Absolutely Maximally Entangled States: 
Existence and Applications

Wolfram Helwig and Wei Cui

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

May 7, 2014

Abstract

We investigate absolutely maximally entangled (AME) states, which 
are multipartite quantum states that are maximally entangled with re-
spect to any possible bipartition. These strong entanglement properties 
make them a powerful resource for a variety of quantum information pro-
tocols. In this paper, we show the existence of AME states for any number 
of parties, given that the dimension of the involved systems is chosen ap-
propriately. We prove the equivalence of AME states shared between an 
even number of parties and pure state threshold quantum secret sharing 
(QSS) schemes, and prove necessary and sufficient entanglement proper-
ties for a wider class of ramp QSS schemes. We further show how AME 
states can be used as a valuable resource for open-destination teleporta-
tion protocols and to what extent entanglement swapping generalizes to 
AME states.

1 Introduction

Entanglement has been a hot topic since the beginning of quantum mechanics 
and fueled a lot of discussions, among them most notable the Einstein-Podolsky-
Rosen (EPR) paradox [1], which finally led Bell to come up with a method of 
actually measuring entanglement [2]. It was not until the advent of quantum 
information, however, that entanglement was recognized as a useful resource. 
Almost all applications in quantum information make either explicit or implicit 
use of entanglement, which makes it crucial to gain as much insight as possible.

While the entanglement of bipartite states is already very well understood [4,5,6], the road to its generalization to more than two parties is paved with 
many obstacles. Therefore we often have to restrict ourselves to special cases 
when analyzing multipartite entanglement. A prominent choice are states that 
 extremize the entanglement for a certain measure of entanglement. In this 
paper we want to do that by focusing on absolutely maximally entangled (AME) 
states, which are defined as states that are maximally entangled for any possible 
bipartition.
Definition 1. An absolutely maximally entangled state is a pure state, shared among \( n \) parties \( P = \{1, \ldots, n\} \), each having a system of dimension \( d \). Hence \( |\Phi\rangle \in \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n \), where \( \mathcal{H}_i \cong \mathbb{C}^d \), 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 \( |A| = \lfloor \frac{n}{2} \rfloor \) is totally mixed, \( \rho_A = d^{-\lfloor \frac{n}{2} \rfloor} \text{I}_{d^{\lfloor \frac{n}{2} \rfloor}} \).

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

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

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

These are all necessary and sufficient condition for a state to be absolutely maximally entangled. We denote such a state as an AME\((n, d)\) state.

The simplest examples of AME states occur for low dimensional systems shared among few parties. Starting with qubits, the most obvious one is an EPR pair, which is maximally entangled for its only possible bipartition. For three qubits shared among three parties, we can recognize the GHZ state as an AME state. It is maximally entangled, with 1 ebit of entanglement with respect to every bipartition. For four qubits, there is no obvious candidate, and in fact it has been shown that for four qubits no AME state exists \[9\]. We can still find an absolutely maximally entangled states for four parties, however, by increasing the dimensions of the involved systems. An AME\((4, 3)\) state for four qutrits shared among four parties exists, and it is given by \[7\]

\[
|\Phi\rangle = \frac{1}{\sqrt{9}} \sum_{i,j=0}^{2} |i\rangle |j\rangle |i + j\rangle |i + 2j\rangle.
\]

This is the first indicator that the search for AME states gets more promising as we increase the dimensions of the systems.

Completing the characterization of AME states for qubits, it is known that AME states exist for 5 and 6 qubits. Explicit forms for them are given in Ref. \[7\], and it turns out that they are closely related to the five-qubit error correction code. For 7 qubits, it is still not known if an AME state exists, whereas for \( \geq 8 \) qubits, it has been shown that no AME states can exist \[8, 10\].

In Ref. \[7\], we showed how AME states can be used for parallel teleportation protocols. In these protocols, the parties are divided into a sets of senders...
and receivers, respectively. One of the two sets is given the ability to perform joint quantum operations, while players in the other set can only perform local quantum operations. Under these conditions, a parallel teleportation of multiple quantum states is possible if the set that performs joint quantum operations is larger than the other set. A closer look at these teleportation scenarios then led to the observation that any AME state shared by an even number of parties can be used to construct a threshold quantum secret sharing (QSS) scheme \[11, 12, 13\]. The opposite direction was also shown, with one additional condition imposed on the QSS scheme, namely that the shared state that encodes the secret is already an AME state.

In this paper, we will give an information-information theoretic proof of this equivalence of AME states and threshold QSS scheme, which shows that the additional condition is not required. We will rather see that it is satisfied for all threshold QSS schemes. We will further give a recipe of how to construct AME states from classical codes that satisfy the Singleton bound \[14\]. This construction can be used to produce AME states for a wide class of parameters, and it even proves that AME states exist for any number of parties for appropriate system dimension. A result that could also be deduced from the equivalence of AME states and QSS schemes and a known construction for threshold QSS schemes \[11\]. We will then show more applications for AME states. The first being the construction of a wider class of QSS schemes, the ramp QSS schemes, of which threshold QSS schemes are a special case. The next one is the utilization of AME states as resources for open-destination teleportation protocols \[15\]. Finally, we investigate to what extend entanglement can be swapped between two AME states.

This paper is structured as follows. In Section 2 we show how AME states can be constructed from classical codes, which also also shows the existence of AME states for any number of parties. In Section 3 we establish an equivalence between even party AME states and threshold QSS schemes, using an information theoretic approach to QSS schemes. Section 4 shows how to share multiple secrets using AME states. In Section 5 we show that AME states can be used for open-destination teleportation. After that, swapping of AME states is investigated in Section 6.

