$

Thus for $m \leqslant N/2$, $d \geqslant 2$, $P > C$. The number of constraints is insufficient to uniquely specify the parameters and so, for N even, the reduced states in $N/2$ parties do not uniquely determine the state; for N odd, reduced states in $(N-1)/2$ parties do not uniquely define the state.

IV. QUANTUM JIGSAW PUZZLES

The considerations in previous sections lead us to address the following general (and related) questions. First, *given* some partial information about a putative quantum state (for example a set of reduced states) how does one check that this partial information is indeed consistent with one (or more) pure or mixed states. For example, for a state of three parties A, B, C one might be given three particular two-party density matrices $\sigma^{AB}, \tau^{BC}, \eta^{AC}$. One would like to be able to determine whether these three states are possible reduced states of any three-party quantum state ρ^{ABC}.

A second, more general, question is to determine conditions under which partial information about a putative quantum state is in fact legitimate. Referring to the example in the previous paragraph, rather than aiming to produce an algorithm which determines whether the *given* $\sigma^{AB}, \tau^{BC}, \eta^{AC}$ are reduced states of any ρ^{ABC}, one would like to have a set of conditions satisfied by the two-party reduced states of ρ^{ABC} (pure or mixed). Despite the similarity of these two questions it should be clear that algorithms for solving them may be rather different.

These questions are two versions of the task of, given a set of parts of quantum states, testing if there exists any state with these parts. In the same spirit, one might take a jumble of puzzle pieces and check to see if there exists a jigsaw puzzle of which these are the parts. One could test if a set of pieces make a whole puzzle by either trying to make that puzzle (testing a given set of parts) or checking the pieces against a system of rules (finding general compatibility conditions).

In this section we aim to show that both questions fall within the area of real algebraic geometry. The physical questions associated with compatibility of partial information about quantum states may be encoded in two polynomials in real variables; one polynomial is quadratic (defining a sphere) and the other cubic. Computational real algebraic geometry is an active field of current research with considerable effort being devoted to finding algorithms for pre-

cisely the problems important here. We believe that it is intrinsically interesting to identify the part of mathematics within which questions of compatibility of partial information about quantum states lie. One would also like to have methods for solving instances of the problems. In fact our problems, perhaps not surprisingly, are hard in a strict algorithmic sense. Unfortunately, the best algorithms that we are aware of are not sufficiently powerful at present to be useful for interesting cases on modest computers. Nonetheless we anticipate that, with increased algorithmic and computational power, this will change. In any case, we argue that techniques, analytic or algorithmic, from real algebraic geometry are required to solve problems concerning parts of quantum states.

We start by showing that necessary and sufficient conditions for a Hermitian matrix H to be the density matrix of a pure state (i.e., to be a positive, Hermitian matrix with trace 1 and exactly one nonzero eigenvalue) are that

$$\mathrm{Tr}(H^2) = \mathrm{Tr}(H^3) = 1. \tag{22}$$

[Note that $\mathrm{Tr}(H^2)=\mathrm{Tr}(H)=1$ are not sufficient conditions since they are satisfied by the nonpositive matrix $H=\mathrm{diag}(\frac{1}{2},\frac{1}{2},\frac{1}{2},-\frac{1}{2})$.] It is obvious that the density matrix of a pure state satisfies (22). To see that (22) is sufficient for H to be a density matrix, consider a basis for H in which it is diagonal with diagonal elements $(\lambda_1,\ldots,\lambda_n)$. Then $\Sigma_{i=1}^n\lambda_i^2=1$ implies that each λ_i satisfies $-1\leqslant\lambda_i\leqslant 1$. Then

$$\sum_{i=1}^{n}\lambda_i^3 \leqslant \sum_{i=1}^{n}\lambda_i^2, \tag{23}$$

with equality only when each $\lambda_i=0$ or $+1$. But our conditions (22) require equality in (23) and hence to be compatible with $\Sigma_{i=1}^n\lambda_i^2=1$, exactly one λ_i must be equal to $+1$.

