Multipartite unlockable bound entanglement in the stabilizer formalism

Guoming Wang* and Mingsheng Ying†
State Key Laboratory of Intelligent Technology and Systems, Department of Computer Science and Technology, Tsinghua University, Beijing 100084 China
(Received 11 March 2007; published 24 May 2007)

We find an interesting relationship between multipartite bound entangled states and the stabilizer formalism. We prove that, if a set of commuting operators from the generalized Pauli group on n qudits satisfy certain constraints, then the maximally mixed state over the subspace stabilized by them is an unlockable bound entangled state. Moreover, the properties of this state, such as symmetry under permutations of parties, undistillability, and unlockability, can be easily explained from the stabilizer formalism without tedious calculation. In particular, the four-qubit Smolin state [Smolin, Phys. Rev. A **63**, 032306 (2001)] and its recent generalization to even numbers of qubits [Bandyopadhyay *et al.*, Phys. Rev. A **71**, 062317 (2005); Augusiak *et al.*, *ibid* **73**, 012318 (2006)] can be viewed as special examples of our results. Finally, we extend our results to arbitrary multipartite systems in which the dimensions of all parties may be different.

DOI: 10.1103/PhysRevA.75.052332 PACS number(s): 03.67.Mn

I. INTRODUCTION

As a peculiar phenomenon of quantum mechanics and a valuable resource for quantum-information processing such as quantum computation [1], quantum cryptography [2], quantum teleportation [3], and superdense coding [4], entanglement has been extensively studied during recent years. One of the central problems about it is entanglement distillation [5], which is the procedure of extracting pure entangled states from many identical copies of a mixed entangled state by means of local operation and classical communication (LOCC). A surprising discovery in this area is that there exist mixed entangled states from which no pure entanglement can be distilled out, and these states are called bound entangled states [6]. Much effort has been devoted to the characterization and detection of bound entanglement [6–13]. Moreover, various properties and applications of bound entanglement have been found, including its irreversibility under LOCC manipulation [14], its capability to assist the LOCC transformation of other entangled states [15] and distilling out classical secret bits [16], its violation of Bell inequalities [17–19], and so on [20,21].

The distillability of multipartite entangled states, however, is much more complicated than that of bipartite entangled states. In the most natural case, we simply say that a multipartite entangled state is bound entangled if no pure entanglement can be distilled between any two parties by LOCC when all the parties remain spatially separated from each other. However, a multipartite bound entangled state may be "unlocked" or "activated" in the following sense. If we divide all the parties into several groups, and let each group join together and perform collective quantum operations (an equivalent way is to let them share *a priori* singlets, since they can use them to teleport their respective particles to a common party via quantum teleportation), then pure entanglement may be distilled between some two different groups. If so, this state is called an unlockable or activable bound entangled state.

There are two famous classes of multipartite unlockable bound entangled states that have been proposed. The first class includes a four-qubit state called the Smolin state [22] and its recent generalization to an even number of qubits [23,24]. These states have been applied in remote information concentration [20], quantum secret sharing [25], and reduction of communication complexity [25–27]. Shor *et al.* also utilized the Smolin state to demonstrate a fascinating effect named "superactivation" of bound entanglement [28,29]. In addition, in [23] Bandyopadhyay *et al.* found that the Hilbert space of even number (≥ 4) of qubits can always be decomposed as a direct sum of four orthogonal subspaces such that the normalized projectors onto the subspaces are activable bound entangled states. The other class, presented by Dür *et al.* [30,31], has been used to demonstrate numerous possible ways in which bound entangled states can be activated. In addition, the relation between multipartite distillability and Bell inequalities was also studied in [12,17,18,32]. Despite this progress, the general structure of multipartite unlockable bound entanglement still remains elusive.

The stabilizer formalism [33,34], on the other hand, has also played a significant role in quantum-information science, especially in quantum error correction codes [35,36] and cluster-state quantum computation [37]. Its essential idea is to describe the quantum state by a set of stabilizing operators rather than the state vector. This formalism provides a very compact and effective way to describe and understand a lot of phenomena in quantum information.

In this paper, we link the two seemingly irrelevant areas and find an interesting relationship between them. Specifically, we prove that, if a set of commuting operators from the generalized Pauli group on n qudits satisfy certain constraints, then the maximally mixed state over the subspace stabilized by them is an unlockable bound entangled state, and its properties can be easily explained from the stabilizer

*Electronic address: wgm00@mails.tsinghua.edu.cn
†Electronic address: yingmsh@tsinghua.edu.cn

formalism. In particular, the Smolin state and its generalization are reinterpreted as one special case of our results. Furthermore, our results can also be extended to arbitrary multipartite systems in which the dimensions of all parties may be different.

This paper is organized as follows. In Sec. II we first briefly recall some facts about the generalized Pauli group and the stabilizer formalism, and then propose our main results. In Sec. III we analyze a series of examples by using our theorems. In Sec. IV, we extend our results to arbitrary multipartite systems. Finally, Sec. V summarizes our results.

II. CONSTRUCTION OF MULTIPARTITE UNLOCKABLE BOUND ENTANGLED STATES

A. The generalized Pauli group and stabilizer formalism

In this section we review some basic facts about the generalized Pauli group and the corresponding stabilizer formalism in the general high-dimensional case. Similar topics have also been explored in [38–41].

Consider a d-dimensional Hilbert space. Define

$$X_{(d)} = \sum_{j=0}^{d-1} |j \oplus 1\rangle\langle j|,$$

$$Z_{(d)} = \sum_{j=0}^{d-1} \omega^j |j\rangle\langle j|, \tag{1}$$

where $\omega = e^{i2\pi/d}$ is the dth root of unity over the complex field and the $\oplus$ sign denotes addition modulo d. Then the matrices $\{\sigma_{i,j} = X_{(d)}^i Z_{(d)}^j : i,j = 0,1,\ldots,d-1\}$ are considered as generalized Pauli matrices over d-dimensional space, and they have the following commutation relation:

$$\sigma_{i,j}\sigma_{m,n} = \omega^{jm-in}\sigma_{m,n}\sigma_{i,j}. \tag{2}$$

It can be checked that, when d is odd, $\sigma_{i,j}$ always have eigenvalues $\{1, \omega^c, \omega^{2c}, \ldots, \omega^{d-c}\}$ for some $c|d$ (i.e., c is a factor of d); but when d is even, the eigenvalues of $\sigma_{i,j}$ may be of either the above form or $\{\omega^{1/2}, \omega^{c+1/2}, \omega^{2c+1/2}, \ldots, \omega^{d-c+1/2}\}$ for some $c|d$.