## 2 Constructing AME States from Classical MDS Codes

There is a subclass of AME\((n,d)\) states that can be constructed from optimal classical error correction codes. A classical code \(C\) consists of \(M\) codewords of length \(n\) over an alphabet \(\Sigma\) of size \(d\). For our purposes, the alphabet is going to be \(\Sigma = \mathbb{Z}_d\) and thus \(C \subset \mathbb{Z}_d^n\). The **Hamming distance** between two codewords is defined as the number of positions in which they differ, and the minimal distance \(\delta\) of the code \(C\) as the minimal Hamming distance between any two codewords. For a given length \(n\) and minimal distance \(\delta\), the number of codewords \(M\) in the code is bounded by the **Singleton bound** \[13, 16\]

\[
M \leq d^{n-\delta+1}.
\]  

Codes that satisfy the Singleton bound are referred to as maximum-distance separable (MDS) codes. They can be used to construct AME states:
Theorem 2(a). From a classical MDS code \( C \subset \mathbb{Z}_d^{2m} \) of length \( 2m \) and minimal distance \( \delta = m + 1 \) over an alphabet \( \mathbb{Z}_d \), an AME(2m, d) state can be constructed as

\[
|AME\rangle = \frac{1}{\sqrt{d^m}} \sum_{c \in C} |c\rangle = \frac{1}{\sqrt{d^m}} \sum_{c \in C} |c_1\rangle_1 \cdots |c_m\rangle_m |c_{m+1}\rangle_{m+1} \cdots |c_{2m}\rangle_{2m}.
\]

Proof. The code \( C \) satisfies the Singleton bound, which means the sum contains a total of \( M = d^{2m-\delta+1} = d^m \) terms. Furthermore, any two of these terms differ in at least one of the first \( m \) kets because the code has minimal distance \( \delta = m + 1 \). Hence the sum contains each possible combination of the first \( m \) basis kets exactly once. Moreover, for any two different terms, the last \( m \) kets must also differ in at least one ket and are thus orthogonal. This means the state has the form of Equation (1) with respect to the bipartition into the first \( m \) and last \( m \) parties. The same argument works for any other bipartition into two sets of size \( m \), hence the state is absolutely maximally entangled.

An analogous argument shows that a similar construction for an odd number of parties results in an AME state.

Theorem 2(b). From a classical MDS code \( C \subset \mathbb{Z}_d^{2m+1} \) of length \( 2m + 1 \) and minimal distance \( \delta = m + 2 \) over an alphabet \( \mathbb{Z}_d \), an AME(2m + 1, d) state can be constructed as

\[
|AME\rangle = \frac{1}{\sqrt{d^m}} \sum_{c \in C} |c\rangle = \frac{1}{\sqrt{d^m}} \sum_{c \in C} |c_1\rangle_1 \cdots |c_m\rangle_{m+1} |c_{m+1}\rangle_{m+1} \cdots |c_{2m}\rangle_{2m+1}.
\]

Proof. The code contains \( M = d^m \) terms. Each of the terms differ in at least one of the first \( m + 1 \) and last \( m \) terms. Thus, with the same argument as above, this is an AME state.

Trivial states of that form are \( d \)-dimensional EPR states, which are represented by the code with codewords \( 00, 11, \ldots, (d-1)(d-1) \). This code has \( n = 2, \delta = 2, M = d^1 \). For \( n = 3 \), we can find the GHZ states for arbitrary dimensions, which can be constructed from the code \( 000, 111, \ldots, (d-1)(d-1)(d-1) \), which has \( \delta = 3 \) and \( M = d^1 \). As already mentioned in the introduction, for \( n = 4 \) no AME state exists for \( d = 2 \), however for \( d = 3 \) the AME(4, 3) state given in Equation (2) can also be constructed from an MDS code, the \([4, 2, 3]_3\) ternary Hamming code.

A wide class of MDS codes is given by the Reed-Solomon codes and its generalizations [17, 18, 19], which give MDS codes for \( n = d - 1 \), \( n = d \), and \( n = d + 1 \), for \( d = p^k \) being a positive power of a prime number \( p \). From the Reed-Solomon codes, MDS codes can also be constructed for \( n < d - 1 \) [14]. This shows that AME states exist for any number of parties if the system dimensions are chosen right.

At this point we would like to mention that after posting a preliminary version of our last paper on this subject [7], it has been brought to our attention by
Gerardo Adesso that the results of this section have already been previously dis-
covered by Ashish Thapliyal and coworkers, and were presented at a conference 
in 2003 [19], but remained unpublished.

3 Equivalence of AME states and QSS schemes

In Ref. [7], we showed that AME(2\(m, d\)) states, i.e., AME states shared between 
an even number of parties, are equivalent to pure state threshold quantum secret 
sharing (QSS) schemes that have AME states as basis states and share and secret 
dimension equal to \(d\). Here we will give an information-theoretic proof of this 
equivalence, which shows that the requirement that the basis states of the QSS 
scheme are AME states is redundant, as it follows from this proof that these 
states are always absolutely maximally entangled. Before stating the theorem 
and the proof, we give a short motivation why AME states and QSS schemes 
are related.

Consider an AME(2\(m, d\)) state shared among an even number of parties. If 
we take any bipartition into two sets of parties \(A\) and \(B\), each of size \(m\), a \(d^m\) 
dimensional state can be teleported from one set to the other due to the maximal 
entanglement between \(A\) and \(B\). Moreover, we have shown in Ref. [7], that the 
teleportation can be performed in such a way that each party in the sending set 
\(B\) performs a local teleportation operation on their qudit, while the parties in the 
receiving set \(A\) perform a joint quantum operation to recover all \(m\) teleported 
qudits. This is depicted in Figure 1 for the case of \(m = 4\). This also works 
if only one party in \(B\), which we call the dealer \(D\), performs the teleportation 
operation, while the others do nothing. Then the teleported \(d\)-dimensional state 
can still be recovered by the players in set \(A\). Furthermore, this also works for 
any other bipartition into sets \(A'\) and \(B'\) of size \(m\), with \(D \in B'\), without 
changing the teleportation operation \(D\) has to perform, but now the parties in 
\(A'\) can recover the teleported state (see Figure 2). This means that any set with 
\(m\) parties can recover the state. Moreover, the no-cloning theorem guarantees 
that the complement of a set that can recover the state has no information about 
the state. Hence all sets with less than \(m\) parties cannot gain any information 
about the state. This, however, are exactly the requirements for a threshold QSS 
scheme, therefore we have constructed a \((m, 2m - 1)\) threshold QSS scheme 
from the AME(2\(m, d\)) state. To formally show this, and moreover that it also 
works in the opposite direction, meaning that a \((m, 2m - 1)\) threshold QSS 
scheme is always related to an AME(2\(m, d\)) state, we will use the information 
theoretic description of QSS schemes as introduced in Ref. [13].

