Absolutely Maximally Entangled Qudit Graph States

Wolfram Helwig

Center for Quantum Information and Quantum Control (CQIQC),
Department of Physics, University of Toronto, Toronto, Ontario,
M5S 1A7, Canada

May 7, 2014

Abstract

Absolutely maximally entangled (AME) states are multipartite entangled states that are maximally entangled for any possible bipartition. In this paper, we study the description of AME states within the graph state formalism. The graphical representation provides an intuitive framework to visualize the entanglement in graph states, which makes them a natural candidate to describe AME states. We show two different methods of determining bipartite entanglement in graph states and use them to define various AME graph states. We further show that AME graph states exist for all number of parties, and that any AME graph states shared between an even number of parties can be used to describe quantum secret sharing schemes with a threshold or ramp access structure directly within the graph states formalism.

1 Introduction

Entanglement is one of the most valuable resources in quantum information processing. The more entangled states are, the more powerful are the operations that can be performed with them. However, for multipartite states, many different types of entanglement exist [1, 2, 3], and it is not always clear, which states are most suitable for a specific task.

One possibility of quantifying multipartite entanglement is to look at the bipartite entanglement the state possesses for various partitions of the parties into two sets. States that maximize this entanglement criterion are absolutely maximally entangled (AME) states [4, 5], which are states that are maximally entangled for every possible bipartition of the state. It was shown that these states exist for any number of parties if the system dimensions are chosen appropriately, and that they can be used for various quantum information tasks, like parallel teleportation of multiple states between arbitrary sets of parties, open-destination teleportation, and quantum secret sharing. Formally, there are different equivalent ways to ascertain that a state is absolutely maximally entangled. Which one to use often depends on the application under consideration.
Definition 1. An absolutely maximally entangled state is a pure state shared between \( n \) parties \( P = \{1, \ldots, n\} \), each having a system of dimension \( d \), so a state \( |\Phi\rangle \in \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n \) and \( \mathcal{H}_i \cong \mathbb{C}^d \), with the following equivalent properties:

(i) \( |\Phi\rangle \) is maximally entangled for any possible bipartition. This means that for any bipartition of \( P \) into disjoint sets \( A \) and \( B \) with \( A \cup B = P \) and, without loss of generality, \( m = |B| \leq |A| = n - m \), the state \( |\Phi\rangle \) can be written in the form

\[
|\Phi\rangle = \frac{1}{\sqrt{d^m}} \sum_{k \in \mathbb{Z}^m} |k_1\rangle_{B_1} \cdots |k_m\rangle_{B_m} |\phi(k)\rangle_A,
\]

with \( \langle \phi(k)|\phi(k') \rangle = \delta_{kk'} \).

(ii) The reduced density matrix of every subset of parties \( A \subset P \) with \( |A| \leq \frac{n}{2} \) is totally mixed.

(iii) The von Neumann entropy of every subset of parties \( A \subset P \) with \( |A| \leq \frac{n}{2} \) is maximal, \( S(A) = |A| \log d \).

We denote such a state as an \text{AME}(n, d)\) state. Note that to check if a state is absolutely maximally entangled, it suffices to check the maximal entanglement for all bipartitions with \( |A| = \lfloor \frac{n}{2} \rfloor \), as the maximal entanglement for smaller bipartitions follows immediately.

In this paper, we will use the graph state formalism to describe AME states. Graph states are a special class of stabilizer states, and have been introduced for qubits and qudits of prime dimension\[6, 7\]. They offer a nice graphical representation of multipartite entangled states and have found its use in a variety of quantum information applications, like quantum computing \[8\], error correction \[9, 10, 11, 12\], and quantum secret sharing \[13, 14\].

We will show two methods for checking bipartite entanglement in graph states. One makes use of the intuitive graphical representation of graph states, while the other one allows to efficiently check if a graph state is absolutely maximally entangled, even for high dimensional systems and a large number of parties – a task that is generally hard to accomplish in the Dirac notation, as it involves tracing over high-dimensional density matrices to verify the condition in Definition 1 (iii).

Examples of AME graph states will be given, among others a previously unknown AME states for seven qutrits that we were able to find in computer searches that used the efficient method to determine bipartite entanglement in graph states. Further, we will show how the method presented in Ref. \[5\] to construct graph states from classical codes can also be used to construct AME graph states for any number of parties. Given a certain graph state, it is straightforward to write down a quantum circuit, consisting of controlled-\( Z \) gates that produces the graph state. Thus this method will enable us to write down a quantum circuit that creates an AME state for any number of parties, and once a method exists to experimentally implement controlled qudit gates, the approach in this paper provides a straightforward way to experimentally create qudit AME states. At this point, graph states have been experimentally created for up to six qubits \[15, 16, 17, 18\].

2
Quantum secret sharing (QSS) with qudits has already been investigated before [13, 14]. However, only a few specific examples of graph states that can be used for QSS could be given, and the question which graph states are generally suitable for QSS has been left open. We answer this question by showing that all AME graph states shared between an even number of parties can be used to construct threshold QSS schemes [19], as well as for QSS schemes with a more general ramp access structure [20]. The connection between AME states and threshold QSS schemes has already been shown before [4, 5], the treatment here is to show that the derivation of QSS schemes from AME states can also be completely described within the graph state formalism. The results of Ref. [5] further show that AME graph states are the only graph states that result in threshold QSS schemes.

This paper is structured as follows. In Section 2 we introduce qudit graph states and their representation as stabilizer states. In Section 3 we show two different methods for checking the bipartite entanglement in graph states. Section 4 gives examples of AME states, which were found by using the methods presented in the previous section. We further show that AME graph states exist for any number of parties. In Section 5 we show how any AME state shared between even number of parties can be used to implement quantum secret sharing right within the graph state formalism. A short summary of the results and open question are provided in Section 6.

Notation: Throughout this paper, if the dimension of a system is denoted by \( p \), it is meant to be a prime number. If we use \( d \) for the dimension of a system, no constraints are imposed.

