JOURNAL OF MATHEMATICAL PHYSICS **47**, 062106 (2006)

GHZ extraction yield for multipartite stabilizer states

Sergey Bravyi
Institute for Quantum Information, Caltech, Pasadena, California 91125
and IBM Watson Research Center, Yorktown Heights, New York 10598

David Fattal
Quantum Entanglement Project, ICORP, JST Ginzton Laboratory, Stanford University, Stanford, California 94305

Daniel Gottesman
Perimeter Institute for Theoretical Physics, Waterloo, Canada N2L2Y5

(Received 20 January 2006; accepted 17 April 2006; published online 26 June 2006)

Let $|\Psi\rangle$ be an arbitrary stabilizer state distributed between three remote parties, such that each party holds several qubits. Let S be a stabilizer group of $|\Psi\rangle$. We show that $|\Psi\rangle$ can be converted by local unitaries into a collection of singlets, GHZ states, and local one-qubit states. The numbers of singlets and GHZs are determined by dimensions of certain subgroups of S. For an arbitrary number of parties m we find a formula for the maximal number of m-partite GHZ states that can be extracted from $|\Psi\rangle$ by local unitaries. A connection with earlier introduced measures of multipartite correlations is made. An example of an undecomposable four-party stabilizer state with more than one qubit per party is given. These results are derived from a general theoretical framework that allows one to study interconversion of multipartite stabilizer states by local Clifford group operators. As a simple application, we study three-party entanglement in two-dimensional lattice models that can be exactly solved by the stabilizer formalism. © *2006 American Institute of Physics.* [DOI: 10.1063/1.2203431]

I. INTRODUCTION

Many quantum cryptographic protocols such as quantum key distribution,[1] coin flipping,[2] or other quantum games[3] operate with a single copy of a pure quantum state shared by three or more parties. Each party has complete control of its subsystem, so the states which can be converted to each other by local unitary (LU) operators may be regarded as equivalent. Unfortunately, in general, LU-equivalence classes lack any known concise analytical description. For tripartite pure states (or, equivalently, bipartite mixed states), substantial progress has been achieved only for Gaussian states of fermions[4] and bosons[5] with some additional symmetry properties.

In the present paper we study LU-equivalence classes of *stabilizer states*. A stabilizer state of n qubits can be thought of as an irreducible representation of an Abelian *stabilizer group* generated by n pairwise commuting operators in the Pauli group (i.e., tensor products of the identity I and the Pauli matrices σ^x, σ^y, σ^z). Important applications of stabilizer states include measurement-based schemes of quantum computation[6] and quantum error correction using ancillas.[7] They also provide exactly solvable models of condensed-matter systems.[8]

In the special case when each party holds exactly one qubit (so that a local operator means a one-qubit operator), LU-equivalence classes of stabilizer states have been already studied by Van den Nest, Dehaene, and De Moor in Refs. 9–11.

We assume that n qubits are distributed between a finite set of parties M. Each party may hold an arbitrary number of qubits. Our main results are summarized below.

Result 1: Three-party entanglement.

We prove that an arbitrary stabilizer state shared by three parties A,B,C is LU equivalent to a collection (tensor product) of states from a set $E_3=\{|0\rangle,|\Psi^+\rangle,|\Psi_3^+\rangle\}$, where

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|0,0\rangle + |1,1\rangle),$$
$$|\Psi_3^+\rangle = \frac{1}{\sqrt{2}}(|0,0,0\rangle + |1,1,1\rangle) \tag{1}$$

are the EPR state and the GHZ state. The set E_3 thus can be called an entanglement generating set (EGS) for three-party systems, as far as stabilizer states are concerned. LU-equivalence classes are completely specified by four integers (a,b,c,p), where a,b,c are the numbers of EPR states $|\Psi^+\rangle$ shared by BC, AC, and AB, respectively, while p is the number of GHZ states $|\Psi_3^+\rangle$ shared by all three parties. A prerequisite to this result is the work in Ref. 12, where a set $E_2=\{|0\rangle,|\Psi^+\rangle\}$ was shown to be an EGS for bipartite systems. It should be emphasized that the set E_3 is not an EGS for arbitrary tripartite states, even if one allows arbitrary local manipulation and classical communication (see Ref. 13).

Result 2: Multipartite entanglement.

Let $|\Psi\rangle$ be an n-qubit stabilizer state shared by a set of parties M, $|M|=m\geq 3$, and let S be its stabilizer group. We are interested in the maximal number of m-party GHZ states

$$|\Psi_m^+\rangle = \frac{1}{\sqrt{2}}(|0^{\otimes m}\rangle + |1^{\otimes m}\rangle)$$

that can be extracted from $|\Psi\rangle$ by local unitaries. Denote this number by p. We prove that

$$p = \dim(S) - \dim(S_{\mathrm{loc}}), \tag{2}$$

where S_{loc} is a subgroup of S generated by all stabilizer operators that act trivially on at least one party. [For bipartite systems the answer is slightly different, $p=(1/2)(\dim(S)-\dim(S_{loc}))$, see Ref. 12.]

In particular, p can be computed in polynomial time in the number of qubits. Interestingly, we will give below a constructive proof of Eq. (2), which translates naturally into an efficient algorithm to perform the GHZ extraction. An implementation of this algorithm will be available online soon.

It should be mentioned that Eq. (2) provides a simple upper bound on p. Indeed, if one can find l independent generators of S, such that each of them acts trivially on at least one party, then $\dim(S_{\mathrm{loc}})\geq l$ and thus $p\leq \dim(S)-l$.

Also, we show that the GHZ extraction yield p, considered as a functional of $|\Psi\rangle$, coincides with an entanglement measure introduced by Linden, Popescu, and Wootters in Ref. 14 to quantify irreducible multipartite correlations.

To illustrate the usefulness of Results 1 and 2, we consider two-dimensional lattice models that can be exactly solved by the stabilizer formalism. Well-known examples of such models include the cluster state used in one-way quantum computation[6] and Kitaev's toric code state.[8,15] In general, the ground state of such models can be specified as an eigenvector of local stabilizer operators. We study tripartite entanglement of the ground state with respect to a partition of the lattice into three angular segments with a common junction point (see Fig. 1 in Sec. VII). We show that the number of GHZ states extractable from the ground state is bounded from above by a constant that depends only upon the structure of stabilizers near the junction point (and does not depend upon the size of the lattice). This is a natural generalization of the entanglement saturation phenomenon found for 1D spin chains (see Ref. 16 and references therein).

The rest of the paper is organized as follows. Section II introduces notation and terminology. Our main technical theorems are proved in Sec. III. In Sec. IV we consider multipartite stabilizer states and prove Eq. (2). Section V establishes a connection between GHZ extraction yield and measures of multipartite correlations. LU-equivalence classes of tripartite states are discussed in

Sec. VI. We apply the developed technique to spin lattices in Sec. VII. The goal of Sec. VIII is to convince the reader that four-party stabilizer states are likely to lack a simple entanglement generating set.

II. PRELIMINARIES AND NOTATION

A. Stabilizer states

The goal of this section is to introduce convenient terminology. Whenever it is possible, we use the notation of Ref. 17, Chap. 15.

The Pauli operators σ^x, σ^y, σ^z, and the identity operator I will be labeled by elements of two-dimensional binary linear space $G=\{00,01,10,11\}$, such that

$$\sigma_{00}=I, \quad \sigma_{10}=\sigma^x, \quad \sigma_{01}=\sigma^z, \quad \sigma_{11}=\sigma^y.$$

For any integer n and $f=(\alpha_1,\beta_1,\ldots,\alpha_n,\beta_n)\in G^n$, define a *σ-operator*

$$\sigma(f)=\sigma_{\alpha_1\beta_1}\otimes\cdots\otimes\sigma_{\alpha_n\beta_n}.$$

For all $f,g\in G^n$, one has $\sigma(f)\sigma(g)=e^{i\theta}\sigma(f+g)$ for some phase factor $e^{i\theta}$. The commutation rules for σ-operators can be written as

$$\sigma(f)\sigma(g)=(-1)^{\omega(f,g)}\sigma(g)\sigma(f).$$

Here $\omega: G^n\otimes G^n\to\{0,1\}$ is a symplectic form,

$$\omega(f,f')=\sum_{j=1}^{n}\alpha_j\beta_j'+\beta_j\alpha_j' \bmod 2.$$

For any subspace $S\subseteq G^n$ define a dual subspace $S^\perp$ as

$$S^\perp=\{f\in G^n:\omega(f,g)=0 \text{ for all } g\in S\}.$$

A subspace S is called *isotropic* iff $S\subseteq S^\perp$, i.e., $\omega(f,g)=0$ for any $f,g\in S$. A subspace S is called self-dual iff $S^\perp=S$. For any isotropic (self-dual) subspace $S\subset G^n$ one has $\dim(S)\leq n$ ($\dim(S)=n$).

The Hilbert space of n qubits will be denoted $\mathcal{B}^n$. A unitary operator $U:\mathcal{B}^n\to\mathcal{B}^n$ belongs to the *Clifford group*, $U\in\mathrm{Cl}(n)$, iff it maps σ-operators to σ-operators (up to a sign) under the conjugation. In other words, $U\in\mathrm{Cl}(n)$ iff there exists a map $u:G^n\to G^n$ and a function $\epsilon:G^n\to\{+1,-1\}$, such that

$$U\sigma(f)U^\dagger=\epsilon(f)\sigma(u(f)) \tag{3}$$

for any $f\in G^n$. Unitarity of U implies that u is a linear invertible map preserving the inner product ω, i.e.,

$$\omega(f,g)=\omega(u(f),u(g))$$

for all $f,g\in G^n$. Such linear maps constitute a binary symplectic group $\mathrm{Sp}_2(n)$. In fact, all $u\in\mathrm{Sp}_2(n)$ can be realized through an appropriate choice of $U\in\mathrm{Cl}(n)$.