Let us quickly review the framework for a pure state \((m, 2m - 1)\) threshold 
QSS scheme [11]. A secret \(S\) is distributed among the players \(P = \{1, \ldots, 2m-1\}\) such that any set \(A \subseteq P\) with \(|A| \geq m\) can recover the secret, while any set 
\(B \subset P\) with \(|B| < m\) cannot gain any information about the secret. We further 
only consider the case where the dimension \(d\) of the secret is the same as the 
dimension of each player’s share.

The secret is assumed to lie in the Hilbert space \(\mathcal{H}_S \cong \mathbb{C}^d\), and the share of 
party \(i\) in \(\mathcal{H}_i \cong \mathbb{C}^d\). The encoding is described by an isometry

\[
U_S : \mathcal{H}_S \rightarrow \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_{2m-1}.
\]

(8)

The secret \(S\) is chosen randomly and thus is described by \(\rho_S = 1/d \sum_i |i\rangle \langle i|\). We
Figure 1: (Color online) Parties in $B$ (green) perform local teleportation operations, parties in $A$ (red) can recover teleported states by performing a joint quantum operation

Figure 2: (Color online) After $D$ (blue) performs her teleportation operation, any set of $m$ parties (red), $A, A', A''$ etc., can recover the teleported state. Any set of parties with $m - 1$ or less parties (any set consisting only of green parties) cannot gain any information about the teleported state.

consider its purification by introducing a reference system $R$ such that $|RS⟩ = 1/\sqrt{d}\sum_i |i⟩|i⟩ ∈ H_R ⊗ H_S$. Let $ρ_{RA}$ denote the combined state of the reference system and a set of players $A ⊆ P$ after $U_S$ has been applied to the secret. Then the players $A$ can recover the secret, if there exists a completely positive map $T_A : H_A → H_S$ such that

$$I_R ⊗ T_A(ρ_{RA}) = |RS⟩.$$  \hspace{1cm} (9)

This can be stated in terms of the mutual information

$$I(X : Y) = S(X) + S(Y) − S(X, Y)$$  \hspace{1cm} (10)

as follows:

**Definition 3.** An isometry $U_S : H_S → H_1 ⊗ H_2 ⊗ ... ⊗ H_{2m-1}$ creates a $((m, 2m-1))$ threshold QSS scheme if and only if, after applying to the system $S$ of the purification $|RS⟩$, the mutual information between $R$ and an authorized (unauthorized) set of players $A$ (B) satisfies

$$I(R : A) = I(R : S) = 2S(S) \hspace{1cm} \text{if } |A| ≥ m \hspace{1cm} \text{(11)}$$

$$I(R : B) = 0 \hspace{1cm} \text{if } |B| < m.$$  \hspace{1cm} (12)
Here $S$ is the von Neumann entropy, and because of $S(i) \geq S(S) \geq S(R) = S(i) = \log d$. (13)

From Equations (10) to (12) it immediately follows that

$$S(R, A) = S(A) - S(R) \quad \text{if } |A| \geq m$$

$$S(R, B) = S(B) + S(R) \quad \text{if } |B| < m.$$ (14) (15)

**Theorem 4.** For a state $|\Phi\rangle$ the following two properties are equivalent:

(i) $|\Phi\rangle$ is an AME$(2m, d)$ state.

(ii) $|\Phi\rangle$ is the purification of a $((m, 2m - 1))$ threshold QSS scheme, whose share and secret dimensions are $d$.

**Proof.** (i) $\rightarrow$ (ii): We need to show that for an AME$(2m, d)$ state Equations (11) and (12) are satisfied, where $R$ can be any of the $2m$ party. This follows directly from the definition of the mutual information, Equation (10), and Definition 1.

(ii) $\rightarrow$ (i): Consider an unauthorized set of players $B$, with $|B| = m - 1$. Then the set is $B \cup i$ is authorized for any additional player $i \notin B$, and from Equation (14) we have

$$S(B, i, R) = S(B, i) - S(R)$$ (16)

On the other hand, using the Araki-Lieb inequality $S(X, Y) \geq S(X) - S(Y)$ and Equation (15) gives

$$S(B, i, R) \geq S(B, R) - S(i) = S(B) + S(R) - S(i).$$ (17)

Combining the last two equations and using $S(S) = S(R) = S(i)$ shows

$$S(B, i) \geq S(B) + S(i),$$ (18)

where equality must hold due to the subadditivity of the entropy $S(X, Y) \leq S(X) + S(Y)$. This means that the entropy increases maximally when adding one player’s share to $m - 1$ shares. The strong subadditivity of the entropy states that adding one system $X$ to a system $Y$ increases the entropy at least by as much as adding the system $X$ to a larger system $Y \cup Z$ that contains $Y$. So in our case, adding one share to less than $m - 1$ shares increases the entropy by at least $S(i)$, and since this is the maximum, it increases the entropy exactly by $S(i)$. Hence, starting out with a set of no shares, and repeatedly adding one share to the set until the set contains any $m$ shares and is authorized, shows that any set of $m$ shares has entropy $mS(i)$. This shows that the entropy is maximal for any subset of $m$ parties and thus $|\Phi\rangle$ is an AME$(2m, d)$ state. □

**Corollary 5.** The encoded state $U_S |S\rangle$ of a specific secret $|S\rangle$ with a $((m, 2m - 1))$ threshold QSS protocol with share and secret dimension $d$ is an AME$(2m - 1, d)$ state.
4 Sharing multiple secrets

In the previous section, we outlined how an AME state can be used to construct a QSS scheme. The role of the dealer is assigned to one of the parties and he performs a teleportation operation on his qudit, which encodes the teleported qudit onto the qudits of the remaining parties such that the criteria for a QSS scheme are met. While Theorem 4 shows the equivalence of AME states and QSS schemes, the actual protocol for the encoding and decoding operations has been presented in Ref. [7]. Note that in the described scenario, the role of the dealer can be assigned to any player. Thus one may ask, what happens if more than one of the players assumes the role of the dealer. The answer is that, given an AME$(2^m, d)$ state, up to $m$ players are able to independently encode one qudit each onto the qudits of the remaining players in such a way that results in a QSS scheme with a more general access structure.

