Tripartite Entanglement in Qudit Stabilizer States and Application in Quantum Error Correction

Shiang Yong Looi and Robert B. Griffiths

Department of Physics, Carnegie Mellon University, Pittsburgh, Pennsylvania 15213, USA

(Dated: Version of 8th of July 2011)

Consider a stabilizer state on \(n\) qudits, each of dimension \(D\) with \(D\) being a prime or a squarefree integer, divided into three mutually disjoint sets or parts. Generalizing a result of Bravyi et al. \[J. Math. Phys. 47, 062106 (2006)\] for qubits \((D = 2)\), we show that up to local unitaries on the three parts the state can be written as a tensor product of unentangled single-qudit states, maximally entangled EPR pairs, and tripartite GHZ states. We employ this result to obtain a complete characterization of the properties of a class of channels associated with stabilizer error-correcting codes, along with their complementary channels.

PACS numbers: 03.67.Mn, 03.67.Hk

Contents

I. Introduction

II. Preliminary Concepts and Definitions
   A. Qudit Pauli Operators
   B. Single-Qudit and Two-Qudit Clifford Operators
   C. Stabilizer Codes and States. Partitions
   D. Decomposition of Stabilizer States of Composite Dimensions
   E. Graph States

III. Bipartition of qudit stabilizer states

IV. Tripartition of qudit stabilizer states

V. Application in Quantum Error Correction
   A. Isomorphism Between Stabilizer Codes and Stabilizer States
   B. Stabilizer Code Channels and Subset Information Groups
   C. Tensor Product Structure of Stabilizer Code Channels
   D. Duality of Subset Information Groups, \(G_B\) and \(G_C\)

VI. Conclusion

Acknowledgments

A. Proof of Theorem

References

I. INTRODUCTION

The study of entangled quantum states of systems consisting of two or more parts is a central problem in quantum information theory. The Schmidt decomposition provides a fairly complete characterization of the pure states of a bipartite system. However, mixed states on bipartite systems and pure states on systems of three or more parts present a much more difficult problem—see [1] for a comprehensive review—and a relatively complete understanding of the situation exists only for some very special cases.

The present paper considers the special case of (pure) stabilizer states on \(n\) qudits, each of dimension \(D\), and addresses the problem of characterizing the corresponding tripartite state when the \(n\) qudits are partitioned into three disjoint sets \(A\), \(B\), and \(C\), and arbitrary unitary transformations are allowed on each of the three parts. The case of qubits, \(D = 2\), was studied by Bravyi et al. \[2\], who showed that such a stabilizer state is equivalent, up to local unitaries on the three parts, to a tensor product of pure unentangled single-qubit states; maximally entangled two-qubit states or EPR pairs, with one qubit in one part and the other qubit in a different part; and GHZ states on three qubits, one lying in each part. In this paper we generalize these results to the case \(D > 2\), where \(D\) is either a prime or a squarefree integer (i.e., not divisible by the square of any integer greater than 1).

The stabilizer formalism \[3–5\] was first introduced to simplify the construction and analysis of quantum error correction codes. Soon thereafter it was generalized from qubits to higher dimensional qudits \[6, 7\]. Most of the codes known when the formalism was introduced, and the majority of those discovered since, are stabilizer codes. The formalism has also been used for measurement-based quantum computation \[8\] and fault-tolerant topological quantum computation \[9\]. There has been a lot of research on single-qubit local unitary (LU) and single-qubit local Clifford (LC) equivalence of qubit stabilizer states/graph states \[10, 11\], but here we consider partitionings where each part can have several qudits and ar-

*Electronic address: slooi@andrew.cmu.edu
†Electronic address: rgrif@andrew.cmu.edu
bititary gates acting on qudits belonging to the same part are permitted.

In [13] we studied a class of channels obtained from qudit stabilizer (equivalently, additive graph) codes where a subset of the carrier qudits is lost. We fully characterized their information carrying capacities in terms of subset information groups, a concept related to the notion of correctable algebras introduced in [14]. We also provided an efficient algorithm to find the subset information group. In this paper we adopt the name stabilizer code channels for such channels.

The paper is organized as follows: Section II introduces various concepts that will be used later: Pauli and Clifford operators, one- and two-qudit gates, stabilizer and graph states. It also contains some mathematical results, one of which, Corollary 5 is of some interest by itself: it allows the decomposition of stabilizer states into a tensor product of such states when $D = d_1 d_2 \cdots$ is a product of mutually coprime factors. In the following Section III we prove that any bipartite stabilizer state in a product of mutually coprime factors. In the following Section VI we prove that any bipartite stabilizer state in a product of mutually coprime factors. In the following Section VI we prove that any bipartite stabilizer state in a product of mutually coprime factors. In the following Section VI we prove that any bipartite stabilizer state in a product of mutually coprime factors. In the following Section VI we prove that any bipartite stabilizer state in a product of mutually coprime factors. In the following Section VI we prove that any bipartite stabilizer state in a product of mutually coprime factors. In the following Section VI we prove that any bipartite stabilizer state in a product of mutually coprime factors. In the following Section VI we prove that any bipartite stabilizer state in a product of mutually coprime factors. In

Section II. PRELIMINARY CONCEPTS AND DEFINITIONS

A. Qudit Pauli Operators

Most of the following preliminary concepts have been introduced in [13], [15] and we present them here again for completeness. We generalize the notion of Pauli operators to higher dimensional Hilbert spaces where $D \geq 2$. The $X$ and $Z$ Pauli operators are defined in the computational basis as

$$Z = \sum_{j=0}^{D-1} \omega^j |j\rangle\langle j|, \quad X = \sum_{j=0}^{D-1} |j\rangle\langle j+1|,$$  \hspace{1cm} (1)

and they satisfy

$$X^D = Z^D = I, \quad XZ = \omega ZX, \quad \omega = e^{2\pi i/D},$$  \hspace{1cm} (2)

where the addition of integers in Eq. (1) is modulo $D$. For a collection of $n$ qudits we use subscripts to identify the corresponding Pauli operators unless otherwise stated: thus $Z_i$ and $X_i$ operate on the space of qudit $i$. The Hilbert spaces of individual qudits are denoted by $\mathcal{H}_{i}$, and that of $n$ qudits by $\mathcal{H}^{\otimes n} := \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_n$.

Operators of the form

$$\lambda^\gamma X^{\omega_1}_{1} Z^{\omega_2}_{1} \otimes X^{\omega_2}_{2} Z^{\omega_3}_{2} \otimes \cdots \otimes X^{\omega_n}_{n} Z^{\omega_n}_{n},$$  \hspace{1cm} (3)

will be referred to as Pauli products, where $\lambda := e^{2\pi i/(2D)}$ (so $\lambda^2 = \omega$) and $\gamma$ is an integer in $\mathbb{Z}_{2D}$, the ring of integers modulo $2D$. For a fixed $n$, the collection of all possible Pauli products in Eq. (3) forms a group under operator multiplication, the Pauli group $\mathcal{P}_n$.

For every $p \in \mathcal{P}_n$, $p^D$ is either $I$ or $-I$. The order of a Pauli product $p \in \mathcal{P}_n$ is defined as the smallest integer $1 \leq \alpha \leq D$ such that $p^\alpha \propto I$. Our definition of order is nonstandard in that we only require the power of the Pauli products to be proportional to the identity. Note that the order of any Pauli product must divide $D$.

While $\mathcal{P}_n$ is not abelian, it has the property that any two elements commute up to a phase: $p_1 p_2 = \omega^{\alpha_1 \gamma_2} p_2 p_1$, with $\alpha_1, \gamma_2$ an integer in $\mathbb{Z}_D$ that depends on $p_1$ and $p_2$. One can find subgroups of $\mathcal{P}_n$ that are abelian, for example the set of Pauli products with only powers of $Z$ on every qudit.

Proposition 1. Let $\mathcal{A}$ be set of mutually commuting Pauli products in $\mathcal{P}_n$ (for example, abelian subgroups of $\mathcal{P}_n$). Then $\mathcal{A}$ can have at most $D^n$ linearly independent elements.

Proof. The elements of $\mathcal{A}$ can be viewed as $D^n$-by-$D^n$ matrices. Then it is impossible to simultaneously diagonalize $D^n + 1$ or more mutually commuting and linearly independent $D^n$-by-$D^n$ matrices.

The collection of $D^{2n}$ Pauli products in Eq. (3) with $\gamma = 0$, i.e. a pre-factor of 1, forms an orthonormal basis of $L(\mathcal{H}^{\otimes n})$, the space of linear operators on $\mathcal{H}^{\otimes n}$, with respect to the Hilbert-Schmidt inner product

$$\frac{1}{D^n} \text{Tr}(q_1^\dagger q_2) = \delta_{q_1, q_2}, \quad \forall q_1, q_2 \in \mathcal{P}_n \text{ with pre-factor of 1}.$$  \hspace{1cm} (4)

B. Single-Qudit and Two-Qudit Clifford Operators

Having defined Pauli operators, we now generalize other single-qubit and two-qubit operators to $D \geq 2$.

The collection of $D^{2n}$ Pauli products in Eq. (3) with $\gamma = 0$, i.e. a pre-factor of 1, forms an orthonormal basis of $L(\mathcal{H}^{\otimes n})$, the space of linear operators on $\mathcal{H}^{\otimes n}$, with respect to the Hilbert-Schmidt inner product

$$\frac{1}{D^n} \text{Tr}(q_1^\dagger q_2) = \delta_{q_1, q_2}, \quad \forall q_1, q_2 \in \mathcal{P}_n \text{ with pre-factor of 1}.$$  \hspace{1cm} (4)
The qudit generalization of the Hadamard gate is the Fourier gate

\[ F := \frac{1}{\sqrt{D}} \sum_{j=0}^{D-1} \omega^{jk} |j\rangle \langle j|, \quad \text{for } D \geq 2 \]

where \( \lambda = e^{2\pi i/(2D)} \). The phase gate was first studied by Nielsen et al. in [16] for the general case.

The three single-qudit operators defined above as well as the Pauli operators defined in Eq. (4) are examples of Clifford unitaries, by which we mean unitaries that map Pauli products to Pauli products under conjugation. For instance, \( FZF^\dagger = X \) and \( XXF^\dagger = Z^{-1} \). The results of conjugating the Pauli operators by \( F \), \( S(\alpha) \) and \( W \) are summarized in Table 1.

| Pauli operator | \( F \) | \( S(\alpha) \) | \( W \) |
|---------------|-------|---------|-------|
| \( Z \)       | \( X \) | \( Z^\ast \) | \( Z \) |
| \( X \)       | \( Z^{-1} \) | \( X^\ast \) | \( \lambda XZ \) (even \( D \)) \( XZ \) (odd \( D \)) |

The requirement that \( \alpha \) be invertible ensures that \( S(\alpha) \) is unitary. (For \( D = 2 \), the only invertible integer is \( \alpha = 1 \), hence \( S(\alpha) \) is just the identity.)