A *stabilizer state* $|\Psi\rangle\in\mathcal{B}^n$ is an irreducible representation of a group $\{\epsilon(f)\sigma(f):f\in S\}$, where $S\subset G^n$ is a self-dual subspace and $\epsilon:S\to\{+1,-1\}$ is a function that accounts for a phase in a product of σ operators. In other words,

$$\sigma(f)|\Psi\rangle=\epsilon(f)|\Psi\rangle, \quad f\in S. \tag{4}$$

The state $|\Psi\rangle$ is uniquely specified by Eq. (4). The subspace S is referred to as a *stabilizer group* of $|\Psi\rangle$. Two stabilizer states have the same stabilizer group iff they can be mapped to each other

by a σ operator, see Ref. 17. Any stabilizer state can be represented as $|\Psi\rangle = U|0^{\otimes n}\rangle$ for some operator $U \in \mathrm{Cl}(n)$.

B. Local Clifford equivalence

A state $|\Psi\rangle \in \mathcal{B}^n$ is called *M-partite* iff the n qubits are distributed between a finite set of parties M, i.e.,

$$n = \sum_{\alpha \in M} n_\alpha, \quad n_\alpha \geq 0. \tag{5}$$

We shall be interested in equivalence classes (orbits) of stabilizer states under local Clifford unitary (LCU) operators.

Definition 1: M-partite stabilizer states $|\Psi\rangle, |\Psi'\rangle \in \mathcal{B}^n$ *are called LCU-equivalent iff there exist Clifford unitaries* $\{U_\alpha \in \mathrm{Cl}(n_\alpha)\}_{\alpha \in M}$ *such that*

$$|\Psi'\rangle = \bigotimes_{\alpha \in M} U_\alpha |\Psi\rangle .$$

For any vector $f \in G^n$ and party α denote by $f_\alpha \in G^{n_\alpha}$ a projection of f onto the party α (if one regards f as a binary string, f_α is a substring that includes all qubits owned by a party α). In particular, $f_\alpha = 0$ iff $\sigma(f)$ acts trivially on the party α.

Definition 2: Suppose n qubits are distributed among a set of parties M. Let $S \subseteq G^n$ *be a linear subspace. For each* $\alpha \in M$ *define a local subspace* $S_\alpha \subseteq S$ *and a colocal subspace* $S_{\hat{\alpha}} \subseteq S$ *as*

$$S_\alpha = \{g \in S : g_\beta = 0 \text{ for all } \beta \in M \setminus \alpha\},$$

and

$$S_{\hat{\alpha}} = \{g \in S : g_\alpha = 0\}.$$

In other words, $f \in S_{\hat{\alpha}}$ iff $\sigma(f)$ acts as the identity on the party α; $f \in S_\alpha$ iff $\sigma(f)$ acts as the identity on all parties $\beta \neq \alpha$. In the case $n_\alpha = 0$ we shall use a convention $S_\alpha = 0$ and $S_{\hat{\alpha}} = S$. If S is a stabilizer group of some state, we shall use the terms local (colocal) subspace and local (colocal) subgroup interchangeably.

Consider an M-party stabilizer state $|\Psi\rangle$. Let ρ_α be the reduced state of the party α. To simplify the discussion we shall assume that $\mathrm{Rk}(\rho_\alpha) = 2^{n_\alpha}$ for all $\alpha \in M$, that is, that all states under consideration have the maximal possible local ranks. Let S be a stabilizer group of $|\Psi\rangle$. One can easily check that the requirement $\mathrm{Rk}(\rho_\alpha) = 2^{n_\alpha}$ is equivalent to the local subgroup S_α being trivial.

Definition 3: An M-party stabilizer state $|\Psi\rangle$ *with a stabilizer group S has full local ranks iff all local subgroups of S are trivial*:

$$S_\alpha = 0 \quad \text{for all } \alpha \in M.$$

In general case, if $\mathrm{Rk}(\rho_\alpha) = 2^k$, one has $\dim(S_\alpha) = n_\alpha - k$. Equivalently, $n_\alpha - k$ copies of the one-qubit state $|0\rangle$ can be extracted from $|\Psi\rangle$ for each $\alpha \in M$ by local Clifford unitaries (this will follow from Theorem 2 with $S' = S_\alpha$). After such local extractions we arrive at a state with full local ranks. A necessary and sufficient criterion for LCU equivalence is given below.

Theorem 1: *Let* $|\Psi\rangle, |\Psi'\rangle \in \mathcal{B}^n$ *be M-party stabilizer states with full local ranks. Let* $S, S' \subset G^n$ *be their stabilizer groups. The state* $|\Psi\rangle$ *is LCU equivalent to* $|\Psi'\rangle$ *iff there exists a linear invertible map* $T : S \to S'$ *such that*

$$\omega(T(f)_\alpha, T(g)_\alpha) = \omega(f_\alpha, g_\alpha) \quad \text{for all } f, g \in S, \alpha \in M.$$

We shall prove Theorem 1 in the next section.

III. LOCAL EXTRACTION

Let $|\Psi\rangle \in \mathcal{B}^n$ be an M-party stabilizer state. The most interesting stabilizer states are *LCU-irreducible* ones (which in this paper we simply refer to as *irreducible*), which are not LCU equivalent to a collection of stabilizer states of smaller dimension. For example, if one considers the finest partition, $M=\{1,2,\ldots,n\}$, a state $|\Psi\rangle$ is irreducible iff it is entangled with respect to any bipartition. On the other hand, we shall see that for bipartite and tripartite systems ($|M|=2$ or $|M|=3$), the only irreducible states are the EPR and GHZ states. If $|\Psi\rangle$ is not irreducible, one can *extract* some simpler stabilizer state from it by LCU operators. Given two M-party states $|\Psi\rangle$ and $|\Psi'\rangle$, one can ask under what circumstances $|\Psi'\rangle$ is extractable from $|\Psi\rangle$. The goal of this section is to answer this question. Note that LCU-equivalence of states is just a special case of extraction, when $|\Psi'\rangle$ and $|\Psi\rangle$ are composed from the same number of qubits.

Definition 4: Let $|\Psi\rangle \in \mathcal{B}^n$ *and* $|\Psi'\rangle \in \mathcal{B}^k$ *be M-party stabilizer states, such that*

$$n=\sum_{\alpha\in M} n_\alpha, \quad k=\sum_{\alpha\in M} k_\alpha, \quad 0\le k_\alpha \le n_\alpha.$$

The state $|\Psi'\rangle$ *is extractable from* $|\Psi\rangle$ *iff* $|\Psi\rangle$ *is LCU-equivalent to* $|\Psi'\otimes\Psi''\rangle$ *for some M-party stabilizer state* $|\Psi''\rangle$.

Remark: An equality $k_\alpha=0$ means that the party α owns no qubits of the state $|\Psi'\rangle$. Analogously, $k_\alpha=n_\alpha$ implies that the party α owns no qubits of the state $|\Psi''\rangle$.

A necessary and sufficient criterion for a state $|\Psi'\rangle$ to be extractable from $|\Psi\rangle$ is given below.

Theorem 2: *Let* $|\Psi\rangle \in \mathcal{B}^n$ *and* $|\Psi'\rangle \in \mathcal{B}^k$ *be M-party stabilizer states with stabilizer groups* $S\subset G^n$ *and* $S'\subset G^k$. *The state* $|\Psi'\rangle$ *is extractable from* $|\Psi\rangle$ *iff there exists a linear injective map* $T:S'\to S$ such that

(i) $\omega(T(f)_\alpha, T(g)_\alpha)=\omega(f_\alpha,g_\alpha)$ *for all* $f,g\in S'$ *and* $\alpha\in M$;
(ii) $(T\cdot S')_{\hat{\alpha}}=T\cdot(S'_{\hat{\alpha}})$ *for all* $\alpha\in M$.

This theorem is a simple consequence of the following lemma.

Lemma 1: Suppose n qubits are distributed among a set of parties M. Let $S,S'\subset G^n$ *be linear subspaces. The following statements are equivalent*:

(1) *There exist local operators* $\{u_\alpha\in \mathrm{Sp}_2(n_\alpha)\}_{\alpha\in M}$ *such that*

$$S'=\left(\bigoplus_{\alpha\in M} u_\alpha\right)\cdot S,$$

(2) *There exists a linear invertible map* $T:S\to S'$ *such that*

(i) $\omega(T(f)_\alpha, T(g)_\alpha)=\omega(f_\alpha,g_\alpha)$ *for all* $f,g\in S$ *and* $\alpha\in M$;
(ii) $T\cdot S_{\hat{\alpha}}=S'_{\hat{\alpha}}$ *for all* $\alpha\in M$.

Here the direct sum $\oplus_{\alpha\in M}u_\alpha$ corresponds to a decomposition of G^n into its local subspaces, i.e., $G^n=\oplus_{\alpha\in M}G^n_\alpha$. A proof of the lemma is presented in Appendix B.

Proof of Theorem 2: The nontrivial part is to prove that existence of T with the properties (i), (ii) implies that $|\Psi'\rangle$ is extractable from $|\Psi\rangle$. Let us split the n_α qubits owned by the party $\alpha\in M$ into two subsets

$$\{1,2,\ldots,n_\alpha\}=A_\alpha\cup B_\alpha,$$

such that $|A_\alpha|=k_\alpha$. We shall refer to a qubit as an A-qubit (B-qubit) if it belongs to one of the subsets A_α (B_α). Any vector $f\in G^n$ can be represented as a direct sum $f=f_A\oplus f_B$, where f_A and f_B are projections of f onto A-qubits and B-qubits, respectively.

Let us define a linear subspace $R'\subset G^n$ that is equal to a direct sum of S' on A-qubits and the zero space on B-qubits, i.e.,

$$R' = \{f \in G^n : f_B = 0 \text{ and } f_A \in S'\}.$$

Define also a subspace $R = T \cdot S' \subseteq S$, i.e.,

$$R = \{f \in G^n : f = T(g) \text{ for some } g \in S'\}. \tag{6}$$

The map T regarded as a map from R' to R obviously satisfies condition (2) of Lemma 1. We conclude that there exists a linear symplectic operator $u : G^n \to G^n$ such that

$$R' = u \cdot R, \quad u = \bigoplus_{\alpha \in M} u_\alpha, \tag{7}$$

where $u_\alpha \in \mathrm{Sp}_2(n_\alpha)$.