The generalized Pauli group on n qudits G_n is generated under multiplication by the Pauli matrices acting on each qudit, together with the phase factor $\gamma = \sqrt{\omega}$, i.e.,

$$G_n = \{\gamma^a \sigma_{i_1,j_1} \otimes \sigma_{i_2,j_2} \otimes \cdots \otimes \sigma_{i_n,j_n} : 0 \le a \le 2d-1, 0 \le i_1, j_1, i_2, j_2, \ldots, i_n, j_n \le d-1\}. \tag{3}$$

Actually, when d is odd, the introduction of γ is unnecessary and it can be replaced by ω (for a detailed discussion about this, one can see [41]). However, this will not affect our results since in the following we consider only elements in $G_n' = \{\otimes_{k=1}^n \sigma_{i_k,j_k} : \forall\ k = 1,2,\ldots,n,\ i_k = 0 \text{ or } j_k = 0\} \subset G_n$. For any element $g \in G_n'$ it has eigenvalues $\{1, \omega^c, \omega^{2c}, \ldots, \omega^{d-c}\}$ for some $c|d$.

Suppose we choose commuting operators $g_1, g_2, \ldots, g_k$ from G_n'. Let $S = \langle g_1, g_2, \ldots, g_k\rangle$ denote the Abelian subgroup generated by them. A state $|\psi\rangle$ is said to be stabilized by S, or S is the stabilizer of $|\psi\rangle$, if $g_i|\psi\rangle = |\psi\rangle$, $\forall\ i = 1,2,\ldots,k$. All the states stabilized by S constitute a subspace denoted by V_S. With the fact that $\Sigma_{i=0}^{d-1} \omega^{ci} = 0$, $\forall\ c = 1,2,\ldots,d-1$, one can verify that the projection operator onto V_S is

$$P_S = \prod_{i=1}^{k} \frac{(I + g_i + g_i^2 + \cdots + g_i^{d-1})}{d}, \tag{4}$$

and the maximally mixed state over V_S is $\rho_S = P_S/\mathrm{tr}(P_S)$. In particular, if there is a unique pure state stabilized by S, i.e., $\dim(V_S) = 1$, $g_1, g_2, \ldots, g_k$ are called a *complete* set of stabilizer generators and S is called a *complete* stabilizer.

In practice we are often interested in the stabilized subspace V_S, which is the subspace spanned by the simultaneous eigenstates of the operators $\{g_1, g_2, \ldots, g_k\}$ with the eigenvalues $\{1,1,\ldots,1\}$. But in general we can also consider the subspaces spanned by the simultaneous eigenstates of $\{g_1, g_2, \ldots, g_k\}$ corresponding to their other eigenvalues $\{\lambda_1, \lambda_2, \ldots, \lambda_k\}$, where λ_i can be an arbitrary eigenvalue of g_i. All these subspaces have the same dimensions and form an orthogonal decomposition of the whole space. In particular, when $\{g_1, g_2, \ldots, g_k\}$ are a complete set of stabilizer generators, each of these subspaces is one dimensional.

B. Main results

In the following, we define a partition of $\{1,2,\ldots,n\}$ to be a set of its proper subsets $\{T_1, T_2, \ldots, T_m\}$ such that $T_i \cap T_j = \emptyset$, $\forall\ i \ne j$, and $\cup_{i=1}^m T_i = \{1,2,\ldots,n\}$, and use $|T_i|$ to denote the number of elements in T_i. An n-qudit state $\rho^{1,2,\ldots,n}$ is said to be separable with respect to a partition $\{T_1, T_2, \ldots, T_m\}$ if it can be written as

$$\rho^{1,2,\ldots,n} = \sum_k p_k \rho_k^{(1)} \otimes \rho_k^{(2)} \otimes \cdots \otimes \rho_k^{(m)} \tag{5}$$

where $\Sigma_k p_k = 1$, $p_k > 0$, and $\rho_k^{(i)}$ is a density operator of the subsystem T_i.

In order to conveniently describe our results, we introduce the following definitions.

Definition 1. Suppose $g = \otimes_{k=1}^n \sigma_{i_k,j_k} \in G_n'$. Then the restriction of g on a subset $T \subset \{1,2,\ldots,n\}$ is defined as $g^{(T)} = \otimes_{k \in T} \sigma_{i_k,j_k}$.

Definition 2. Two operators $g, h \in G_n'$ are said to commute locally with respect to a partition $\{T_1, T_2, \ldots, T_m\}$ of $\{1,2,\ldots,n\}$ if $g^{(T_\alpha)} h^{(T_\alpha)} = h^{(T_\alpha)} g^{(T_\alpha)}$, $\forall\ \alpha = 1,2,\ldots,m$.

Definition 3. Suppose $g_1, g_2, \ldots, g_k$ are commuting elements in G_n'. $S = \langle g_1, g_2, \ldots, g_k\rangle$ is said to be separable with respect to a partition $\{T_1, T_2, \ldots, T_m\}$ of $\{1,2,\ldots,n\}$ if $g_1, g_2, \ldots, g_k$ commute locally with respect to this partition. Otherwise, if such a partition does not exist, S is said to be inseparable.

Note that, in the third definition, the separability of a stabilizer with respect to any partition does not depend on the choice of its generators, so it is well defined.

The following lemma establishes a connection between the separability of a stabilizer S and the separability of the maximally mixed state over the stabilized subspace V_S.

