Multipartite Entanglement: Transformations, Quantum Secret Sharing, Quantum Error Correction

by

Wolfram Helwig

A thesis submitted in conformity with the requirements
for the degree of Doctor of Philosophy
Graduate Department of Physics
University of Toronto

Abstract

Multipartite Entanglement: Transformations, Quantum Secret Sharing, Quantum Error Correction

Wolfram Helwig
Doctor of Philosophy
Graduate Department of Physics
University of Toronto
2014

Most applications in quantum information processing make either explicit or implicit use of entanglement. It is thus important to have a good understanding of entanglement and the role it plays in these protocols. However, especially when it comes to multipartite entanglement, there still remain a lot of mysteries. This thesis is devoted to getting a better understanding of multipartite entanglement, and its role in various quantum information protocols.

First, we investigate transformations between multipartite entangled states that only use local operations and classical communication (LOCC). We mostly focus on three qubit states in the GHZ class, and derive upper and lower bounds for the successful transformation probability between two states.

We then focus on absolutely maximally entangled (AME) states, which are highly entangled multipartite states that have the property that they are maximally entangled for any bipartition. With them as a resource, we develop new parallel teleportation protocols, which can then be used to implement quantum secret sharing (QSS) schemes. We further prove the existence of AME states for any number of parties, if the dimension of the involved quantum systems is chosen appropriately. An equivalence between threshold QSS schemes and AME states shared between an even number of parties is established, and further protocols are designed, such as constructing ramp QSS schemes and open-destination teleportation protocols with AME states as a resource.

As a framework to work with AME states, graph states are explored. They allow for

efficient bipartite entanglement verification, which makes them a promising candidate for the description of AME states. We show that for all currently known AME states, absolutely maximally entangled graph states can be found, and we were even able to use graph states to find a new AME state for seven three-dimensional systems (qutrits). In addition, the implementation of QSS schemes from AME states can be conveniently described within the graph state formalism.

Finally, we use the insight gained from entanglement in QSS schemes to derive necessary and sufficient conditions for quantum erasure channel and quantum error correction codes that satisfy the quantum Singleton bound, as these codes are closely related to ramp QSS schemes. This provides us with a very intuitive approach to codes for the quantum erasure channel, purely based on the entanglement required to protect information against losses by use of the parallel teleportation protocol.

Contents

List of Figures

Chapter 1

Introduction

Quantum mechanics was developed at the beginning of the 20th century to cope with several problems like the black body radiation, describing the atomic model and the photoelectric effect. While the theory that developed was able to solve these problems, it also created a lot of discomfort among many physicists, because interpreting the predictions often seemed counterintuitive to their acquired classical intuition.

Among the most famous is Heisenberg's uncertainty principle, which says that the position and momentum of a particle cannot have definite values at the same time. Instead, the more constrained the position of a particle is, the more uncertain is its momentum, and vice versa. Thus, there is always an intrinsic uncertainty when performing measurements in quantum mechanics. A view that, among others, Einstein did not want to accept. His dissatisfaction with a theory that only gives probabilities for certain outcomes is famously captured in his quote "God does not play dice". In his eyes, a theory that can only give probabilities for certain measurement outcomes had to be incomplete.

Oddly enough, Einstein, Podolsky, and Rosen (EPR) [36] used another striking phenomenon predicted by quantum mechanics to construct an apparent paradox to demonstrate the incompleteness of quantum mechanics. Said phenomenon was entanglement, a term coined by Schrödinger when he introduced his famous Schrödinger's cat gedankenexperiment, which made its way into countless discussions among physicists and philosophers. Entanglement refers to correlations between quantum systems, which can have a much stronger bond between the involved systems than ever possible with classical correlations.

An example of creating classical correlations is to take two pieces of paper, one blue and one red, and put them into two envelopes. Then one of the envelopes is randomly given to Albert and the other to Erwin. They go their different ways and the moment one opens his envelope, he knows what the other one will see when he opens his. Thus

these two events are correlated. In a similar fashion, for a quantum system, two particles can be *entangled* in such a way that by measuring the position of one particle, one knows what a position measurement of the other particle will give. For such an entangled state, however, it is also possible for one party to measure the momentum instead of the position, and from the result deduce the momentum of the other particle. If we now again assume that Albert and Erwin each take one of the entangled particles and go far away from each other, Erwin's position measurement outcome is determined when Albert measures the position of his particle. Similarly, when he measures the momentum, the momentum of Erwin's particle is determined. If we now assume that Albert and Erwin moved so far apart that Erwin's particle cannot receive a signal from Albert's measurement before Erwin performs his, Erwin's measurement outcome cannot depend on which measurement Albert performs and thus position as well as momentum have to be predetermined, which is in contradiction to Heisenberg's uncertainty principle. This is the paradox that EPR constructed to argue that the theory of quantum mechanics is incomplete and is missing some local hidden variables that actually predetermine the measurement outcomes for which quantum mechanics only predicts a probability distribution.