For a secret sharing scheme with a general access structure, each set of players falls into one of three categories [22, 23].

1. Authorized: A set of players is authorized, if it can recover the secret
2. Forbidden: A set of players is called a forbidden set, if the players cannot gain any information about the encoded secret
3. Intermediate: A set of players is classified as an intermediate set, if they cannot recover the secret, but may be able to gain part of the information.

This means that the reduced density matrix of that set of players depends on the encoded secret, but not enough as to recover the secret.

A special kind of access structure is a $(m, L, n)$ ramp secret sharing scheme [24]. Here $n$ is the total number of players, $m$ is the number of players needed to recover the secret, and $L$ is the number of shares that have to be removed from a minimal authorized set to destroy all information about the secret. In terms of the above defined set categories that means that any set of $m$ or more players is authorized, any set of $m - L$ or less players is forbidden, and any set consisting of more than $m - L$, but less than $m$ players is an intermediate set. This is the access structure we get from an AME$(2^m, d)$ state if more than one party assumes the role of the dealer.

**Theorem 6.** Given an AME$(2^m, d)$ state, a QSS scheme with secret dimension $d^L$ and a $(m, L, 2^m - L)$ ramp access structure can be constructed for all $1 \leq L \leq m$.

**Proof.** The encoding of the secret is done by assigning the role of dealer to $L$ of the $2^m$ players. For simplicity we choose them to be the first $L$ players. Each of them performs a Bell measurement on their respective qudit of the AME state and one qudit of the secret. The Bell measurement is described by the general $d$-dim Bell states $|\Psi_{kl}\rangle$ and the unitaries $U_{kl}$ that transform among them [25]

$$|\Psi_{qp}\rangle = \frac{1}{\sqrt{d}} \sum_j e^{2\pi ijq/d} |j\rangle |j + p\rangle$$

$$U_{qp} = \sum_j e^{2\pi ijq/d} |j\rangle \langle j + p|.$$  

8
where the kets are understood to be mod $d$. For a secret $|s\rangle$ and outcomes $(q_1, p_1) \ldots (q_L, p_L)$ for the Bell measurement of the dealers, the initial AME($2m, d$) state is transformed to

$$|\Phi_S\rangle = \frac{1}{\sqrt{d^{m-L}}} \sum_{k \in \mathbb{Z}_d^m} s_{qp,k_1 \ldots k_L} |k_{L+1}\rangle_{B_1} \cdots |k_m\rangle_{B_{m-L}} |\phi(k)\rangle_A.$$  \hspace{1cm} (22)

Here

$$s_{qp,k_1 \ldots k_L} = \langle k_1 \cdots k_L | U_{q_1p_1}^\dagger \otimes \cdots \otimes U_{q_Lp_L}^\dagger | s\rangle,$$  \hspace{1cm} (23)

and the partition of the remaining $2m - L$ parties into two sets $A$ and $B$ of size $m$ and $m - L$, respectively, is arbitrary. After obtaining their measurement outcomes, the dealers broadcast their results to all of the remaining players. This concludes the encoding process.

To show that any set of $m$ or more players is authorized, it suffices to show that set $A$ in Equation (22) can recover the secret. They can do so by applying the unitary operation

$$U = (U_{q_1p_1} \otimes \cdots \otimes U_{q_Lp_L} \otimes 1) V$$  \hspace{1cm} (24)

with

$$V = \sum_{k \in \mathbb{Z}_d^m} |k_1\rangle \cdots |k_m\rangle \langle \phi(k)|,$$  \hspace{1cm} (25)

to their system. This changes the state to

$$U |\Phi_S\rangle = \frac{1}{\sqrt{d^{m-L}}} \sum_{(k_{L+1}, \ldots, k_m) \in \mathbb{Z}_d^{m-L}} |k_{L+1}\rangle_{B_1} \cdots |k_m\rangle_{B_{m-L}} |s\rangle_{A'} |k_{L+1}\rangle_{A_{L+1}} \cdots |k_m\rangle_{A_m}$$  \hspace{1cm} (26)

where $A' = \{A_1, \ldots, A_L\}$. Thus the players in set $A$ have the secret in their possession. It immediately follows from the no-cloning theorem that $B$, and thus any set of size $m - L$ or less, cannot have any information about the secret since all information is located in the complement set. Alternatively, this also follows from the observation that the reduced density matrix of $B$ is always completely mixed, independent of the secret.

The last thing left to show is that all sets with more than $m - L$ but fewer than $m$ players are indeed intermediate sets. To see that, consider the case $L = 1$, where a set $C$ of $m - 1$ players is not authorized to recover the secret. If one more player in the complement of $C$ assumes the role of the dealer, the scheme is changes to $L = 2$. This operation does not change the fact that $C$ cannot recover the first secret, and thus it is still not authorized for $L = 2$. This argument can be continued to any other $1 < L \leq m$ by adding more dealers. Hence a set of $m - 1$ (or fewer) players is not authorized to recover the secret for all value of $1 \leq L \leq m$. That a set of more than $m - L$ players is not forbidden follows from the fact that information cannot be lost and thus the complement of a forbidden set has to be authorized. However, we just argued that the complement of a set of more than $m - L$ players is not authorized (since it consists of less than $m$ players). Hence any set with more than $m - L$ and fewer than $m$ players is an intermediate set.
A closer look at the proof shows us that it actually is not absolutely necessary for the initial state to be maximally entangled with respect to any bipartition, but only for bipartitions for which all dealers are in the same set. In fact, we can generalize the proof of Theorem 4 to the case of ramp QSS to show that this is a necessary and sufficient condition for the construction of \((m, L, 2m - L)\) ramp QSS schemes.