2 Qudit Graph States

2.1 Generalized Pauli Operators

The generalized Pauli operators \([21, 22, 23, 14]\) for qudits of dimension \( d \) are defined as

\[
Z |k\rangle = \omega^k |k\rangle, \\
X |k\rangle = |k + 1\rangle,
\]

where \( \omega = e^{2\pi i/d} \). Controlled gates are generalized straightforward, with the controlled-\( Z \) operator between qudit \( i \) and \( j \) being

\[
CZ_{ij} = \sum_{k=0}^{d-1} |k\rangle \langle k|_i \otimes Z^j_k = \sum_{k,l=0}^{d-1} \omega^{kl} |k\rangle \langle k|_i \otimes |l\rangle \langle l|_j
\]

It is easily seen that \( Z^d = X^d = CZ^d = \mathbb{1} \). Furthermore we have the commutation relation \( ZX = \omega XZ \). The Fourier gate

\[
F = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{kl} |k\rangle \langle l|,
\]

3
the generalization of the Hadamard gate, transforms between the $Z$-eigenbasis $|k\rangle$, and the $X$-eigenbasis $|\bar{k}\rangle$,

$$|\bar{k}\rangle = F^\dagger |k\rangle = \frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} \omega^{-kl} |l\rangle. \quad (6)$$

### 2.2 Graph States

We are now ready to define graph states for $n$ qudits of dimension $p$, where $p$ is a prime number. The qudits are graphically represented by vertices $V = \{v_i\}$, which are connected by edges $E = \{e_{ij} = \{v_i, v_j\}\}$. Each edge is assigned a weight $A_{ij} \in \mathbb{Z}_p$, where weight zero is equivalent to no edge. The weights $A_{ij}$ form the symmetric $n \times n$ adjacency matrix with $A_{ii} = 0$ that captures all the relevant information about the graph.

**Definition 2.** For a given graph $G$ with $n$ vertices and adjacency matrix $A \in \mathbb{Z}_p^{n \times n}$, where $p$ is prime, we define the corresponding graph state $|G\rangle \in \mathcal{H}^\otimes n$ as

$$|G\rangle = \prod_{i>j} CZ^{A_{ij}}_{ij} |\bar{0}\rangle^\otimes n. \quad (7)$$

We further define a labeled graph states by attaching an additional label $\mathbf{z} = (z_1, \ldots, z_n) \in \mathbb{Z}_p^n$ to the graph state $|G\rangle$ as

$$|G_\mathbf{z}\rangle = Z^\mathbf{z} |G\rangle, \quad (8)$$

Here and in the following we use the notation

$$Z^\mathbf{z} = Z^{z_1} \otimes Z^{z_2} \otimes \cdots \otimes Z^{z_n}. \quad (9)$$

A graph state can be constructed by a quantum circuit that first prepares all systems in the $|\bar{0}\rangle$ state, and then applies pairwise controlled-$Z$ gates between the systems according to the entries of the adjacency matrix.

### 2.3 Stabilizer States

Stabilizer states have first been introduced for qubits [24] and later generalized to qudits [25, 26]. The connection to qudit graph states has been made in Ref. [9, 7]. The **Pauli Group**, the group that is generated by the $X$ and $Z$ operators for qubits is defined as

$$G = \{ \alpha X^a Z^b; a, b \in \mathbb{Z}_2 \}, \quad (10)$$

with $\alpha \in \{1, -1, i, -i\}$, and its generalization for the qudit Pauli operators of Equations (2) and (3) is

$$G = \{ \omega^c X^a Z^b; a, b, c \in \mathbb{Z}_p \}, \quad (11)$$

with $\omega = e^{2\pi i/p}$. The Pauli group over $n$ qudits is the $n$-fold tensor product of $G$ and is denoted $G_n$.

The **stabilizer code** is defined as the common eigenspace for eigenvalue one of a subgroup $S$ of $G_n$. The stabilizer code is non-trivial if $S$ is abelian and
does not contain any scalar multiples of the identity, except for 1 itself. Given such a subgroup and a minimal set of generators, $g_i = \omega^{c_i} X^{a_i} Z^{b_i}$, for the group, $S = \langle g_1, \ldots, g_k \rangle$, the generator matrix is defined as

\[
M = \begin{pmatrix}
  a_1 & b_1 \\
  \vdots & \vdots \\
  a_k & b_k
\end{pmatrix}.
\]

(12)

The stabilizer code does not depend on the scalar coefficients $\omega^{c_i}$, and is thus fully specified by the generator matrix $M$. The fact that $S$ is abelian translates to $a_i \cdot b_j - b_i \cdot a_j = 0$ for two different rows of $M$. It has been shown in Ref. [7] that a stabilizer group $S$ with $k$ generators corresponds to a stabilizer code of dimension $n - k$. Thus if the minimal set of generators for $S$ is of size $n$, then the stabilizer code only contains one state, the stabilizer state to the generator matrix $M$.

A special class of stabilizer states are the above introduced graph states. Given the adjacency matrix $A$, a minimal set of generators for the stabilizer group is given by

\[
g_i = X_i \prod_j Z_j^{A_{ij}}.
\]

(13)

Here the indices label on which qudit the operator act. This means the generator matrix is simply given by

\[
M = (I | A)
\]

(14)

The Clifford group, the group of operators that maps the Pauli group onto itself, can also be generalized to qudits (for details on the generalized Clifford group, see Ref. [27]). The local Clifford group for a system of $n$ qudits is the $n$-fold tensor product of the Clifford group. The following lemma, which shows when two states can be transformed into each other by an element of the local Clifford group, is proved in Ref. [7].

**Lemma 3** (Lemma 6 of Ref. [7]). Two stabilizer states with generator matrices $A, B$ are equivalent under the action of the local Clifford group, if and only if there exist invertible matrices $U$ and $Y$, such that $B = UAY$, and $Y$ has the form

\[
Y = \begin{pmatrix}
  E & F \\
  E' & F'
\end{pmatrix},
\]

(15)

where

\[
E = \text{diag}(e_1, \ldots, e_n), \quad F = \text{diag}(f_1, \ldots, f_n)
\]

(16)

\[
E' = \text{diag}(e'_1, \ldots, e'_n), \quad F' = \text{diag}(f'_1, \ldots, f'_n)
\]

(17)

and $e_i f'_i = f_i e'_i = 1$ for all $i$.

It has been further shown that every stabilizer state is equivalent to a graph state under the action of the local Clifford group [7] [9] [10]. Thus if we want to consider possible entanglement properties of stabilizer states, it suffices to consider graph states, since for any stabilizer state there exists a graph state with the same entanglement properties.
3 Entanglement in Graph States

Now that we have introduced qudit graph states, the next question is, given a certain graph state, described by the adjacency matrix $A$ for $n$ qudits, how to determine the entanglement of the associated quantum state. Specifically, we are interested in the entanglement between bipartitions of the $n$ parties. If all these bipartitions are maximally entangled, the state is an absolutely maximally entangled state.

We present two different methods for checking the entanglement between bipartitions. The first uses the fact that the entanglement can be determined just by looking at the graph, if it is in the right form. The problem in this method is to bring the graph state into the right form for any bipartition. This is generally not so easy and thus we also present a second method that is computationally more helpful to actually determine the bipartite entanglement in graph states.