This controversy resulted in heated discussions between Albert Einstein and Niels Bohr, but it was not until 30 years later that Bell showed how this dispute can be settled once and for all [9]. He formulated an inequality for two spin 1/2 particles that would hold for a theory in which the measurements are predetermined due to local hidden variables as Einstein suggested, but which is violated by predictions made by quantum mechanics. Experimental testing showed that inequalities that have to be satisfied by local hidden variable theories can indeed be violated, showing that EPR's claim of incompleteness of quantum mechanics does not hold. There still exist minor loopholes in the experiments that have been carried out, but due to the overwhelming evidence these experiments provide, almost all physicists now rule out the existence of local hidden variable theories.

After the existence of entanglement had been confirmed, people slowly started to recognize entanglement as a valuable resource, and the field of quantum information was born. Since then a multitude of information processing protocols have been proposed and experimentally implemented that make heavy use of entangled states to accomplish tasks that are impossible in a classical setting.

Hence, in order to find new ways of making use of these quantum correlations, it is important to have as good an understanding of entanglement as possible. And while entanglement between two systems is already relatively well understood, the entanglement structure of more than two systems is very complicated and only little progress has been made in understanding this structure. This thesis is devoted to gaining a better under-

standing of multipartite entanglement and its role in quantum information processing protocols.

1.1 Overview of the Thesis

My PhD study was directed towards gaining a deeper understanding of multipartite entanglement and its role in quantum information protocols. First, I studied possible transformation between multipartite entangled state within the regime of local operations and classical communications (LOCC). During this part I was mostly dealing with pure three qubit states.

After that I focused on a special kind of highly entangled multipartite states, called absolutely maximally entangled (AME) states, which have the property that they are maximally entangled with respect to any bipartition. These states are then used to develop a new parallel teleportation protocol, which leads to the derivation of threshold quantum secret sharing (QSS) protocols [30] that solely rely on the entanglement of the initial AME state. We then use that insight to derive necessary and sufficient entanglement condition for a wider class of "ramp" QSS schemes.

Due to fact that quantum information cannot be copied, QSS schemes are intrinsically very similar to quantum codes that protect quantum information against losses, described by a quantum erasure channel (QEC) [48]. Thus, with our entanglement based approach, we can also provide a very intuitive treatment of the quantum erasure channel that only relies on the entanglement of the state used for encoding and the parallel teleportation protocol. The necessary and sufficient entanglement condition of the QSS schemes translate to *"optimal"* codes for the QEC, those that satisfy the quantum Singleton bound. Furthermore, since codes for the QEC are equivalent quantum error correction codes (QECC) [48, 72], this also gives necessary and sufficient entanglement conditions for QECCs that satisfy the quantum Singleton bound, also referred to as quantum MDS codes or optimal quantum codes.

When dealing with multipartite entangled states in the Dirac notation, a lot of the entanglement features are "hidden" within the notation. Hence, when looking for other methods to represent quantum states, I found graph states to be a particularly useful tool [20]. Entanglement in graph states is either "on or off", which is ideal to study maximally entangled states. Thus, in addition to the standard Dirac notation, I used the graph state formalism for d-dimensional systems (qudits) to investigate AME states. This approach also leads naturally to quantum error correction codes, this time in the form of graph codes [113, 49].

Additionally, graph states have the benefit, that they, at no extra cost, provide a quantum circuit that generates the state. This should prove useful for the actual implementation of AME states once our experimentalist friends figure out how to implement controlled-Z gates for qudits. At the moment, experimental implementations of graph states still mostly focus on qubits, with the successful generation of an eight qubit graph states with photons [64, 139], and a 14 qubit graph state with ions [92]. This will be further discussed in the Conclusion.

The thesis is structured into the following chapters:

Chapter 2: This chapter provides a short overview of the basic tools used in entanglement theory.