Consider a linear subspace

$$Q = u \cdot S \subset G^n. \tag{8}$$

The fact that $u \in \mathrm{Sp}_2(n)$ implies that Q is self-dual. Let $|\Phi\rangle \in \mathcal{B}^n$ be a stabilizer state with the stabilizer group Q. ($|\Phi\rangle$ is unique up to multiplication by a σ operator.) Since u is a direct sum of local symplectic operators, $|\Phi\rangle$ is LCU equivalent to $|\Psi\rangle$.

We still must show that $|\Phi\rangle$ is a tensor product of two stabilizer states, $|\Phi\rangle = |\Phi_A \otimes \Phi_B\rangle$, that live on the A-qubits and B-qubits, respectively. Indeed, since R is a subgroup of S, it follows from Eqs. (7) and (8) that

$$R' \subseteq Q.$$

Thus the state $|\Phi\rangle$ satisfies stabilizer equations

$$\sigma(f)|\Phi\rangle = \epsilon(f)|\Phi\rangle, \quad f \in R', \tag{9}$$

for some function $\epsilon : R' \to \{+1, -1\}$. By the definition of R', any operator $\sigma(f)$, $f \in R'$ acts trivially on B-qubits. If we restrict our attention to A-qubits only, R' is a self-dual subspace (since $R \cong S'$). Thus the stabilizer equations (9) completely specify the state of the A-qubits [see the remarks following Eq. (4)]. Denote this state $|\Phi_A\rangle$. Since the states $|\Phi_A\rangle$ and $|\Psi'\rangle$ have the same stabilizer group, they coincide up to a σ operator. Thus $|\Phi\rangle$ is LCU equivalent to $|\Psi' \otimes \Phi_B\rangle$ for some stabilizer state $|\Phi_B\rangle$. On the other hand, $|\Phi\rangle$ is LCU equivalent to $|\Psi\rangle$. We have proved that $|\Psi'\rangle$ is extractable from $|\Psi\rangle$.

Conversely, suppose $|\Psi\rangle$ is LCU equivalent to $|\Psi' \otimes \Psi''\rangle$. This means that $S = u \cdot (S' \oplus S'')$, where S'' is a self-dual subspace, $u = \oplus_{\alpha \in M} u_\alpha$ is a local symplectic operator, and the direct sum corresponds to the bipartition of all qubits in the state $|\Psi' \otimes \Psi''\rangle$. One can easily check that a map

$$T(f) = u \cdot (f \oplus 0)$$

from S' to S satisfies conditions (i) and (ii). The theorem is proved. □

Remark: Condition (ii) in Theorem 2 cannot be dropped. Indeed, consider as an example three-party states, $M = \{A, B, C\}$. Let $|\Psi\rangle = |\Psi_3^+\rangle$ be the GHZ state and $|\Psi'\rangle = |\Psi^+\rangle$ be the EPR state shared by A and B. Obviously, $|\Psi'\rangle$ cannot be extracted from $|\Psi\rangle$ without classical communication. However, the linear injective map T satisfying condition (i) exists. Indeed, consider a mapping

$$\sigma^x \otimes \sigma^x \to \sigma^x \otimes \sigma^x \otimes \sigma^x,$$

$$\sigma^z \otimes \sigma^z \to \sigma^z \otimes \sigma^z \otimes I$$

between stabilizer generators of $|\Psi'\rangle$ and $|\Psi\rangle$. It can be easily converted to a map $T : S' \to S$ between the stabilizer groups. This map preserves local commutation rules, so condition (i) is satisfied.

Proof of Theorem 1: Consider a special case of Theorem 2 with $k_\alpha = n_\alpha$ for all $\alpha \in M$, i.e., with

the state $|\Psi''\rangle$ being a complex number. In this case $S, S' \subset G^n$ are self-dual subspaces, so that $\dim(S)=\dim(S')=n$. Thus T is a linear invertible map and $T\cdot S'=S$. On the other hand, the statement "$|\Psi'\rangle$ is extractable from $|\Psi\rangle$" translates into "$|\Psi'\rangle$ is LCU equivalent to $|\Psi\rangle$." What we obtain is exactly Theorem 1 with T replaced by T^{-1} and with the extra condition (ii). We will show now that (ii) can be derived from (i), the equality $T\cdot S'=S$, and the maximal local rank assumption.

Indeed, consider some particular α and take any vector $f \in S'_{\hat{\alpha}}$, so $f_\alpha=0$. Denote $h=T(f) \in S$. Condition (i) tells us that

$$\omega(h_\alpha, g_\alpha) = \omega(f_\alpha, (T^{-1}(g))_\alpha) = 0 \quad \text{for any } g \in S.$$

Consider a vector $\tilde{h} \in G^n_\alpha$ such that $\tilde{h}_\alpha=h_\alpha$. Then $\omega(\tilde{h}, g)=0$ for any $g \in S$, that is $\tilde{h} \in S^\perp$. Since $S^\perp=S$ we have $\tilde{h} \in S \cap G^n_\alpha = S_\alpha = 0$. We conclude that $h_\alpha=0$, that is $h \in S_{\hat{\alpha}}$. This proves that

$$T \cdot S'_{\hat{\alpha}} \subseteq S_{\hat{\alpha}}.$$

Applying the same arguments to the map $T^{-1}: S \to S'$ [which, of course, also satisfies condition (i)] one gets

$$T^{-1} \cdot S_{\hat{\alpha}} \subseteq S'_{\hat{\alpha}}.$$

Therefore $S'_{\hat{\alpha}}$ and $S_{\hat{\alpha}}$ have the same dimension, and thus $T\cdot S'_{\hat{\alpha}}=S_{\hat{\alpha}}$. □

Remark: In fact, a little bit more work shows that the full local ranks assumption in Theorem 1 can be dropped. We sacrifice some generality for the sake of readability.

IV. GHZ-EXTRACTION FORMULA

Given a set of parties M, $|M|=m$, consider an M-party analogue of the GHZ state

$$|\Psi^+_m\rangle = \frac{1}{\sqrt{2}}(|0^{\otimes m}\rangle + |1^{\otimes m}\rangle) \in \mathcal{B}^m.$$

It is a stabilizer state with a stabilizer group generated by a vector $\bar{f} \in G^m$ such that

$$\sigma(\bar{f}) = \sigma^x_1 \otimes \sigma^x_2 \otimes \cdots \otimes \sigma^x_m, \tag{10}$$

and vectors $\{f_{\alpha\beta} \in G^m\}_{\alpha,\beta \in M}$ such that

$$\sigma(f_{\alpha\beta}) = \sigma^z_\alpha \otimes \sigma^z_\beta \tag{11}$$

(the identity factors are suppressed). The vectors $\bar{f}$, $f_{\alpha\beta}$ constitute an overcomplete basis of the stabilizer group.

Given an M-party stabilizer state $|\Psi\rangle \in \mathcal{B}^n$, one can ask how many copies of $|\Psi^+_m\rangle$ can be extracted from $|\Psi\rangle$ by local Clifford unitaries. The goal of this section is to answer this question. Let S be a stabilizer group of $|\Psi\rangle$, and $S_{\hat{\alpha}} \subseteq S$, $\alpha \in M$, be its colocal subgroups (see Definition 2). Define a subgroup

$$S_{\text{loc}} = \sum_{\alpha \in M} S_{\hat{\alpha}} \tag{12}$$

generated by all colocal subgroups. The sum above is generally not a direct one, since the colocal subgroups may overlap. By definition, $S_{\text{loc}} \subseteq S$, and, in general, $S_{\text{loc}} \subset S$. In the latter case one has a deficit of local stabilizer elements, meaning that for any choice of a basis in S there will be at least $n-\dim(S_{\text{loc}})$ basis vectors having support on all m parties $\alpha \in M$. We will see that each of these nonlocal basis vectors can be identified with the $\bar{f}$ element of the stabilizer of a state $|\Psi^+_m\rangle$ [see Eq. (10)].

It was pointed out in Ref. 12 that a functional

$$\Delta(\Psi) = n - \dim(S_{\mathrm{loc}}) = \dim(S) - \dim(S_{\mathrm{loc}}) \tag{13}$$

can be used as an entanglement measure that quantifies truly multipartite correlations in $|\Psi\rangle$. In the present paper we go further and prove the following theorem.

Theorem 3: *Let $|\Psi\rangle \in \mathcal{B}^n$ be an M-party stabilizer state with a stabilizer group S. Suppose that $m=|M| \geq 3$. The maximal number of states $|\Psi_m^+\rangle$ extractable from $|\Psi\rangle$ by local Clifford unitaries is equal to $\Delta(\Psi)$.*

Remarks: (1) Note that the functional $\Delta(\Psi)$ is invariant under extraction of local $|0\rangle$ states. Thus we can safely assume that $|\Psi\rangle$ has full local ranks. (2) The generalization of the theorem to arbitrary LU operators is discussed in Sec. V. (3) A shorter but less constructive proof of the theorem is given in Appendix A.