Next we define the phase gate as

\[ W := \left\{ \begin{array}{ll}
\sum_{j=0}^{D-1} \lambda^{-j} \langle j | j \rangle & \text{if } D \text{ is even} \\
\sum_{j=0}^{D-1} \lambda^{-j} \langle j | j \rangle & \text{if } D \text{ is odd}
\end{array} \right. \]

where \( \lambda = e^{2\pi i/(2D)} \). (7)

The generalizations to \( D \geq 2 \) of CP and CNOT gates are the Clifford unitaries

\[ \text{CP}_{12} = \sum_{j=0}^{D-1} | j \rangle \langle j |_1 \otimes Z^2 = \sum_{j,k=0}^{D-1} \omega^{jk} | j \rangle \langle j |_1 \otimes | k \rangle \langle k |_2 \]

and

\[ \text{CNOT}_{12} := \sum_{j=0}^{D-1} | j \rangle \langle j |_1 \otimes X^2 = \sum_{j,k=0}^{D-1} | j \rangle \langle j |_1 \otimes | k \rangle \langle k | + j \rangle \langle j |_2, \]

where qudit 1 is the control while qudit 2 is the target. The CP and CNOT gates are related by a local Fourier gate defined in Eq. (5), similar to the \( D = 2 \) case,

\[ \text{CNOT}_{12} = (I_1 \otimes F_2) \text{CP}_{12}(I_1 \otimes F_2)^\dagger. \]

Proposition 2. For \( D \) prime, let \( p \in \mathbb{P}_n \) be a Pauli product on \( n \) qudits \([\text{Eq. (3)}]\) and assume that \( p \) is not the identity on qudit 1, i.e. \( x_1 \neq 0 \) or \( z_1 \neq 0 \) or both. Then there exists a Clifford unitary \( U \) such that \( UpU^\dagger X_1 I_2 \cdots I_n \). Further if \( p^D = I \), then it is possible to have \( UpU^\dagger = X_1 I_2 \cdots I_n \).

Proof. If \( x_1 = 0 \), then conjugate \( p \) by the Fourier gate, \( F \) so that \( x_1 \neq 0 \). Then transform \( X_1^{x_1} Z_{1}^{z_1} \) to \( X_{1}^{x_1} \) by conjugating it with the \( W \) gate a sufficient number of times. Next use the \( S(\alpha) \) gate to produce \( X_1 \). See Table 1 for the result of these conjugations. (Note that we relied on the fact that \( Z_{D} \) is a field when \( D \) is prime in the last two operations. The more general result for arbitrary \( D \) is studied in [16].) If \( p \) is now the identity on all the other qudits \( i = 2, 3, \ldots, n \) we are done. Otherwise, for each non-identity qudit, set the Pauli operator to \( X \) employing the procedure above. If at this point \( p \) is not identity on qudit 2, i.e. \( p = X_1 X_2 \cdots \), then \( X_2 \) can be changed to \( I_2 \) by performing \( \text{CNOT}_{12} \). This is repeated where needed so that the Pauli product is the identity on every qudit except qudit 1, which proves \( UpU^\dagger \) is proportional to \( X_1 \). If now \( p^D = I \), any remaining phase is necessarily some power of \( \alpha \), and can be removed by conjugation with powers of \( Z_1 \).

C. Stabilizer Codes and States. Partitions

Let \( S \subset \mathbb{P}_n \) be an abelian subgroup consisting of linearly independent Pauli products. Then \( |S| \) must divide \( D^n \) and \( s^D = I \) for all \( s \in S \). (For prime \( D \), every element except the identity is necessarily of order \( D \) so \( |S| \) is always a power of \( D \).) Given \( S \), define the set of states, \( C := \{ |\psi\rangle \in \mathcal{H}^{\otimes n} : s|\psi\rangle = |\psi\rangle, \forall s \in S \} \). It is easy to check that \( C \) forms a linear space, which we call the stabilizer code, with \( S \) its stabilizer group \([32]\).

In [13] it was shown that \( C \) and \( S \) are dual in the sense that one completely specifies the other and they satisfy the relation \( |S| \times \dim(C) = D^n \); \( \dim(C) \) is the dimension of \( C \). In quantum error correction literature, if \( \dim(C) = D^k \) for some integer \( 0 \leq k \leq n \), then it is customary to write \( C = \{|n,k\rangle \} \) because one can think of encoding \( k \) qudits in the \( D^k \)-dimensional subspace contained in the space of \( n \) carrier qudits. Let \( U \) be a Clifford unitary and \( S \) a stabilizer group with \( C \) being its corresponding stabilizer code. Then \( S' := USU^\dagger = \{UsU^\dagger : s \in S \} \) is also a stabilizer group stabilizing the code \( C' = \{U|\psi\rangle : |\psi\rangle \in C \} \). For a detailed review on Clifford unitaries and stabilizer states for arbitrary \( D \) see [17].

If \( |S| = D^n \), then \( S \) stabilizes a unique state and we call it the stabilizer state, denoted by \( |S\rangle \). The projector onto the state can be written as a sum of elements in \( S \), as shown in [18]

\[ |S\rangle \langle S| = \frac{1}{D^n} \sum_{s \in S} \langle s |. \]
Two simple examples of stabilizer states are the EPR pair and the GHZ state, expressed below for any $D \geq 2$ with their respective stabilizer groups,

$$|\text{EPR}\rangle_{12} = \frac{1}{\sqrt{D}} \sum_{i=0}^{D-1} |i\rangle_1 |i\rangle_2,$$

$$S = \langle X_1X_2, Z_1Z_2^{-1} \rangle \quad (12)$$

and

$$|\text{GHZ}\rangle_{123} = \frac{1}{\sqrt{D}} \sum_{i=0}^{D-1} |i\rangle_1 |i\rangle_2 |i\rangle_3,$$

$$S = \langle X_1X_2X_3, Z_1Z_2^{-1}, Z_1Z_3^{-1} \rangle \quad (13)$$

where the angular brackets denote the group generated by products of the elements in the list.

When $D$ is prime, $S$ can always be generated by $n$ suitably chosen group elements, $S = \langle s_1, s_2, \ldots, s_n \rangle$ such that the order of each $s_i$ is $D$. For non-prime $D$, one might need more than $n$ generators in some cases. We call these group elements stabilizer generators or generators. Note that the set of generators is not unique – there are many distinct choices of generators that generate the same group, for example $S = \langle s_1s_2, s_3, \ldots, s_n \rangle$.

**Proposition 3.** Let $S$ be a stabilizer group with $D^n$ elements where $D$ is prime. Let $T = \langle t_1, t_2, \ldots, t_m \rangle$ be a subgroup of $S$ with $D^m$ elements where $1 \leq m < n$. Then there exists a set of $n - m$ elements, $\{t_{m+1}, \ldots, t_n\} \subseteq S$ such that $S = \langle t_1, t_2, \ldots, t_m, t_{m+1}, \ldots, t_n \rangle$.

**Proof.** First pick an element of $S$ not in $T$ and call it $t_{m+1}$. Since $D$ is prime, the order of $t_{m+1}$ must be $D$. Then the set $\{t' t_{m+1}^{-1} \mid t' \in \langle t_1, t_2, \ldots, t_m \rangle, \alpha \in Z_D\} = \langle t_1, t_2, \ldots, t_m, t_{m+1} \rangle$ is a subgroup of $S$ with $D^{m+1}$ elements. Repeat this incremental addition of generators until the set of generators generates $S$. \hfill \Box

A stabilizer state $|S\rangle \in H^{\otimes n}$ naturally “lives” in a tensor product space of $n$ qudits but one can imagine a coarser-grained partitioning where the $n$ qudits are divided into two parts, labeled $A$ and $B$, which we will call a bipartition. One can regard any state on the total Hilbert space as an entangled state on $H_A \otimes H_B$ and we will also refer to such a state as a bipartition. Tripartitions and generalizations to higher number of partitions can be analogously defined. (Obviously partitions can be defined on any multi-partite state, not just stabilizer states.)

A useful expression for reduced density operators of multipartite stabilizer states is the following. For a bipartite stabilizer state $|S\rangle \in H_A \otimes H_B$ let

$$S_A := \{s \in S : \text{Tr}_B \{s\} \neq 0 \} \quad (14)$$

be the elements of $S$ equal to the identity on $H_B$. They form a subgroup of $S$ (e.g., [13]), and in light of Eq. (11),

$$\rho_A = \text{Tr}_B \{|S\rangle \langle S|\} = \frac{1}{D^n A} \sum_{s \in S_A} s, \quad (15)$$

If we square both sides we see that $\rho_A^2 = (|S_A|/D^n A) \rho_A$, which means that the reduced density operator of a stabilizer state has identical positive eigenvalues, so it is proportional to a projector. Additionally it satisfies

$$\text{rank}(\rho_A) = \frac{D^n A}{|S_A|} \quad (16)$$

Therefore, $\rho_A$ is proportional to the identity if and only if the subgroup $S_A$ has only the identity element.

Finally let $|S\rangle$ and $|T\rangle$ be stabilizer states on distinct sets of $n$ and $m$ qudits with stabilizer group $S = \langle s_1, \ldots, s_n \rangle$ and $T = \langle t_1, \ldots, t_m \rangle$. Then clearly the tensor product of these states $|V\rangle = |S\rangle \otimes |T\rangle$ is also a stabilizer state with the stabilizer group

$$V = \langle s_1, \ldots, s_n \rangle \otimes \langle t_1, \ldots, t_m \rangle$$

$$= \langle s_1 \otimes I, \ldots, s_n \otimes I, I \otimes t_1, \ldots, I \otimes t_m \rangle. \quad (17)$$

Conversely, given a stabilizer state $|V\rangle \in H^{\otimes n} \otimes H^{\otimes m}$, if the stabilizer group can be written as a tensor product of two stabilizer groups, $V = \langle s_1, \ldots, s_n \rangle \otimes \langle t_1, \ldots, t_m \rangle$, then $|V\rangle = |S\rangle \otimes |T\rangle$, since $|S\rangle$ and $|T\rangle$ are uniquely determined by their respective stabilizer groups.

**D. Decomposition of Stabilizer States of Composite Dimensions**

Let the integer $D$ have the prime decomposition

$$D = p_1^{\epsilon_1} p_2^{\epsilon_2} \cdots p_m^{\epsilon_m}, \quad (18)$$

where the $p_i$ are distinct primes and the $\epsilon_i$ positive integers. The following theorem is useful when the qudit dimension $D$ is composite.

**Theorem 4** (Chinese Remainder Decomposition of Stabilizer State). Let $A$ be an abelian group of linearly independent Pauli products on $n$ qudits, each of dimension $D$, and let Eq. (18) be the prime decomposition of $D$.