Chapter 3: In collaboration with Wei Cui and Hoi-Kwong Lo. Here we derive upper and lower bounds for the probabilities of LOCC transformations between multipartite entangled states, for the most part dealing with three qubit states in the GHZ class. I collaborated in deriving upper and lower bounds for the transformation from the GHZ state to a GHZ class state. I had little part in deriving the upper bound provided in Section 3.4 for a more general initial state, which was almost entirely my coauthors' work, but is included for completeness. The results of this chapter are published in Ref. [32].

Chapter 4: In collaboration with Wei Cui, José Ignacio Latorre, Arnau Riera, and Hoi-Kwong Lo. This chapter introduces the concept of AME states and presents protocols for new parallel teleportation scenarios and threshold QSS schemes based on AME states. I derived the general protocols for the construction of parallel teleportation protocols and threshold QSS schemes from AME states. The results of this chapter are published in Ref. [58].

Chapter 5: In collaboration with Wei Cui. In this chapter, we further investigate AME states. We show their existence for a general number of parties and prove that there is a one-to-one correspondence between AME states for an even number of parties and threshold QSS schemes. More applications for AME states are presented in form of ramp QSS schemes and open-destination teleportation. I formulated the proofs that show the general existence of AME states and their equivalence with threshold QSS schemes. I further developed the protocols leading to ramp QSS schemes and open-destination teleportation. The results of this chapter can be found in Ref. [57].

Chapter 6: For this chapter, I used the graph states formalism for qudits of prime dimension to describe AME states. I showed two methods for checking the bipartite entanglement in graph states: one graphical method, and one that can be efficiently implemented on a computer. I showed that for all parameters, for which we know that AME states exist, AME graph states can also be found, and I additionally found a new AME graph state for 7 qutrits. I further showed that the derivation of ramp and threshold QSS schemes can be conveniently formulated in the graph states formalism and elaborated on methods of dealing with non-prime dimensions, which was demonstrated by giving an example of an AME graph state for four 4-dimensional systems. To investigate AME graph states, I wrote a simulation that can check the entanglement properties of graph states efficiently using the methods presented in this chapter. The results of this chapter can be found in Ref. [56].

Chapter 7: In this last project, I extended the previously derived one-to-one correspondence between AME states and threshold QSS schemes to derive necessary and sufficient entanglement conditions for the ramp QSS schemes introduced in Chapter 5. This then led to necessary and sufficient entanglement conditions for optimal codes of the quantum erasure channel, and thus optimal QECCs. Again, graph states proved to be a useful tool in this investigation, and I showed a one-to-one correspondence between the existence of stabilizer codes that satisfy the Singleton bound and highly entangled graph states. The results of this chapter can be viewed as first step to a very intuitive, purely entanglement based approach to quantum error correction.

Chapter 8: In this last chapter, I give a quick summary of the key results of the thesis and provide an outlook on possible future research directions based on this thesis.

Chapter 2

Background Information

In this chapter, we give a short introduction to the basic tools of entanglement theory that are used throughout this thesis. This is by no means an exhaustive coverage of the subject. For a more extensive treatment, which we refer the reader to the excellent review of quantum entanglement by Horodecki et al., found in Ref. [62], and to Ref. [96] for an introduction to quantum information in general. Anyone already familiar with the material may want to skip this chapter.

2.1 Bipartite Entanglement

2.1.1 Definition

A bipartite entangled state is a state consisting of two systems that possess correlations that are stronger than anything that is possible in a classical setting. Operationally that means it is a state that cannot be created by only performing local (quantum) operations on each system when the two systems are only allowed to exchange classical information. Thus a pure state $|\Psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_A$, is entangled if and only if it cannot be written in the form

$$|\Psi\rangle = |\Psi_A\rangle_A |\Psi_B\rangle_B \tag{2.1}$$

for some $|\Psi_A\rangle_A \in \mathcal{H}_A$ and $|\Psi_B\rangle_B \in \mathcal{H}_B$. A state of that form is called *separable*. A mixed state ρ_{AB} is separable if it can be written in the form

$$\rho_{AB} = \sum_i p_i \rho_A^i \otimes \rho_B^i, \tag{2.2}$$

where $p_i \geq 0$, and ρ_A^i are states in system A and ρ_B^i in system B, respectively. In this case, there exist correlations between the two systems, but they can be created by merely performing local operations and classical communications (LOCC) between the two systems and thus can be regarded as classical correlations. Entanglement is only created if a joint quantum operation is performed on both systems together.