3.1 Graphical Representation

Recall that an edge of the graph represents the application of a controlled-Z gate. If a controlled-Z gate is applied between two qudits in the $|0\rangle$ state, they are maximally entangled. We say they share 1 “edit” of entanglement. For $n$ qudits, divided into two sets $A$ and $B$, the maximal amount of entanglement between the two sets is $\min(|A|,|B|)$ edits. This can, for instance, be achieved by preparing each qudit in the $|0\rangle$ state, and then applying controlled-Z gates between the qudits, such that each party of the smaller set is connected to a different party in the larger set. An example of a resulting graph for four qudits is depicted in Figure 1(a).

![Figure 1: Graph states for four qudits with maximal entanglement between the sets $A$ and $B$. The graph in (a) is the simplest graph that shows maximal entanglement between the sets $A$ and $B$. Adding edges within each set is only a local operation with regard to that bipartition and thus does change the entanglement properties between the sets. Thus all the shown graphs have the same amount of entanglement between $A$ and $B$.](image)

Applying the controlled-Z gate up to $p - 1$ times between two qudits also creates 1 edit of entanglement, thus we may assign any non-zero weight to the connecting edges, without changing the maximal entanglement. Furthermore, applying local unitary operations within each set after the entanglement between the sets has been created will not change the entanglement between these sets. Thus we may add as many edges with arbitrary weight as we like within each set, and the sets $A = \{1, 2\}$ and $B = \{3, 4\}$ will still remain maximally entangled.
This is demonstrated in the graphs in Figures 1(b) and 1(c), which are both still maximally entangled for the bipartition into the sets $A$ and $B$.

Checking the entanglement in these graphs between the sets $A$ and $B$ is easy, because we specifically constructed the state that way. The entanglement for the bipartition $\{1, 3\}/\{2, 4\}$ is also obvious, it is 0, 1, and 2 edits for the states in Figures 1(a), 1(b) and 1(c) respectively. However, the entanglement for a different bipartition, for example between $C = \{1, 4\}$ and $D = \{2, 3\}$ in the graph of Figure 1(c) is not immediately obvious. To determine the entanglement, we need a graph in which each party in $C$ is connected to at most one party in $D$ and vice versa. Then counting the number of connecting edges gives the number of edits shared between $C$ and $D$. Changes allowed on the graph are the ones that don’t change the entanglement properties of the graph, like the ones achieved by local Clifford operations as described in Lemma 3. For graph states this lemma can be restated as operations on the graph [7].

**Theorem 4** (Theorem 5 of Ref. [7]). Two graph states are equivalent under local Clifford operations if and only if one can be obtained from the other by a sequence of the two graph operations on a vertex $v$

$\odot_v$ The weight of each edge connected to the vertex $v$ is multiplied by $b$, where $0 \neq b \in \mathbb{Z}_p$.

$\ast_a v$ For $a \in \mathbb{Z}_p$, the entries of the adjacency matrix are transformed as $A_{jk} \rightarrow A_{jk} + aA_{v_j}A_{vk}$ for $j \neq k$.

A graphical representation of these operations, is given in Figures 1 and 2 of Ref. [7]. For qubits the $\odot$ operation is always the identity, and the $\ast$ operation for $a = 1$ is known as the local complementation. Returning to the question what the entanglement between sets $C = \{1, 4\}$ and $D = \{2, 3\}$ is in the graph of Figure 1(c) we can see that by applying the operations $(\ast_1 1, \ast_3 3, \ast_4 4)$, the graph is in fact local Clifford equivalent to the graph of Figure 1(b) with vertices 3 and 4 interchanged. Hence it shares only 1 edit of entanglement for the bipartition into sets $C = \{1, 4\}$ and $D = \{2, 3\}$, and therefore is not absolutely maximally entangled. Examples of states where this method confirms absolutely maximal entanglement will be given in Section 4.

### 3.2 Efficient Method

While the above presented method to determine bipartite entanglement is very intuitive, it is generally not easy to find the right graph operations to bring the graph into the right form for a given bipartition. Thus we will present a second method that makes it computationally relatively easy to check the bipartite entanglement for a given graph for an arbitrary bipartition. We will make use of the following notations

**Definition 5.** Let $|G\rangle$ be a graph state shared between a set of parties $P$. Then, for $K \subset P$, we define the truncated graph state $|G^{\backslash K}\rangle$, shared by $P \backslash K$, as the state that is represented by the graph $G$ with the vertices in $K$ and all edges that are connected to the parties in $K$ removed.

**Definition 6.** For an $n \times n$ adjacency matrix $A$, we denote the $i$th row of the matrix by $A_i$, so $A_i = (A_{i1}, \ldots, A_{in})$. Further for $K = \{k_1, k_2, \ldots, k_m\}$, with
\[ k_1, \ldots, k_m \] between 1 and \( n \), we define \( A_i \setminus K \) to be the vector \( A_i \) with the entries \( \{A_{ik_1}, \ldots, A_{ik_m}\} \) removed. For instance,
\[ A_i \setminus \{2, 6\} = (A_{i1}, A_{i3}, A_{i4}, A_{i5}, A_{i7}, \ldots, A_{im}). \] (18)

First note that a \( Z \)-measurement \( \dagger \) on the \( k \)th qudit of the graph
\[ |G\rangle = \prod_{i>j} CZ_{ij} \{ \langle 0 \rangle \}^\otimes n \]
\[ = \prod_{l \neq k} \sum_{m=0}^{p-1} |m\rangle \langle m|_k \otimes Z_{l}^m A_{k} \prod_{i>j, l \neq k} CZ_{ij} \{ \langle 0 \rangle \}^\otimes n, \] (19)
with measurement outcome \( a \) gives
\[ \langle a|G\rangle = \frac{1}{\sqrt{p}} \prod_{l \neq k} Z_{l}^a A_{k} \prod_{i>j, l \neq k} CZ_{ij} \{ \langle 0 \rangle \}^\otimes n-1 \]
\[ = \frac{1}{\sqrt{p}} |G_{aA_k \setminus \{k\}}\rangle. \] (22)

So this is a labeled graph state for the remaining \( n-1 \) qudit, with the label given by \( A_k \setminus \{k\} \) with each component multiplied by the measurement outcome \( a \). All measurement outcomes are equally likely, and given that \( A_k \setminus \{k\} \neq 0 \), meaning that the \( k \)th qudit in \( |G\rangle \) is connected by at least one edge, the label is different for each possible measurement outcome. Since labeled graph states with different labels are orthogonal, the measurement outcome can be deduced from \( G_{aA_k \setminus \{k\}} \). Hence qudit \( k \) is maximally entangled with the other \( n-1 \) qudits in \( |G\rangle \).