Then $A$ is unitarily equivalent to a tensor product of $m$ abelian groups in the sense that

$$A = \bigotimes_{i=1}^{m} A_i, \quad (19)$$

where $A_i$ is a unitary acting on the $D$-dimensional space of a single qudit, each $A_i$ is an abelian group of linearly independent Pauli products on $n$ qudits of dimension $p_i^{\epsilon_i}$, and

$$|A| = |A_1| \cdot |A_2| \cdots |A_m|. \quad (20)$$

The proof is in Appendix A. As stabilizer groups are examples of such abelian groups, one has:

**Corollary 5.** Let $|S\rangle$ be a stabilizer state on $n$ qudits of dimension $D$, prime decomposition given by Eq. (18).
Then there exists a single-qudit unitary $\mathcal{U}$ such that
\[ \mathcal{U} \otimes \cdots \otimes \mathcal{U} |S\rangle = \bigotimes_{i=1}^{M} |S_i\rangle \] (21)
where each $|S_i\rangle$ is a stabilizer state on $n$ qudits of dimension $p_i^D$.

Proof. Let $S$ denote the stabilizer group of $|S\rangle$ which has $D^n$ linearly independent Pauli products. Then by the theorem above, an abelian group of linearly independent Pauli products, is equivalent up to local unitaries to a tensor product of $m$ stabilizer groups of dimensions $p_1^D, p_2^D, \ldots, p_m^D$, each stabilizing its own stabilizer state $|S_i\rangle$.

When applied to an arbitrary stabilizer state $|S_0\rangle$ on qudits of $D = 6$, this corollary states that it is equivalent up to local single-qudit unitaries to a tensor product of two stabilizer states $|S_2\rangle \otimes |S_3\rangle$, one on $n$ qubits and the other on $n$ qutrits. Essentially each $D = 6$ qudit has an internal tensor product structure that can be decomposed into a qubit and a qutrit. Therefore in studies of entanglement of stabilizer states of $D = 6$, it is sufficient to just consider qubit and qutrit stabilizer states.

In this paper, the corollary above is used to extend various results on stabilizer states that hold for prime $D$ to the case where $D$ is squarefree, meaning that $\epsilon_i = 1$ in Eq. (24) for every $i$.

E. Graph States

Let $\Gamma_{ij} = \Gamma_{ji}$ be the adjacency matrix of an undirected graph $G$ on $n$ vertices with no loops ($\Gamma_{ii} = 0$). Each $\Gamma_{ij}$, the weight of the edge connecting vertices $i$ and $j$, can take any value in $\mathbb{Z}_D$, with (as usual) $\Gamma_{ij} = 0$ in the absence of an edge.

The graph state $|G\rangle$ is a state on $n$ qudits of dimension $D$ defined as
\[ |G\rangle := \left( \prod_{i=1}^{n-1} \prod_{j=i+1}^{n} \text{CP}_{ij}^{\Gamma_{ij}} \right) |\rangle_1 \otimes \cdots \otimes |\rangle_n \] (22)
where
\[ |\rangle := \frac{1}{\sqrt{D}} \sum_{j=0}^{D-1} |j\rangle \] (23)
and the two-qudit gate $\text{CP}_{ij}$ is defined in Eq. 8. Note that the CP gates all commute with each other so there is no need to specify the order in which they act on the kets. For non-prime $D$, there are alternative ways to define graph states; see, e.g., 19.

All graph states are stabilizer states but the converse is not true; however it was shown in 20 and 19 for prime $D$ (and therefore also for squarefree $D$ by Corollary 5) that all stabilizer states are equivalent up to local Clifford unitaries to graph states. It is often more convenient to work with the stabilizer group (denoted by $\mathcal{S}_G$) rather than the ket itself. For a given graph state $|G\rangle$ with adjacency matrix $\Gamma$, there is a canonical set of $n$ stabilizer generators, $\{g_i\}$ given by
\[ g_i := X_i \left( \prod_{j=1}^{n} Z_j^{-\Gamma_{ij}} \right) \] for $i = 1, 2, \ldots, n$ (24)
which of course satisfies $g_i|G\rangle = |G\rangle$ for all $g_i$, so we have $\mathcal{S}_G = \{g_1, g_2, \ldots, g_m\}$. These operators are called correlation operators in 21.

III. BIPARTITION OF QUDIT STABILIZER STATES

Entanglement across bipartitions of stabilizer states has been studied in Section 3 of 22 and 18. Here we shall extend their result to all squarefree $D \geq 2$ with the theorem below. The entanglement of a bipartite state can always be studied in terms of its Schmidt decomposition but we present an alternative approach here because it is helpful in explaining the techniques that will be used in the Tripartition Theorem in Section IV.

Before stating the Bipartition Theorem let us study some simple stabilizer states to understand how unentangled subsystems in stabilizer states is by inspecting the Tripartition Theorem in Section IV.

In the second case, it is harder to tell how entangled the state is by just looking at the stabilizer group $\mathcal{S}_G^{(2)}$, even though it differs only by a local unitary on part $A$ from the previous state, $|\mathcal{S}_G^{(2)}\rangle = \text{CP}_{A,B}\mathcal{S}_G^{(1)}$. This tells us there must be some hidden unentangled subsystem in part $A$ that upon removal will result in a simpler two-qudit stabilizer state, just like the first example.

A systematic way to “detect” the presence of unentangled subsystems in stabilizer states is by inspecting the reduced density operator on each part or equivalently the subgroups $\mathcal{S}_A, \mathcal{S}_B$ (see Subsection IIC). The Bipartition Theorem below is essentially just a formal statement that once all the unentangled subsystems are removed, all that remains is a collection of EPR pairs.
Theorem 6 (Bipartition of stabilizer state). For squarefree $D$, let $|S\rangle$ be a stabilizer state on $n \geq 2$ qudits. For any bipartition of $|S\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$, there exists Clifford unitaries $U_A, U_B$ on each part such that $U_A U_B |S\rangle$ is a collection of maximally entangled EPR pairs and unentangled single-qudit states, i.e.

$$U_A U_B |S\rangle_{AB} = |\text{EPR}_{\gamma A B} \otimes (|+\rangle \otimes m_A) \otimes |+\rangle \otimes m_B\rangle.$$  

(26)

Note that $m_A$, $m_B$ or $m_{AB}$ can be zero.

Proof. By invoking Corollary 5 we can decompose $|S\rangle$ into several stabilizer states where each of them is on $n$ qudits of prime dimension. Therefore it is sufficient to prove the theorem only for prime $D$.

If the subgroups $S_A$ and $S_B$ both contain only the identity element, then by Eq. (15) both $\rho_A$ and $\rho_B$ are proportional to the identity. This is equivalent to $S$ not containing any element that is non-trivial only in one part, such as $X_A B$. This also means $|S\rangle$ is maximally entangled and therefore is equivalent to a collection of EPR pairs.

Otherwise assume that $S_A$ has at least one element, $s \in \mathcal{P}_A$ not equal to the identity, a Pauli product which acts non-trivially on at least one qudit in part $A$. Without loss of generality we can assume that qudit is $A_1$. Then by Proposition 2 we know there exists a Clifford operation, $U_A$ such that $U_A S_A U_A^\dagger = X_{A_1} I_{A_2} \cdots I_{A_n}$. The end result is a stabilizer group, $U_A S_A U_A^\dagger$, of the form $s_2 = X_{A_1} \otimes p_{A_1 A_1}$, where $p_{A_1 A_1}$ is some Pauli product on qudits $A_2, \ldots, A_n$. If $s_2 \neq 0$, then do nothing. Otherwise replace $s_2$ with $s_2' := X_{A_1}^{-1} s_2 = I_{A_1} \otimes p_{A_1 A_1}$, so that the new generator is the identity on qudit $A_1$. This replacement does not change the group being generated.

Repeat this procedure for all the other generators $s_3, \ldots, s_n$. In doing so we now have a new set of generators such that there is only one generator that is non-trivial on qudit $A_1$ while all other generators have identity on $A_1$. The end result is a stabilizer group that can be written as a tensor product, $U_A S_A U_A^\dagger = \langle X_{A_1} \rangle \otimes \langle s_2', \ldots, s_n' \rangle$.

Following the discussion at the end of Subsection 1C we can write $U_A |S\rangle = |+\rangle_{A_1} \otimes |S'\rangle$ where $|+\rangle$ is defined in Eq. (23) and $|S'\rangle$ is stabilized by $\langle s_2', \ldots, s_n' \rangle$. In other words, we have extracted an unentangled subsystem from part $A$ and are left with a stabilizer state with $n - 1$ qudits. Repeat this process on both parts until both $S_A$ and $S_B$ contain only the identity element. This concludes the proof. □

In fact this extraction of unentangled subsystems works for stabilizer states with any number of parts since we can always view the part of interest as $A$ and all the other parts as $B$.

IV. TRIPARTITION OF QUDIT STABILIZER STATES

The problem of tripartition of qubit ($D = 2$) stabilizer states has been studied by Bravyi et al. They proved that such states are always equivalent up to unitaries on each part to a collection of GHZ states, maximally entangled EPR pairs and unentangled single-qudit states; see Figure 1 for a simple illustration. In the same paper, they also provided partial solutions to the general problem with more than three parties. Here we extend their tripartition result to squarefree $D \geq 2$ using a method mentioned but not used in their paper.

Theorem 7 (Tripartition of stabilizer state). For squarefree $D$, let $|S\rangle$ be a stabilizer state on $n \geq 3$ qudits. For any tripartition of $|S\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$, there exists Clifford unitaries $U_A, U_B, U_C$ on each part such that $U_A U_B U_C |S\rangle$ is a collection of GHZ states, maximally entangled EPR pairs and unentangled single-qudit states, i.e.

$$U_A U_B U_C |S\rangle = |\text{GHZ}_{\gamma ABC} \otimes |\text{EPR}_{\gamma AB} \otimes |+\rangle_{\gamma m_B} \otimes |+\rangle_{\gamma m_C} \rangle,$$

where $m_A, m_B, m_C, m_{AB}, m_{BC}, m_{AC}, m_{ABC}$ are non-negative integers that can be zero.

Proof. It is sufficient to prove the theorem only for prime $D$ because Corollary 5 extends the proof to squarefree $D$. The proof can be divided into three major steps. In Step 1 we simply repeat the unentangled subsystem extraction procedure explained in the previous section; the details will not be repeated here. As a consequence the three reduced density operators $\rho_A, \rho_B, \rho_C$ are all proportional to the identity. In Step 2, we extract EPR pairs using local Clifford unitaries acting on two parts at a time. Thus for parts $A$ and $B$, we try to find $U_A, U_B$ such that $U_A U_B |S\rangle = |\text{EPR}_{\gamma AB} \otimes |S'\rangle$. The identical procedure can be used to extract EPR pairs from $A$ and $C$, and from $B$ and $C$, so we only need to discuss how it works for $A$ and $B$. Finally in Step 3 we prove that the state remaining after all these extractions must be a collection of GHZ states.
We begin Step 2 with the observation that the reduced density operator \( \rho_{AB} \) for the combined parts \( A \) and \( B \) is given by
\[
\rho_{AB} = \text{Tr}_C[|S\rangle\langle S|] = D^{-\left(n_A+n_B\right)} \sum_{i=1}^{\left|S_{AB}\right|} s_{AB}^{(i)}
\]
where \( S_{AB} := \{ s \in S : \text{Tr}_C(s) = 0 \} \) and \( s_{A}^{(i)}, s_{B}^{(i)} \) are Pauli products on \( A \) and \( B \) respectively. There is some phase ambiguity in the final expression because a phase on \( s_A^{(i)} \) can be moved to \( s_B^{(i)} \) or vice versa, but the following proof does not depend on how the phase is assigned.