A state that cannot be written in the form of Equation (2.1) is the state

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle_A |\uparrow\rangle_B + |\downarrow\rangle_A |\downarrow\rangle_B), \tag{2.3}$$

which is the spin 1/2 analog of the state used by EPR to construct their paradox. It is thus commonly referred to as a *EPR pair* or *Bell state*. For two d-dimensional systems, one can always write a pure state in the form of its *Schmidt decomposition*

$$|\Psi\rangle = \sum_{i=0}^{d-1} \lambda_i |i\rangle_A |i\rangle_B \tag{2.4}$$

where $\lambda_i \geq 0$, and $|i\rangle_A$ and $|i\rangle_B$ form an orthonormal basis in system A and B, respectively. The *Schmidt coefficients* λ_i are unique and we will always assume that they are ordered, $\lambda_i \geq \lambda_{i+1}$. They satisfy $\sum \lambda_i^2 = 1$, and contain all the information about the entanglement in the state. If there is only one $\lambda_i \neq 0$, then the state is separable.

2.1.2 Entanglement Transformations

Given two states, $|\Psi\rangle$ and $|\Phi\rangle$, with Schmidt coefficients x_i and y_i, respectively, one may ask the question which one is more entangled. A question that turns out to be much more difficult to answer than one might expect. One thing we can certainly say, however, is that if one $|\Psi\rangle$ can be transformed into $|\Phi\rangle$ by only using LOCC, $|\Psi\rangle$ possesses at least as much entanglement as $|\Phi\rangle$. The answer when this is possible in the bipartite setting has been answered by Nielsen [96]. This is elegantly done by using the concept of vector majorization. A d-dimensional vector y majorizes x, written as $y \prec x$, if

$$y \prec x: \quad \sum_{j=0}^{k} y_j \leq \sum_{j=0}^{k} x_j \quad \text{for all} \quad k = 0, \ldots, d-1. \tag{2.5}$$

Then $|\Psi\rangle$ with Schmidt coefficients x_i can be transformed into $|\Phi\rangle$ with Schmidt coefficients y_i by LOCC if and only if $y^2 \prec x^2$. Here x^2 refers to the vector with the entries x_i^2. For two-dimensional system, this gives a strict ordering, the closer the two Schmidt coefficients are, the more entangled the state is. However, for higher dimensional systems,

it is possible that neither $y^2 \prec x^2$, nor $x^2 \prec y^2$, and thus neither transformation can be deterministically performed by LOCC. A state for which all Schmidt coefficients have the same value $(1/\sqrt{d})$ is maximally entangled, as it can be transformed into all other d-dimensional states by LOCC. As such the EPR pair in Equation (2.4) is maximally entangled for two spin 1/2 particles.

Instead of requiring a success probability of one, we may consider transformations that succeed with a non-zero probability, not necessarily one, while allowing only local operations and classical communication. If such a transformation exists from $|\Psi\rangle$ to $|\Phi\rangle$, we say that $|\Psi\rangle$ can be transformed into $|\Phi\rangle$ by stochastic local operations and classical communications (SLOCC).

The problem of finding the maximal transformation probability by SLOCC was considered by Lo and Popescu [81] for a maximally entangled target state, and by Vidal [131] for the general case. They found that the maximal transformation probability from a state $|\Psi\rangle$ to $|\Phi\rangle$ with Schmidt coefficients x_i and y_i, respectively, is given by [131]

$$P(|\Psi\rangle \to |\Phi\rangle) = \min_{l \in [0,d-1]} \frac{\sum_{i=l}^{d-1} x_i^2}{\sum_{i=l}^{d-1} y_i^2}. \tag{2.6}$$

This includes Nielsen's majorization result, since the probability is 1 if and only if $y^2 \prec x^2$.

2.1.3 Entanglement Measures

The treatment of possible entanglement transformations already gives us a good idea about which states are more entangled than others. However, it is still helpful to formally define functions that quantify entanglement. This will especially turn out to be helpful in the treatment of multipartite entanglement, for which the maximum probability for SLOCC transformations is far from solved. The formal definition is not particularly difficult, an entanglement measure is defined as a function over the state space that cannot increase under LOCC operations [129, 132]. Thus an entanglement measure $E(\rho)$ satisfies

$$E(\Lambda(\rho)) \leq E(\rho) \tag{2.7}$$

for all LOCC operations Λ.