Lemma 1. Suppose $g_1, g_2, \ldots, g_k$ are commuting elements

in G_n'. $S=\langle g_1,g_2,\ldots,g_k\rangle$ is separable with respect to a partition $\{T_1,T_2,\ldots,T_m\}$ of $\{1,2,\ldots,n\}$ if and only if the maximally mixed state ρ_S over the stabilized subspace V_S is separable with respect to the same partition. So if S is inseparable then ρ_S is a genuine n-qudit entangled state.

Proof. $\Rightarrow$: Suppose $S=\langle g_1,g_2,\ldots,g_k\rangle$ is separable with respect to a partition $\{T_1,T_2,\ldots,T_m\}$. Then for $\forall\ \alpha=1,2,\ldots,m$, the operators $g_1^{(T_\alpha)},g_2^{(T_\alpha)},\ldots,g_k^{(T_\alpha)}$ are mutually commutative and thus can be simultaneously diagonalized. Suppose $\{|\psi_{\beta_\alpha}^{(\alpha)}\rangle:\beta_\alpha=1,2,\ldots,d^{|T_\alpha|}\}$ are their simultaneous eigenstates corresponding to the eigenvalue $\lambda_{\beta_\alpha,j}^{\alpha}$ for each $j=1,2,\ldots,k$. Then it is obvious that the n-qudit states $|\psi_{\beta_1,\beta_2,\ldots,\beta_m}\rangle\equiv\otimes_{\alpha=1}^m|\psi_{\beta_\alpha}^{(\alpha)}\rangle$ are the simultaneous eigenstates of $\{g_j=\otimes_{\alpha=1}^m g_j^{(T_\alpha)}\}$ with the eigenvalue $\Pi_{\alpha=1}^m\lambda_{\beta_\alpha,j}^{\alpha}$ for each $j=1,2,\ldots,k$. They also form an orthonormal basis of the n-qudit space. In particular, let $P=\{(\beta_1,\beta_2,\ldots,\beta_m):\Pi_{\alpha=1}^m\lambda_{\beta_\alpha,j}^{\alpha}=1,\forall j=1,2,\ldots,k\}$. Then we have

$$\rho_S=\frac{1}{|P|}\sum_{(\beta_1,\beta_2,\ldots,\beta_m)\in P}\bigotimes_{\alpha=1}^{m}|\psi_{\beta_\alpha}^{(\alpha)}\rangle\langle\psi_{\beta_\alpha}^{(\alpha)}|, \tag{6}$$

which implies that ρ_S is separable with respect to the partition $\{T_1,T_2,\ldots,T_m\}$.

$\Leftarrow$: Suppose ρ_S is separable with respect to the partition $\{T_1,T_2,\ldots,T_m\}$. Then there exists a state $|\psi\rangle\in V_S$ such that $|\psi\rangle$ can be written as $|\psi\rangle=\otimes_{\alpha=1}^m|\psi^{(\alpha)}\rangle$, where $|\psi^{(\alpha)}\rangle$ is a state of the subsystem T_α. Since $|\psi\rangle$ is stabilized by S, we have $|\psi\rangle=g_j|\psi\rangle=\otimes_{\alpha=1}^m g_j^{(T_\alpha)}|\psi^{(\alpha)}\rangle$, $\forall j=1,2,\ldots,k$, which means that $|\psi^{(\alpha)}\rangle$ should be a simultaneous eigenstate of $g_1^{(T_\alpha)},g_2^{(T_\alpha)},\ldots,g_k^{(T_\alpha)}$ for each $\alpha=1,2,\ldots,m$. This is impossible if $g_1^{(T_\alpha)},g_2^{(T_\alpha)},\ldots,g_k^{(T_\alpha)}$ do not commute. To see this, we prove that any two elements $g,h\in G_l'$ for any l do not have a simultaneous eigenstate if g,h do not commute. From Eqs. (2) and (3) one can see that $gh=\omega^{f(g,h)}hg$ for some integer $f(g,h)$ determined by g and h. If g and h do not commute, i.e., $\omega^{f(g,h)}\neq 1$, and they share a simultaneous eigenstate $|\psi\rangle$ which corresponds to the eigenvalues λ, μ of g, h, respectively, then we have

$$\begin{aligned}gh|\psi\rangle&=g(\mu|\psi\rangle)=\lambda\mu|\psi\rangle=\omega^{f(g,h)}hg|\psi\rangle\\&=\omega^{f(g,h)}h(\lambda|\psi\rangle)=\omega^{f(g,h)}\mu\lambda|\psi\rangle,\end{aligned} \tag{7}$$

which implies that at least one of λ and μ must be zero. But this contradicts the fact that any operator in the generalized Pauli group has only nonzero eigenvalues. So $g_1,g_2,\ldots,g_k$ commute locally with respect to the partition $\{T_1,T_2,\ldots,T_m\}$ and $S=\langle g_1,g_2,\ldots,g_k\rangle$ is separable with respect to this partition. ■

With the help of Lemma 1, we find that the distillability and unlockability of ρ_S generated by an incomplete stabilizer $S=\langle g_1,g_2,\ldots,g_k\rangle$ are determined by the separability of S, as the following theorem states.

Theorem 1. Suppose $g_1,g_2,\ldots,g_k$ are commuting elements in G_n'. Let $S=\langle g_1,\ldots,g_k\rangle$. If

(1) for any $i\neq j\in\{1,2,\ldots,n\}$, there exists a partition $\{Q_1,Q_2,\ldots,Q_m\}$ with $i\in Q_1$, $j\in Q_2$ such that S is separable with respect to this partition;

(2) there exists a partition $\{T_1,T_2,\ldots,T_m\}$ with $|T_1|>1$ such that S is separable with respect to this partition and $S^{(T_1)}=\langle g_1^{(T_1)},g_2^{(T_1)},\ldots,g_k^{(T_1)}\rangle$ is an inseparable and complete stabilizer on T_1.

Then the maximally mixed state ρ_S over the stabilized subspace V_S is an unlockable bound entangled state. Moreover, for any partition $\{T_1,T_2,\ldots,T_m\}$ satisfying condition 2, pure entanglement among the parties inside T_1 can be distilled by letting the parties inside $T_2,T_3,\ldots,T_m$ join together, respectively.