**STEP 2A** - If the collection \( \{ s_A^{(i)} \} \) defined in Eq. (28) contains two elements \( s_A^{(j)}, s_A^{(k)} \) that do not commute, then at least one EPR pair can be extracted from parts \( A \) and \( B \) as we now show. We can always assume those two elements satisfy the commutation relation
\[
s_A^{(j)} s_A^{(k)} = \omega s_A^{(k)} s_A^{(j)}, \tag{29}
\]
where if the phase picked up is instead some higher power of \( \omega \), we can replace \( s_A^{(k)} \) with an appropriate power of \( s_A^{(k)} \), since \( D \) is prime. Now transform \( s_{AB}^{(j)} \) so that it is the identity on every qudit except \( A_1 \) and \( B_1 \), i.e.
\[
s_{AB}^{(j)} = Z_{A_1} \otimes Z_{B_1}^{-1}, \tag{30}
\]
by applying Proposition 2 twice, first on part \( A \) and then on part \( B \), using Clifford unitaries local to each part. The commutation relation between \( s_{AB}^{(j)}, s_A^{(k)} \) in Eq. (29) is unchanged because it is invariant under conjugations by unitaries.

**STEP 2B** - The fact that \( \{ s_{AB}^{(j)}, s_{AB}^{(k)} \} = 0 \) together with Eqs. (29) and (30) imply that
\[
s_{AB}^{(k)} = X_{A_1} Z_{A_1}^p P_{A_1} \otimes X_{B_1} Z_{B_1}^q q_{B_1}, \tag{31}
\]
where \( p, q \) are some Pauli products on the remaining qudits on part \( A, B \) respectively and \( \alpha, \beta \in Z_D \). To see this, first observe that Eqs. (29) and (30) tell us the exponent on \( X_{A_1} \) is necessarily 1 while imposing no conditions on the exponent of \( Z_{A_1} \), nor the Pauli operators on the other qudits in part \( A \). Next, \( s_{AB}^{(j)} \) commuting with \( s_{AB}^{(k)} \) fixes the exponent of \( X_{B_1} \) to be 1, resulting in Eq. (31).

In Eq. (31) the \( Z \) operators on qudits \( A_1 \) and \( B_1 \) can be removed by conjugating \( s_{AB}^{(k)} \) with the phase gate \( W \) applied to these qudits (see Table I). Lastly, the Pauli products \( p \) and \( q \) can be set to \( I \) using methods outlined in the proof of Proposition 2. The conjugations by CNOT gates described there with \( A_1, B_1 \) being the control qudits do not modify \( s_{AB}^{(j)} \) at all. At the end of all these transformations we have
\[
s_{AB}^{(k)} = X_{A_1} \otimes X_{B_1}. \tag{32}
\]

**STEP 2C** - Keeping track of all the Clifford unitaries that have acted so far on the two parts and combining them as \( U_A, U_B \), we can write the new stabilizer group as \( (U_A U_B I_C)(U_A U_B I_C)^{\dagger} = \{ t_1 = X_{A_1} X_{B_1}, t_2 = Z_{A_1} Z_{B_1}, t_3, \ldots \} \) by Proposition 3. Since \( t_3 \) must commute with \( t_1 \) and \( t_2 \), it must be of the form
\[
t_3 = X_{A_1}^\alpha Z_{A_1}^\beta P_{A_1} \otimes X_{B_1}^{-\beta} Z_{B_1}^{-\alpha} q_{B_1} \otimes r_C \tag{33}
\]
for some \( \alpha, \beta \in Z_D \), where \( p, q, r \) are some Pauli products on subsystem \( A \) less \( A_1 \), \( B \) less \( B_1 \) and \( C \) respectively, reusing arguments that produced Eq. (31). Next replace the generator \( t_3 \) by \( t_3 = t_2^{-\beta} t_1^{-\alpha} t_3 \) so that \( t_3 \) has identities on qudits \( A_1, B_1 \). The same can be done for all other generators, \( t_4, \ldots, t_n \).

**STEP 2D** - Given this, we can write the new stabilizer group as \( \langle X_{A_1} X_{B_1}, Z_{A_1} Z_{B_1} \rangle \otimes \langle t_3', \ldots, t_n' \rangle \) an EPR pair stabilized by \( \langle X_{A_1} X_{B_1}, Z_{A_1} Z_{B_1} \rangle \) and a stabilizer state \( |S'\rangle \) stabilized by \( \langle t_3', \ldots, t_n' \rangle \) The reduced density operators \( \rho_A \) and \( \rho_B \) corresponding to \( |S'\rangle \) are again proportional to the identity operators on the parts \( A \) and \( B \) that remain after the extraction. Were it otherwise in the case of \( \rho_A' \), the reduced density operator on the (full) system \( A \) corresponding to the state stabilized by \( \langle X_{A_1} X_{B_1}, Z_{A_1} Z_{B_1} \rangle \otimes \langle t_3', \ldots, t_n' \rangle \) would not be proportional to the identity, contradicting the fact that after Step 1 (extraction of unentangled subsystems), and thus at the beginning of Step 2, \( \rho_A \) was proportional to the identity; of course the same applies to \( \rho_B \).

**STEP 2E** - Next examine the expansion of \( \rho_A' \) putting \( |S'\rangle \) in (28). If some of the \( s_A^{(i)} \) do not commute with each other a further extraction is possible, and one can repeat the process until all of these operators commute. Now apply the same extraction process to \( A \) and \( C \), and then to \( B \) and \( C \), until all EPR pairs have been extracted.

The final step is showing that the tripartite stabilizer state after extracting all unentangled states and EPR pairs is a collection of GHZ states.

**STEP 3A** - We prove that after the preceding extractions have been carried out, the three parts must have the same number of qudits, \( n_A = n_B = n_C \). Since \( \rho_C \) is proportional to the identity, \( |S\rangle \) is maximally entangled across the \( C-AB \) cut. Using its Schmidt form allows the the projector on \( |S\rangle \) to be written as
\[
|S\rangle\langle S| = \frac{1}{D^{nc}} \sum_{i,j=0}^{D^{nc}-1} |i\rangle\langle j| \otimes |\phi_i\rangle\langle \phi_j|_{AB}. \tag{34}
\]
with \( \{|\phi_i\rangle\} \) a set of orthonormal kets in \( \mathcal{H}_A \otimes \mathcal{H}_B \). The \( \{|i\rangle\langle j|\} \) are a set of \( D^{2nc} \) linearly independent operators, as are the \( \{|\phi_i\rangle\langle \phi_j|_{AB}\} \), which means the operator Schmidt rank of \( |S\rangle\langle S| \) is \( D^{2nc} \).

From Eq. (14) the projector can also be expressed as a sum of the \( D^n \) linearly independent stabilizer elements.
where the $r_{AB}^{(k)}$ and $r_C^{(k)}$ are Pauli products on $AB$ and $C$, respectively. In general, the collection $\{r_C^{(k)}\}$ is not linearly independent; e.g., each $r_C^{(k)}$ that belongs to the subgroup $\mathcal{S}_{AB}$ satisfies $r_C^{(k)} \propto I_C$. Indeed, two elements $r_C^{(k)}$ and $r_C^{(l)}$ belong to the same coset of $\mathcal{S}_{AB}$ if and only if $r_C^{(k)} \propto r_C^{(l)}$. Therefore the number of cosets of $\mathcal{S}_{AB}$ is the number of linearly independent elements in the collection $\{r_C^{(k)}\}_{k=1}^D$. We shall now prove that this number is $D^{2nc}$.

We can re-express Eq. (35) as a sum over linearly independent Pauli products on parts $C$

$$|S\rangle\langle S| = \frac{1}{D^n} \sum_{k=1}^{D^n} r_{AB}^{(k)}$$

where $\{x_{AB}^{(k)}\}$ are sums of Pauli products on parts $A$ and $B$. We know there must be $D^{2nc}$ linearly independent terms since that is the operator Schmidt rank and thus none of the $x_{AB}^{(k)}$ can vanish. Hence the number of cosets of $\mathcal{S}_{AB}$ is $D^{2nc}$. Thus by Lagrange’s theorem,

$$|\mathcal{S}_{AB}| = |S|/D^{2nc} = D^{n_A+n_B-n_C}. \quad (37)$$

We now go on a digression to show that the collection of Pauli products on subsystem $A$, $\{s_A^{(j)}\}$, on the right side of Eq. (28), is linearly independent when $\rho_B \propto I_B$; similarly, the collection $\{s_B^{(i)}\}$ is linearly independent if $\rho_A \propto I_A$. Because they are Pauli products it suffices to show that no two of them are proportional in order to demonstrate linear independence. Assume the contrary, that $s_A^{(j)} \propto s_A^{(k)}$ for some $j \neq k$. Since the $\{s_{AB}^{(j)}\}$ are group elements, $s_{AB}^{(j)}$ must have an inverse, $\left(s_{AB}^{(j)}\right)^{-1}$, which inserted in Eq. (28) yields

$$\left(s_{AB}^{(j)}\right)^{-1} s_A^{(j)} = \left(s_A^{(j)} \otimes s_B^{(i)}\right)^{-1} (s_A^{(k)} \otimes s_B^{(i)}) \propto I_A \otimes \left(s_B^{(j)}\right)^{-1} s_B^{(i)}.$$  \quad (38)

The final term cannot be proportional to the identity, as that would imply $s_A^{(j)} \propto s_A^{(k)}$. But these are elements of $S$, so they must be linearly independent for $j \neq k$. Therefore $S_B$ contains an element that is not the identity, contradicting the fact that $\rho_B \propto I_B$. Hence it cannot be the case that $s_A^{(j)} \propto s_A^{(k)}$ for $j \neq k$.

Thus the collection $\{s_A^{(j)}\}$ contains $|\mathcal{S}_{AB}|$ linearly independent and mutually commuting elements, and by Proposition \[ this means that $|\mathcal{S}_{AB}| \leq D^{n_A}$. The same argument applies to the collection $\{s_B^{(i)}\}$, so $|\mathcal{S}_{AB}| \leq D^{n_B}$. Combining these inequalities with Eq. (37), it follows that both $n_A$ and $n_B$ cannot be larger than $n_C$. Identical arguments applied to different pairs of subsystems implies that

$$n_A = n_B = n_C,$$ \quad (39)

and, using Eq. (37), $|\mathcal{S}_{AB}| = |\mathcal{S}_{BC}| = |\mathcal{S}_{AC}| = D^{n_A}$.