Proof: For each $\alpha \in M$ define a subspace $\mathcal{L}_\alpha \in G^n$ as

$$\mathcal{L}_\alpha = \{f \in G_\alpha^n : \omega(f,g) = 0 \text{ for all } g \in S_{\mathrm{loc}}\}.$$

Here G_α^n is the local subspace of G^n corresponding to the party α (see Definition 2). To illustrate the usefulness of this definition, consider as an example $|\Psi\rangle = |\Psi_m^+\rangle$. Then the subgroup S_{loc} is generated by vectors $\{f_{\alpha\beta}\}$ [see Eq. (11)], while $\mathcal{L}_\alpha$ is a one-dimensional subspace generated by σ_α^z. The remaining stabilizer generator of the GHZ state $\bar{f}$ anticommutes with σ_α^z for any $\alpha \in M$. Thus any product $\sigma_\alpha^z \otimes \sigma_\beta^z$ commutes with both $\bar{f}$ and stabilizer elements from S_{loc}. Therefore, $\sigma_\alpha^z \otimes \sigma_\beta^z$ is in the stabilizer of $|\Psi\rangle$. Similarly, in the general case, we shall use the subspaces $\mathcal{L}_\alpha$ to construct 2-local stabilizer elements of $|\Psi\rangle$ that are analogous to $\sigma_\alpha^z \otimes \sigma_\beta^z$ stabilizer elements of the GHZ state.

Our first goal is to prove that

$$\dim(\mathcal{L}_\alpha) = \Delta(\Psi) \quad \text{for any } \alpha \in M. \tag{14}$$

Choose an arbitrary subgroup $S_{\mathrm{ent}} \subseteq S$ such that

$$S = S_{\mathrm{loc}} \oplus S_{\mathrm{ent}}. \tag{15}$$

By definition of S_{loc}, any nonzero vector $f \in S_{\mathrm{ent}}$ has support on all parties, i.e., $f_\alpha \neq 0$ for all $\alpha \in M$. Define a bilinear form

$$\eta_\alpha : \mathcal{L}_\alpha \otimes S_{\mathrm{ent}} \to \{0,1\}, \quad \eta_\alpha(f,g) = \omega(f_\alpha, g_\alpha).$$

We claim that the form η_α is nonsingular, that is

$$\eta_\alpha(f,g) = 0 \quad \text{for all } g \in S_{\mathrm{ent}} \text{ iff } f = 0, \tag{16}$$

and

$$\eta_\alpha(f,g) = 0 \quad \text{for all } f \in \mathcal{L}_\alpha \quad \text{iff } g = 0. \tag{17}$$

Indeed, suppose $f \in \mathcal{L}_\alpha$ and $\omega(f,g)=0$ for all $g \in S_{\mathrm{ent}}$. By definition of $\mathcal{L}_\alpha$, we have $\omega(f,g)=0$ for all $g \in S_{\mathrm{loc}}$. Thus the decomposition Eq. (15) implies that $f \in S^\perp$. But since $S^\perp = S$, one has $f \in S$. Since the state $|\Psi\rangle$ has full local ranks (see the remark after the theorem), $\mathcal{L}_\alpha \cap S \subseteq S_\alpha = 0$, that is $f=0$. The property Eq. (16) is proved.

Suppose $g \in S_{\mathrm{ent}}$ and $\omega(f,g)=0$ for all $f \in \mathcal{L}_\alpha$ (for some particular $\alpha \in M$), that is $g \in \mathcal{L}_\alpha^\perp$. The definition of $\mathcal{L}_\alpha$ implies that

$$g \in \mathcal{L}_\alpha^\perp \text{ iff } g_\alpha = h_\alpha \quad \text{for some } h \in S_{\mathrm{loc}}.$$

[Here we use the fact that $(\mathcal{L}^\perp)^\perp = \mathcal{L}$ for any binary subspace $\mathcal{L}$.] Thus there exists a vector $h \in S_{\mathrm{loc}}$ such that $(h+g)_\alpha = 0$, i.e., $h+g \in S_{\mathrm{loc}}$. But this means that $g \in S_{\mathrm{loc}}$. Since decomposition Eq. (15) is a direct sum, the inclusion $g \in S_{\mathrm{ent}} \cap S_{\mathrm{loc}}$ implies $g=0$. The property Eq. (17) is proved.

The fact that η_α is nonsingular implies that the subspaces $\mathcal{L}_\alpha$ and S_{ent} have the same dimension. But from Eq. (15) we infer that $\dim(S_{\text{ent}})=\Delta(\Psi)$. The formula Eq. (14) is proved.

Denote $p=\Delta(\Psi)$ and choose an arbitrary basis $\bar{g}_1,\bar{g}_2,\ldots,\bar{g}_p$ in the subspace S_{ent}. For each $\alpha\in M$ choose the dual basis $g_{\alpha 1},g_{\alpha 2},\ldots,g_{\alpha p}$ in the subspace $\mathcal{L}_\alpha$ with respect to the form η_α. That is, the set of vectors $\{g_{\alpha j}\}_j$ must satisfy equations

$$\eta_\alpha(g_{\alpha j},\bar{g}_k)=\delta_{jk} \quad \text{for all } 1\le j,k\le p \quad \text{and } \alpha\in M. \tag{18}$$

Define vectors $g_{\alpha\beta j}\in G^n$ by

$$g_{\alpha\beta j}=g_{\alpha j}+g_{\beta j}, \quad j=1,\ldots,p.$$

It follows from Eq. (18) that

$$\omega(g_{\alpha\beta j},\bar{g}_k)=\eta_\alpha(g_{\alpha j},\bar{g}_k)+\eta_\beta(g_{\beta j},\bar{g}_k)=\delta_{jk}+\delta_{jk}=0.$$

Thus $g_{\alpha\beta j}\in S_{\text{ent}}^{\perp}$. On the other hand, by definition of the subspaces $\mathcal{L}_\alpha$, one has $\mathcal{L}_\alpha\subseteq S_{\text{loc}}^{\perp}$ for all $\alpha\in M$, that is $g_{\alpha\beta j}\in S_{\text{loc}}^{\perp}$. We infer from Eq. (15) that $g_{\alpha\beta j}\in S^{\perp}$. Since S is self-dual, we conclude that $g_{\alpha\beta j}\in S$.

All arguments above apply equally well to $m=2$ and $m\ge 3$. From now on we shall focus on the case $m\ge 3$.

We would like to show that the subspaces $\mathcal{L}_\alpha$ are isotropic, i.e.,

$$\omega(f,g)=0 \quad \text{for all } f,g\in\mathcal{L}_\alpha, \quad \alpha\in M. \tag{19}$$

Indeed, it suffices to show that $\omega(g_{\alpha j},g_{\alpha k})=0$ for any j,k. Assuming that $m\ge 3$, choose an arbitrary triple $\alpha,\beta,\gamma\in M$, such that $\alpha\ne\beta\ne\gamma$. Taking into account that $g_{\alpha\beta j}\in S$, $g_{\alpha\gamma k}\in S$, we obtain that

$$0=\omega(g_{\alpha\beta j},g_{\alpha\gamma k})=\omega(g_{\alpha j},g_{\alpha k}).$$

The property Eq. (19) is proved.

By definition, a vector $g_{\alpha\beta j}$ has a support only on two parties. If $m\ge 3$ it means that

$$g_{\alpha\beta j}\in S_{\text{loc}} \tag{20}$$

for all pairs of parties $\alpha,\beta\in M$ and $j=1,\ldots,p$.

Our next goal is to adjust the subspace S_{ent} to make it "locally isotropic," i.e., to fulfill the following property:

$$\omega(f_\alpha,g_\alpha)=0 \quad \text{for all } f,g\in S_{\text{ent}}, \quad \alpha\in M.$$

This adjustment can be achieved by adding a proper "local shift" taken from the subspaces $\mathcal{L}_\alpha$. Namely, the basis vectors $\bar{g}_j\in S_{\text{ent}}$ must be replaced by new basis vectors according to

$$\bar{g}_j\to\bar{g}_j+\sum_{\alpha\in M}\sum_{l=1}^{j-1}\Gamma_{jl}^{\alpha}g_{\alpha l}, \quad j=1,\ldots,p, \tag{21}$$

where

$$\Gamma_{jl}^{\alpha}=\omega((\bar{g}_j)_\alpha,(\bar{g}_l)_\alpha).$$

One can easily check that after this replacement we end up with

$$\omega((\bar{g}_j)_\alpha,(\bar{g}_k)_\alpha)=0$$

for all $\alpha\in M$ and all j,k. In addition, the fact that S_{ent} is an isotropic subspace, i.e., $\omega(\bar{g}_j,\bar{g}_k)=0$, implies that

$$\sum_{\alpha\in M}\Gamma^{\alpha}_{jl}=0$$

for any fixed j,l. This means that the vector added to $\bar{g}_j$ in Eq. (21) belongs to the stabilizer group S. Accordingly, the adjusted $S_{\rm ent}$ is still a subspace of S. Moreover, Eq. (20) implies that the added vector belongs to $S_{\rm loc}$, so the decomposition $S=S_{\rm loc}\oplus S_{\rm ent}$ remains a direct sum.

Summarizing, after the adjustment described above we can assume that

$$\omega(g_{\alpha j},g_{\alpha k})=0,\quad \omega((\bar{g}_j)_\alpha,(\bar{g}_k)_\alpha)=0,\quad \omega(g_{\alpha j},\bar{g}_k)=\delta_{jk}, \tag{22}$$

for all $\alpha\in M$. Here j and k are arbitrary integers in the range $1,\ldots,p$.

Denote by $S_{\rm ghz}\subset G^{m\cdot p}$ a stabilizer group of p copies of the GHZ state $|\Psi^+_m\rangle$. As generators of $S_{\rm ghz}$ let us choose p copies of the canonical GHZ generators [see Eqs. (10) and (11)]. Denote them as $\bar{f}_j$ and $f_{\alpha\beta j}$, where $j=1,\ldots,p$ refers to different copies of $|\Psi^+_m\rangle$. Define a linear map $T:S_{\rm ghz}\to S$ such that its action on the generators is as follows:

$$T(\bar{f}_j)=\bar{g}_j,\quad T(f_{\alpha\beta j})=g_{\alpha\beta j},$$

where $j=1,\ldots,p$ and $\alpha,\beta\in M$. We would like to prove that T satisfies all conditions of Theorem 2.