Proof. First, we prove that ρ_S is undistillable. Consider any two parties $i,j\in\{1,2,\ldots,n\}$. By condition 1 and Lemma 1 we can find a partition $\{Q_1,Q_2,\ldots,Q_m\}$ with $i\in Q_1$ and $j\in Q_2$ such that ρ_S is separable with respect to it. So it is impossible to distill out pure entanglement between i and j, even between Q_1 and Q_2, by LOCC, as long as Q_1 and Q_2 remain spatially separated.

Next, we prove that ρ_S can be unlocked. Consider the partition $\{T_1,T_2,\ldots,T_m\}$ which satisfies condition 2. Since S is separable with respect to this partition, we can repeat exactly the same argument presented in the first part of the proof of Lemma 1 without changing any notations introduced. Now suppose all the parties inside T_α join together and perform the projection measurement in the basis $\{|\psi_{\beta_\alpha}^{(\alpha)}\rangle:\beta_\alpha=1,\ldots,d^{|T_\alpha|}\}$ for each $\alpha=2,3,\ldots,m$, and obtain the outcomes $\beta_2',\beta_3',\ldots,\beta_m'$, respectively. Then by Eq. (6) we have the remaining state of the subsystem T_1 as

$$\rho_S^{(1)}=\frac{1}{|P_{\beta_2',\beta_3',\ldots,\beta_m'}|}\sum_{\beta_1\in P_{\beta_2',\beta_3',\ldots,\beta_m'}}|\psi_{\beta_1}^{(1)}\rangle\langle\psi_{\beta_1}^{(1)}|, \tag{8}$$

where $P_{\beta_2,\beta_3,\ldots,\beta_m}=\{\beta_1:\lambda_{\beta_1,j}^{1}=1/\Pi_{\alpha=2}^m\lambda_{\beta_\alpha,j}^{\alpha},\ \forall\ j=1,2,\ldots,k\}$. Since $S^{(T_1)}=\langle g_1^{(T_1)},g_2^{(T_1)},\ldots,g_k^{(T_1)}\rangle$ is a complete stabilizer on T_1, we have that $P(\beta_2',\beta_3',\ldots,\beta_m')$ actually contains only one element and therefore $\rho_S^{(1)}$ is a pure state. Moreover, because $S^{(T_1)}$ is inseparable, by Lemma 1 we know that $\rho_S^{(1)}$ is a genuine $|T_1|$-qudit entangled state. Therefore we have obtained an activation strategy. ■

Note that, by a similar argument, we can easily prove that Lemma 1 and Theorem 1 will still hold if we replace ρ_S by a maximally mixed state over the subspace spanned by the simultaneous eigenstates of $\{g_1,g_2,\ldots,g_k\}$ corresponding to their eigenvalues $\{\lambda_1,\lambda_2,\ldots,\lambda_k\}$, where λ_i is an arbitrary eigenvalue of g_i. Recalling that all these subspaces have the same dimensions, we reach the following conclusion.

Theorem 2. Suppose $g_1,g_2,\ldots,g_k$ are k commuting elements in G_n'. If they satisfy the conditions 1 and 2 in Theorem 1, and the subspace stabilized by them is b dimensional with $b|d^n$, then the Hilbert space of n qudits can be decomposed into d^n/b orthogonal subspaces such that the normalized projection operator onto each of them is an unlockable bound entangled state.

The two theorems above provide a simple method of constructing a wide class of unlockable bound entangled states in arbitrary multiqudit systems. What we need to do now is

to appropriately choose several commuting operators from the generalized Pauli group on n qudits. It is worth noting that our construction essentially utilizes the symmetry of the generalized Pauli matrices. Consequently the constructed states also own some inherent symmetry. With the help of Lemma 1, the properties of these states can be easily explained from the stabilizer formalism, as shown in the subsequent section.

III. ILLUSTRATIONS

In this section we will analyze several concrete examples by using our theorems. Without being explicitly pointed out, the matrices X and Z appearing below are $X_{(d)}$ and $Z_{(d)}$ defined by Eq. (1) with the corresponding dimension d. We will also use the notation X_j to denote the operation X acting on the jth party, and similarly for Z_j.

Example 1. Consider a four-qubit system. Define

$$g_1 = X_1X_2X_3X_4,$$

$$g_2 = Z_1Z_2Z_3Z_4. \tag{9}$$

The maximally mixed state over the subspace stabilized by g_1 and g_2 is

$$\rho^{(4)} \equiv \rho_{\langle g_1,g_2\rangle} = \frac{1}{16}(I+g_1)(I+g_2). \tag{10}$$

Because $X\otimes X$ and $Z\otimes Z$ commute, $S=\langle g_1,g_2\rangle$ is separable with respect to any 2:2 partition of $\{1,2,3,4\}$, which assures that the condition 1 in Theorem 1 is satisfied. Any 2:2 partition also satisfies the condition 2 in Theorem 1 since $S=\langle X\otimes X, Z\otimes Z\rangle$ is an inseparable and complete stabilizer on two qubits. So $\rho^{(4)}$ is an unlockable bound entangled state, and pure entanglement can be distilled between any two parties.

Actually, this state is exactly the Smolin state, which was originally defined as

$$\rho^{(4)} = \frac{1}{4}\sum_{\alpha,\beta=0}^{1} |\Phi_{\alpha\beta}\rangle_{12}\langle\Phi_{\alpha\beta}| \otimes |\Phi_{\alpha\beta}\rangle_{34}\langle\Phi_{\alpha\beta}|, \tag{11}$$

where

$$|\Phi_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad |\Phi_{01}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle),$$

$$|\Phi_{10}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \quad |\Phi_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \tag{12}$$