STEP 3B - If $\mathcal{S}_{BC}$ contains only the identity element, then $n_A = n_B = n_C = 0$ and no GHZ state can be extracted. Otherwise $n_A \geq 1$ and $\mathcal{S}_{BC}$ has at least one non-trivial element which we will label as $t_1$. By Proposition 2 it can be transformed to

$$t_1 = Z_{B_1} \otimes Z_{C_1}^{-1}.$$ \quad (40)

Now consider the group $\mathcal{S}_{AB}$. We showed previously that the operators $\{s_B^{(i)}\}$ defined in Eq. (28) are both linearly independent and mutually commuting, and $|\{s_B^{(i)}\}| = D^{n_B}$. Hence, if there is an element $p \in \mathcal{P}_{n_B}$ that commutes with every element in $\{s_B^{(i)}\}$, it must belong to $\{s_B^{(i)}\}$ up to a phase. This is because, by Proposition 4, sets of mutually commuting Pauli products on $n_B$ qudits cannot have more than $D^{n_B}$ linearly independent elements.

Note that if $t_1$ commuting with every element of $\mathcal{S}_{AB}$ (as they are all just elements of $S$) implies $Z_{B_1}$ commutes with every $s_B^{(i)}$ since $t_1$ is identity on part $A$ and every $s \in \mathcal{S}_{AB}$ is identity on part $C$. Then by the argument in the previous paragraph, there exists an element of $\mathcal{S}_{AB}$ of the form $p_A \otimes Z_{B_1}$. Let $t_2$ denote this element and note that $p_A \neq I_A$ as otherwise this would contradict the assumption that $\rho_B$ is proportional to the identity. Then by Proposition 2 there exists unitary transformations such that

$$t_2 = Z_{A_1}^{-1} \otimes Z_{B_1}.$$ \quad (41)

and they do not affect $t_1$ since all the operations are done on part $A$.

STEP 3C - Since each of the $D^{2nc}$ Pauli products for part $C$ must appear in Eq. (38)—none of $x_{AB}^{(k)}$ can vanish—there exists an element in $S$ which satisfies $q_C^{(k)} \propto X_{C_1} \otimes \chi_{C_1}^{(i)}$ on the $C$ subsystem. We call that element $t_3$. The most general form it can have, given that it has to commute with $t_1 = Z_{B_1}Z_{C_1}^{-1}$ and $t_2 = Z_{A_1}^{-1}Z_{B_1}$, is

$$t_3 = X_{A_1} Z_{A_1}^{a_1} p_{A_1} A_{1} \otimes X_{B_1} Z_{B_1}^{b_1} q_{B_1} B_{1} \otimes X_{C_1},$$ \quad (42)

where $p, q$ are Pauli products on the remaining qudits in part $A, B$ respectively and $\alpha, \beta \in \mathbb{Z}_D$; see STEP 2B for the explanation. Finally we transform this element to $t_3 = X_{A_1} X_{B_1} X_{C_1}$ without modifying $t_1, t_2$ by using the techniques described in STEP 2B and in the proof of Proposition 2.

STEP 3D - Invoking Proposition 3 and letting $U_A, U_B, U_C$ denote all the unitary operations we have made so far, we can write
\((U_A U_B U_C) S(U_A U_B U_C)^\dagger = |t_1 = Z_B Z_C, t_2 = Z_A Z_B, t_3 = X_A X_B X_C, t_4, \ldots, t_n\rangle\). As was done in STEP 2C and the proof of Bipartition Theorem, the generators \(t_4, \ldots, t_n\) can all be made to be the identity on qudits \(A_1, B_1, C_1\) simultaneously, so we can write \(U_A U_B U_C S(U_A U_B U_C)^\dagger = Z_{B_1} Z_{C_1}, Z_A, X_A X_B X_C \otimes |t_4, \ldots, t_n\rangle\). Therefore we have a GHZ state, see Eq. (13), on qudits 1, 2, 3.

Next assume that \(d_A \leq d_B\) and define an isometry \(V : \mathcal{H}_A \rightarrow \mathcal{H}_B\) as

\[ V := \sum_{i=0}^{d_A} |v_i\rangle_B \langle i|_A, \tag{46} \]

where \(|v_i\rangle\) is an orthonormal basis spanning a \(d_A\)-dimensional subspace of \(\mathcal{H}_B\) that we call the coding space. The isomorphism carries it into

\[ |V\rangle := \Phi(V) = \frac{1}{\sqrt{d_A}} \sum_{i=0}^{d_A} |v_i\rangle_B \langle i|_A. \tag{47} \]

where, since \(V\) is an isometry, \(\rho_A = \text{Tr}_B \{ |V\rangle \langle V| \} = I_A/d_A\). One can think of \(|V\rangle\), where \(\mathcal{H}_A\) and \(\mathcal{H}_B\) enter on an equal footing, as an atemporal representation of the isometry.

The following lemma uses the Choi-Jamiolkowski isomorphism to relate isometries corresponding to stabilizer codes to stabilizer states.

**Lemma 8** (Isomorphism between stabilizer code and bipartite stabilizer state). Let \(D\) be the dimension of any one of the qudits. The two statements below are true for any prime \(D\)

1. Given an \([n,k]_D\) stabilizer code (Subsection 1C) that defines an isometry \(V : \mathcal{H}^n \rightarrow \mathcal{H}^n\), the isomorphism \(\Phi\) in Eq. (44) carries \(V\) to a stabilizer state \(|V\rangle\) on \(k+n\) qudits.

2. Let \(|S\rangle_{AB}\) be a stabilizer state on \(k+n\) qudits, where the first \(k\) qudits constitute part \(A\) and the remaining \(n\) qudits constitute part \(B\), and assume that \(\text{Tr}_B \{ |S\rangle \langle S| \} = I_A/D^k\). Then the inverse isomorphism \(\Phi^{-1}\) in Eq. (44) carries \(|S\rangle\) to an isometry \(V : \mathcal{H}_A \rightarrow \mathcal{H}_B\) whose image or coding space is an \([n,k]_D\) stabilizer code.

**Proof.** The proof can be simplified by noting that, as shown in \([19,20]\), any stabilizer code when \(D\) is prime is equivalent to an additive graph code, up to products of single-qudit Clifford unitaries. In turn it was shown in \([19,20]\) that an additive \([n,k]_D\) graph code when \(D\) is prime can be described using a graph state \(|G\rangle \in \mathcal{H}^n\) and an abelian group \(\mathcal{F} = \{ c_i \}_{i=0}^{D^k-1}\) with \(D^k\) linearly independent Pauli products in \(\mathcal{P}_n\), composed only of \(Z\) operators. The coding space is spanned by the set \(\{ g_i \}_{i=0}^{n}\) of mutually orthogonal kets. Recall from Subsection 1C that any graph state \(|G\rangle\) on \(n\) qudits can be fully specified by its stabilizer group, \(|g_1, \ldots, g_n\rangle\) with
The coding space, and commute with the elements, see Eq. (41). Similarly, the coding group \( \mathcal{F} \) can be generated by \( k \) suitably chosen group elements, \( \mathcal{F} = \{ f_1, f_2, \ldots, f_k \} \), so the coding space is spanned by \( f_i^1, \ldots, f_i^k |G\rangle \) for \( i_1, i_2, \ldots, i_k = 0, 1, \ldots, D - 1 \).

To prove statement 1, define the isometry
\[
V = \sum_{i_1=0}^{D-1} \cdots \sum_{i_k=0}^{D-1} f_i^1 \cdots f_i^k |G\rangle \langle i_1 \cdots i_k |_A \tag{48}
\]
that maps \( \mathcal{H}_A = \mathcal{H}^{\otimes k} \), a collection of \( k \) qudits, into the coding space, and
\[
|V\rangle = \frac{1}{\sqrt{D^k}} \sum_{i_1=0}^{D-1} \cdots \sum_{i_k=0}^{D-1} |i_1 \cdots i_k\rangle_A \otimes f_i^1 \cdots f_i^k |G\rangle_B \tag{49}
\]
the corresponding ket on \( \mathcal{H}_A \otimes \mathcal{H}_B \) as per Eq. (44).

We shall show that \( |V\rangle \) is a stabilizer state by exhibiting the \( k+n \) stabilizer generators. The first \( n \) are derived from the generators \( \{ g_j \} \), for \( j = 1, 2, \ldots, n \) of the stabilizer group of \(|G\rangle\), now regarded as operators on \( \mathcal{H}_A \otimes \mathcal{H}_B \), so that
\[
(V 
\otimes g_j)|V\rangle = \frac{1}{\sqrt{D^k}} \sum_{i_1=0}^{D-1} \cdots \sum_{i_k=0}^{D-1} \sum_{i_l=0}^{D-1} |i_1 \cdots i_k\rangle_A \otimes \omega^{i_1 \beta_j^l} \cdots \omega^{i_k \beta_j^k} f_i^1 \cdots f_i^k |G\rangle_B, \tag{50}
\]
where the phases result from commuting the \( g_j \) with the \( f_l \) operators:
\[
g_j f_l = \omega^{\beta_j^l} f_l g_j \quad \text{for } j = 1, \ldots, n \text{ and } l = 1, \ldots, k; \tag{51}
\]
with the \( \beta_j^l \) integers in \( \mathbb{Z}_D \). The phases can be removed using an appropriate Pauli product of \( Z \) operators:
\[
(Z_{A_1}^{-\beta_j^1} \cdots Z_{A_k}^{-\beta_j^k} \otimes g_j) |V\rangle = |V\rangle \quad \text{for } j = 1, \ldots, n, \tag{52}
\]
That these \( n \) generators mutually commute follows from the fact that \( \{ g_j \} \) is a mutually commuting set.

The remaining \( k \) stabilizer generators are simply
\[
X_{A_l} \otimes (f_l^{-1})_B \quad \text{for } l = 1, \ldots, k. \tag{53}
\]
They obviously commute among themselves. It is not hard to show that they leave \( |V\rangle \) in Eq. (19) invariant, and commute with the \( n \) previous generators on the left side of Eq. (52). Since we have constructed \( k+n \) linearly independent commuting Pauli operators that leave \( |V\rangle \) invariant, and thus generate a stabilizer group, \( |V\rangle \) is a stabilizer state.