**Theorem 7.** For a state \(|\Phi\rangle \in \mathcal{H}_P \otimes \mathcal{H}_R\), shared between \(2m - L\) players \(P\), each holding a qudit, and \(L\) reference qudits, the following two properties are equivalent:

(i) \(|\Phi\rangle\) is maximally entangled for any bipartition for which the \(L\) reference qudits are in the same set.

(ii) \(|\Phi\rangle\) is the purification of a \((m, L, 2m - L)\) ramp QSS schemes. The encoded secret of the ramp QSS scheme has dimension \(d^L\), and each share has dimension \(d\).

The proof is a straightforward generalization of the proof of Theorem 4 and is provided in Appendix A.

## 5 Open-destination teleportation

Given a state with such high amount of entanglement as the AME state has, one cannot help thinking about ways of using these resources for teleportation protocols. In Ref. [7] we already showed how AME states can be used for two different teleportation scenarios that require either sending or receiving parties to perform joint quantum operations, while the other end may only use local quantum operations.

Another teleportation scenario that uses genuine multipartite entanglement, and has already been demonstrated experimentally [15], is open-destination teleportation. In this scenario, a genuinely multipartite entangled state is shared between \(n\) parties, each in the possession of one qudit. One of the parties, the dealer, performs a teleportation operation on her qudit and an ancillary qudit \(|\Phi\rangle\). After this teleportation operation, the final destination of \(|\Phi\rangle\) is still undecided, thus open-destination teleportation. The destination is decided upon in the next step, where a subset \(A\) of the remaining parties \(P\) performs a joint quantum operation on their qudits such that a player in \(P \setminus A\) ends up with the state \(|\Phi\rangle\) – up to local operations that depend on measurement outcomes of the dealer and parties \(A\). Here we want to show that open-destination teleportation can also be performed with AME states.

Assume that an AME\((n, d)\) state has been distributed among \(n\) parties. One of the \(n\) parties is assigned the role of the dealer. She performs a Bell measurement on her qudit and the secret \(|S\rangle = \sum a_i |i\rangle\). This transforms the state to

\[
|S\rangle |\Phi\rangle \rightarrow |\Phi_S\rangle = \frac{1}{\sqrt{d^n}} \sum_{(k, i) \in \mathbb{Z}_d^n} a_{pq, i} |k_1\rangle_{B_1} \cdots |k_{m-1}\rangle_{B_{m-1}} |\phi(k, i)\rangle_A, \tag{27}
\]

where \(pq\) labels the outcome of the Bell measurement and has to be made public. The remaining \(n - 1\) parties that share the resulting state have been divided
into two sets $A$ and $B$ of size $\lceil n/2 \rceil$ and $m - 1 = \lfloor n/2 \rfloor - 1$, respectively. Now, after the teleportation operation has been completed, the parties in set $A$ may choose one party $B_i \in B$ as the final destination for the state $|S\rangle$. Then, after performing the joint unitary operation of Equation (25) followed by a Bell measurement on qudits $A_t$ and $A_{m}$ with outcome $rs$, the party $B_i$ ends up with the state $|\Phi\rangle_{B_i} = U_{rs}^\dagger U_{pq}^\dagger |S\rangle$, which can be easily transformed to $|S\rangle$ if the measurement results $pq$ and $rs$ are known.

Note that with the parallel teleportation protocol introduced in Ref. [7], also one of the parties in $A$ can be chosen to receive the state $|S\rangle$. Thus, after the dealer’s teleportation operation is completed, any set of size greater or equal $\lceil n/2 \rceil$ can choose any of the remaining $n - 1$ parties as the final destination of the teleportation.
6 Swapping of AME states

Entanglement swapping \cite{26} is a very useful tool for the application of entanglement in communication. By making a Bell measurement on Bob’s side, two entangled states shared between Alice and Bob, and Bob and Charlie, respectively, can be transformed into an entangled state shared by Alice and Charlie. Employing this procedure in quantum repeaters \cite{27} allows entangled states to be used for long distance communications. In this section, we show to what extent a generalization of the entanglement swapping protocol can be constructed to allow swapping of entanglement between absolutely maximally entangled states shared between different parties.

Assume that parties \( \{1, 2, \ldots, 2n\} \) share an AME\((2n, d)\) state,

\[
|\Phi\rangle_{1, \ldots, 2n} = \sum |i_1 \cdots i_n\rangle_{1, \ldots, n} |\phi(i_1, \ldots, i_n)\rangle_{n+1, \ldots, 2n} \tag{28}
\]

where \( U \) is a unitary transformation with \( U |i_1 \cdots i_n\rangle = |\phi(i_1, \ldots, i_n)\rangle \).