are the four Bell states. To see this, one only needs to realize that $|\Phi_{00}\rangle, |\Phi_{01}\rangle, |\Phi_{10}\rangle, |\Phi_{11}\rangle$ are the simultaneous eigenstates of $\{X\otimes X, Z\otimes Z\}$, with the eigenvalues $\{+1,+1\}$, $\{-1,+1\}$, $\{+1,-1\}$,$\{-1,-1\}$, respectively. Considering the 2:2 partition $\{\{1,2\},\{3,4\}\}$, we have $g_1^{(\{1,2\})}=X_1X_2$, $g_2^{(\{1,2\})}=Z_1Z_2$, $g_1^{(\{3,4\})}=X_3X_4$, and $g_2^{(\{3,4\})}=Z_3Z_4$. So the four states $\{|\Phi_{\alpha\beta}\rangle_{12}|\Phi_{\alpha\beta}\rangle_{34}: \alpha,\beta=0,1\}$ are simultaneous eigenstates of $g_1=g_1^{(\{1,2\})}\otimes g_1^{(\{3,4\})}$ and $g_2=g_2^{(\{1,2\})}\otimes g_2^{(\{3,4\})}$ with the eigenvalues $\{1,1\}$. Thus by Eq. (6) $\rho^{(4)}$ can be written in the form of Eq. (11).

Furthermore, one can repeat the above argument by considering two other 2:2 partitions $\{\{1,3\},\{2,4\}\}$ and $\{\{1,4\},\{2,3\}\}$, and can easily conclude that $\rho^{(4)}$ can also be written as

$$\rho^{(4)} = \frac{1}{4}\sum_{\alpha,\beta=0}^{1} |\Phi_{\alpha\beta}\rangle_{13}\langle\Phi_{\alpha\beta}| \otimes |\Phi_{\alpha\beta}\rangle_{24}\langle\Phi_{\alpha\beta}|$$

$$= \frac{1}{4}\sum_{\alpha,\beta=0}^{1} |\Phi_{\alpha\beta}\rangle_{14}\langle\Phi_{\alpha\beta}| \otimes |\Phi_{\alpha\beta}\rangle_{23}\langle\Phi_{\alpha\beta}|, \tag{13}$$

which implies that $\rho^{(4)}$ is invariant under arbitrary permutation of the four parties. Note that this symmetry essentially arises from the fact that g_1 and g_2 both act identically on the four qubits.

By Eqs. (11) and (13), $\rho^{(4)}$ is separable with respect to any 2:2 partition, and, moreover, when any two parties come together and perform the projective measurement in the Bell basis, if their subsystem collapses into the state $|\Phi_{\alpha\beta}\rangle$, then the other two parties are in the same state $|\Phi_{\alpha\beta}\rangle$.

Example 2. Consider a system of $2n$ $(n\geq 2)$ qubits. Define

$$g_1^{(2n)} = X_1X_2X_3X_4\cdots X_{2n-1}X_{2n},$$

$$g_2^{(2n)} = Z_1Z_2Z_3Z_4\cdots Z_{2n-1}Z_{2n}. \tag{14}$$

Then the maximally mixed state over the subspace stabilized by $g_1^{(2n)}$ and $g_2^{(2n)}$ is

$$\rho^{(2n)} \equiv \rho_{\langle g_1^{(2n)},g_2^{(2n)}\rangle} = \frac{1}{4^n}(I+g_1^{(2n)})(I+g_2^{(2n)}). \tag{15}$$

One can easily check that $S=\langle g_1^{(2n)}, g_2^{(2n)}\rangle$ is separable with respect to any $2:2:\cdots:2$ partition of $\{1,2,\ldots,2n\}$, which ensures the satisfaction of condition 1 in Theorem 1. Moreover, any $2:2:\cdots:2$ partition satisfies the condition 2 in Theorem 1. So $\rho^{(2n)}$ is an unlockable bound entangled state and a pure entangled state can be distilled between any two parties by letting the other $2n-2$ parties group together pairwise.

Actually, $\rho^{(2n)}$ is equivalent to the generalized Smolin state proposed in Refs. [23] and [24], up to an unimportant local Pauli operation. To see this, consider the $(2n-2):2$ partition $\{\{1,2,\ldots,2n-2\},\{2n-1,2n\}\}$. It is observed that $g_1^{(2n)}, g_2^{(2n)}$ commute locally with respect to this partition, and their restrictions on the subset $\{1,2,\ldots,2n-2\}$ are $g_1^{(2n-2)}, g_2^{(2n-2)}$, respectively. Let $\sigma_{00}=I_1$, $\sigma_{01}=Z_1$, $\sigma_{10}=X_1$, and $\sigma_{11}=Y_1$ be the four Pauli operations acting on the first qubit. Then $\sigma_{\alpha\beta}\rho^{(2n-2)}\sigma_{\alpha\beta}^\dagger$ is actually the maximally mixed state over the subspace spanned by the simultaneous eigenstate of $g_1^{(2n-2)}, g_2^{(2n-2)}$ with the eigenvalues $\{(-1)^\beta,(-1)^\alpha\}$. Consequently by Eq. (6) we have

$$\rho^{(2n)} = \frac{1}{4}\sum_{\alpha,\beta=0}^{1} \sigma_{\alpha\beta}\rho^{(2n-2)}\sigma_{\alpha\beta}^\dagger \otimes |\Phi_{\alpha\beta}\rangle\langle\Phi_{\alpha\beta}|, \tag{16}$$

which is the recursive definition of the generalized Smolin states in [23,24] up to a local Pauli operation. Moreover,

continuing this induction on n, one could finally get

$$\rho^{(2n)} = \frac{1}{4^{n-1}} \sum_{\oplus_{i=1}^{n}\alpha_i=\oplus_{i=1}^{n}\beta_i=0} \otimes_{i=1}^{n} |\Phi_{\alpha_i\beta_i}\rangle\langle\Phi_{\alpha_i\beta_i}|, \quad (17)$$

where $\oplus$ denotes addition modulo 2. Noting that the two stabilizer generators $g_1^{(2n)}$ and $g_2^{(2n)}$ both act symmetrically on $2n$ qubits, one can see that $\rho^{(2n)}$ is invariant under arbitrary permutation of parties, which means that Eq. (17) holds not only for the partition $\{\{1,2\},\{3,4\},\ldots,\{2n-1,2n\}\}$ but also for an arbitrary $2:2:\cdots:2$ partition.