To prove statement 2 of the lemma we use the fact that for prime \( D \), any stabilizer state \(|S\rangle\) is equivalent up to single-qudit Clifford unitaries, thus a choice of basis for the individual qudits, to a graph state. Hence without loss of generality we can assume that \(|S\rangle\) is a graph state on \( \mathcal{H}_A \otimes \mathcal{H}_B \) written in the form, see Eq. (22),
\[
|S\rangle_{AB} = \left( \prod_{i<j}^{n+k} \text{CP}_{A_{ij}}^f \right) |+\rangle^\otimes A |+\rangle^\otimes B . \tag{54}
\]
Let \( \text{CP}_A \) be the product of those CP gates on the right side that act only on qudits in \( A \), and let \(|G\rangle_B = \text{CP}_B |+\rangle^\otimes \mathcal{H}_B \) be the graph state on \( \mathcal{H}_B \) resulting from the CP gates that act only on qudits in \( B \), denoted by \( \text{CP}_B \). The action of the remaining CP gates that connect \( A \) and \( B \) qudits can be written out explicitly in terms of \( Z \) operators, see Eq. (5), to obtain
\[
|S\rangle = \text{CP}_A \left( \prod_{i=1}^{k} \prod_{j=k+1}^{n+k} \text{CP}_{ij}^f \right) |+\rangle^\otimes A |+\rangle^\otimes B \tag{55}
\]
where
\[
f_l := \prod_{j=k+1}^{n+k} Z_j \quad \text{for } l = 1, 2, \ldots, k, \tag{56}
\]
and so
\[
\prod_{j=k+1}^{n+k} \text{CP}_{ij}^f = \sum_{i_0=0}^{D-1} \sum_{i_l=0}^{D-1} \langle i_1 \cdots i_k |_A \otimes f_1^i \cdots f_k^i |G\rangle_B \tag{57}
\]
Comparing the last line of Eq. (55) with Eq. (19) yields
\[
\Phi^{-1}([\text{CP}_A]) |S\rangle = \sum_{i_0=0}^{D-1} \cdots \sum_{i_k=0}^{D-1} f_i^1 \cdots f_i^k |G\rangle_B \langle i_1 \cdots i_k |_A \tag{58}
\]
which is an isometry corresponding to an additive graph code with graph state \(|G\rangle_B \in \mathcal{H}^\otimes n \) and coding group \( \mathcal{C} = \{ f_1, \ldots, f_k \} \). Therefore, using Eq. (55)
\[
\Phi^{-1}(|S\rangle) = \sum_{i_0=0}^{D-1} \sum_{i_k=0}^{D-1} U_B f_i^1 \cdots f_i^k |G\rangle_B \tag{59}
\]
where the transpose is taken in the computational basis. The final factor is simply a unitary transformation on the input and thus does not change its image, which is the graph or stabilizer code spanned by the \( f_1^1 \cdots f_k^k |G\rangle_B \). That these last are a collection of \( D^k \) mutually orthogonal kets follows from the assumption that \( \text{Tr}_B \langle S| S\rangle = 1 \), and the fact that the final equality in Eq. (55) is a Schmidt decomposition of \(|S\rangle\). \( \square \)
B. Stabilizer Code Channels and Subset Information Groups

Consider an isometry $V : \mathcal{H}_A = \mathcal{H}^\otimes k \to \mathcal{H}^\otimes n$ corresponding to an $[[n, k]]_D$ stabilizer code where $D$ is prime and the $n$ output qudits are partitioned into two disjoint non-empty subsets, $B$ and $C$. Such bipartitions of stabilizer/graph codes have been studied in [13] and [23]. (Qubit stabilizer codes with input qudits partitioned into two parts have also been studied in [24] but in this paper we will only consider bipartitions of the output qudits.) We can think of the $B$ qudits as the output of a direct quantum channel, and the $C$ qudits either as the environment or as the output of complementary channel, with corresponding superoperators

$$\mathcal{E}_B(\rho) := \text{Tr}_C\{V\rho V^\dagger\}, \quad \mathcal{E}_C(\rho) := \text{Tr}_B\{V\rho V^\dagger\}. \quad (60)$$

We shall refer to channels derived in this way from stabilizer codes as stabilizer code channels. The analysis below applies to any stabilizer code regardless of its error correction properties such as channel capacity.

In Section V of [13], we studied the information-carrying capacity of stabilizer code channels and to this end introduced the subset information group

$$\mathcal{G}_B := \{ p \in \mathcal{P}_k \mid \mathcal{E}_B(p) \neq 0 \}, \quad (61)$$

a subgroup of the Pauli group on the $k$ input qudits. It was shown that $\mathcal{G}_B$ is a group, and its elements satisfy the isomorphism

$$\mathcal{E}_B(p) \mathcal{E}_B(q) = c \mathcal{E}_B(pq) \quad \forall \, p, q \in \mathcal{G}_B, \quad (62)$$

where $c$ is an appropriately chosen positive constant independent of $p$ and $q$.

We also presented an efficient algorithm to find $\mathcal{G}_B$ given the isometry $V$ (defined by an additive graph code) and the subset $B$, by solving a set of linear equations modulo $D$. The subset information group $\mathcal{G}_C$ for the complementary channel can be defined in the same way. The previous work discussed additive graph codes, but the results apply to stabilizer codes as well since they are equivalent up to local unitaries.

One can think of the group $\mathcal{G}_B$ or the operator algebra that it spans, a subalgebra of the algebra $L(\mathcal{H}_A)$ of operators on the channel input, as representing the information that is perfectly transmitted from the input to the output $\mathcal{H}_B$ of the channel by $\mathcal{E}_B$. Since it is present in the output, this information can be perfectly recovered, which is to say mapped to a Hilbert space $\mathcal{H}_A'$ isomorphic to $\mathcal{H}_A$, by a recovery operation (recovery channel) $\mathcal{R} : L(\mathcal{H}_B) \to L(\mathcal{H}_A')$, as shown in [13]. The recovery operation has the property that $[\mathcal{R} \circ \mathcal{E}_B]^\dagger (x) = x$, where $x$ is any Pauli product in $\mathcal{G}_B$ or any operator in the subalgebra that it spans. Thus the last is an example of a correctable algebra, as defined in [14] in their formalism of operator algebra quantum error correction.

In the following subsections we show that stabilizer code channels can be decomposed into tensor products of simple channels, which has important implications for the properties of $\mathcal{G}_B$ and $\mathcal{G}_C$.

C. Tensor Product Structure of Stabilizer Code Channels

Before stating the main result in Theorem 9, let us indicate by means of some simple examples its main idea, which is that the isomorphism proven in Lemma 8 with Theorem 7 imply stabilizer code channels have a very simple structure.

First consider the stabilizer state, $|V\rangle = |\text{EPR}\rangle_{A_1B_1C_1}$, Eq. (12), which by Eqs. (60) and (17) corresponds to the isometry

$$\Phi^{-1}(|V\rangle) = V_{\text{EPR}} = \sum_{i=0}^{D-1} |i\rangle_{B_1} \langle i|_{A_1}, \quad (63)$$

for a perfect quantum channel from $\mathcal{H}_{A_1}$ to $\mathcal{H}_{B_1}$, with quantum (and classical) channel capacity equal to $\log_2 D$. The subset information group contains every Pauli operator on qudit $A_1$, i.e. $\mathcal{G}_B = \langle \lambda I_{A_1}, X_{A_1}, Z_{A_1} \rangle$.

Next consider the tripartite state $|V\rangle = |\text{EPR}\rangle_{A_1B_1C_1}$, Eq. (60), which by Eqs. (60) and (17) corresponds to the isometry

$$\Phi^{-1}(|V\rangle) = V_{\text{EPR}} = \sum_{i=0}^{D-1} |i\rangle_{B_1} \langle i|_{A_1}, \quad (63)$$

for a perfect quantum channel from $\mathcal{H}_{A_1}$ to $\mathcal{H}_{B_1}$, with quantum (and classical) channel capacity equal to $\log_2 D$. The subset information group contains every Pauli operator on qudit $A_1$, i.e. $\mathcal{G}_B = \langle \lambda I_{A_1}, X_{A_1}, Z_{A_1} \rangle$ as before, while the complementary channel $\mathcal{E}_C$ is the completely noisy or completely depolarizing channel whose subset information group is (multiples of) the identity, $\mathcal{G}_C = \langle \lambda I_{A_1} \rangle$. Therefore, attaching the state $|\text{EPR}\rangle_{B_2C_1}$ to that of the previous example increases the dimension of the output Hilbert space while leaving the $\mathcal{H}_A$ to $\mathcal{H}_B$ channel unchanged. This is not surprising, since the $|\text{EPR}\rangle_{B_2C_1}$ part has nothing to do with the input Hilbert space $\mathcal{H}_A$.

As a third example, the multipartite $|\text{GHZ}\rangle$ state from Eq. (13)

$$|V\rangle = |\text{GHZ}\rangle_{A_1B_1C_1} = \frac{1}{\sqrt{D}} \sum_{i=0}^{D-1} |i\rangle_{A_1} |i\rangle_{B_1} |i\rangle_{C_1}, \quad (64)$$

carried by the inverse map in Eq. (34) to the isometry

$$\Phi^{-1}(|V\rangle) = V_{\text{GHZ}} = \sum_{i=0}^{D-1} |i\rangle_{B_1} |i\rangle_{C_1} \langle i|_{A_1}, \quad (65)$$

In this case, $\mathcal{E}_B$ and $\mathcal{E}_C$ are perfectly decohering channels whose Kraus representation is

$$\mathcal{E}_B(\rho) = \mathcal{E}_C(\rho) = \sum_{i=0}^{D-1} |i\rangle\langle i| \rho |i\rangle\langle i|, \quad (66)$$

generalizing the qubit phase-flip channel (see Chap. 8 of [3]) to arbitrary $D$. The quantum channel capacity is zero while the classical channel capacity is $\log_2 D$. The subset information groups for both channels are identical: $\mathcal{G}_B = \mathcal{G}_C = \langle \lambda I_{A_1}, Z_{A_1} \rangle$. 


The following theorem states that the isometry of any stabilizer code with a bipartition defined on the output qudits is equivalent to a tensor product of isometries of the form $V_{EPR}$ and $V_{GHZ}$. See Figure 2 for an example of a decomposition of an isometry of a $[[7, 3]]_D$ stabilizer code with $n_B = 3$ and $n_C = 4$.

**Theorem 9.** (Tensor product structure of stabilizer code isometries) For prime $D$, let $V : \mathcal{H}_A \rightarrow \mathcal{H}_B \otimes \mathcal{H}_C$ be an isometry corresponding to an $[[n, k]]_D$ stabilizer code with a $B$-$C$ bipartition of the $n$ output qudits. Then up to unitaries $U_A, U_B, U_C$ on $\mathcal{H}_A, \mathcal{H}_B$ and $\mathcal{H}_C$, $V$ is a tensor product,

$$U_B U_C V U_A = V_{GHZ}^{m_{ABC}} \otimes V_{EPR}^{m_{AB}} \otimes V_{EPR}^{m_{AC}},$$

where $m_{ABC}, m_{AB}, m_{AC}, m_{BC}, m_B, m_C$ are non-negative integers, and $V_{EPR}$ and $V_{GHZ}$ are defined in Eqs. (63) and (65).