In the first instance, we will illustrate the general issues concerning partial data for quantum states by considering the case of states of three qubits. In this setting it is helpful to write the state in terms of the Bloch decomposition. Any Hermitian, trace 1, 8×8 matrix may be written as

$$\begin{aligned}\rho_{ABC} = \frac{1}{8}(&1\otimes 1\otimes 1 + \alpha_i\sigma_i\otimes 1\otimes 1 + \beta_i 1\otimes\sigma_i\otimes 1 + \gamma_i 1\otimes 1\\ &\otimes\sigma_i + R_{ij}\sigma_i\otimes\sigma_j\otimes 1 + S_{ij}\sigma_i\otimes 1\otimes\sigma_j + T_{ij}1\otimes\sigma_i\\ &\otimes\sigma_j + Q_{ijk}\sigma_i\otimes\sigma_j\otimes\sigma_k),\end{aligned} \tag{24}$$

where the σ_i's are the Pauli matrices (which are Hermitian and traceless) and "1" is the 2×2 identity matrix. $(1,\sigma_x,\sigma_y,\sigma_z)$ form a basis for all 2×2 matrices. Note that $\alpha_i=\mathrm{Tr}(\rho_A\sigma_i)$, $R_{ij}=\mathrm{Tr}(\rho_{AB}\sigma_i\otimes\sigma_j)$, etc. Using this parametrization of ρ^{ABC}, (22) becomes

$$\begin{aligned}\mathrm{Tr}\rho^2 = \frac{1}{8}(&1+\alpha_i\alpha_i+\beta_i\beta_i+\gamma_i\gamma_i+S_{ij}S_{ij}+R_{ij}R_{ij}+T_{ij}T_{ij}\\ &+Q_{ijk}Q_{ijk})\\ =&\,1,\end{aligned} \tag{25}$$

$$\begin{aligned}\mathrm{Tr}\rho^3 = \frac{1}{64}[&1+3(\alpha_i\alpha_i+\beta_i\beta_i+\gamma_i\gamma_i+S_{ij}S_{ij}+R_{ij}R_{ij}+T_{ij}T_{ij}\\ &+Q_{ijk}Q_{ijk})+6(R_{ij}\alpha_i\beta_j+S_{ij}\alpha_i\gamma_j+T_{ij}\beta_i\gamma_j+Q_{ijk}\alpha_iT_{jk}\\ &+Q_{ijk}\beta_jS_{ik}+Q_{ijk}\gamma_kR_{ij}+R_{ki}T_{ij}S_{kj})-6(R_{ij}R_{kl}R_{mn}\\ &+S_{ij}S_{kl}S_{mn}+T_{ij}T_{kl}T_{mn})\epsilon_{ikm}\epsilon_{jln}\\ &-6Q_{ijk}Q_{nop}(R_{lm}\epsilon_{inl}\epsilon_{jom}\delta_{kp}+S_{lm}\epsilon_{inl}\epsilon_{kpm}\delta_{jo}\\ &+T_{lm}\epsilon_{jol}\epsilon_{kpm}\delta_{in})]\\ =&\,1.\end{aligned} \tag{26}$$

Note that Eq. (25) defines a sphere. If ρ satisfies these conditions it is a pure quantum state.

A. Testing a given set of parts

At the beginning of the last section we described two types of questions concerning parts of quantum states. The first was, given a particular set of partial information about a putative state, can one determine whether this information is legitimate. In the case of three qubits we might be given, for example, three two-party density matrices $\sigma^{AB},\tau^{BC},\eta^{AC}$. There are some simple compatibility relations which are easily checked, namely, we must have that the one-party states derived from these two-party states are consistent, i.e.,

$$\mathrm{Tr}_B\sigma^{AB}=\mathrm{Tr}_C\eta^{AC},\quad \mathrm{Tr}_B\tau^{BC}=\mathrm{Tr}_A\eta^{AC},\quad \mathrm{Tr}_A\sigma^{AB}=\mathrm{Tr}_C\tau^{BC}. \tag{27}$$

If these conditions are satisfied, specifying $\sigma^{AB},\tau^{BC},\eta^{AC}$ is equivalent to specifying α_i, β_i, γ_i, R_{ij}, S_{ij}, T_{ij} for all i,j. Substituting these values into Eqs. (25) and (26) leads to two polynomials in the 27 variables Q_{ijk} (in fact they are both quadratics in this case). σ^{AB}, τ^{BC}, and η^{AC} are legitimate reduced states of some three-qubit pure state when there is a set of Q_{ijk} satisfying both conditions: i.e., testing compatibility of particular parts of quantum states is equivalent to finding real roots of polynomials.