Suppose parties \( \{n+1, \ldots, 3n\} \) also share an AME\((2n, d)\) state

\[
|\Phi\rangle_{n+1, \ldots, 3n} = \sum |i_1 \cdots i_n\rangle_{n+1, \ldots, 2n} U |i_1 \cdots i_n\rangle_{2n+1, \ldots, 3n} \tag{30}
\]

Now each of the parties \( \{n+1, \ldots, 2n\} \) performs a Bell measurement on their qudits from both AME states. Without loss of generality, we can assume the measurement result is \((q, p) = (0, 0)\) (see Equation \ref{eq:20} for the notation), since other measurement outcomes produce the same state up to local transformations. Then the state shared by the parties \( \{1, \ldots, n, 2n+1, \ldots, 3n\} \) becomes

\[
|\Phi\rangle_{1, \ldots, n, 2n+1, \ldots, 3n} = \sum |i_1 \cdots i_n\rangle_{1, \ldots, n} U^2 |i_1 \cdots i_n\rangle_{2n+1, \ldots, 3n} \tag{31}
\]

Consecutive applications of the above procedure gives the following lemma:

**Lemma 8.** Suppose each group of parties \( \{1, \ldots, 2n\}, \{n+1, \ldots, 3n\}, \ldots, \{mn+1, \ldots, (m+1)n\} \) shares an AME\((2n, d)\) state,

\[
|\Phi\rangle = \sum |i_1 \cdots i_n\rangle U |i_1 \cdots i_n\rangle \tag{32}
\]

Then, if each of the parties \( \{n+1, n+2, \ldots, mn\} \) performs a Bell measurement on their two qudits, the resulting state shared by the parties \( \{1, \ldots, n, mn+1, \ldots, (m+1)n\} \) is locally equivalent to

\[
|\Phi\rangle_{1, \ldots, n, mn+1, \ldots, (m+1)n} = \sum |i_1 \cdots i_n\rangle_{1, \ldots, n} U^m |i_1 \cdots i_n\rangle_{mn+1, \ldots, (m+1)n} \tag{33}
\]

**Proof by induction.** The case for \( m = 2 \) is demonstrated in the above discussion already. If the lemma holds for \( m, \) for \( m+1 \) the two remaining states, after the parties \( \{n+1, n+2, \ldots, mn\} \) performed their Bell measurements, are

\[
|\Phi\rangle_{1, \ldots, n, mn+1, \ldots, (m+1)n} = \sum |i_1 \cdots i_n\rangle_{1, \ldots, n} U^m |i_1 \cdots i_n\rangle_{mn+1, \ldots, (m+1)n} \tag{34}
\]
and

\[ |\Phi\rangle_{mn+1,\ldots,(m+1)n,(m+1)n+1,\ldots,(m+2)n} = \sum |i_1 \cdots i_n\rangle_{mn+1,\ldots,(m+1)n} U |i_1 \cdots i_n\rangle_{(m+1)n+1,\ldots,(m+2)n} \cdot \quad (35) \]

After the parties \( \{ mn+1, \ldots, (m+1)n \} \) all perform a Bell measurement, the state shared by \( \{ 1, \ldots, n, (m+1)n+1, \ldots, (m+2)n \} \) becomes

\[ |\Phi\rangle_{1,\ldots,n,(m+1)n+1,\ldots,(m+2)n} = \sum |i_1 \cdots i_n\rangle_{1,\ldots,n} U |i_1 \cdots i_n\rangle_{(m+1)n+1,\ldots,(m+2)n}. \quad (36) \]

The state in Equation (33) is generally not an AME state, however, depending on the exact form of the unitary \( U \), the resulting state can be absolutely maximally entangled again for certain \( m \), as expressed in the following corollary.

**Corollary 9 (Swapping of AME States).** Suppose each set of parties \( \{ 1, \ldots, 2n \}, \{ n+1, \ldots, 3n \}, \cdots, \{ mn+1, \ldots, (m+1)n \} \) shares an AME(\( 2n,d \)) state,

\[ |\Phi\rangle = \sum |i_1 \cdots i_n\rangle U |i_1 \cdots i_n\rangle. \quad (37) \]

If \( U^m \) is locally unitary equivalent to \( U \) up to some permutation of parties, then, by making a Bell measurement on each of the parties \( (n+1, \ldots, mn) \), parties \( (1, \ldots, n, mn+1, \ldots, (m+1)n) \) will share an AME(\( 2n,d \)) state.

In the following we will show an example for AME swapping, the swapping of an AME(4,3) state. As an application we will show that different from the EPR state, the AME(4,3) state

\[ |\Phi\rangle = |0000\rangle + |0111\rangle + |0222\rangle \]

\[ + |1012\rangle + |1120\rangle + |1201\rangle \]

\[ + |2021\rangle + |2102\rangle + |2210\rangle \quad (38) \]

needs two steps of Bell measurements for the swapping to reproduce an AME(4,3) state.

**Example 10.** Assume we have three AME(4,3) states, shared by the players \( \{ A, B, C, D \}, \{ C, D, E, F \}, \) and \( \{ E, F, G, H \} \), respectively. After \( C, D, E, \) and \( F \) all perform a Bell measurement on their two qutrits, the parties \( \{ A, B, G, H \} \) will share an AME(4,3) state. This is illustrated in Figure 3.

**Calculation.** From Equation (38) we can see that the unitary \( U \) of Lemma 8 is given by

\[ U |00\rangle = |00\rangle \quad U |01\rangle = |11\rangle \quad U |02\rangle = |22\rangle \]

\[ U |10\rangle = |12\rangle \quad U |11\rangle = |20\rangle \quad U |12\rangle = |01\rangle \quad (39) \]

\[ U |20\rangle = |21\rangle \quad U |21\rangle = |02\rangle \quad U |22\rangle = |10\rangle \]
Figure 3: Entanglement swapping between three AME(4,3) states results in a new AME(4,3) state between previously unentangled parties. Dotted circles indicate where Bell measurements have to be performed.

Applying this unitary twice gives

$$U^2|00⟩ = |00⟩ \quad U^2|01⟩ = |20⟩ \quad U^2|02⟩ = |10⟩$$
$$U^2|10⟩ = |01⟩ \quad U^2|11⟩ = |21⟩ \quad U^2|12⟩ = |01⟩$$
$$U^2|20⟩ = |21⟩ \quad U^2|21⟩ = |02⟩ \quad U^2|22⟩ = |10⟩$$

It can be easily seen that by permuting the two parties and exerting a unitary transformation that exchange $|1⟩$ and $|2⟩$ in the second party, this unitary transformation becomes the identity. Thus $U^3$ is locally unitary equivalent to $U$ up to permutation of parties, and together with Corollary 9, it is easily to see that after the Bell measurement, the resulting state would be locally unitary equivalent with an AME(4,3) state up to a permutation of party G and H. Since the AME(4,3) state satisfies permutation symmetry, which means by permuting any two parties the resulting state is still an AME(4,3) state, A, B, G, H really share the same AME(4,3) state that was swapped.