Similarly, if \( Z \)-measurements are performed on \( m \) qudits \( K = \{k_1, \ldots, k_m\} \), with measurement outcomes \( \{a_1, \ldots, a_m\} \), the resulting state is
\[ k_1,\ldots,k_m \langle a_1,\ldots,a_m|G\rangle = \frac{1}{\sqrt{p^m}} |G_{\sum_{i} a_i A_{k_i} \setminus K}\rangle. \] (23)
This again is a labeled graph state with the measured qudits and associated edges removed, and the \( Z \) operations applied for each measurement independently, because \( Z \) measurements and \( Z \) operators commute. Note that \( Z \) operations on qudits in \( K \) only contribute as a global phase, which we have omitted.

If the label is different for each different possible combination of measurement outcomes \( \{a_1, \ldots, a_m\} \), the resulting labeled graph states are all orthogonal and the remaining parties can determine the measurement outcome. Thus the parties in \( K \) share \( m \) edits of entanglement with the other \( n-m \) parties. The labels are all different if and only if the \( m \) vectors \( A_{k_i} \setminus \{k_1, \ldots, k_m\} \) are linearly independent in \( \mathbb{Z}_p^{n-m} \). Thus we have the following theorem:

**Theorem 7.** A graph state with adjacency matrix \( A \) is absolutely maximally entangled, if and only if for all sets \( K = \{k_1, \ldots, k_m\} \) of size \( m = \left\lfloor \frac{n}{2} \right\rfloor \), the vectors \( A_{k_i} \setminus K \) are linearly independent in \( \mathbb{Z}_p^{n-m} \). Here \( A_{k_i} \setminus K \) denotes the \( k_i \)th row of the adjacency matrix with the entries \( \{A_{k_i k_1}, \ldots, A_{k_i k_m}\} \) removed.\footnote{\( Z \) is not technically an observable, what we mean by a \( Z \)-measurement is a projection onto the eigenstates with (complex) eigenvalues \( \omega^k \). For simplicity we then call the measurement result \( k \).}
As a concrete example, we take a look at the graph of Figure 1(c) again and use this method to determine if it is absolutely maximally entangled. For the bipartition into the sets $K = \{1, 2\}$ and $L = \{3, 4\}$, we get the two vectors $A_1 \{1, 2\} = (1, 0)$ and $A_2 \{1, 2\} = (0, 1)$. These are independent and thus we have maximal entanglement between the sets $K$ and $L$. We get the same vectors for the bipartition $\{1, 3\}/\{2, 4\}$, so we also have maximal entanglement there. However, for the bipartition into $C = \{1, 4\}$ and $D = \{2, 3\}$, we get the vectors $A_1 \{1, 4\} = (1, 1)$ and $A_4 \{1, 4\} = (1, 1)$. These are not independent and thus we do not have maximal entanglement for this bipartition. Since their is only one independent vector, this bipartition shares 1 edit of entanglement.

## 4 Absolutely Maximally Entangled Graph States

### 4.1 Qubits, Qutrits, and Beyond

It is known [4, 5] that for qubits there exist absolutely maximally entangled states for 2, 3, 5 and 6 qubits. In all these cases, we can also find absolutely maximally entangled graph states. They are given in Figure 2. The ones for two and three qubits are the well Einstein-Podolsky-Rosen (EPR) pair and the Greenberger-Horne-Zeilinger (GHZ) state, respectively. The AME states in Figures 2(c) and 2(d) for five and six qubits can be used for quantum secret sharing protocols [13], as will also be discussed in the next section. We also included a second graph for six qubits in Figure 2(e), which illustrates the maximal entanglement for the bipartition $\{1, 2, 3\}/\{4, 5, 6\}$, when using the graphical method to check for maximal entanglement. This is also the representation with the least number of edges and it is locally Clifford equivalent (related by a $\ast_{1V}$ operation) to the one in Figure 2(d).

For four and more than eight qubits no AME states exist. For seven qubits no AME states are known, and an exhaustive search of all seven qubit graph states showed that no seven qubit AME graph state exists. Increasing the system dimension, however, can can help us to find AME states for scenarios where no qubit AME states exist. The reason for that is that with higher system dimension $p$, the graph can have $p - 1$ different types of weighted edges. This exponential growth of possible graphs results in a greater variety of entanglement properties, which allows to construct more graphs that are absolutely maximally entangled.

The first time we see that is for four qudits. If we only consider graphs with edges of weight one, which are the only ones available for qubits, the graph with the most amount of entanglement we can construct is the one in Figure 1(c). This graph is maximally entangled for two of the three possible bipartition, but not for the third as discussed in the last section. Hence we have to consider graphs that have edges with higher weights, for instance the graph state shown in Figure 3(a) where we have assigned the weight 2 to one of the four edges. This graph is obviously still maximally entangled for the $\{1, 2\}/\{3, 4\}$ and $\{1, 3\}/\{2, 4\}$ bipartitions. To check the entanglement for the $C = \{1, 4\}/D = \{2, 3\}$ bipartition with the graphical method, we have to perform the operations ($\ast_{1V}$, $\ast_{3V}$, $\ast_{2V}$) to obtain the graph shown in Figure 3(b) from which we see that the $C/D$ bipartition is also maximally entangled. Likewise, we could have considered the two vectors $A_1 \{1, 4\} = (1, 1)$ and $A_4 \{1, 4\} = (2, 1)$, to see that
Figure 2: Absolutely maximally entangled qubit graph states exist for two, three, five and six systems. The two qubit state is locally equivalent to an EPR pair and the three qubit state to a GHZ state. The five qubit AME state finds application in the five qubit code and quantum secret sharing. The six qubit state in Figure 2(d) emphasizes the connection to the five qubit state, while the locally equivalent state of Figure 2(e) nicely demonstrates the maximal entanglement.

they are linearly independent in $\mathbb{Z}_3$. Hence we have just confirmed that this graph is maximally entangled for four qutrits.

By doing a computer search over highly entangled seven qutrit states, the efficient method of Section 3.2 for checking bipartite entanglement in graph states allowed us to find an AME(7, 3) graph state. It is displayed in Figure 4.

These examples nicely illustrate that by increasing the system dimension, more AME graph states can be found due to the increased number of graph configurations.

Another nice property of the AME graph states is that the same graph state often works for more than one dimension. For instance the qubit graph states of Figure 2 are AME states for any prime dimension, because if a set of vectors is independent in $\mathbb{Z}_2$, they are also independent in $\mathbb{Z}_p$. Also the graph state in Figure 3(a) is an AME state for any prime dimension $p \geq 3$, because the vectors $(1, 1)$ and $(2, 1)$ are independent in all $\mathbb{Z}_p^2$ for $p \geq 3$. However, it is not always the case that AME graph states generalize to all higher prime dimensions. A counter-example is given in Figure 5 which shows a graph state that is absolutely maximally entangled for $p = 5$, but not for $p = 7$ because for the bipartition $\{1, 4\}/\{2, 3\}$, we have to check the two vectors $(2, 3)$ and $(3, 1)$ for independence, and these two vectors are independent in $\mathbb{Z}_5^2$, but not in $\mathbb{Z}_7^2$. 
Figure 3: Absolutely maximally entangled graph states for four qutrits. The first one demonstrates the maximal entanglement for the bipartitions \{1, 2\}/\{3, 4\} and \{1, 3\}/\{2, 4\}. The second graph is locally Clifford equivalent to the first and shows the maximal entanglement for the bipartition \{1, 4\}/\{2, 3\}.