Thus far we have considered the set $\sigma^{AB},\tau^{BC},\eta^{AC}$ and asked whether they are parts of a three-qubit pure state, but it should be noted that the structure of the problem is essentially the same (albeit involving more variables) for much more general situations. More general partial data could be supplied. For example, one might be given only σ^{AB} and τ^{BC} or perhaps only R_{ij} and α_i. We might also have asked whether $\sigma^{AB},\tau^{BC},\eta^{AC}$ are consistent with any mixed state of ABC (not just a three-qubit pure state). One can always purify a mixed state of three qubits by introducing three further qubits DEF. [The most general state of six qubits may be expressed in a form analogous to (24) but now with terms up to one of the form $Z_{ijklmn}\sigma_i\otimes\cdots\otimes\sigma_n$.] Thus the question of the existence of a mixed state compatible with $\sigma^{AB},\tau^{BC},\eta^{AC}$ is again that of asking if there is a real solution to a pair of polynomial equations (i.e., the equations expressing the purity of ρ^{ABCDEF}) given some of the variables. It should be clear that very general questions concerning compatibility of some particular partial information about a multiqubit state can be phrased as whether there are solutions to a pair of polynomial equations, one quadratic and one at most cubic in

the variables. Finally in this context we note that for any dimension of local Hilbert space there are bases consisting of the identity, together with traceless Hermitian matrices; thus our description is not restricted to qubits.

While it is useful to understand the general framework within which questions of compatibility of reduced states lie, unfortunately, Eqs. (25) and (26) are hard to solve in practice. Finding the real roots of systems of equations in a large number of variables is a frontier area of computational research [8–11]. Our pair of polynomials, the quadratic $p_1 = \mathrm{Tr}(\rho^2) - 1 = 0$ and the cubic $p_2 = \mathrm{Tr}(\rho^3) - 1 = 0$, can be expressed as a single order-6 polynomial: $p_1^2 + p_2^2 = 0$. One of the best algorithmic bounds for the number of arithmetic steps to find a real root is exponential in the number of unknowns [12] (see also [13,14]), and so doubly exponential in the number of parties.

B. Finding compatibility conditions

In the introductory remarks to this section we described a slightly different question which we would like to answer. What conditions must a set of parts of quantum states satisfy such that there exists a compatible quantum state?

In the case of three qubits, rather than solving for Q_{ijk} for particular $\alpha_i, \ldots, T_{ij}$ values (as in Sec. IV A), one would rather find the range of $\alpha_i, \ldots, T_{ij}$ values such that there always exist real Q_{ijk} satisfying Eqs. (25) and (26). Here one solves Eqs. (25) and (26) for general $\alpha_i, \ldots, T_{ij}$, eliminating Q_{ijk}, with the constraint that the variables are reals. Finding rules that parts of quantum states must satisfy such that there exists a whole is equivalent to solving a system of equations, in real variables, for a subset of those variables.

Both analytically and algorithmically this is a hard task. The first implementable algorithm for eliminating real variables from systems of equations was Collins's [15] "cylindrical algebraic decomposition." In terms of the number of arithmetical steps required, this has a worst-case running time doubly exponential in the number of variables (here the number of variables is the number of real coefficients in our decomposition, $\sim d^N$ for N d-dimensional subsystems). Subsequent authors (e.g., [16]) have produced theoretical algorithms that are singly exponential in the number of variables. It should be noted that this approach generalizes to N parties, in higher dimensions, and for different sets of parts of interest.