It is often easier to define entanglement measures for pure states and then extend them to mixed states. This can be done with the *convex roof* extension. Given an entanglement measure $E(|\Psi\rangle)$ for pure states, an entanglement measure for mixed states

is given by its convex roof extension [128]

$$E(\rho) = \inf \sum_j p_j E(|\Psi_k\rangle), \tag{2.8}$$

where the infinum is taken over all possible pure states ensembles $\{p_j, |\Psi_j\rangle\}$ for which $\rho = \sum_j p_j |\Psi\rangle \langle\Psi|$. In the following, we will give examples of entanglement measures that will become useful in the following chapters.

Maximum SLOCC Transformation Probability

Quite trivial, but nonetheless useful is the observation that for a given state σ, the maximum probability to transform to that state from ρ by SLOCC cannot be increased by LOCC. This means

$$E(\rho) = P_{\max}(\rho \to \sigma) \tag{2.9}$$

is an entanglement measure.

Schmidt Rank

For a pure state $|\Psi\rangle$ with Schmidt coefficients λ_i, the Schmidt rank k, defined as the number of non-zero Schmidt coefficients, is an entanglement measure [81]. This can be seen directly from Equation (2.6). The Schmidt rank has the interesting property, that if $k(|\Phi\rangle) > k(|\Psi\rangle)$, the transformation probability from $|\Psi\rangle$ to $|\Phi\rangle$ by SLOCC is zero.

In general, this is not a property that holds for an entanglement measure E. If $E(|\Phi\rangle) > E(|\Psi\rangle)$, we only know that $|\Psi\rangle$ cannot be transformed to $|\Phi\rangle$ by LOCC, i.e., with probability 1. What can be deduced from the defining equation for an entanglement measure, Equation (2.9), is that

$$P_{\max}(|\Psi\rangle \to |\Phi\rangle) \leq \frac{E(|\Psi\rangle)}{E(|\Phi\rangle)}. \tag{2.10}$$

In fact, this is what Vidal used to show that Equation (2.6) is an upper bound for the SLOCC transformation, since $E_l(|\Psi\rangle) = \sum_{i=l}^{d-1} x_i^2$ are entanglement monotones and then he provided an actual protocol that accomplished this upper bound.

Concurrence

For two pure state of two qubits, it is not hard to determine which one is more entangled, we just have to look at the Schmidt decomposition, and the state for which the Schmidt

coefficients are closer together is more entangled. However, there is no such simple method for mixed states of two qubits. In this case we need a proper entanglement measure. Such an entanglement measure is the concurrence, which for pure states is defined as [60, 136]

$$C(|\Psi\rangle) = |\langle\Psi|\tilde{\Psi}\rangle|, \tag{2.11}$$

where $|\tilde{\Psi}\rangle = \sigma_y \otimes \sigma_y |\Psi^*\rangle$, and $|\Psi^*\rangle$ is the complex conjugate of $|\Psi\rangle$ when expressed in the Z-Basis. One can show that the concurrence for pure states is equal to $C(|\Psi\rangle) = 2\sqrt{\det \rho_A}$, where ρ_A is the reduced state of the first qubit [31].

The nice thing about the concurrence is that a closed form for its convex roof extension exists. It is given by [136]

$$C(\rho) = \max\{0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4\}, \tag{2.12}$$

where λ_i are the square roots of the eigenvalues of $\rho\tilde{\rho}$ in decreasing order, where

$$\tilde{\rho} = (\sigma_y \otimes \sigma_y)\rho^*(\sigma_y \otimes \sigma_y), \tag{2.13}$$

and ρ^* again is the complex conjugation of ρ when expressed in the Z-basis.

2.2 Multipartite Entanglement

2.2.1 Definition

The basic definition for entanglement in multipartite states is the same as for bipartite systems. A state is entangled if it cannot be created by LOCC from previously uncorrelated systems. A state that possesses no entanglement is called separable. A pure multipartite state shared among n parties is separable if it can be written in product form

$$|\Psi\rangle = |\Psi_1\rangle \otimes \cdots \otimes |\Psi_n\rangle . \tag{2.14}$$

For a mixed state ρ we have that it is separable if it can be written as

$$\rho = \sum_i p_i \rho_1^i \otimes \cdots \otimes \rho_n^i, \tag{2.15}$$

with $p_i \geq 0$, and ρ_j^i density matrices for the individual systems. This definition also classifies, e.g., the tripartite state

$$|\Psi\rangle = \frac{1}{\sqrt{2}} |0\rangle_A (|0\rangle_B |0\rangle_C + |1\rangle_B |1\rangle_C) \tag{2.16}$$

as entangled, although party A possesses no correlations with B and C. The state thus contains only bipartite entanglement and is not really entangled between all systems. Hence it makes sense to further classify a state shared between n parties as being truly n-partite entangled if it is entangled for any possible bipartition of the n parties. An example of a state for n qubits that possesses n-partite entanglement is the Greenberger-Horne-Zeilinger (GHZ) state [51]

$$|\mathrm{GHZ}_n\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes n} + |1\rangle^{\otimes n}). \tag{2.17}$$