Now suppose any $2n-2$ parties join together pairwise and perform the projective measurement in the Bell basis. If the $n-1$ obtained outcomes are $|\Phi_{\alpha_2,\beta_2}\rangle, |\Phi_{\alpha_3,\beta_3}\rangle, \ldots, |\Phi_{\alpha_n,\beta_n}\rangle$, respectively, then by Eq. (17) the remaining two parties get one of the four Bell states $|\Phi_{\alpha_1,\beta_1}\rangle$ with $\alpha_1 = \oplus_{i=2}^{n}\alpha_i$ and $\beta_1 = \oplus_{i=2}^{n}\beta_i$.

In addition, by applying Theorem 2 to $g_1^{(2n)}, g_2^{(2n)}$, we know that the Hilbert space of $2n$ (≥ 2) qubits can be decomposed into four orthogonal subspaces such that the normalized projection operator onto each of them is an unlockable bound entangled state, which was first pointed out in [23].

One may wonder whether there exists an analog of the Smolin state in systems of odd numbers of qubits. We believe that such a state is unlikely to exist, and, even if it exists, it cannot be obtained by our method, because if we want the constructed state to be symmetric under arbitrary permutation of parties, all the stabilizer generators should act equally on each qubit. But the tensor products of odd numbers of X's and Z's, or X's and Y's, or Y's and Z's, do not commute. Instead they anticommute, e.g., $X^{\otimes 2n+1}Z^{\otimes 2n+1} = -Z^{\otimes 2n+1}X^{\otimes 2n+1}$. Therefore they cannot be simultaneously used as stabilizer generators.

From Examples 1 and 2, we can see that the properties of the Smolin state and its generalization become very clear when they are redefined and reinterpreted in the stabilizer formalism. However, they are only two special instances that have the strongest symmetry. At the cost of losing symmetry to different extents, many more unlockable bound entangled states can be found in a similar way.

Example 3. Consider a nine-qubit system. Let

$$g_1 = X_1X_2Z_3X_4X_5Z_6X_7X_8Z_9,$$

$$g_2 = X_1Z_2X_3X_4Z_5X_6X_7Z_8X_9,$$

$$g_3 = Z_1X_2X_3Z_4X_5X_6Z_7X_8X_9. \quad (18)$$

The maximally mixed state over the subspace stabilized by them is

$$\rho_{\langle g_1,g_2,g_3\rangle} = \frac{1}{2^9}(I+g_1)(I+g_2)(I+g_3). \quad (19)$$

The nine qubits of this state can be classified into three groups: $\{1,4,7\}$, $\{2,5,8\}$, and $\{3,6,9\}$. g_1, g_2, and g_3 all act symmetrically on the three qubits of each group. So the state remains invariant when exchanging any two parties inside the same group. However, when we exchange two parties that belong to two different groups, such as 1 and 6, the state will change.

Now consider two different partitions: $\{\{1,2,3\},\{4,5,6\},\{7,8,9\}\}$ and $\{\{1,6,8\},\{2,4,9\},\{3,5,7\}\}$. It can be verified that $S=\langle g_1,g_2,g_3\rangle$ is separable with respect to both of them and this fact ensures the satisfaction of the condition 1 in Theorem 1. Furthermore, the first partition $\{\{1,2,3\},\{4,5,6\},\{7,8,9\}\}$ also satisfies condition 2 in Theorem 1. Therefore, $\rho_{\langle g_1,g_2,g_3\rangle}$ is an unlockable bound entangled state, and it can be unlocked as follows. Let the parties $4,5,6$ join together and similarly for $7,8,9$. Then each of the two groups performs a projective measurement in the basis of the simultaneous eigenstates of three operators $\{X\otimes X\otimes Z, X\otimes Z\otimes X, Z\otimes X\otimes X\}$; then depending on their measurement outcomes a genuine three-qubit pure entangled state, which is also a simultaneous eigenstate of the three operators, is distilled out among the parties 1,2, and 3. In addition, by the symmetry of $\rho_{\langle g_1,g_2,g_3\rangle}$ presented above, we know that any three parties $i\in\{1,4,7\}$, $j\in\{2,5,8\}$, and $k\in\{3,6,9\}$ can obtain a genuine three-qubit pure entangled state among them by appropriately grouping the other six parties.

Example 4. Consider a seven-qutrit system, i.e., $d=3$. Let

$$g_1 = X_1^2Z_2Z_3^2X_4Z_5^2X_6Z_7,$$

$$g_2 = Z_1X_2X_3^2Z_4X_5^2Z_6X_7. \quad (20)$$

The maximally mixed state over the subspace stabilized by them is

$$\rho_{\langle g_1,g_2\rangle} = \frac{1}{3^7}(I+g_1+g_1^2)(I+g_2+g_2^2). \quad (21)$$

The seven qutrits of this state can be classified into four groups: $\{1\},\{2,7\},\{3,5\}$ and $\{4,6\}$. g_1, g_2 both act symmetrically on the qutrits of each group. So the state remains invariant when exchanging any two parties inside the same group. However, it will vary when we exchange two parties that belong to two different groups, such as 1 and 2.

Consider two partitions $\{\{1,2,3\},\{4,5\},\{6,7\}\}$ and $\{\{1,4\},\{2,5,7\},\{3,6\}\}$. It can be checked that $S=\langle g_1,g_2\rangle$ is separable with respect to both of them, which satisfies the condition 1 in Theorem 1. Also, the partition $\{\{1,4\},\{2,5,7\},\{3,6\}\}$ satisfies condition 2 in Theorem 1. So $\rho_{\langle g_1,g_2\rangle}$ is an unlockable bound entangled state and can be activated in the following way. Let the parties $2,5,7$ join together and similarly for $3,6$. Then the first group performs the projective measurement in the basis of the simultaneous eigenstates of the operators $\{Z_2Z_5^2Z_7, X_2X_5^2X_7\}$, and for the second group $\{Z_3^2X_6, X_3^2Z_6\}$. Depending on their measurement outcomes, a two-qutrit pure entangled state, which is one of the simultaneous eigenstates of $\{X_1^2X_4, Z_1Z_4\}$, is distilled out between the parties 1 and 4.