Remark 1. In the above example, we require that party C acts as the third party of the first AME state and the first party of the second AME state. This is actually not required. Since the AME(4,3) state is permutationally invariant, we only need C to posses any qudit of each AME state. The same requirement applies for D. In fact, most of the AME states we found are permutational invariant, and in these cases we do not need to have restriction on which specific qudits the parties control.
7 Conclusion

In this paper, we have shown the existence of AME states for a wide range of parameters, in particular, the derivation of AME states from classical MDS codes proves that AME states exist for any number of parties if the system dimension is chosen large enough. We have proven an equivalence between AME states and threshold quantum secret sharing schemes. By extending the idea of how threshold QSS schemes follow from the entanglement properties of AME states, we have shown that a wider class, namely ramp QSS schemes can be constructed from AME states. The entanglement requirements to construct ramp QSS schemes are over-satisfied by AME states, and we prove the necessary and sufficient entanglement conditions for the construction of ramp QSS schemes.

Two more applications for AME states have been given in form of open-destination teleportation and entanglement swapping of AME states. The quantum secret sharing and teleportation scenarios that have been presented here and in Ref. [7], indicate that AME states can be used for a wide variety of quantum information protocols that involve the displacement of quantum states.

Acknowledgements

We acknowledge financial support by NSERC and the CRC program. We also want to thank Hoi-Kwong Lo, José Ignacio Latorre, Arnau Riera, and David Gosset for helpful discussions and comments.

A Entanglement in Ramp QSS Schemes

Here, we give a generalization of the methods used in Theorem 4 to prove the equivalence of AME states and threshold QSS schemes to \((m, L, 2m - L)\) ramp QSS schemes for arbitrary \(L\). The generalization is very straightforward, the secret dimension is now \(d^L\) instead of \(d\), changing also the dimension of the reference system to \(d^L\). We define an isometry \(U_S\) that encodes the \(d^L\) dimensional secret \(S\) into a state shared by the \(2m - L\) players, each holding a \(d\) dimensional system, \(U_S : \mathcal{H}_S \rightarrow \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_{2m-L}\). Where \(\mathcal{H}_i \cong \mathbb{C}^d\) and \(\mathcal{H}_S \cong \mathbb{C}^{d^L}\).

We further introduce a reference system \(\mathcal{H}_R \cong \mathcal{H}_S\) and consider the state \(|\Phi\rangle\) that is generated by applying the encoding operation to \(\mathcal{H}_S\) for a maximally entangled state \(|RS\rangle = 1/\sqrt{d}\sum |i\rangle |i\rangle \in \mathcal{H}_R \otimes \mathcal{H}_S\), i.e., \(|\Phi\rangle = \mathbb{I}_R \otimes U_S |RS\rangle\). A set of players \(A \subset P\) shares the state \(\rho_{RA} = \text{Tr}_{P\setminus A} |\Phi\rangle\) with the reference system. \(A\) is authorized, if there exists a completely positive map \(T_A : \mathcal{H}_A \rightarrow \mathcal{H}_S\) such that \([13, 20]\)

\[ \mathbb{I}_R \otimes T_A(\rho_{RA}) = |RS\rangle. \]  

For the mutual information between an authorized set (i.e., \(|A| \geq m\)) and the reference system is

\[ I(R : A) = I(R : S) = 2S(S) \quad \text{if} \quad |A| \geq m, \]
and for a forbidden set, we must have
\[ I(R : B) = 0 \quad \text{if } |B| \leq m - L. \tag{44} \]

\(U_S\) defines a \((m, L, 2m - L)\) ramp QSS scheme if and only if these two equations are satisfied.

Since any set of players \(C \subseteq P\) with \(|C| = L\) can change some forbidden set into an authorized set, we have \(S(C) \geq S(S)\) \[13\] for all sets with \(L\) players. And because \(S(S)\) is maximal and equal to \(S(R)\),
\[ S(S) = S(R) = S(C) = L \log d. \tag{45} \]

Equations \[43\] and \[44\] can be rewritten to give
\[ S(R, A) = S(A) - S(R) \quad \text{if } |A| \geq m \tag{46} \]
\[ S(R, B) = S(B) + S(R) \quad \text{if } |B| \leq m - L. \tag{47} \]

This sums up the changes in the lead-up to Theorem \[3\] whose version we may now state and prove for ramp QSS schemes. For this we regard the reference system of dimension \(d^L\) as consisting of \(L\) systems, each of dimension \(d\), so that \(|\Phi\rangle\) is a state shared between \(2m\) parties, \(2m - L\) players that share the secret and \(L\) in the reference system, each possessing a qudit.\]

**Theorem \[7\]** For a state \(|\Phi\rangle \in H_P \otimes H_R\) shared between \(2m - L\) players \(P\), each holding a qudit, and \(L\) reference qudits, the following two properties are equivalent:

(i) \(|\Phi\rangle\) is maximally entangled for any bipartition for which the \(L\) reference qudits are in the same set.

(ii) \(|\Phi\rangle\) is the purification of a \((m, L, 2m - L)\) ramp QSS schemes. The encoded secret of the ramp QSS scheme has dimension \(d^L\), and each share has dimension \(d\).

**Proof.** (i) \(\rightarrow\) (ii): In the equations for the mutual information, all occurring sets, \(A, B, R, A \cup R\) and \(B \cup R\), are maximally entangled with the rest because for all of them all reference qudits are in the same set of the bipartition. Hence we have \(S(A) = (2m - |A|) \log d\), \(S(B) = |B| \log d\), \(S(R) = S(S) = L \log d\), \(S(A, R) = (2m - |A| - L) \log d\) and \(S(A, B) = (|B| + L) \log d\). Plugging these into Equations \[43\] and \[44\] while using the definition of the mutual information (Equation \[10\]), confirms that these are satisfied.