2.2.2 Entanglement Measures

Entanglement in the multipartite setting has a much richer structure than in the bipartite case. As outlined above, in addition to the bipartite entanglement that can exist in multipartite states, and which can be quantified with bipartite entanglement measures by dividing the parties into two sets, there also exists true multipartite entanglement that calls for appropriate measures to quantify it. In the following, we present two entanglement measures that are crucial in classifying entanglement classes for three qubits.

3-tangle

Given three qubits, one may ask, if qubit A is entangled with B, does that affect its ability to be entangled with C? If A and B are maximally entangled, their state has to be locally equivalent to an EPR pair, i.e., a pure state. This means that in this case the pair AB, and therefore also A, cannot be entangled with C. However, if A is only partially entangled with B, then it seems plausible that it can also at the same time be partially entangled with C.

It turns out, that this can be nicely expressed by quantifying the bipartite entanglement between the systems in terms of the concurrence. If $\mathcal{C}_{AB}$, C_{AC} and $C_{A(BC)}$ denote the concurrence between A and B, A and C, and A and the pair BC, respectively, than the following inequality holds [31]

$$C^2_{A(BC)} \geq C^2_{AB} + C^2_{AC}. \tag{2.18}$$

We can interpret this in the sense that the entanglement that A shares with B and C individually cannot be more than the entanglement that A shares with BC when regarded as one system. And since the possible entanglement between A and BC is limited, if A already shares all that entanglement with B, there is no more entanglement left that can be shared with C.

Furthermore, if Equation (2.18) is a strict inequality, the difference of the two sides can be regarded as new form of mulitpartite entanglement that the three qubits share as a whole, and is called the *3-tangle* τ_{ABC},

$$C^2_{A(BC)} = C^2_{AB} + C^2_{AC} + \tau_{ABC}. \tag{2.19}$$

Although not obvious from this equation, the 3-tangle is in fact permutationally symmetric, and it has been shown to satisfy the requirements of an entanglement measure [34].

Schmidt Rank

Similar to the case of bipartite states, one can define the Schmidt rank $r(|\Psi\rangle)$ for a pure multipartite state $|\Psi\rangle$ as the minimum number of terms required, when it is expressed as a superposition of product states,

$$|\Psi\rangle = \sum_{i=1}^{k} \alpha_i \, |\Psi_1^i\rangle \otimes \cdots \otimes |\Psi_n^i\rangle \, . \tag{2.20}$$

The Schmidt rank, as in the bipartite case, tells us that $|\Psi\rangle$ cannot be transformed into $|\Phi\rangle$ by SLOCC if $r(|\Phi\rangle) > r(|\Psi\rangle)$.

2.2.3 Classification of Pure Three Qubit States

For two qubits in a pure state, the classification of entanglement is fairly easy. If two states are entangled, then they can be transformed into each other with a non-zero probability by SLOCC, and the maximum probability can be determined by Equation (2.6). Furthermore, there exists only one type of entanglement, and, given two pure states, we can definitely say which one is more entangled, e.g., by using the concurrence as entanglement measure, and the more entangled state can be deterministically transformed into the other one by LOCC.

For the multipartite case, however, things get a lot more complicated. Even for the simplest case of pure states of three qubits, there exist different types of entanglement

that cannot be transformed into each other. Hence it makes sense to categorize states into different entanglement classes. Every state of one class is SLOCC-convertible into any other state of the same class, i.e., there exists a SLOCC protocol that has a success probability greater 0 for the transformation in either direction. We say that two such states are equivalent under SLOCC, or in the same SLOCC equivalence class. There are six different SLOCC equivalent classes for pure states of three qubits [34]

1. The *GHZ-class* with its representative

$$|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \tag{2.21}$$

2. The *W-class* with its representative

$$|W\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle) \tag{2.22}$$

3. Three *bipartite entanglement* classes, which contain states that are entangled in only two of the parties, i.e., states of the form $|0\rangle_A |\Phi\rangle_{BC}$ and equivalently for disentangled Bob and Charlie.

4. *Separable states* of the form $|a\rangle |b\rangle |c\rangle$.