Using the fact that the vectors $\{\bar{g}_j,g_{\alpha k}\}$, $j,k=1,\ldots,p$, $\alpha\in M$ are linearly independent, one can easily show that T is a linear injection. Taking into account that $\bar{g}_1,\ldots,\bar{g}_p$ span the subspace $S_{\rm ent}$ that has no intersection with $S_{\rm loc}$, we conclude that $(T\cdot S_{\rm ghz})_{\hat{\alpha}}=T\cdot(S_{\rm ghz})_{\hat{\alpha}}$. Condition (i) of Theorem 2 follows from the local commutation relations Eq. (22). Thus one can extract *at least* p copies of the state $|\Psi^+_m\rangle$ from $|\Psi\rangle$.

Conversely, to prove the upper bound, assume that one can extract q copies of $|\Psi^+_m\rangle$ from $|\Psi\rangle$. Denote by $S_{\rm ghz}$ the stabilizer group of $|q\cdot\Psi^+_m\rangle$ and let $\bar{f}_1,\ldots,\bar{f}_q$ be the canonical σ^x-type stabilizers [see Eq. (10)]. Let $T:S_{\rm ghz}\to S$ be the linear injective map whose existence is guaranteed by Theorem 2. Clearly, a linear span of $\bar{f}_1,\ldots,\bar{f}_q$ has no intersection with colocal subspaces $(S_{\rm ghz})_{\hat{\alpha}}$. According to Theorem 2, vectors $T(\bar{f}_1),\ldots,T(\bar{f}_q)$ are linearly independent and their linear span has no intersection with $S_{\rm loc}$. This means that $\dim(S_{\rm loc})\le n-q$. Therefore $p\ge q$, i.e., one can extract *at most* p copies of $|\Psi^+_m\rangle$. □

V. BEYOND STABILIZER STATES

In this section we argue that the functional $\Delta(\Psi)$ defined in Eq. (13) for stabilizer states can be naturally extended to arbitrary multipartite states. Namely, it coincides with a measure of multipartite correlations introduced by Linden, Popescu, and Wootters in Ref. 14. A similar measure has been introduced also for multipartite probability distributions in Ref. 18. It will allow us to show that $\Delta(\Psi)$ is equal to the number of GHZ states extractable from $|\Psi\rangle$ by *arbitrary* local unitaries.

Denote by $D(\mathcal{B}^n)$ a set of all mixed n-qubit states. Assume that n qubits are distributed between a set of parties M. Let $|\Psi\rangle\in\mathcal{B}^n$ be an arbitrary M-party state. Define a set

$$\Gamma(\Psi)=\{\rho\in D(\mathcal{B}^n):{\rm Tr}_\alpha(\rho)={\rm Tr}_\alpha(|\Psi\rangle\langle\Psi|)\ \alpha\in M\},$$

where Tr_α is the partial trace. In other words, $\rho\in\Gamma(\Psi)$ iff ρ agrees with $|\Psi\rangle$ on any subset of $|M|-1$ parties. Following Ref. 14, define a functional

$$\Omega(\Psi)=\max_{\rho\in\Gamma(\Psi)}S(\rho), \tag{23}$$

where $S(\rho)=-{\rm Tr}\,\rho\log(\rho)$ is the von Neumann entropy. For bipartite states $\Omega(\Psi)$ coincides with the entanglement entropy (except for a factor 2) (see Ref. 14). The main result of this section is the following.

Theorem 4: *For any M-party stabilizer state $|\Psi\rangle$ with a stabilizer group S one has*

$$\Omega(\Psi) = \dim(S) - \dim(S_{\mathrm{loc}}),$$

where $S_{\mathrm{loc}} = \Sigma_{\alpha \in M} S_{\hat{\alpha}}$.

The proof is based on the following observation.

Lemma 2: *Let* $|\Psi\rangle$ *be an* M*-party stabilizer state with a stabilizer group* S*. If* S *is generated by its colocal subgroups*, $S = S_{\mathrm{loc}}$, *then* $|\Psi\rangle\langle\Psi|$ *is the only state that belongs to the set* $\Gamma(\Psi)$.

In other words a state $|\Psi\rangle$ with $S = S_{\mathrm{loc}}$ is the unique (mixed) state compatible with partial traces of $|\Psi\rangle$.

Proof: We shall use stabilizer equations $\sigma(f)|\Psi\rangle = \epsilon(f)|\Psi\rangle$, $f \in S$, uniquely specifying $|\Psi\rangle$ [see Eq. (4)]. Take any state $\rho \in \Gamma(\Psi)$. For any $f \in S_{\hat{\alpha}}$ one has

$$\mathrm{Tr}(\sigma(f)\rho) = \langle\Psi|\sigma(f)|\Psi\rangle = \epsilon(f).$$

Now consider a projector $\Pi = (1/2)(I + \epsilon(f)\sigma(f))$. Then $\mathrm{Tr}(\Pi\rho) = 1$. This is possible only if the range of ρ coincides with the range of Π. Thus, $\Pi\rho = \rho$, i.e.,

$$\sigma(f)\rho = \rho\sigma(f) = \epsilon(f)\rho \quad \text{for any } f \in S_{\hat{\alpha}}, \quad \alpha \in M. \tag{24}$$

Since S is generated by the subgroups $S_{\hat{\alpha}}$, the equalities Eq. (24) actually hold for any $f \in S$. But equations $\sigma(f)\rho = \epsilon(f)\rho$, $f \in S$, mean that ρ has support on the subspace stabilized by S, that is $\rho = |\Psi\rangle\langle\Psi|$. □

Corollary 1: *Let* $|\Psi\rangle = |\Psi' \otimes \Phi\rangle$ *be a collection of two* M*-party stabilizer states*, *such that* $|\Phi\rangle$ *satisfies the conditions of Lemma 2. Then*

$$\Gamma(\Psi) = \Gamma(\Psi') \otimes |\Phi\rangle\langle\Phi|. \tag{25}$$

To prove the corollary, take any state $\rho \in \Gamma(\Psi)$ and apply Lemma 2 to the partial trace of ρ over the first subsystem. Now we are ready to prove Theorem 4.

Proof: Let $p = \dim(S) - \dim(S_{\mathrm{loc}})$ and $m = |M|$. Obviously, $\Omega(\Psi)$ is invariant under local unitaries. As we know from Theorem 3, $|\Psi\rangle$ is LCU equivalent to a collection of p M-party GHZ states, $|p \cdot \Psi_m^+\rangle$, and some M-party stabilizer state $|\Phi\rangle$ satisfying the conditions of Lemma 2. Taking into account the factorization property Eq. (25), we obtain

$$\Omega(\Psi) = \Omega(p \cdot \Psi_m^+).$$

It remains to be shown that

$$\Omega(p \cdot \Psi_m^+) = p. \tag{26}$$

First of all, consider a mixed version of the GHZ state,

$$\rho = (1/2)|0^{\otimes m}\rangle\langle 0^{\otimes m}| + (1/2)|1^{\otimes m}\rangle\langle 1^{\otimes m}|. \tag{27}$$

It is clear that $\rho \in \Gamma(\Psi_m^+)$. Thus

$$\Omega(p \cdot \Psi_m^+) \geq S(\rho^{\otimes p}) = pS(\rho) = p. \tag{28}$$

To get an upper bound, take any $\rho \in \Gamma(\Psi)$. Divide M into three nonempty subsets by an arbitrary way: $M = M_1 \cup M_2 \cup M_3$. Let ρ_j and ρ_{jk} be the reduced states of the subset M_j and $M_j \cup M_k$ (with respect to ρ). The strong subadditivity inequality shows that

$$S(\rho) + S(\rho_1) \leq S(\rho_{12}) + S(\rho_{13}).$$

But the condition $\rho \in \Gamma(p \cdot \Psi_m^+)$ implies that all the states ρ_1, ρ_{12}, and ρ_{13} are the mixed versions of the GHZ state [Eq. (27)], that is $S(\rho_1) = S(\rho_{12}) = S(\rho_{13}) = p$. Thus we get $S(\rho) \leq p$. Combining it with the lower bound Eq. (28) we get Eq. (26). □

Corollary 2: *Theorem 3 gives the GHZ extraction yield from a stabilizer state for arbitrary local unitary operators*.

Proof: Let $p = \Delta(\Psi)$ and q be the number of GHZ states extractable from $|\Psi\rangle$ by local

unitaries. Obviously, $q \geq p$. Since the functional $\Omega(\Psi)$ is LU invariant, we infer from Eq. (26) that $\Omega(\Psi) \geq \Omega(q \cdot \Psi_m^+) = q$. It follows from Theorem 4 that $p \geq q$. Thus $p = q$. □

VI. TRIPARTITE STABILIZER STATES

As a simple application of Theorem 3 let us show that any tripartite stabilizer state is LCU equivalent to a collection of states from the set $E_3 = \{|0\rangle, |\Psi^+\rangle, |\Psi_3^+\rangle\}$. After extraction of all local $|0\rangle$ states one can consider only states with full local ranks.

Theorem 5: *Let $|\Psi\rangle \in \mathcal{B}^n$ be a stabilizer state with full local ranks shared by a set of parties $M = \{A, B, C\}$. Let S be a stabilizer group of $|\Psi\rangle$ and $S_{\mathrm{loc}} = \Sigma_{\alpha \in M} S_{\hat{\alpha}}$. Denote $p = \dim(S) - \dim(S_{\mathrm{loc}})$ and $d(\alpha) = \dim(S_{\hat{\alpha}})$. The state $|\Psi\rangle$ is LCU equivalent to a collection of*

(i) $(d(A) - p)/2$ *copies of* $|\Psi^+\rangle$ *shared by B and C*,
(ii) $(d(B) - p)/2$ *copies of* $|\Psi^+\rangle$ *shared by C and A*,
(iii) $(d(C) - p)/2$ *copies of* $|\Psi^+\rangle$ *shared by A and B*,
(iv) p *copies of the GHZ state* $|\Psi_3^+\rangle$.