Actually, one can verify that for any two parties $i\in\{1,2,3,5,7\}$ and $j\in\{4,6\}$, a partition $\{\{i,j\},T_2,T_3\}$ satisfying the condition 2 in Theorem 1 could be found, so i and

j can share a two-qutrit pure entangled state by forming the groups T_2 and T_3. For example, for $i=2$ and $j=4$, such a partition is $\{\{2,4\},\{1,3,7\},\{5,6\}\}$.

To our knowledge, this state is the first presented unlockable bound entangled state in multiqutrit systems. In addition, by Theorem 2 we know that the Hilbert space of seven qutrits can be decomposed into nine orthogonal subspaces such that the normalized projection operator onto each of them is an unlockable bound entangled state.

In a similar manner, numerous unlockable bound entangled states in arbitrary multiqudit systems can also be found. Moreover, one can similarly use our lemma and theorems to analyze the properties of these constructed states, such as symmetry under permutation of parties, separability, and unlockability, from the stabilizer formalism.

IV. EXTENSION TO ARBITRARY MULTIPARTITE SYSTEMS

In the previous sections, we considered only multiqudit systems. Actually, the distillability and unlockability of the constructed states ρ_S depend mostly on the local commutation relation of the stabilizer generators. The constraint that all parties should have the same dimensions is really unnecessary. Our definitions and theorems in Sec. II can be readily extended to arbitrary multipartite systems.

More precisely, consider a $d_1\times d_2\times\cdots\times d_n$ system where the ith party has a d_i-dimensional space. Define $G'(d_1,d_2,\ldots,d_n)=\{g: g=\otimes_{i=1}^n g_i$ with $g_i=X_{(d_i)}^{a_i}$ or $Z_{(d_i)}^{b_i}$ for some $a_i,b_i\}$. Then one can verify that, for any element $g\in G'(d_1,d_2,\ldots,d_n)$, its eigenvalues are in the form $\{1,\omega^c,\omega^{2c},\ldots,\omega^{D-c}\}$, where $\omega=e^{i2\pi/D}$, D is the least common multiple of $d_1,d_2,\ldots,d_n$, and $c|D$.

Suppose we choose commuting elements $g_1,g_2,\ldots,g_k$ from $G'(d_1,d_2,\ldots,d_n)$. Let $S=\langle g_1,g_2,\ldots,g_k\rangle$ denote the Abelian group generated by them. Still we use V_S to denote the subspace stabilized by S. Then, with the fact that $\Sigma_{i=0}^{D-1}\omega^{ci}=0, \forall c=1,2,\ldots,D-1$, one can see that the projection operator onto V_S is given by

$$P_S=\prod_{i=1}^{k}\frac{(I+g_i+g_i^2+\cdots+g_i^{D-1})}{D}, \tag{22}$$

and the maximally mixed state over V_S is $\rho_S=P_S/\mathrm{tr}(P_S)$. Then, following the same route as in Sec. II B, we can generalize the three definitions and Lemma 1, Theorem 1, and Theorem 2 to the elements in $G'(d_1,d_2,\ldots,d_n)$.

Next we would like to use an example to illustrate this general case. Consider a $2\times2\times4\times4\times6\times6$ system. Let

$$g_1=X_{(2)}\otimes Z_{(2)}\otimes X_{(4)}^2\otimes Z_{(4)}\otimes X_{(6)}^3\otimes Z_{(6)},$$

$$g_2=Z_{(2)}\otimes X_{(2)}\otimes Z_{(4)}\otimes X_{(4)}^2\otimes Z_{(6)}\otimes X_{(6)}^3, \tag{23}$$

where $X_{(d)},Z_{(d)}$ are defined as in Eq. (1). g_1 and g_2 both have eigenvalues $1,\omega,\omega^2,\ldots,\omega^{11}$ where $\omega=e^{i\pi/6}$. The maximally mixed state over the subspace stabilized by g_1,g_2 is

$$\rho_{\langle g_1,g_2\rangle}=\frac{1}{N}\left(\sum_{i=0}^{11}g_1^i\right)\left(\sum_{j=0}^{11}g_2^j\right), \tag{24}$$

where $N=2\times2\times4\times4\times6\times6$ is the dimension of the whole space.

One can verify that $S=\langle g_1,g_2\rangle$ is separable with respect to any 2:2:2 partition, e.g., $\{\{1,2\},\{3,4\},\{5,6\}\}$. So this state is separable with respect to any 2:2:2 partition. In addition, any two parties can obtain a pure entangled state by letting the other four parties join together pairwise in an arbitrary fashion. This is because, as one may check, any 2:2:2 partition satisfies the condition 2 in Theorem 1. For instance, consider the partition $\{\{1,6\},\{2,3\},\{4,5\}\}$. Suppose the parties 2 and 3 join together, and similarly for 4 and 5. If the group $\{2,3\}$ perform the projective measurement in the basis of the simultaneous eigenstates of $\{Z_{(2)}\otimes X_{(4)}^2, X_{(2)}\otimes Z_{(4)}\}$, and the group $\{4,5\}$ perform the projective measurement in the basis of the simultaneous eigenstates of $\{Z_{(4)}\otimes X_{(6)}^3, X_{(4)}^2\otimes Z_{(6)}\}$, then depending on their outcomes, a pure entangled state, which is a simultaneous eigenstate of $\{X_{(2)}\otimes Z_{(6)}, Z_{(2)}\otimes X_{(6)}^3\}$, will be obtained between 1 and 6.

It is worth noting that in this example, although the six particles have three different kinds of dimensions 2,4,6, as shown above, the unlockability of this state is very strong. So we learn that the distinction between the dimensions of different parties is not really an obstacle in building unlockable bound entangled states in such systems. Nonetheless, we should point out that the conditions in Theorem 1 may not be satisfiable for some multipartite systems. One instance is the multipartite system in which the dimensions of all parties are mutually relatively prime. But what we guarantee is that when the conditions in Theorem 1 are satisfied, we can use the theorem to build a class of unlockable bound entangled states in the corresponding multipartite system.