States from the GHZ-class and the W-class cannot be transformed into each other via SLOCC. Two states $|\Psi\rangle$ and $|\Phi\rangle$ are equivalent under SLOCC if an invertible local operator $A \otimes B \otimes C$ transforming $|\Psi\rangle$ into $|\Phi\rangle$ exists. However, by employing non-invertible operators, GHZ-class and W-class states can be converted into states from the bipartite and separable class, and bipartite entangled states can be converted into separable states. These processes, however, do not work in the opposite directions. The GHZ-state itself can be converted with probability 1 into a maximally entangled bipartite state and thus also with probability 1 into any bipartite entangled state.

By calculating the 3-tangle τ_{ABC}, and the rank of the three reduced density matrices ρ_A, ρ_B, and ρ_C, we can determine to which class a state belongs. For GHZ- and W-class states, all reduced density matrices, ρ_A, ρ_B, and ρ_C have rank 2, for bipartite entangled states, the one of the qubit that is not entangled with the other two has rank 1, and all of them have rank 1 for separable states. States in the GHZ-class have $\tau_{ABC} > 0$. For the other five classes, the 3-tangle is 0. This can be used to distinguish states in the GHZ- and W-class. It further tells us that a state of the W-class cannot be transformed by SLOCC to a state in the GHZ-class because the 3-tangle is an entanglement measure.

Another way to distinguish GHZ- and W-class states is by its Schmidt rank. States in the W-class have Schmidt rank of 3 (i.e., the minimal number required for writing the state as a sum of product states is 3), separable states obviously have a Schmidt rank of 1, and states from the other four classes have a Schmidt rank of 2. Since the Schmidt rank is an entanglement measure, SLOCC transformations from GHZ-class states to W-class states are not possible.

2.3 Quantum Information Protocols

Entanglement is a valuable resource in a lot of quantum information protocols. In this section, we quickly review three protocols that will play a major role later in this thesis. The first, teleportation of a quantum state [13], makes explicit use of entangled states as a resource. For the other two, quantum secret sharing (QSS) [30, 45] and quantum error correction codes (QECC) [72, 44], the importance of entanglement is not immediately obvious from its formulation. However, we will see later that highly entangled multipartite states are a crucial requirement for these protocols to exist.

2.3.1 Quantum Teleportation

In quantum mechanics, it is not possible to copy quantum states, something known as the no-cloning theorem [135]. Thus, if Alice and Bob are at two separated positions and only able to exchange classical information, and Alice possesses an unknown quantum state $|\Psi\rangle$, it does not seem possible for her to acquire classical information by some sort of measurements, that would allow Bob to generate $|\Psi\rangle$ if he receives this information. Otherwise Alice could just send copies of this classical information to more people, who can then all generate $|\Psi\rangle$, and they together would have created multiple copies of the initial state.

This task, moving an unknown quantum state from one place to another by only exchanging classical information, can, however, be achieved if the two parties share entanglement by performing a *quantum teleportation* protocol [13]. The trick is that the required measurement on Alice's side destroys her state $|\Psi\rangle$, and the classical information is only valuable for the other party of the entangled state that is used in the measurement. Thus only one copy of the state can exist after performing the protocol, and thus the no-cloning theorem is not violated.

2.3.2 Quantum Secret Sharing

In quantum secret sharing (QSS) [30, 45], a dealer wants to encode a quantum state, the secret, into a multipartite state that is then distributed among a number of players. The part of the multipartite state that a player gets is referred to as his *share*. The encoded state should have the property that only certain sets of players are able to recover the secret from their shares by applying joint quantum operations to them, i.e., they must be at the same location or have some way to exchange quantum information. A set that is able to recover the secret is called an authorized set. The sets that are not authorized can be further divided into forbidden sets, which are not able to gain any information about the encoded secret, and intermediate sets, which are able to gain partial information about the secret.