Using a more advanced version of Collins's algorithm [17] we made a proof of principle in the simplest case. The conditions for two one-party reduced states ρ_A and ρ_B to be compatible with a two-party pure state are known: the eigenvalues of ρ_A and ρ_B must be the same. This is equivalent to the conditions $\alpha_i = \pm\beta_i$, $\alpha_i^2 \leqslant 1$. The algorithm showed that these are sufficient conditions by elimination of R_{ij} from simplified two-party versions of Eqs. (25) and (26) [18] (showing necessity was not tractable during the time allocated). Despite the unfavorable complexity of finding compatibility conditions algorithmically, there is hope that, with optimized programs, advances can be made. Known necessary conditions [5,19] could be shown to be sufficient for small numbers of parties.

Given these algorithmic challenges, it is natural to apply *ad hoc* techniques to solve specific subproblems. A restricted form of the above question is whether a set of parts have a compatible *pure* state. There are two conditions which are necessary but, in general, not sufficient for a set of reduced states to be parts of a pure quantum states. (1) As noted above, if the states have parties in common, their reduced states in these common parties alone must be the same. For example, for σ_{AB} and τ_{BC}, $\mathrm{Tr}_A \sigma_{AB} = \mathrm{Tr}_C \tau_{BC}$. (2) By the Schmidt decomposition, pairs of reduced states that are a bipartite division of pure states must have the same eigenvalues. Satisfying property 1 alone is insufficient for there to exist a compatible pure state: the set $\sigma^{AB} = \tau^{BC} = \eta^{AC} = 1/2(|00\rangle + |11\rangle)(\langle 00| + \langle 11|)$ has consistent one-party reduced states but there is no pure three-party state with these reduced states [1]. Both (1) and (2) are still not sufficient for a set of states to be compatible with a pure state. Consider the states

$$\sigma_{AB} = \frac{1}{4}[|00\rangle\langle 00| + |11\rangle\langle 11| + |01\rangle\langle 01| + |10\rangle\langle 10| + |00\rangle\langle 01| - |10\rangle\langle 11| + |01\rangle\langle 00| - |11\rangle\langle 10|], \tag{28}$$

$$\tau_{BC} = \frac{1}{2}[|00\rangle\langle 00| + |11\rangle\langle 11|], \tag{29}$$

$$\eta_{AC} = \frac{1}{2}[|00\rangle\langle 00| + |11\rangle\langle 11|]. \tag{30}$$

These satisfy both properties 1 and 2 but there is no state compatible with σ_{AB}, τ_{BC}, η_{AC} (the most general pure state compatible with τ_{BC} and η_{AC} is $(1/\sqrt{2})(|000\rangle + e^{i\theta}|111\rangle)$ but this cannot reduce to σ_{AB}).

Diosi [20] notes that, by the Schmidt decomposition, given any pair of overlapping reduced states of a pure state $|\phi\rangle_{ABC}$ (e.g., ρ_{AB}, ρ_{BC} where systems A, B, C, might not be equidimensional) the original state is almost always the only *pure* state compatible with them [21]. We note that it is fairly straightforward to convert this result into a set of compatibility conditions that are necessary and sufficient for reduced states ρ_{AB}, ρ_{BC} to be the reduced states of a pure state.

V. CONCLUSION

We have provided tight bounds on the size of the parts that are a sufficient description of almost all pure states and we have placed these questions in the framework of real algebraic geometry which is suitable for all such tasks involving parts of quantum states.

The first part of this paper tells us that almost all pure quantum states contain no higher-order correlations which are not determined by correlations within parts slightly bigger than half the whole state. Exceptional states that do not have this property are of interest. The N-party Greenberger-Horne-Zeilinger state, $(1/\sqrt{2})[|0\rangle^{\otimes N} + e^{i\theta}|1\rangle^{\otimes N}]$ has irreducible N-party entanglement: its entanglement cannot be asymptotically and reversibly converted into entanglement between fewer than N parties [22,23]. It is also "partwise"

irreducible—no set of its reduced states can uniquely determine the state. A better understanding of the connection between these two kinds of irreducibility, and whether one implies the other, would be desirable. It is easy to construct nongeneric N-party states that are not determined by their m-party reduced states: it is interesting to understand what properties these states have, and to find the set of all such states (this was done for three-qubit states in [1]). Finally, while we have given *proofs* that reduced states of roughly half the number of parties determine N-party pure states, we do not have a simple understanding of why this should be the case.