**Proof.** Use Lemma 8 to map the stabilizer code isometry $V$ to a stabilizer state $\Phi(V) = |V\rangle$ on $k + n$ qudits. Use Theorem 7 to express the result, up to local unitaries, in the form given in Eq. (27). Apply to this the inverse map $\Phi^{-1}$, noting that unitaries can be pulled outside, as shown in Eq. (45). \qed

An immediate corollary is that stabilizer code channels, up to unitaries on the input and output spaces, are always tensor products of just three types of simple channel: (i) Perfect quantum channel, (ii) Perfectly decohering or phase-flip channel, (iii) Completely noisy or completely depolarizing channel. This determines the quantum and classical capacities since, e.g., the quantum capacity of $\mathcal{E}_B$ is just the number of EPR pairs that can be extracted from the $A$-$B$ bipartition of $|V\rangle$ multiplied by $\log_2 D$, while the classical capacity is the quantum capacity plus the number of GHZ states linking $A$, $B$, and $C$.

Hence it follows that if $\mathcal{E}$ is a stabilizer code channel and its classical and quantum channel capacities are known, then one can deduce the decomposition of the isometry as in Eq. (67) and Figure 2 since the dimension of the input is known. From here it is straightforward to work out the classical and quantum channel capacities of the complementary channel.

**D. Duality of Subset Information Groups, $\mathcal{G}_B$ and $\mathcal{G}_C$**

Here we shall demonstrate how the tensor product structure of stabilizer code channels enables us to easily determine the subset information groups, $\mathcal{G}_B$ and $\mathcal{G}_C$. We also prove a duality relation between the $\mathcal{G}_B$ and $\mathcal{G}_C$ which implies that each of them is determined by the other.

Recall that the subset information groups $\mathcal{G}_B$ and $\mathcal{G}_C$ are subgroups of the Pauli group $\mathcal{P}_k$ on the $k$ input qudits, and that the centralizer $\text{Cent}_G(A)$ of any subset $A$ of elements of a group $G$ consists of all elements of $G$ that commute with every member of $A$.

**Theorem 10.** For $D$ prime, let $V : \mathcal{H}_A \rightarrow \mathcal{H}_B \otimes \mathcal{H}_C$ be an isometry corresponding to an $[[n, k]]_D$ stabilizer code, with $\mathcal{P}_k$ the Pauli group on the input qudits. Assume a $B$-$C$ bipartition of the $n$ output qudits is defined, with $\mathcal{G}_B$ and $\mathcal{G}_C$ the corresponding subset information groups as defined in Eq. (61) and its counterpart with $C$ replaced with $B$, for the stabilizer code channels $\mathcal{E}_B$ and $\mathcal{E}_C$.

Then $\mathcal{G}_B$ and $\mathcal{G}_C$ are dual in the sense that

$$\mathcal{G}_B = \text{Cent}_{\mathcal{P}_k}(\mathcal{G}_C) \quad \text{and} \quad \mathcal{G}_C = \text{Cent}_{\mathcal{P}_k}(\mathcal{G}_B),$$

i.e., each is the centralizer of the other in the group $\mathcal{P}_k$.

**Proof.** First we show that the duality relation holds for $V_{EPR}$ and for $V_{GHZ}$, as defined in Eqs. (63) and (65) respectively. For $V_{EPR}^{A_1 \rightarrow B_1}$, we have $\mathcal{G}_B = \langle \lambda I_{A_1}, X_{A_1}, Z_{A_1} \rangle$ from the previous subsection. The complementary channel is $\mathcal{E}_C(p) = \text{Tr}_B[V_{EPR}^{B_1 \rightarrow C_1} V_{EPR}^{A_1 \rightarrow B_1}^\dagger] = \text{Tr}_B(p)$, and by Eq. (61) we have $\mathcal{G}_C = \langle \lambda I_{A_1} \rangle$. Thus $\mathcal{G}_B$ is the full Pauli group, and $\mathcal{G}_C$ consists of multiples of the identity, so they are centralizers of each other in the Pauli group on qudit $A_1$. Next, for the isometry $V_{GHZ}^{A_1 \rightarrow B_1}$, we have $\mathcal{G}_B = \mathcal{G}_C = \langle \lambda I_{A_1}, Z_{A_1} \rangle$ and again the duality is satisfied.

But Theorem 9 says that $V$ is equivalent up to local unitaries to tensor products of these two types of elementary isometries, where we ignore the single-qudits states on $B$, $C$ and the EPR pairs between parts $B$ and $C$ as they are not involved in the transmission of information. It is straightforward to show that since the Pauli group for part $A$ and the information groups are themselves tensor products, the latter are again centralizers of each other. Since the duality is invariant under conjugation by unitaries, the local unitaries play no role. \qed

Here is an illustrative example. Suppose that

$$V = V_{EPR}^{A_1 \rightarrow B_1} \otimes V_{EPR}^{A_2 \rightarrow C_1} \otimes V_{GHZ}^{A_3 \rightarrow B_2 C_2}.$$ (69)
Then the subset information groups have the same tensor products structure as the isometries above
\[
G_B = \langle \lambda I \rangle \otimes \langle X_{A_1}, Z_{A_1} \rangle \otimes \langle I_{A_2} \rangle \otimes \langle Z_{A_3} \rangle \\
= \langle \lambda I, X_{A_1}, Z_{A_1}, Z_{A_3} \rangle, \\
G_C = \langle \lambda I \rangle \otimes \langle I_{A_1} \rangle \otimes \langle X_{A_2}, Z_{A_2} \rangle \otimes \langle Z_{A_3} \rangle \\
= \langle \lambda I, X_{A_2}, Z_{A_2}, Z_{A_3} \rangle. 
\]

(70)

While the results presented in this section only hold for stabilizer code isometries, we now show that they can sometimes be used to derive bounds for more general isometries \(V\), with channels \(E_B\) and \(E_C\) defined as in Eq. (69) for some bipartition of the output qubits. Given a general coding space \(V\), one can ask if there are stabilizer subspaces or subcodes contained in \(V\). If these subcodes are not one-dimensional subspaces, then meaningful lower bounds on channel capacities can be calculated for \(E_B^c\) and \(E_C^c\).

For example consider the nonadditive (or non-stabilizer) qubit graph code denoted by \((5, 6, 2)\), mentioned in [15] and [25]. (It was first described in [26], but not using the graph code formalism.) Also assume the following bipartition of the five output qubits, \(B = \{1, 2\}\) and \(C = \{3, 4, 5\}\). The six-dimensional coding space is spanned by
\[
\begin{align*}
V &= \text{span}\{ |G\rangle, Z_1 Z_2 Z_4 |G\rangle, Z_2 Z_3 Z_5 |G\rangle, \\
&\quad Z_1 Z_3 Z_4 |G\rangle, Z_2 Z_4 Z_5 |G\rangle, Z_1 Z_2 Z_5 |G\rangle \}
\end{align*}
\]

(71)

where \(|G\rangle\) is a five-qubit graph code stabilized by the group \(\langle X_1 Z_2 Z_5, X_1 X_2 Z_3, Z_2 X_3 Z_4, Z_3 X_4 Z_5, Z_1 Z_4 X_5 \rangle\) and the corresponding graph is a pentagon [13].

Obviously, \(V\) contains the two-dimensional stabilizer subcode \(\mathcal{V}_0 \subset V\),
\[
\mathcal{V}_0 = \text{span}\{ |G\rangle, Z_1 Z_2 Z_4 |G\rangle \}
\]

(72)

By applying the techniques used in proving Lemma 5 and Theorem 7 one can show that \(\mathcal{V}_0\) corresponds to a one qubit quantum channel from \(A\) to \(C\), which means that the quantum channel capacity of \(E_C\) is greater or equal to \(\log_2(2)\). Similarly, by considering the subcode
\[
\mathcal{V}_1 = \text{span}\{ |G\rangle, Z_2 Z_3 Z_5 |G\rangle \}
\]

(73)

one can identify a GHZ state in the corresponding tripartition, and thus deduce that the classical channel capacity of \(E_B^c\) and of \(E_C^c\) is at least \(\log_2(2)\).

Working from the other direction, one can also consider stabilizer codes that contain \(V\) as a subcode. Provided these stabilizer codes are not the whole Hilbert space, useful upper bounds on channel capacities of \(E_B\) and \(E_C\) can be calculated.

VI. CONCLUSION

The most important results of our paper are those in Corollary 5, Theorem 7, and Theorem 9. The first of these allows stabilizer states for composite \(D\) to be expressed as tensor products of stabilizer states associated with the different prime factors of \(D\). This is a valuable technical tool used later in the paper, but also a helpful conceptual tool as it allows more complicated cases to be “pulled apart” into simpler situations. For example, a graph state for \(D = 6\) can be regarded as the tensor product of \(D = 2\) and \(D = 3\) graph states.

Our main result, Theorem 7 that a tripartite stabilizer state can be considered the tensor product of single-qubit states, two-qubit EPR pairs and three-qubit GHZ states, generalizes the \(D = 2\) (qubit) result in [2] to any squarefree \(D > 2\). This allows us to provide a very simple and essentially complete characterization, Theorem 9 up to unitaries on the input and output, of channels constructed from stabilizer quantum codes. Knowledge of the information carrying properties of such a channel leads immediately tells one the properties of the complementary channel, and there is a simple relationship between the corresponding subset information groups introduced in [10]. In some cases one can use these results to put bounds on capacities of other types of channel.

There are various directions in which one might hope to extend these results. We have encountered technical difficulties in attempting to generalize our tripartition theorem from squarefree to arbitrary composite \(D\), where it may no longer be true. It follows from Corollary 5 that it is sufficient to resolve the situation in which \(D\) is a prime power, so if that could be solved one could have results that apply for general \(D\). Can any of our results be extended beyond the narrow confines of stabilizer states? The fact that the proofs depend heavily on group-theoretical properties makes this seem unlikely, but it would certainly be of interest to understand what it is that makes stabilizer states so special, and stabilizer quantum codes so useful.

Another possible direction is to move on from tripartitions to those involving four or more parts. Here the results in [2] for qubits suggest a situation that is distinctly more complicated than found for bipartitions and tripartitions, and \(D > 2\) is unlikely to be simpler. But it would still merit study.

Acknowledgments

The authors would like to thank Patrick Coles, Vlad Gheorghiu and Dan Stahlke for helpful comments on the manuscript. The research described here received support from the National Science Foundation through Grant No. PHY-0757251.

Appendix A: Proof of Theorem 4

Proof. It is crucial to first note that there are two different notions of tensor product used in the statement of the theorem and in this proof. The first and more
obvious notion is the tensor product of $n$ qudits, each of dimension $D$. The second notion is defined on the space of each qudit of dimension $D$, which is isomorphic to a tensor product of $m$ spaces on qudits of dimensions $d_1, d_2, \ldots, d_m$.