(ii) \(\rightarrow\) (i): Consider an unauthorized set of players \(B\), with \(|B| = m - L\). Then the set is \(B \cup C\) is authorized for any additional set \(C\) with \(|C| = L\) and \(C \cap B = \emptyset\). From Equation \[16\] we have
\[ S(B, C, R) = S(B, C) - S(R) \tag{48} \]

On the other hand, using the Araki-Lieb inequality \[23\] \(S(X, Y) \geq S(X) - S(Y)\) and Equation \[47\] gives
\[ S(B, C, R) \geq S(B, R) - S(C) = S(B) + S(R) - S(C). \tag{49} \]

Combining the last two equations and using \(S(S) = S(R) = S(C)\) shows
\[ S(B, C) \geq S(B) + S(C), \tag{50} \]
where equality must hold due to the subadditivity of the entropy $S(X, Y) \leq S(X) + S(Y)$. This means that the entropy increases maximally when adding $L$ shares to $m - L$ shares. The strong subadditivity of the entropy [21]

$$S(X, Y) - S(Y) \geq S(X, Y, Z) - S(Y, Z)$$

states that adding system $X$ to system $Y$ increases the entropy at least by as much as adding system $X$ to a larger system $Y \cup Z$ that contains $Y$. So in our case, adding $L$ shares to less than $m - L$ shares increases the entropy by at least $S(C)$, and since this is the maximum, it increases the entropy exactly by $S(C)$. Moving the shares over one by one from $C$ to $m - L$ or less shares must increase the entropy maximally with each share for it to be maximally increased when all shares are added. Hence adding one share to a set that contains less than $m$ shares increases the entropy maximally. Hence, starting out with a set of no shares, and repeatedly adding one share to the set until the set contains any $m$ shares and is authorized, shows that any set of $m$ shares has entropy $m \log d$. This shows that the entropy is maximal for any subset of $m$ players, i.e., $|\Phi\rangle$ is maximally entangled for any bipartition into $m$ players $A$ and its complement $P \setminus A \cup R$, which contains all $L$ reference qudits, and thus is maximally entangled for any bipartition where all reference qudits are in the same set.

References

[1] A. Einstein, B. Podolsky, and N. Rosen, “Can quantum-mechanical description of physical reality be considered complete?,” Phys. Rev., vol. 47, pp. 777–780, May 1935.

[2] J. Bell, “On the einstein podolsky rosen paradox,” Physics, vol. 1, p. 195, 1964.

[3] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, “Quantum entanglement,” Rev. Mod. Phys., vol. 81, pp. 865–942, Jun 2009.

[4] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, “Mixed-state entanglement and quantum error correction,” Phys. Rev. A, vol. 54, pp. 3824–3851, Nov 1996.

[5] M. A. Nielsen, “Conditions for a class of entanglement transformations,” Physical Review Letters, vol. 83, p. 436, 1999.

[6] G. Vidal, “Entanglement of pure states for a single copy,” Phys. Rev. Lett., vol. 83, pp. 1046–1049, Aug 1999.

[7] 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.

[8] N. Gisin and H. Bechmann-Pasquinucci, “Bell inequality, bell states and maximally entangled states for n qubits,” Physics Letters A, vol. 246, no. 1-2, pp. 1 – 6, 1998.

[9] G. Gour and N. R. Wallach, “All maximally entangled four-qubit states,” Journal of Mathematical Physics, vol. 51, no. 11, p. 112201, 2010.
[10] E. M. Rains, “Quantum codes of minimum distance two,” Information theory, IEEE Transactions on, vol. 45, pp. 266–271, 1999.

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

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

[13] H. Imai, J. J. Mueller-Quade, A. Nascimento, P. Tuyls, and A. Winter, “An information theoretical model for quantum secret sharing schemes,” Quant. Inf. & Comp., vol. 5, p. 068, 2005.

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

[15] Z. Zhao, Y.-A. Chen, A.-N. Zhang, T. Yang, H. J. Briegel, and J.-W. Pan, “Experimental demonstration of five-photon entanglement and open-destination teleportation,” Nature, vol. 430, pp. 54–58, 2004.

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

[17] I. Reed and G. Solomon, “Polynomial codes over certain finite fields,” Journal of the Society for Industrial and Applied Mathematics, vol. 8, no. 2, pp. 300–304, 1960.

[18] G. Seroussi and R. Roth, “On mds extensions of generalized reed- solomon codes,” Information Theory, IEEE Transactions on, vol. 32, pp. 349 –354, may 1986.

[19] A. V. Thapliyal, “Multipartite maximally entangled states, minimal entanglement generating states and entropic inequalities.” unpublished presentation (2003).

[20] B. Schumacher and M. A. Nielsen, “Quantum data processing and error correction,” Phys. Rev. A, vol. 54, pp. 2629–2635, Oct 1996.

[21] M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information. 2000.

[22] M. Iwamoto and H. Yamamoto, “Strongly secure ramp secret sharing schemes,” in Information Theory, 2005. ISIT 2005. Proceedings. International Symposium on, pp. 1221–1225, 2005.

[23] V. Gheorghiu, “Generalized semi-quantum secret-sharing schemes,” Phys. Rev. A, vol. 85, p. 052309, May 2012.

[24] Security of Ramp Schemes, 1984.

[25] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, “Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels,” Phys. Rev. Lett., vol. 70, pp. 1895–1899, Mar 1993.
[26] B. Yurke and D. Stoler, “Einstein-podolsky-rosen effects from independent particle sources,” *Phys. Rev. Lett.*, vol. 68, pp. 1251–1254, Mar 1992.

[27] W. Dür, H.-J. Briegel, J. I. Cirac, and P. Zoller, “Quantum repeaters based on entanglement purification,” *Phys. Rev. A*, vol. 59, pp. 169–181, Jan 1999.