Proof: As we already know from Theorem 3, one can extract p copies of $|\Psi_3^+\rangle$ from $|\Psi\rangle$. This allows us to consider only the case $p = 0$. Equivalently, we can assume that S is equal to the sum of its colocal subgroups, $S = S_{\mathrm{loc}}$. The full local ranks assumption means that the colocal subgroups do not overlap, i.e., $S_{\hat{\alpha}} \cap S_{\hat{\beta}} = 0$ for $\alpha \neq \beta$. Thus S can be represented as a direct sum,

$$S = S_{\hat{A}} \oplus S_{\hat{B}} \oplus S_{\hat{C}}. \tag{29}$$

Let us prove that $|\Psi\rangle$ is LCU equivalent to a collection of EPR states $|\Psi^+\rangle$. The proof consists of applying the same arguments to each pair of parties, so let us focus on the pair AB.

Denote $R \equiv S_{\hat{C}}$ and consider a bilinear form

$$\eta : R \otimes R \to \{0,1\}, \quad \eta(f,g) = \omega(f_A, g_A),$$

for any $f, g \in R$. We claim that η is a nonsingular form. Indeed, suppose that

$$\eta(f,g) = 0 \quad \text{for all } g \in R \tag{30}$$

and prove that $f = 0$. Indeed, Eq. (30) and decomposition Eq. (29) imply that $\omega(f_A, h_A) = 0$ for any $h \in S$. We can rewrite this as $\omega(\tilde{f}, h) = 0$ for any $h \in S$, where $\tilde{f} \in G_A^n$ is chosen such that $\tilde{f}_A = f_A$. It means that $\tilde{f} \in S^{\perp}$, that is $\tilde{f} \in S \cap G_A^n = S_A = 0$. Therefore, $f_A = 0$ and so $f \in S_B = 0$. We conclude that $f = 0$ and η is nonsingular.

Applying the Gram-Schmidt orthogonalization procedure, one can check that R must have an even dimension, $\dim(R) = 2l$, and that there exists a symplectic basis $\{g_j, \bar{g}_j\}_{j=1,\ldots,l}$ of R such that

$$\eta(g_j, g_k) = 0, \quad \eta(\bar{g}_j, \bar{g}_k) = 0, \quad \eta(g_j, \bar{g}_k) = \delta_{jk}. \tag{31}$$

(For a proof see Dickson's theorem in Ref. 19, Chap. 15.)

Denote by $S_{\mathrm{EPR}} \subset G^{2l}$ a stabilizer group of l copies of the EPR state, $|l \cdot \Psi^+\rangle$. We consider $|l \cdot \Psi^+\rangle$ as a tripartite state, such that C holds no qubits at all, and there are l EPR states shared by A and B. The group S_{EPR} has independent generators $\{f_j, \bar{f}_j\}_{j=1,\ldots,l}$ such that

$$\sigma(f_j) = \sigma_j^z \otimes \sigma_j^z, \quad \sigma(\bar{f}_j) = \sigma_j^x \otimes \sigma_j^x,$$

where j labels the copies of $|\Psi^+\rangle$, i.e., $j = 1, \ldots, l$. Define a linear map $T : S_{\mathrm{EPR}} \to S$ such that

$$T(f_j) = g_j, \quad T(\bar{f}_j) = \bar{g}_j, \quad j = 1, \ldots, l.$$

Obviously, $T(S_{\mathrm{EPR}}) = R$. We would like to check that T satisfies all the conditions of Theorem 2. Indeed, it is a linear injection because the images of the basis vectors of S_{EPR} are linearly independent. Condition (i) follows directly from Eq. (31). Condition (i) holds because S_{EPR} has trivial

colocal subgroup and so does R. Thus l copies of $|\Psi^+\rangle$ shared between A and B can be extracted from $|\Psi\rangle$.

Applying the same arguments to other pairs of parties, we conclude that AB, BC, and AC can extract $d(C)/2$, $d(A)/2$, and $d(B)/2$ EPR states, respectively. The total number of qubits in the extracted EPR states is $d(A)+d(B)+d(C)$ which coincides with $\dim(S)=n$, see Eq. (29). Thus no qubits are left after the extraction.

To conclude the proof it is sufficient to note that extraction of a single GHZ state $|\Psi_3^+\rangle$ reduces each of the dimensions $\dim(S_{\hat{\alpha}})$ by one. □

A simple corollary of Theorem 5 is that two tripartite stabilizer states $|\Psi\rangle, |\Psi'\rangle$ are LU-equivalent iff their decompositions into $|\Psi^+\rangle$, $|\Psi_3^+\rangle$, and local $|0\rangle$ states coincide. Indeed, make use of the fact that a partial trace of $|\Psi_3^+\rangle$ over any qubit is a separable state. LU equivalence of $|\Psi\rangle$ and $|\Psi'\rangle$ implies that all partial traces of $|\Psi\rangle$ and $|\Psi'\rangle$ are LU equivalent; that is, the number of singlets $|\Psi^+\rangle$ extractable by each pair of parties is the same for $|\Psi\rangle$ and $|\Psi'\rangle$. By counting the remaining dimensions we conclude that the numbers of GHZ's $|\Psi_3^+\rangle$ extractable from $|\Psi\rangle$ and $|\Psi'\rangle$ are the same. Thus LU-equivalence classes of tripartite stabilizer states are completely specified by the numbers of $|\Psi^+\rangle$ and $|\Psi_3^+\rangle$ in the decomposition of Theorem 5.

Remark: One could prove Theorem 5 by making use of mixed stabilizer states. A mixed stabilizer state is a maximally mixed state encoded by some stabilizer code. Bipartite mixed stabilizer states can be classified using the techniques of the paper.[12] It turns out that any bipartite mixed stabilizer state is LCU equivalent to a collection of (i) local pure states; (ii) local maximally mixed states; (iii) EPR states; (iv) two-qubit mixed states $(1/2)|0,0\rangle\langle 0,0|+(1/2)|1,1\rangle\langle 1,1|$. Combining this fact with the purification theorem one immediately gets Theorem 5. We refrain from pushing this approach further, because it is less symmetric than the one presented above.

VII. SATURATION OF MULTIPARTITE ENTANGLEMENT ENTROPY IN SPIN LATTICES

As was mentioned in the introduction, characterization of multipartite entangled states might be useful for quantum cryptography and quantum game theory. Another natural area to look for applications is condensed matter physics. It has been realized recently that ground states of d-dimensional spin lattices with spatially uniform short-range interactions are distinguished among all other states by obeying the *entropic area law* (see Ref. 16 and references therein). According to this law, entanglement entropy of a block of spins with a spatial size L (thus containing about L^d spins) scales as $E(L)=b\cdot L^{d-1}+o(L^{d-1})$, where b is a constant (critical systems are set aside). This law can be understood, at least very roughly, if one regards the ground state as a collection of short-range EPR states. Then $E(L)$ is equal to the number of EPR states that stretch between the interior and exterior of the block. It is obviously proportional to the area of the boundary. From this standpoint (which is of course only a rude approximation) $E(L)$ can be regarded as the maximal number of EPR states extractable from the ground state by local unitaries.

To get more insight into the structure of entanglement of the ground state, one can consider a partition of the lattice into several blocks of spins (which may or may not have junction points), and ask how many multipartite GHZ states can be extracted from the ground state by local unitaries. In this section we shall try to follow this program.

Let us first set the problem more strictly. We shall focus on the two-dimensional case (a generalization to an arbitrary d is trivial). Suppose that the system under consideration consists of n qubits that are assigned to sites of a 2D regular lattice. Let $|\Psi_0\rangle \in \mathcal{B}^n$ be the ground state of the system. Consider a partition of the lattice into three segments A, B, and C which have a common junction point O, while pairwise intersections are one-dimensional rays incident to O (see Fig. 1). The problem is to compute the quantity

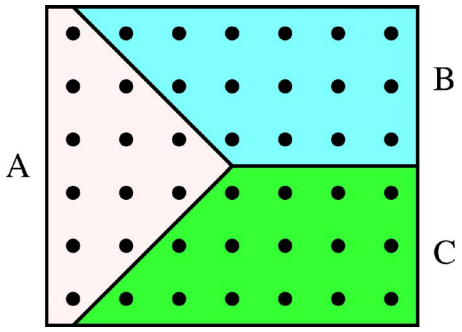

FIG. 1. (Color online) A junction point.

$$E_3(n) = \Omega(\Psi_0),$$

defined by Eq. (23). As was argued in Sec. V, the quantity $\Omega(\Psi_0)$ is a natural generalization of the GHZ extraction yield beyond stabilizer states. We are particularly interested in the asymptotic behavior of $E_3(n)$ when n goes to infinity (the thermodynamic limit).

It is natural to expect that $E_3(n)$ does not diverge as $n \to \infty$, since tripartite correlations must be formed by interactions acting on spins near the junction point O. As long as the Hamiltonian of the system is short ranged, there is only a finite number of such interactions. In other words, a natural conjecture is that

$$\sup_n E_3(n) < \infty . \tag{32}$$

This inequality says that $E_3(n)$ can be bounded from above by a constant that does not depend on the size of the system (this constant may depend upon the details of the system's Hamiltonian, however). The conjecture Eq. (32), if it is true, would generalize the entanglement saturation phenomenon found for one-dimensional spin chains[16] to higher dimensions.

In the rest of this section we prove Eq. (32) for a special case when (i) $|\Psi_0\rangle$ is a stabilizer state; (ii) the stabilizer group of $|\Psi_0\rangle$ has a set of geometrically local generators. Well-known examples of such states are the 2D cluster state[6] or the planar analogue of Kitaev's toric code state.[15]

Let $|\Psi_0\rangle \in \mathcal{B}^n$ be a stabilizer state and $S \subset G^n$ be its stabilizer group. Let us say that S has an *interaction length* l, iff there exists a family of vectors $f_1, \ldots, f_p \in S$, such that (i) S is generated by $f_1, \ldots, f_p$; (ii) for any j, the support of the vector f_j can be covered by a $l \times l$ rectangular block. We do not assume that the f_j are linearly independent, so in general $p > n$. However we assume that any vector $u \in G^n$ appears in the list $f_1, \ldots, f_p$ with multiplicity at most one (which, of course, is not a restriction at all). For example, one can easily check that the 2D cluster state and Kitaev's state have interaction length $l=3$ and $l=2$, respectively.