First of all, we show that Pauli operators on a single qudit of dimension $D$ are equivalent to tensor products of $m$ Pauli products on the constituent qudits. We will be relying primarily on the Chinese Remainder Theorem which states that there exists a ring isomorphism between $\mathbb{Z}_D$ and the tensor product of rings, $\mathbb{Z}_{d_1} \otimes \mathbb{Z}_{d_2} \cdots \otimes \mathbb{Z}_{d_m}$, whenever $D$ has the prime decomposition in Eq. (11).

For brevity it is sufficient to prove the theorem for the case of $D = d_1 d_2$ where $d_1 = p_1^\alpha$ and $d_2 = p_2^\beta \cdots p_m^\gamma$ because $d_2$ can subsequently be further decomposed by induction. The Chinese Remainder theorem isomorphism map, $\phi : \mathbb{Z}_D \rightarrow \mathbb{Z}_{d_1} \otimes \mathbb{Z}_{d_2}$ is defined as

$$\phi(a) = (\phi_1(a), \phi_2(a))$$

where

$$\phi_i(a) := a \mod d_i.$$  \hspace{1cm} (A1)

The inverse map $\phi^{-1} : \mathbb{Z}_{d_1} \otimes \mathbb{Z}_{d_2} \rightarrow \mathbb{Z}_D$ is given by

$$\phi^{-1}(a_1, a_2) := a_1 r_1 d_2 + a_2 r_2 d_1 \mod D$$

with $r_i := (D/d_i)\mod d_i$ being constants that depend only on $d_1, d_2$ and not inputs $a_1, a_2$. Note that $r_i$ is always coprime to $d_i$ for $i = 1, 2$.

Next we show the mapping $\phi$ induces a unitary transformation from a Hilbert space of dimension $D$ to a tensor product space of qudits of dimensions $d_1, d_2$. We define the action of the unitary $U : \mathcal{H}_D \rightarrow \mathcal{H}_{d_1} \otimes \mathcal{H}_{d_2}$ on the $D$-dimensional basis kets as

$$U(a) = |\phi_1(a)\rangle \otimes |\phi_2(a)\rangle$$

for $a = 0, 1, \ldots, D - 1$.  \hspace{1cm} (A2)

Next the $Z$ operator is transformed as

$$UZU^\dagger = \sum_{a=0}^{D-1} \omega^a|\phi_1(a)\rangle \langle \phi_1(a)| \otimes |\phi_2(a)\rangle \langle \phi_2(a)| = \sum_{a=0}^{d_1-1} \sum_{a_2=0}^{d_2-1} \omega^{a \delta_2} |a_1\rangle \langle a_1| \otimes |a_2\rangle \langle a_2|$$

with

$$\omega = e^{2\pi i / d}, \quad \delta_2 = n \mod d_2.$$  \hspace{1cm} (A3)

where $\delta_2$ is defined in Eq. (A3).

We are now ready to prove the theorem. Let $\mathcal{A}$ be generated by $k$ elements, $\mathcal{A} = \langle g^{(1)}, \ldots, g^{(k)} \rangle$ and the generators can always be chosen such that

$$\prod_{i=1}^{k} \text{order}(g^{(i)}) = |\mathcal{A}|.$$  \hspace{1cm} (A4)

Next we claim that

$$\text{order}(g_1) = \delta_1 \quad \text{and} \quad \text{order}(g_2) = \delta_2$$

To prove this, recall that $\langle g^{(i)} \rangle^{\delta_1 \delta_2} = I$ which implies $q^{\delta_1 \delta_2} \preceq I$. Since $\delta_2$ is coprime to $\delta_1$ and also to $d_1$, the unique multiplicative inverse of $\delta_2 \mod d_1$ exists. Then it follows that $q^{\delta_1 \delta_2 \delta_2^{-1}} = q^{\delta_1} \preceq I$. Therefore, the order of $q_1$ must be a divisor of $\delta_1$ and by the same reasoning, the order of $q_2$ must be a divisor of $\delta_2$. The orders cannot be less than $\delta_1, \delta_2$ respectively as that would imply the order of $g^{(i)}$ is less than $\delta$.

Having proven Eq. (A3), we define Pauli products of qudits of dimension $d_1$ and $d_2$, $h_1^{(i)}$ and $h_2^{(i)}$ respectively as

$$I_1 \otimes h_2^{(i)} := (Ug^{(i)}U^\dagger)^{\mu_2 \delta_2},$$

$$h_1^{(i)} \otimes I_2 := (Ug^{(i)}U^\dagger)^{\mu_1 \delta_1}.$$  \hspace{1cm} (A5)
where $\mu_i := (\delta/\delta_i)^{-1} \mod \delta_i$. Next for all $\alpha_1 \in \mathbb{Z}_{d_1}$ and $\alpha_2 \in \mathbb{Z}_{d_2}$, we can rewrite Eq. (A10) as

$$
(h^{(i)}_1)^{\alpha_1} \otimes (h^{(i)}_2)^{\alpha_2} = (U_g^{(i)}U_1)^{\alpha_1 \mu_1 + \alpha_2 \mu_2}. \tag{A11}
$$

Observe that the exponent on the right side is just the inverse Chinese Remainder map of $\alpha_1$ and $\alpha_2$ in Eq. (A3) applied to this situation, so

$$
\left\langle U_g^{(i)}U_1 \right\rangle = (h^{(i)}_1) \otimes (h^{(i)}_2). \tag{A12}
$$

Decomposing every generator into two generators on subsystems of dimensions $d_1$ and $d_2$ gives us

$$
U A U^\dagger = \left\langle U_g^{(1)}U_1 \right\rangle, \ldots, \left\langle U_g^{(k)}U_1 \right\rangle
$$

$$
= \left(h^{(1)}_1, \ldots, h^{(k)}_1 \right) \otimes \left(h^{(1)}_2, \ldots, h^{(k)}_2 \right)
$$

$$
= \mathcal{A}_1 \otimes \mathcal{A}_2. \tag{A13}
$$

That $\mathcal{A}_1 = \langle h^{(1)}_1, \ldots, h^{(k)}_1 \rangle$ and $\mathcal{A}_2 = \langle h^{(1)}_2, \ldots, h^{(k)}_2 \rangle$ form collections of mutually commuting Pauli products are consequences of the fact that $\{g^{(i)}\}$ are mutually commuting and that conjugation by $U$ does not change the commutation relation. Finally, Eq. (A13) also tells us there are as many linearly independent elements in $\mathcal{A}$ as there are in $\mathcal{A}_1 \otimes \mathcal{A}_2$, which implies that $|\mathcal{A}| = |\mathcal{A}_1| \cdot |\mathcal{A}_2|$.

[1] M. B. Plenio and S. Virmani, Quant. Inf. Comp. 7, 1 (2007), arXiv:quant-ph/0504163.
[2] S. Bravyi, D. Temme, and D. Gottesman, J. Math. Phys. 47, 062106 (2006), e-print arXiv:quant-ph/0504208.
[3] D. Gottesman, Phys. Rev. A 54, 1862 (1996).
[4] D. Gottesman, Stabilizer codes and quantum error correction, e-print arXiv:quant-ph/9705052.
[5] M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information (Cambridge University Press, Cambridge, 2000), 5th ed.
[6] E. Knill, Non-binary unitary error bases and quantum codes, e-print arXiv:quant-ph/9608048.
[7] A. Ashikhmin and E. Knill, Nonbinary quantum stabilizer codes, e-print arXiv:quant-ph/0005008.
[8] R. Raussendorf, D. E. Browne, and H. J. Briegel, Phys. Rev. A 68, 022312 (2003).
[9] A. Kitaev, Annals of Physics 303, 2 (2003), arXiv:quant-ph/9707021.
[10] M. Van den Nest, J. Dehaene, and B. De Moor, Phys. Rev. A 72, 014307 (2005).
[11] M. Van den Nest, J. Dehaene, and B. De Moor, Phys. Rev. A 71, 062326 (2005).
[12] B. Zeng, H. Chung, A. W. Cross, and I. L. Chuang, Phys. Rev. A 75, 032325 (2007).
[13] V. Gheorghiu, S. Y. Looi, and R. B. Griffiths, Phys. Rev. A 81, 032326 (2010).
[14] C. Bény, A. Kempf, and D. W. Kribs, Phys. Rev. A 76, 042303 (2007).
[15] S. Y. Looi, L. Yu, V. Gheorghiu, and R. B. Griffiths, Phys. Rev. A 78, 042303 (2008).
[16] M. A. Nielsen, M. J. Bremner, J. L. Dodd, A. M. Childs, and C. M. Dawson, Phys. Rev. A 66, 022317 (2002).
[17] E. Hostens, J. Dehaene, and B. Moore, Phys. Rev. A 71, 042315 (2005).
[18] D. Fattal, T. S. Cubitt, Y. Yamamoto, S. Bravyi, and I. L. Chuang, Entanglement in the stabilizer formalism (2004), e-print arXiv:quant-ph/0406168.
[19] M. Grassl, A. Klappenecker, and M. Roetteler, Proceedings of IEEE ISIT 2002 p. 45 (2002), e-print arXiv:quant-ph/0703112.
[20] D. Schlingemann, Stabilizer codes can be realized as graph codes (2001), e-print arXiv:quant-ph/0111080.
[21] M. Hein, W. Dur, J. Eisert, R. Raussendorf, M. V. den Nest, and H. J. Briegel, Entanglement in graph states and its applications, e-print arXiv:quant-ph/0602096.
[22] M. Hein, J. Eisert, and H. J. Briegel, Phys. Rev. A 69, 062311 (2004).
[23] R. B. Griffiths, S. Wu, L. Yu, and S. M. Cohen, Phys. Rev. A 73, 052309 (2006).
[24] B. Yoshida and I. L. Chuang, Phys. Rev. A 81, 052302 (2010).
[25] M. Wilde and D. Fattal, Quantum Information Processing 9, 591 (2010).
[26] A. Cross, G. Smith, J. Smolin, and B. Zeng, Information Theory, IEEE Transactions on 55, 433 (2009), ISSN 0018-9448.
[27] E. M. Rains, R. H. Hardin, P. W. Shor, and N. J. A. Sloane, Phys. Rev. Lett. 79, 953 (1997).
[28] M. Choi, Linear Algebra Appl. 10, 285 (1975).
[29] A. Jamiołkowski, Reports on Mathematical Physics 3, 275 (1972).
[30] K. Życzkowski and I. Bengtsson, Open Syst. Inf. Dyn. 11, 3 (2004).
[31] P. Arrighi and C. Patricot, Annals of Phys. 311, 26 (2004), arXiv:quant-ph/0307024.
[32] Note that all elements of $S$ leave each element of the subspace $C$ unchanged. The larger subgroup that maps $C$ into itself without the requirement that each $|\psi\rangle$ in $C$ be mapped to itself could also be called its “stabilizer,” but we are not using “stabilizer” in this second sense.
[33] The idea goes back to Choi [28] and Jamiołkowski [29] and even earlier; see [30] for extensive references to the literature. The isomorphism is usually defined between quantum channels and bipartite density operators so technically our definition is just “half” of the standard form, see [23, 51].