Figure 4: AME(7, 3) graph state. The use of double edges allows us to find an AME graph state for seven qutrits, while no such graph state exists for qubits.

4.2 AME Graph States from Classical Codes

By now we have seen AME graph states for systems with up to seven parties. In Ref. [5], it was shown that AME states can be constructed from classical error correction codes and that linear codes of the required form exist for any number of parties if the dimension of the systems is chosen appropriately. A linear code \(C\), which encodes \(k\) dits of information into \(n\) dits, is described by a generator matrix \(G\) such that the codewords \(c \in C\) are given by \(Gx\) for \(x \in \mathbb{Z}_p^k\). An equivalent description of a linear code as the kernel of the parity check matrix \(H\). For every linear code \(C\) one can define a parity check matrix \(H : \mathbb{Z}_p^n \rightarrow \mathbb{Z}_p^{n-k}\) such that \(c \in C\) if and only if \(Hc = 0\). From \(HGx = 0\), it follows that the rows of \(H\) are orthogonal to the columns of \(G\).

The Hamming distance between two codewords is defined as the number of

Figure 5: An AME state for one dimension is not necessarily a graph state for a higher dimension. For instance, this graph states is absolutely maximally entangled for four qudits of dimension 5, but not for qudits of dimension 7.
positions at which the codewords differ. The minimal distance \( \delta \) of a code is the minimum Hamming distance between any two codewords. The larger \( \delta \), the more robust the encoding is against errors. The minimal distance is bounded by the Singleton bound, \( \delta \leq n - k + 1 \) \([28, 29]\). Codes that satisfy the Singleton bound are called maximum distance separable (MDS) codes.

A MDS code with the properties \( n = 2k, \delta = k + 1 \) can be used to construct an AME state. The AME state is then given by \([5]\).

\[
|AME\rangle = \frac{1}{\sqrt{d^k}} \sum_{x \in \mathbb{Z}_p^k} |Gx\rangle.
\]

(24)

Note that

\[
X^y |AME\rangle = \frac{1}{\sqrt{d^k}} \sum_{x \in \mathbb{Z}_p^k} |Gx + Gy\rangle
\]

(25)

\[
= \frac{1}{\sqrt{d^k}} \sum_{x \in \mathbb{Z}_p^k} |Gx\rangle
\]

(26)

\[
= |AME\rangle,
\]

(27)

where we have used that \( C \) is a linear code and the sum goes over all codewords of the code. Thus adding the same codeword to all other codewords is just a relabeling of the terms in the sum. Thus \( X^y \) is a stabilizer to the AME state for all \( y \in \mathbb{Z}_p^k \). Another set of stabilizers can be constructed from the \( Z \)-Operators. The action of a tensor product of \( Z \)-operators on the AME state is given by

\[
Z^y |AME\rangle = \frac{1}{\sqrt{d^k}} \sum_{x \in \mathbb{Z}_p^k} \omega^{x^T Gx} |Gx\rangle.
\]

(28)

Thus \( Z^y \) is a stabilizer for the AME state if \( y \) is a linear combination of rows of the parity check matrix \( H \), \( y^T = z^T H \). This gives us a full set of stabilizers that we can describe by the generator matrix

\[
M = \left( \begin{array}{cc} G^T & 0 \\ 0 & H \end{array} \right).
\]

(29)

It is easy to see that all the generators are independent, since the columns of \( G \) and rows of \( H \) are linearly independent. They are also abelian as they satisfy \( a_i \cdot b_j - b_j \cdot a_i = 0 \) because the rows of \( H \) are orthogonal to the columns of \( G \). Thus \( M \) is a proper generator matrix to the stabilizer state \( |AME\rangle \). Given the generator matrix \( M \), the AME state can now be transformed into a graph state by local Clifford operations that change the generator matrix according to Lemma \([3, 7]\).

The whole procedure of constructing an AME graph state from an MDS code is illustrated in the following example for the \([4, 2, 3]_3 \) ternary Hamming code that results in an AME\((4, 3) \) graph state.

Example 8. The generator matrix for the \([4, 2, 3]_3 \) ternary Hamming code \( C \) is given by

\[
G = \left( \begin{array}{cc} 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 2 & 1 \end{array} \right).
\]

(30)
and the parity check matrix by \( H = G^T \) (\( C \) is a self-dual code). Thus the generator matrix for the AME state \(|\text{AME}\rangle = \frac{1}{4} \sum_{c \in C} |c\rangle\) is

\[
M = \begin{pmatrix}
1 & 0 & 1 & 2 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 1 & 2 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 1
\end{pmatrix}
\]

(31)

Now we have to choose the matrices \( U \) and \( Y \) of Lemma 3 such that \( UMY \) is the identity matrix in the first block. For that note that by choosing \( f_i = 0 \) and \( e_i = f'_i = 1 \), the condition for \( Y \) is satisfied for arbitrary \( e'_i \). The effect of the value \( e'_i \) is to add the \( i \)th column of the second block to the \( i \)th column of the first block. We want to choose them such that the first block has full rank, which is accomplished by \( e_1 = e_2 = 0 \) and \( e_3 = e_4 = 1 \). This transforms the generator matrix to

\[
M \rightarrow MY = \begin{pmatrix}
1 & 0 & 1 & 2 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 2 & 1 & 0 & 1 & 2 \\
0 & 0 & 1 & 1 & 0 & 1 & 1 & 1
\end{pmatrix}
\]

(32)

Then we have to choose \( U \) such that it transforms the first block into the identity. This is achieved by

\[
U = \begin{pmatrix}
1 & 0 & 2 & 0 \\
0 & 1 & 0 & 2 \\
0 & 0 & 2 & 2 \\
0 & 0 & 1 & 2
\end{pmatrix}
\]

(33)

which results in the generator matrix

\[
M \rightarrow UMY = \begin{pmatrix}
1 & 0 & 0 & 0 & 2 & 0 & 2 & 1 \\
0 & 1 & 0 & 0 & 2 & 2 & 2 \\
0 & 0 & 1 & 2 & 2 & 1 & 0 \\
0 & 0 & 0 & 1 & 1 & 2 & 0 & 1
\end{pmatrix}
\]

(34)

This generator matrix has the desired form except for the entries on the diagonal of the second block, which may be transformed to zero by an additional application of a \( Y \) matrix with \( e'_i = 0 \), \( e_i = f'_i = 1 \), and \((e_1, e_2, e_3, e_4) = (1, 1, 2, 2)\). Thus we arrived at the graph state shown in Figure 6 which is an absolutely maximally entangled graph state for four qutrits.