V. CONCLUSION

In sum, we find an interesting relationship between two important areas in quantum-information science—multipartite bound entangled states and the stabilizer formalism. Our results provide a simple way of constructing unlockable bound entangled states in arbitrary multiqudit systems. These states not only can be concisely described, but also possess properties which can be easily explained from the stabilizer formalism. In particular, the previous four-qubit Smolin state and its generalization to an even number of qubits can be viewed as special examples of our results. Our theorems can also be extended to arbitrary multipartite systems in which the dimensions of all parties may be different, although their conditions may be in fact unsatisfiable in some cases.

Finally, we would like to point out several directions for further investigation using this method. The first one would be to extend our work to more general situations. In our work we utilized the inherent symmetry of Pauli matrices to construct our unlockable bound entangled states. However, as the reader may have already found out, our construction actually mainly relies on the local commutation relation of

the stabilizer generators. This relation can also be defined over arbitrary multipartite operations which can be written as the tensor products of unitary operations on each subsystem, not just the generalized Pauli operations. Therefore it is entirely possible that our definitions and theorems can be appropriately adjusted so as to be applicable to a wider class of multipartite operations and states. Another direction would be to study the properties and applications of our constructed unlockable bound entangled states, such as their violation of Bell inequalities, whether they also show the superactivation phenomenon, and whether they can be used in information processing tasks such as remote information concentration and multipartite key distribution. We hope that in this way more interesting results about the structures and features of multipartite bound entanglement will be found in the future.

ACKNOWLEDGMENTS

We would like to thank Runyao Duan, Zhengfeng Ji, Yuan Feng, and Chi Zhang for helpful discussions. This work was partly supported by the Natural Science Foundation of China (Grants No. 60621062 and No. 60503001) and the Hi-Tech Research and Development Program of China (863 project) (Grant No. 2006AA01Z102).

[1] P. W. Shor, in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (IEEE Computer Society Press, Los Alamos, CA, 1994), p. 124.
[2] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore* (IEEE, Piscataway, NJ, 1984), pp. 175–179; A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[3] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[4] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
[5] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996); C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, Phys. Rev. A **53**, 2046 (1996).
[6] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **80**, 5239 (1998).
[7] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).
[8] P. Horodecki, M. Horodecki, and R. Horodecki, Phys. Rev. Lett. **82**, 1056 (1999).
[9] C. H. Bennett, D. P. DiVincenzo, Tal Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal, Phys. Rev. Lett. **82**, 5385 (1999).
[10] P. W. Shor, J. A. Smolin, and B. M. Terhal, Phys. Rev. Lett. **86**, 2681 (2001).
[11] T. Hiroshima, Phys. Rev. Lett. **91**, 057902 (2003).
[12] L. Masanes, Phys. Rev. Lett. **97**, 050503 (2006).
[13] W. Dür, J. I. Cirac, M. Lewenstein, and D. Bruß, Phys. Rev. A **61**, 062313 (2000).
[14] D. Yang, M. Horodecki, R. Horodecki, and B. Synak-Radtke, Phys. Rev. Lett. **95**, 190501 (2005).
[15] S. Ishizaka, Phys. Rev. Lett. **93**, 190501 (2004).
[16] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, Phys. Rev. Lett. **94**, 160502 (2005).
[17] W. Dür, Phys. Rev. Lett. **87**, 230402 (2001).
[18] A. Acín, Phys. Rev. Lett. **88**, 027901 (2002).
[19] R. Augusiak and P. Horodecki, Phys. Rev. A **74**, 010305(R) (2006).
[20] M. Murao and V. Vedral, Phys. Rev. Lett. **86**, 352 (2001).
[21] L. Masanes, Phys. Rev. Lett. **96**, 150501 (2006).
[22] J. A. Smolin, Phys. Rev. A **63**, 032306 (2001).
[23] S. Bandyopadhyay, I. Chattopadhyay, V. Roychowdhury, and D. Sarkar, Phys. Rev. A **71**, 062317 (2005).
[24] R. Augusiak and P. Horodecki, Phys. Rev. A **73**, 012318 (2006).
[25] R. Augusiak and P. Horodecki, Phys. Rev. A **74**, 010305(R) (2006).
[26] C. Brukner, M. Żukowski, and A. Zeilinger, Phys. Rev. Lett. **89**, 197901 (2002).
[27] C. Brukner, M. Żukowski, J.-W. Pan, and A. Zeilinger, Phys. Rev. Lett. **92**, 127901 (2004).
[28] P. W. Shor, J. A. Smolin, and A. V. Thapliyal, Phys. Rev. Lett. **90**, 107901 (2003).
[29] S. Bandyopadhyay and V. Roychowdhury, Phys. Rev. A **72**, 060303(R) (2005).
[30] W. Dür, J. I. Cirac, and R. Tarrach, Phys. Rev. Lett. **83**, 3562 (1999).
[31] W. Dür and J. I. Cirac, Phys. Rev. A **62**, 022302 (2000).
[32] A. Acín, V. Scarani, and M. M. Wolf, Phys. Rev. A **66**, 042323 (2002).
[33] D. Gottesman, Phys. Rev. A **54**, 1862 (1996).
[34] D. Gottesman, Ph.D. thesis, California Institute of Technology, 1997 (unpublished).
[35] P. W. Shor, Phys. Rev. A **52**, R2493 (1995).
[36] A. M. Steane, Phys. Rev. A **54**, 4741 (1996).
[37] R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).
[38] D. Gottesman, in *Quantum Computing and Quantum Communications: First NASA International Conference*, edited by C. P. Williams (Springer-Verlag, Berlin, 1999).
[39] A. Y. Vlasov, Proc. SPIE **5128**, 29 (2003).
[40] M. A. Nielsen, M. J. Bremner, J. L. Dodd, A. M. Childs, and C. M. Dawson, Phys. Rev. A **66**, 022317 (2002).
[41] E. Hostens, J. Dehaene, and B. De Moor, Phys. Rev. A **71**, 042315 (2005).