Consider a subgroup $S' \subseteq S$ generated by vectors f_j that have support on all three parties A, B, and C. Obviously, f_j is supported on all three parties only if the $l \times l$ block representing the support of f_j covers the junction point O. Since there are only l^2 different blocks that cover O and each block can represent at most l^2 independent vectors f_j, we conclude that

$$\dim(S') \leq l^4.$$

Consider now a subgroup $S_{\mathrm{loc}} \subseteq S$ generated by colocal subgroups of S [see Eq. (12)]. Since each f_j belongs to at least one of the subgroups S', S_{loc}, we infer that

$$S = S_{\mathrm{loc}} + S' \quad \text{and } \dim(S_{\mathrm{loc}}) \geq \dim(S) - \dim(S').$$

Taking into account Theorem 4, one gets

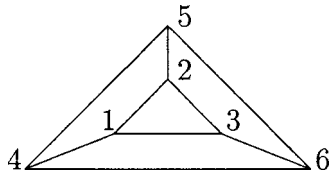

FIG. 2. Graph $\mathcal{G}$ used in the definition of $|\mathcal{G}\rangle$.

$$\Omega(\Psi_0) = \dim(S) - \dim(S_{\text{loc}}) \leq \dim(S') \leq l^4$$

which gives us an upper bound on the number of GHZ states $|\Psi_3^+\rangle$ that can be extracted from $|\Psi_0\rangle$. This bound does not depend upon n—only upon the interaction length l. Therefore Eq. (32) is proved.

Remark: Since the state $|\Psi_0\rangle$ is uniquely specified by stabilizer equations $\sigma(f)|\Psi_0\rangle = \epsilon(f)|\Psi_0\rangle$, $f \in S$ [see Eq. (4)], it can be regarded as the nondegenerate ground state of a Hamiltonian

$$H = -\sum_{j=1}^{p} \epsilon(f_j)\sigma(f_j).$$

This Hamiltonian is a sum of local interactions each of which affects the qubits inside some $l \times l$ block.

VIII. FOUR-PARTY STABILIZER STATES

As we learned from Sec. VI, there exists essentially one irreducible tripartite stabilizer state—the GHZ state $|\Psi_3^+\rangle$. What about four-party states? As the simplest example, consider a system of four qubits distributed between four parties. As was pointed out in Ref. 20, there exist only two irreducible four-qubit stabilizer states: the GHZ state $|\Psi_4^+\rangle$ and a state

$$|C_4\rangle = (1/2)(|0000\rangle + |0011\rangle + |1100\rangle - |1111\rangle),$$

such that $|C_4\rangle = \Lambda(\sigma^z)[2,3]|\Psi^+ \otimes \Psi^+\rangle$ (one can check that $|C_4\rangle$ is LCU equivalent to the cluster state of a four-qubit linear chain).

Is it true that a set $E_4 = \{|0\rangle, |\Psi^+\rangle, |\Psi_3^+\rangle, |\Psi_4^+\rangle, |C_4\rangle\}$ is an entanglement generating set for four-party stabilizer states? In this section we give an example of a state that is not LCU equivalent to any collection of states from E_4, thus answering this question in the negative.

Consider a graph $\mathcal{G} = (V,E)$ with six vertices shown in Fig. 2. For each vertex $u \in V$ define a stabilizer $f_u \in G^6$ such that

$$\sigma(f_u) = \sigma_u^x \bigotimes_{(u,v)\in E} \sigma_v^z. \tag{33}$$

The vectors $\{f_u\}_{u\in V}$ generate a self-dual subspace $S \subset G^6$. Let $|\mathcal{G}\rangle \in \mathcal{B}^6$ be the corresponding stabilizer state [it is known as a *graph state* associated with the graph $\mathcal{G}$; one can also define $|G\rangle$ using a classical GF(4)-linear code known as *hexacode*, see Ref. 21]. This state has the following curious property.

Proposition: A partial trace of $|\mathcal{G}\rangle$ over any triple of qubits is maximally mixed:

$$\text{Tr}_{uvw}\big(|\mathcal{G}\rangle\langle\mathcal{G}|\big) = \tfrac{1}{8}I, \quad \text{for any } u \neq v \neq w. \tag{34}$$

For a proof see Ref. 22.

Suppose now that $|\mathcal{G}\rangle$ is shared by a set of parties $M = \{A,B,C,D\}$ such that

$$A = \{1,4\}, \quad B = \{3,6\}, \quad C = \{2\}, \quad D = \{5\}.$$

Lemma 3: *If* $|\mathcal{G}\rangle$ *is shared by the set of parties* $M=\{A,B,C,D\}$ *as above*, *it is irreducible*, *i.e.*, *no stabilizer state can be extracted from* $|\mathcal{G}\rangle$.

(Here we talk about extraction in the sense of Definition 4 and ignore the trivial possibility of extracting $|\mathcal{G}\rangle$ from itself.)

Proof: We shall first show that neither of the states $|\Psi^+\rangle$, $|\Psi_3^+\rangle$ can be extracted from $|\mathcal{G}\rangle$.

(a) $|\Psi_3^+\rangle$ *extraction*: Suppose one can extract one copy of $|\Psi_3^+\rangle$ which is shared by a subset of parties $M' \subset M$, $|M'|=3$. Obviously, M' contains at least one of A, B, and at least one of C, D. By the symmetry, assume that $A \in M'$ and $D \in M'$. Then the reduced state of the qubits $1,4,5$ has a rank at most 4, contradicting Eq. (34).

(b) $|\Psi^+\rangle$ *extraction*: Obviously, $|\Psi^+\rangle$ cannot be shared by C and D (the reduced state of any pair of qubits is maximally mixed). Thus there are only two possibilities: (i) $|\Psi^+\rangle$ is shared by one of $\{A,B\}$ and one of $\{C,D\}$. Then one of the triple of qubits AC, AD, BC, BD has a rank at most 2, contradicting Eq. (34). (ii) $|\Psi^+\rangle$ is shared by A and B. Then there must be two vectors $f,\bar{f} \in S$ such that

$$f_C = f_D = \bar{f}_C = \bar{f}_D = 0, \tag{35}$$

$$\omega(f_A,\bar{f}_A) = \omega(f_B,\bar{f}_B) = 1. \tag{36}$$

Taking into account the explicit form of the stabilizer generators Eq. (33), one can check that the only nontrivial stabilizer elements having a support on A and B are the following:

$$\sigma_1^y \otimes \sigma_4^z \otimes \sigma_3^y \otimes \sigma_6^z, \quad \sigma_1^z \otimes \sigma_4^y \otimes \sigma_3^z \otimes \sigma_6^y, \quad \sigma_1^x \otimes \sigma_4^x \otimes \sigma_3^x \otimes \sigma_6^x.$$

(All identity factors are suppressed.) Any pair of them commute locally on A and B. Thus the equations Eqs. (35) and (36) have no solutions and we get a contradiction.

Extraction of a four-party state from $|\mathcal{G}\rangle$ is impossible, since it leaves a bipartite (or a local pure state) which would also be extractable from $|\mathcal{G}\rangle$. As we already know, this would lead to a contradiction. □

This observation means that we must add the state $|\mathcal{G}\rangle$ to the entanglement generating set E_4. It raises a question: Is there a *finite* EGS for four-party stabilizer states? (Note that we allow an arbitrary number of qubits per party, so the total number of stabilizer states is infinite.) To the authors' best knowledge, the answer is unknown.

A closely related problem is to find LCU-equivalence classes of *bipartite* unitary operators from the Clifford group (it suffices to take two copies of a maximally entangled state and apply a unitary operator to one-half of each state, see Ref. 23 for more details).

Another open question is the relation between LU equivalence and LCU equivalence of stabilizer states. To the authors' best knowledge, there are no known examples of LU-equivalent stabilizer states which are not LCU equivalent. On the other hand, it was shown by Van den Nest, Dehaene, and De Moor in Ref. 11, extending the work of Rains,[24] that for a large class of stabilizer states, including the states specified by GF(4) linear codes, LCU equivalence coincides with LU equivalence (this statement applies only to one-qubit-per-party partitions).

ACKNOWLEDGMENTS

The authors acknowledge Ike Chuang for fruitful discussion. One of the authors (S.B.) received support from the National Science Foundation under Grant No. EIA-0086038. One of the authors (D.G.) is supported by CIAR and by NSERC of Canada.

APPENDIX A

In this section we give a shorter (but less constructive) proof of the GHZ extraction formula, see Theorem 3.

Denote p the maximal number of states $|\Psi_m^+\rangle$ extractable from $|\Psi\rangle$. Clearly, $p>0$ implies $S \neq S_{\mathrm{loc}}$, and thus $\Delta(\Psi)>0$. Since $\Delta(\Psi)$ is additive under a tensor product of states, and $\Delta(\Psi_m^+)=1$ (for $m\geq 3$), it suffices to prove that $\Delta(\Psi)>0$ implies $p>0$.

(1) Consider a linear map $\Pi_\alpha: S\to G^{n_\alpha}$ that sends $f\in S$ to f_α (a projection onto party α). By definition of a colocal subspace, $\mathrm{Ker}(\Pi_\alpha)=S_{\hat{\alpha}}$. The fact that $|\Psi\rangle$ has full local ranks (see the remark after the statement of Theorem 3) implies that $\mathrm{Im}(\Pi_\alpha)=G^{n_\alpha}$. Therefore $\dim(S)=n_\alpha+\dim(S_{\hat{\alpha}})$ for any $\alpha\in M$. Thus any linear function $\lambda: S\to\{0,1\}$ such that $\lambda(S_{\hat{\alpha}})=0$ can be uniquely represented as $\lambda(f)=\omega(x_\alpha,f)$for some $x_\alpha\in G_\alpha^n$.