![Figure 6: AME(4,3) graph state constructed from the [4,2,3] ternary Hamming code](image)

Notice that the procedure of constructing a stabilizer state from classical codes is reminiscent of the construction of Calderbank-Shor-Steane (CSS) codes \[30, 31\]. In fact we may interpret the AME states that are constructed in this form as one-dimensional generalized CSS codes \( \text{CSS}_p(C, C') \).
4.3 Non-prime dimensions

So far all we considered were scenarios where the parties shared systems of prime dimension. This was because although the initial definition of graph states in terms of controlled-$Z$ gates applied to qudits in the $|0\rangle$ state works for any dimension, the following treatment in terms of stabilizers does not. This includes, in particular, the methods we derived to check the entanglement of graph states in Section 3. In reality, however, we might have to deal with systems that are not of prime dimension, so how can we still describe them while taking advantage of the tools the graph state formalism provides us with for prime dimensions?

The answer is, we take the prime factorization for the system dimension $d = p_1 \cdot p_2 \cdots p_m$ and look for AME states for $p_1, \ldots, p_m$ independently, and if we have an AME state for each of the prime factors, then we can just construct an AME state for $d$ by taking the tensor product of the $m$ AME states and assigning one qudit of each AME state to each of the parties. In this way, we can, for instance, construct AME states for any dimension for the number of parties $n = 2, 3, 5, 6$, since the known qubit AME graph states work for any dimensions. Likewise, we can construct a four qudit AME state for any uneven dimension, since the AME graph state of Figure 3(a) generalizes to all prime dimensions $p \geq 3$.

Furthermore, if two or more of the prime factors are the same, for instance for $d = 4 = 2 \cdot 2$, we may apply controlled-$Z$ operations between one qubit of one party and either qubit of the other parties. This is best illustrated in an example. Imagine we want to find an AME(4, 4) state. It is not possible to simply take two AME(4, 2) states, because they do not exist. We can, however, consider each 4-dimensional systems as consisting of two qubits and construct the graph state shown in Figure 7 for eight qubits. This state is maximally entangled with 4 ebits (=2 edits) of entanglement for the bipartitions $\{P_1, P_2\}/\{P_3, P_4\}$, $\{P_1, P_3\}/\{P_2, P_4\}$ and $\{P_1, P_4\}/\{P_2, P_3\}$. Thus this graph state describes an AME(4, 4) state. Note that this state is generally not maximally entangled for bipartitions where we split up the two qubits belonging to one party, and is thus not an AME(8, 2) state (which does not exist).

![Figure 7](image)

Figure 7: By grouping qudits together, we can construct AME graph states for non-prime dimensions. This figure shows eight qudits that are grouped into four 4-dimensional systems to form an AME(4, 4) graph state. This, however, is not an AME(8, 2) state if each qudit is regarded as a single party.
5 Quantum Secret Sharing

One application for AME states is to construct quantum secret sharing (QSS) protocols \[19, 32\]. In a quantum secret sharing protocol, a secret is encoded into a quantum state shared between \( n \) players \( P \) such that certain subsets of \( P \), the authorized sets, are able to recover the secret by performing joint quantum operations, while other subsets, the forbidden sets, are not able to gain any information about the secret. In some secret sharing protocols, for instance in threshold QSS schemes \[19, 32\], any subset is either authorized or forbidden. However, in general there may also exist a third category, the intermediate sets, which are subsets of players that are not able to recover the full secret, but are able to gain some information about the secret.

Describing quantum secret sharing protocols with the help of graph states has already been studied before for qubit \[13\] and qudit graph states of prime dimension \[14\]. In these papers it was shown that threshold quantum secret sharing schemes can be constructed from the graph state shown in Figure 2(d) for 6 qudits of arbitrary prime dimension \( p \geq 3 \). However, the question which graph states are generally suitable for quantum secret sharing remained an open question.

5.1 Threshold QSS Schemes

In a pure state \((m, 2m - 1)\) threshold QSS scheme, the secret is encoded into a pure state that is distributed among an odd number of players \( P = \{1, \ldots, 2m - 1\} \) such that a subset \( B \subset P \) of players is authorized if and only if the set contains more than half the players, \(|B| \geq m\). Furthermore, a subset \( B \subset P \) of players with less than \( m \) players is always a forbidden set.

It was already shown, that there exists a one-to-one correspondence between pure state \((m, 2m - 1)\) threshold QSS schemes and AME(2\( m \), \( d \)) states \[4, 5\]. The dimension \( d \) of the systems in the AME state translate to a \( d \)-dimensional secret and \( d \)-dimensional share sizes for each player in the QSS scheme. Here, we want to show how this construction of threshold QSS schemes from AME states work in the presented graph state formalism.

Given an AME(2\( m \), \( p \)) graph state \( |G\rangle \), the role of the dealer \( D \) is assigned to one of the 2\( m \) parties. The dealer possesses an additional state, the secret \( |s\rangle = \sum \alpha_i |i\rangle \), and his job is to encode this secret onto the qudits shared by the other 2\( m - 1 \) players. He does that by performing a generalized Bell measurement, which is a projective measurement onto the basis

\[
|\Psi_{gh}\rangle = \frac{1}{\sqrt{p}} \sum_j e^{2\pi i j g / p} |j\rangle |j + h\rangle , \tag{35}
\]

on the secret and his qudit of the graph state. This results in the encoded state