ACKNOWLEDGMENTS

We are grateful to Fabrice Rouillier, Stanly Steinberg, Tobias Osborne, Andreas Winter, and William Wootters for helpful discussions. We are grateful for support from the EU, via the project RESQ.

[1] N. Linden, S. Popescu, and W. K. Wootters, Phys. Rev. Lett. **89**, 207901 (2002).
[2] N. Linden and W. K. Wootters, Phys. Rev. Lett. **89**, 277906 (2002).
[3] A. Higuchi, A. Sudbery, and J. Szulc, Phys. Rev. Lett. **90**, 107902 (2003).
[4] A. Higuchi, e-print quant-ph/0309186.
[5] Y. Han, Y. Zhang, and G. Guo, e-print quant-ph/0403151.
[6] S. Bravyi, e-print quant-ph/0301014.
[7] S. Basu, R. Pollack, and M.-F. Roy, *Algorithms in Real Algebraic Geometry* (Springer-Verlag, New York, 2003).
[8] F. Rouillier, in *Algorithmic and Quantitative Real Algebraic Geometry*, edited by S. Basu and L. Gonzalez-Vega (AMS, Boston, 2003), p. 123.
[9] P. Aubry, F. Rouillier, and M. S. El Din, J. Symb. Comput. **34**, 543 (2002).
[10] M.-F. Roy, in *Lectures in Real Geometry* edited by F. Broglia (de Gruyter, Berlin, 1996), p. 1.
[11] L. Gonzalez-Vega, F. Rouillier, M.-F. Roy, and G. Trujillo, in *Some Tapas of Computer Algebra*, edited by A. Cohen *et al.* (Springer-Verlag, Berlin, 1999), p. 121.
[12] J. Renegar, J. Symb. Comput. **13**, 255 (1992).
[13] L. Blum, F. Cucker, M. Shub, and S. Smale, *Complexity and Real Computation* (Springer-Verlag, Berlin, 1998).
[14] L. Blum, M. Shub, and S. Smale, Bull., New Ser., Am. Math. Soc. **21**, 1 (1989).
[15] G. E. Collins, in *Second GI Conference on Automata Theory and Formal Languages*, edited by H. Barkhage (Springer-Verlag, Berlin, 1975), p. 134.
[16] S. Basu, R. Pollack, and M.-F. Roy, J. ACM **43**, 1002 (1996).
[17] G. E. Collins and H. Hong, J. Symb. Comput. **12**, 299 (1991); www.cs.usna.edu/qepcad/B/QEPCAD.html
[18] On a 2 GHz Pentium 4 with 500 Mbytes RAM this took seconds.
[19] Algorithmically, it is exponentially easier to derive sufficient compatibility conditions than necessary ones (though it is still very hard). By asking questions like "Does there exist a compatible state of kind X?" rather than "Does there exist *any* compatible state?" one puts constraints on the variable to be eliminated and this reduces the complexity of the task.
[20] L. Diosi, e-print quant-ph/0403200.
[21] The fact that pure states $|\phi\rangle_{ABC}$ can be distinguished from all other *pure* states by reduced states ρ_{AB}, ρ_{BC} is not the same as being distinguished from all other states. The result does not tell us if there exist compatible *mixed* states ρ_{ABC} and so cannot tell us if higher-order correlations in pure quantum states are independent of lower-order correlations. The analysis in Secs. II and III is required for this.
[22] C. H. Bennett, S. Popescu, D. Rohrlich, J. A. Smolin, and A. V. Thapliyal, Phys. Rev. A **63**, 012307 (2000).
[23] N. Linden, S. Popescu, B. Schumacher, and M. Westmoreland, e-print quant-ph/9912039.