(2) Choose a nonzero linear function $\lambda: S\to\{0,1\}$ such that $\lambda(S_{\mathrm{loc}})=0$. As shown above, for any $\alpha\in M$ we can choose $x_\alpha\in G_\alpha^n$ such that $\lambda(f)=\omega(x_\alpha,f)$ for all $f\in S$. Then $\omega(x_\alpha+x_\beta,f)=0$ for all $f\in S$ and thus $x_\alpha+x_\beta\in S$ (recall that S is self-dual).

(3) Choose $\bar{g}\in S$ such that $\lambda(\bar{g})=1$. Define a linear subspace $V\subseteq S$, such that V is spanned by vectors $g_{\alpha,\beta}=x_\alpha+x_\beta$, $\alpha,\beta\in M$, and $\bar{g}$. From $\lambda(\bar{g})=1$ we infer that $\bar{g}\notin S_{\mathrm{loc}}$, and thus that $\bar{g}_\alpha\neq 0$ for all $\alpha\in M$. Besides, the fact that $\omega(x_\alpha,g)=\lambda(g)=1$ implies that x_α and g_α are linearly independent. Thus a colocal subspace $V_{\mathrm{loc}}\subset V$ is spanned by vectors $g_{\alpha,\beta}$.

(4) Let $S_{\mathrm{ghz}}\subset G^m$ be a stabilizer group of $|\Psi_m^+\rangle$ with canonical generators $f_{\alpha,\beta}$ and $\bar{f}$, see Eqs. (10) and (11). Define a linear map $T: S_{\mathrm{ghz}}\to S$ according to $T(f_{\alpha,\beta})=g_{\alpha,\beta}$ and $T(\bar{f})=\bar{g}$. Let us verify that T obeys conditions of Theorem 2. Indeed, T is the injective map since x_α and g_α are linearly independent. The property (i) follows from equality $\omega(x_\alpha,g_\alpha)=\lambda(g)=1$. The property (ii) follows from equality $T((S_{\mathrm{ghz}})_{\mathrm{loc}})=V_{\mathrm{loc}}$. Thus$|\Psi_m^+\rangle$ is extractable from $|\Psi\rangle$, i.e., $p>0$.

APPENDIX B

The goal of this section is to prove Lemma 1. We start by stating one more lemma.

Lemma 4: *Let $f_1,\ldots,f_p$ and $f_1',\ldots,f_p'$ be two families of vectors in G^n satisfying the following conditions*:

$$\omega(f_j,f_k)=\omega(f_j',f_k') \quad \textit{for all } 1\leq j,k\leq p, \tag{B1}$$

$$\sum_{j=1}^{p} x_j f_j=0 \quad \textit{iff} \sum_{j=1}^{p} x_j f_j'=0. \tag{B2}$$

Here $x_1,\ldots,x_p\in\{0,1\}$ are arbitrary binary coefficients. Then there exists a symplectic operator $u\in \mathrm{Sp}_2(n)$ such that

$$f_j'=u(f_j) \quad \textit{for all } j=1,\ldots,p.$$

Proof: Let us call a basis $e_1,\bar{e}_1,\ldots,e_n,\bar{e}_n$ of the space G^n canonical iff the following relations hold:

$$\omega(e_j,e_k)=0, \quad \omega(\bar{e}_j,\bar{e}_k)=0, \quad \omega(e_j,\bar{e}_k)=\delta_{jk}. \tag{B3}$$

One can extend the family $f_1,\ldots,f_p$ to a canonical basis $\{e_j,\bar{e}_j\}$ using the Gram-Schmidt orthogonalization algorithm. After that one can write

$$f_j = \sum_{k=1}^{n} F_{jk} e_k + \bar{F}_{jk} \bar{e}_k, \quad j = 1, \ldots, p,$$

where F and $\bar{F}$ are some binary $p \times n$ matrices. It is a property of the Gram-Schmidt algorithm that the coefficients F_{jk} and $\bar{F}_{jk}$ depend only upon the inner products Eq. (B1) and upon the set of linear dependencies Eq. (B2). Thus if we apply the same algorithm in parallel to the family $f'_1, \ldots, f'_p$, we shall end up with a canonical basis $\{e'_1, \bar{e}'_1, \ldots, e'_n, \bar{e}'_n\}$ such that

$$f'_j = \sum_{k=1}^{n} F_{jk} e'_k + \bar{F}_{jk} \bar{e}'_k, \quad j = 1, \ldots, p.$$

The symplectic group $\mathrm{Sp}_2(n)$ acts transitively on the set of canonical bases. Thus

$$e'_j = u(e_j), \quad \bar{e}'_j = u(\bar{e}_j), \quad j = 1, \ldots, n,$$

for some $u \in \mathrm{Sp}_2(n)$. This implies that $f'_j = u(f_j)$ for all $j = 1, \ldots, p$. □

Now we are ready to prove Lemma 1. The nontrivial part is to prove that statement 1 follows from statement 2. Choose an arbitrary basis $f_1, \ldots, f_p$ of the subspace S. Denote $f'_j = T(f_j) \in S'$. The condition that T is an invertible map implies that $f'_1, \ldots, f'_p$ is a basis of S'. For each $\alpha \in M$, consider projections $f_{\alpha j} = (f_j)_\alpha$ and $f'_{\alpha j} = (f'_j)_\alpha$. The condition (2-i) is equivalent to

$$\omega(f_{\alpha j}, f_{\alpha k}) = \omega(f'_{\alpha j}, f'_{\alpha k}) \quad \text{for all } \alpha \in M \tag{B4}$$

and any j, k in the range $1, \ldots, p$.

In addition, we have the following chain of implications: $\Sigma_{j=1}^{p} x_j f_{\alpha j} = 0$ iff $\Sigma_{j=1}^{p} x_j f_j \in S_{\hat{\alpha}}$ iff $T(\Sigma_{j=1}^{p} x_j f_j) \in S'_{\hat{\alpha}}$ iff $\Sigma_{j=1}^{p} x_j f'_{\alpha j} = 0$. The second implication is the condition (2-ii) of the lemma, while all others follow from the definition of the colocal subspace. Summarizing, we have

$$\sum_{j=1}^{p} x_j f_{\alpha j} = 0 \quad \text{iff} \sum_{j=1}^{p} x_j f'_{\alpha j} = 0. \tag{B5}$$

Now, for each $\alpha \in M$, let us apply Lemma 4 to the families of vectors $f_{\alpha 1}, \ldots, f_{\alpha p} \in G^{n_\alpha}$ and $f'_{\alpha 1}, \ldots, f'_{\alpha p} \in G^{n_\alpha}$. The conditions of Lemma 4 are equivalent to Eqs. (B4) and (B5). Thus there exist operators $u_\alpha \in \mathrm{Sp}_2(n_\alpha)$ such that

$$f'_{\alpha j} = u_\alpha(f_{\alpha j}), \quad \alpha \in M, \quad j = 1, \ldots, p.$$

This means that

$$f'_j = (\bigoplus_{\alpha \in M} u_\alpha)(f_j), \quad j = 1, \ldots, p.$$

This is equivalent to statement 1 of Lemma 1.

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Proceedings of IEEE International Conference on Computers Systems and Signal Processing*, Bangalore India, 1984, pp. 175–179.
[2] C. Mochon, "Quantum weak coin-flipping with bias of 0.192," 45th Symposium on foundations of computer science (FOCS '04), IEEE Computer Society, 2004, pp. 2–11.
[3] S. C. Benjamin and P. M. Hayden, quant-ph/0007038v2.
[4] A. Botero and B. Reznik, Phys. Lett. A **331**, 39 (2004).
[5] A. Serafini, G. Adesso, and F. Illuminati, quant-ph/0411109.
[6] R. Raussendorf, D. E. Browne, and H. J. Briegel, Phys. Rev. A **68**, 022312 (2003).
[7] A. Steane, Phys. Rev. Lett. **78**, 2252 (1997).
[8] A. Kitaev, Ann. Phys. (N.Y.) **303**, 2 (2003).
[9] M. Van den Nest, J. Dehaene, and B. De Moor, Phys. Rev. A **69**, 022316 (2004).
[10] M. Van den Nest, J. Dehaene, and B. De Moor, Phys. Rev. A **71**, 022310 (2005).
[11] M. Van den Nest, J. Dehaene, and B. De Moor, quant-ph/0411115.
[12] D. Fattal, T. Cubitt, Y. Yamamoto, S. Bravyi, and I. Chuang, quant-ph/0406168.
[13] A. Acin, G. Vidal, and J. I. Cirac, Quantum Inf. Comput. **3**, 55 (2003).
[14] N. Linden, S. Popescu, and W. K. Wootters, Phys. Rev. Lett. **89**, 207901 (2002).
[15] S. Bravyi and A. Kitaev, quant-ph/9811052.
[16] J. I. Latorre, E. Rico, and G. Vidal, Quantum Inf. Comput. **4**, 048 (2004).

[17] A. Kitaev, A. Shen, and M. Vyalyi, *Classical and Quantum Computation*, Graduate Studies in Mathematics, Vol. 47 (American Mathematical Society, Providence, RI, 2002).
[18] E. Schneidman, S. Still, M. Berry II, and W. Bialek, Phys. Rev. Lett. **91**, 238701 (2003).
[19] F. J. MacWilliams and N. J. Sloane, *The Theory of Error-Correcting Codes* (North-Holand, Amsterdam, 1977).
[20] M. Hein, J. Eisert, and H. J. Briegel, Phys. Rev. A **69**, 062311 (2004).
[21] A. Calderbank, E. Rains, P. Shor, and N. Sloane, IEEE Trans. Inf. Theory **44**, 1369 (1998).
[22] S. Bravyi, Phys. Rev. A **67**, 012313 (2003).
[23] W. Dür and J. I. Cirac, quant-ph/0201112.
[24] E. Rains, IEEE Trans. Inf. Theory **45**, 266 (1999).