\[
|\Phi_S\rangle = \sum_{i=0}^{p-1} \beta_i |G_{iAD \setminus \{D\}}\rangle , \tag{36}
\]
where $\beta_i = \langle i | U_{gh}^\dagger | s \rangle$, with
\begin{equation}
U_{gh} = \sum_j e^{2\pi i j g/p} | j \rangle \langle j + h | ,
\end{equation}
depends on the outcome of the Bell measurement $(g, h)$. This outcome has to be broadcasted to the remaining $2m - 1$ players $P$. To see that the resulting state is a $(m, 2m - 1)$ threshold QSS scheme, we have to confirm that any subset $B$ of $m$ players can recover the secret. Tracing out the other $2m - 1$ parties $K = P \setminus B = \{k_1, \ldots, k_{m-1}\}$ gives
\begin{equation}
\rho = \text{Tr}_K | \Phi_S \rangle \langle \Phi_S | \\
= \sum_{i,j} \sum_{a \in \mathbb{Z}_{m-1}} \beta_i \beta_j^* \langle D,K \rangle | i, a_1, \ldots, a_{m-1} \rangle \langle G \rangle | j, a_1, \ldots, a_{m-1} \rangle_{D,K} \\
= \sum_{i,j} \sum_{a \in \mathbb{Z}_{m-1}} \beta_i \beta_j^* \langle G_{iA_{D+\sum_i a_i A_{k_i} \setminus \{D,K\}}} \rangle_{jA_{D+\sum_i a_i A_{k_i} \setminus \{D,K\}}} \\
| D,K \rangle_{iA_{D+\sum_i a_i A_{k_i} \setminus \{D,K\}}} \\
\text{(40)}
\end{equation}
Since the vectors $\{ A_{D \setminus \{D,K\}}, A_{k_1 \setminus \{D,K\}}, \ldots, A_{k_{m-1} \setminus \{D,K\}} \}$ are linearly independent,
\begin{equation}
V : |G_{iA_{D+\sum_i a_i A_{k_i} \setminus \{D,K\}}} \rangle \rightarrow | i, a_1, \ldots, a_{m-1} \rangle
\end{equation}
is a unitary operation on the qudits shared by the players in $B$. Applying it to $\rho$ gives
\begin{equation}
V \rho V^\dagger = | s' \rangle \langle s' | \otimes \sum_{a_1, \ldots, a_{m-1}} | a_1, \ldots, a_{m-1} \rangle \langle a_1, \ldots, a_{m-1} | \\
\text{(42)}
\end{equation}
with $| s' \rangle = \sum_i \beta_i | i \rangle$. Thus after applying $U_{gh}$ to the first qudit, the secret is restored.

That any set with less than $m$ players is forbidden follows directly from the no-cloning theorem. Thus we can construct a $(m, 2m - 1)$ threshold QSS scheme with graph states from any AME$(2m, d)$ graph state.

### 5.2 Ramp QSS Schemes

A generalization of threshold secret sharing schemes are $(m, L, n)$ ramp secret sharing schemes [20]. In these schemes $n$ players share a state such that any set of $m$ or more players can recover the secret and any set of $m - L$ or less players is a forbidden set, while any set in between is an intermediate set. The special case of $L = 1$ is a threshold secret sharing scheme.

It was shown in Ref. [5] that a $(m, L, 2m - L)$ ramp QSS scheme can be constructed from an AME$(2m, d)$ state for all $1 \leq L \leq m$. In this scenario each of the $2m - L$ players possesses a system of dimension $d$, while the dimension of the secret is $d^L$. This is achieved by assigning the role of the dealer to more than one party in the previously presented threshold QSS scheme. This method also works in the graph state formalism. Note that in this scenario, contrary to the the threshold scheme presented earlier, the secret dimension can be larger than the system of each player. This is achieved by having a “weaker” security structure with intermediate sets.
Consider an AME(2m, p) graph state. We assign L dealers $D = \{d_1, \ldots, d_L\}$. Each of them performs a bell measurement on their qudit of the graph state and a secret $|s_m\rangle = \sum_i \alpha_{m,i} |i\rangle$. Without loss of generality we assume that the measurement result is $(0, 0)$, different measurement outcomes could be corrected in the end in the same way as for the threshold QSS scheme. After the Bell measurements, the remaining $2m - L$ players $P$ share the state

$$|\Phi_S\rangle = \sum_{i_1, \ldots, i_L} \alpha_{1,i_1} \cdots \alpha_{L,i_L} |G_{\sum_{m', m''} A_{dm'} \setminus D} \rangle.$$

(43)

Now any subset $B \subset P$ of $m$ players should be able to recover the secret. Tracing out $K = P \setminus B = \{k_1, \ldots, k_{m-L}\}$ gives

$$\rho = \text{Tr}_K |\Phi_S\rangle \langle \Phi_S|$$

$$= \sum_{i_1, \ldots, i_L} \sum_{a \in \mathbb{Z}^{p-m-L}} \alpha_{1,i_1} \cdots \alpha_{L,i_L} \alpha_{1,j_1}^* \cdots \alpha_{L,j_L}^* |G_{\sum_{m', m''} A_{dm'} + \sum_i A_{ki} \setminus \{D,K\}} \rangle \langle G_{\sum_{m', m''} A_{dm'} + \sum_i A_{ki} \setminus \{D,K\}}|.$$

(45)

(46)

And applying $V$ recovers the secrets:

$$V \rho V^\dagger = |s_1\rangle \langle s_1| \otimes \cdots \otimes |s_L\rangle \langle s_L| \otimes \sum_a |a_1, \ldots, a_{m-L}\rangle \langle a_1, \ldots, a_{m-L}|$$

(47)

That any subset of $m - L$ players or less cannot gain any information about the secrets follows again from the no-cloning theorem. For a discussion while sets of players with more than $m - L$ but less than $m$ players are indeed intermediate sets, which means they cannot recover the full secrets, but gain some information, see Ref. [5].

6 Conclusion and Open Questions

In this paper, we have shown how the graph state formalism can be used to describe absolutely maximally entangled states. Due to the high degree of multipartite entanglement in graph states, they provide an optimal framework for the investigation of AME states. Furthermore, they intrinsically provide a quantum circuit to generate the state, which should be very useful for actually implementing AME states in the future, once it is possible to experimentally design CNOT gates for qudits. Two different methods to check bipartite entanglement in graph states have been presented. One uses a graphical illustration of the existing entanglement in the graph, while the other one provides a very efficient method to check if a given graph state is absolutely maximally entangled.

With the efficient method, we are able to numerically check the entanglement of millions of graph states per minute, which we were able to use to find a previously unknown AME state for seven qutrits. Unfortunately, with increasing system dimensions and number of parties, the number of possible graph states grows exponentially, which makes an exhaustive search already infeasible for eight qutrits. Hence for future investigations, a goal would be to combine both methods. Using insight gained from the graphical representation might help us cut down on the number of graph states that are candidates for AME states.
In addition to the seven qutrit AME graph state, we were able to construct an AME graph state for all previously known AME states, in particular for each number of parties, an AME graph state can be constructed from classical MDS codes. Thus the question arises if we can always find an AME($n,d$) graph state if an AME($n,d$) state exists. So far, we were not able to either proof that or construct a counterexample.

Finally, we showed how AME graph states can be used for quantum secret sharing within the graph states formalism. QSS with graph states has already been introduced before [13, 14], but only two examples for threshold QSS schemes for 4 and 6 qudits, corresponding to the graph states in Figures 3 and 2(d) respectively, were given. However, it remained an open question, with other graph states are suitable for threshold QSS schemes. Here we showed that all AME graph states shared between an even number of parties can be used to derive threshold QSS schemes, as well as ramp QSS schemes, which have not been covered before in the graph state formalism.

Acknowledgements

I acknowledge financial support by NSERC and the CRC program. I also want to thank Hoi-Kwong Lo and David Gosset for helpful discussions and comments.

References

[1] C. H. Bennett, S. Popescu, D. Rohrlich, J. A. Smolin, and A. V. Thapliyal, “Exact and asymptotic measures of multipartite pure-state entanglement,” Phys. Rev. A, vol. 63, p. 012307, Dec 2000.

[2] G. Vidal, W. Dür, and J. I. Cirac, “Reversible combination of inequivalent kinds of multipartite entanglement,” Phys. Rev. Lett., vol. 85, pp. 658–661, Jul 2000.

[3] W. Dür, G. Vidal, and J. I. Cirac, “Three qubits can be entangled in two inequivalent ways,” Phys. Rev. A, vol. 62, p. 062314, Nov 2000.

[4] W. Helwig, W. Cui, J. I. Latorre, A. Riera, and H.-K. Lo, “Absolute maximal entanglement and quantum secret sharing,” Phys. Rev. A, vol. 86, p. 052335, Nov 2012.

[5] W. Helwig and W. Cui, “Absolutely maximally entangled states: Existence and applications,” arXiv:quant-ph/1306.2536, 2013.

[6] H. J. Briegel and R. Raussendorf, “Persistent entanglement in arrays of interacting particles,” Phys. Rev. Lett., vol. 86, pp. 910–913, Jan 2001.

[7] M. Bahramgiri and S. Beigi, “Graph states under the action of local clifford group in non-binary case,” arXiv:quant-ph/0610267, 2006.

[8] R. Raussendorf and H. J. Briegel, “A one-way quantum computer,” Phys. Rev. Lett., vol. 86, pp. 5188–5191, May 2001.

[9] D. Schlingemann, “Stabilizer codes can be realized as graph codes,” Quant. Inf. & Comp., vol. 2, p. 307, 2002.
[10] M. Grassl, A. Klappenecker, and M. Rotteler, “Graphs, quadratic forms, and quantum codes,” in Information Theory, 2002. Proceedings. 2002 IEEE International Symposium on, pp. 45–, 2002.

[11] S. Y. Looi, L. Yu, V. Gheorghiu, and R. B. Griffiths, “Quantum-error-correcting codes using qudit graph states,” Phys. Rev. A, vol. 78, p. 042303, Oct 2008.

[12] S. Beigi, I. Chuang, M. Grassl, P. Shor, and B. Zeng, “Graph concatenation for quantum codes,” Journal of Mathematical Physics, vol. 52, no. 2, p. 022201, 2011.

[13] D. Markham and B. C. Sanders, “Graph states for quantum secret sharing,” Phys. Rev. A, vol. 78, p. 042309, Oct 2008.

[14] A. Keet, B. Fortescue, D. Markham, and B. C. Sanders, “Quantum secret sharing with qudit graph states,” Phys. Rev. A, vol. 82, p. 062315, Dec 2010.

[15] P. Walther, K. J. Resch, T. Rudolph, E. Schenck, H. Weinfurter, V. Vedral, M. Aspelmeyer, and A. Zeilinger, “Experimental one-way quantum computing,” Nature, vol. 434, pp. 169–176, Mar. 2005.

[16] C.-Y. Lu, X.-Q. Zhou, O. Gühne, W.-B. Gao, J. Zhang, Z.-S. Yuan, A. Goebel, T. Yang, and J.-W. Pan, “Experimental entanglement of six photons in graph states,” Nat Phys, vol. 3, pp. 91–95, Feb. 2007.

[17] R. Ceccarelli, G. Vallone, F. De Martini, P. Mataloni, and A. Cabello, “Experimental entanglement and nonlocality of a two-photon six-qubit cluster state,” Phys. Rev. Lett., vol. 103, p. 160401, Oct 2009.

[18] W.-B. Gao, P. Xu, X.-C. Yao, O. Gühne, A. Cabello, C.-Y. Lu, C.-Z. Peng, Z.-B. Chen, and J.-W. Pan, “Experimental realization of a controlled-not gate with four-photon six-qubit cluster states,” Phys. Rev. Lett., vol. 104, p. 020501, Jan 2010.

[19] R. Cleve, D. Gottesman, and H.-K. Lo, “How to share a quantum secret,” Phys. Rev. Lett., vol. 83, pp. 648–651, Jul 1999.

[20] G. R. Blakley and C. Meadows, “Security of ramp schemes,” in CRYPTO, pp. 242–268, 1984.

[21] J. Patera and H. Zassenhaus, “The pauli matrices in n dimensions and finest gradings of simple lie algebras of type a[sub n - 1],” Journal of Mathematical Physics, vol. 29, no. 3, pp. 665–673, 1988.

[22] D. Gottesman, A. Kitaev, and J. Preskill, “Encoding a qubit in an oscillator,” Phys. Rev. A, vol. 64, p. 012310, Jun 2001.

[23] S. D. Bartlett, H. de Guise, and B. C. Sanders, “Quantum encodings in spin systems and harmonic oscillators,” Phys. Rev. A, vol. 65, p. 052316, May 2002.

[24] D. Gottesman, Stabilizer Codes and Quantum Error Correction. PhD thesis, California Institute of Technology, 1997.
[25] A. Ashikhmin and E. Knill, “Nonbinary quantum stabilizer codes,” *Information Theory, IEEE Transactions on*, vol. 47, pp. 3065–3072, nov 2001.

[26] A. Ketkar, A. Klappenecker, S. Kumar, and P. Sarvepalli, “Nonbinary stabilizer codes over finite fields,” *Information Theory, IEEE Transactions on*, vol. 52, pp. 4892–4914, nov. 2006.

[27] E. Hostens, J. Dehaene, and B. De Moor, “Stabilizer states and clifford operations for systems of arbitrary dimensions and modular arithmetic,” *Phys. Rev. A*, vol. 71, p. 042315, Apr 2005.

[28] R. Singleton, “Maximum distance q -nary codes,” *Information Theory, IEEE Transactions on*, vol. 10, pp. 116 – 118, apr 1964.

[29] F. MacWilliams and N. Sloane, *The Theory of Error-Correcting Codes*. North Holland Publishing Co., 1977.

[30] A. R. Calderbank and P. W. Shor, “Good quantum error-correcting codes exist,” *Phys. Rev. A*, vol. 54, pp. 1098–1105, Aug 1996.

[31] A. Steane, “Multiple-particle interference and quantum error correction,” *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, vol. 452, no. 1954, pp. 2551–2577, 1996.

[32] D. Gottesman, “Theory of quantum secret sharing,” *Phys. Rev. A*, vol. 61, p. 042311, Mar 2000.