Here we only consider pure state QSS schemes, which means that the secret and the encoded secret are both pure states. One popular access structure for QSS schemes are threshold schemes. They have the encoded secret distributed among n players such that authorized sets are all sets with more than a threshold value, k, of players, and any set with less than k players is forbidden. Such a QSS scheme is referred to as a ((k,n)) threshold QSS scheme. For pure state threshold QSS scheme, we always have that $n = 2k - 1$, and dimension of each share is the same as the secre0t [30, 45].[1]

An example of a $((2, 3))$ threshold QSS scheme for qutrits is given by the encoding

$$\begin{aligned} \alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle \rightarrow \quad & \alpha(|000\rangle + |111\rangle + |222\rangle) \\ & + \beta(|012\rangle + |120\rangle + |201\rangle) \\ & + \gamma(|021\rangle + |102\rangle + |210\rangle). \end{aligned} \tag{2.23}$$

Each party by itself has a completely mixed state that is independent of the secret, thus one party is forbidden. Two parties can apply the joint unitary operation $U|i\rangle|j\rangle = |2i + j\rangle|i + j\rangle$ (all kets are understood to be modulus 3) to obtain the state

$$(\alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle)\ (|00\rangle + |12\rangle + |21\rangle), \tag{2.24}$$

which recovers the secret in the first qutrit. Similar joint unitary operations exist for the sets of player $\{1, 3\}$ and $\{2, 3\}$.

[1] Of course a player can chose to store his data in a higher dimensional system and thus hold a higher dimensional share, however the important information for recovery will always only be a d-dimensional subspace of the system.

2.3.3 Quantum Error Correction Codes

Quantum error correction is a very large field. Here we only give a very quick overview of the basic notation that is needed in later chapters. For a more extensive introduction, see, e.g., Refs. [96, 44]. Quantum error correction is the task of protecting quantum information against errors or loss. For classical information, there are quite intuitive ways to protect information against errors or loss. If we have some classical information, and we are worried that we might lose it, we can simply make an identical copy of the information, and now if we either lose the original or the copy, we will still have an exemplar of the information left. Similarly, if for instance we want to send some information and while sending it, it might pick up an error, i.e., change, we can send multiple copies of the same information, and assuming that the error probability is small, compare the information

For quantum information, things get a bit more complicated. Since we cannot copy a quantum state, the methods used for classical information cannot simply be used for quantum information as well. For instance to protect against loss, we cannot make multiple copies of an arbitrary quantum state and then just use the ones that did not get lost. So at first glance, it would seem that the no-cloning theorem prevents us from protecting quantum information against loss. Surprisingly, it turns out that there is still a way. In fact, we have already seen an example of how it works in Equation (2.23), because quantum secret sharing is in a way the same as protecting against loss, although with a different motivation. In quantum secret sharing we want to make sure that certain subsets of players don't have any information about the encoded secret. At the same time, this means that these players are not needed to recover the secret and thus losing their shares can be corrected.

In the case of loss we know which error occurred - we know which qudit was lost. For general error correction, where it is not known which specific error occurred, but we want to be able to correct a certain set

It was shown by Knill and Laflamme [72], that if the encoding $U : \mathcal{H}_s \to \mathcal{H}_e$ encodes states of a smaller Hilbert space $\mathcal{H}_s \cong \mathbb{C}^D$ with basis states $|0\rangle, \ldots, |D-1\rangle$ into a larger Hilbert space[2], where we denote the encoded basis states by $|\bar{i}\rangle = U|i\rangle$, errors in $\mathcal{E}$ can be corrected if and only if, for $E_a, E_b \in \mathcal{E}$,

$$\langle \bar{i}|E_a^\dagger E_b|\bar{j}\rangle = f(E_a^\dagger E_b)\delta_{ij}. \tag{2.25}$$

This equation combines two conditions, first that $\langle \bar{i}|E_a^\dagger E_b|\bar{j}\rangle = 0$ for $i \neq j$, which ensures

[2]Unless otherwise noted, we always assume that the basis states are orthonormal, $\langle i|j\rangle = \delta_{ij}$.

that $|i\rangle$ and $|j\rangle$ stay orthogonal if an error occurs. The second condition $\langle\bar{i}|E_a^\dagger E_b|\bar{i}\rangle = \langle\bar{j}|E_a^\dagger E_b|\bar{j}\rangle$ makes sure that by learning which error occurred, no information is gained about the encoded state.

Generally, for quantum error correction codes, we assume that the encoding is into a state of n qudits, i.e., $\mathcal{H}_e = \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n$, with $\mathcal{H}_i \cong \mathbb{C}^d$, and that the correctable errors $\mathcal{E}$ are any errors on up to a certain number t of qudits. Then Equation (2.25) must hold for any operator $E = E_a^\dagger E_b$ that acts non-trivially on up to $2t$ qudits. Thus we define the *distance* δ of a code as the smallest value for which an operator $E = E_a^\dagger E_b$ exists that acts non-trivially on δ qudits and violates Equation (2.25). Such a code is denotes as a $((n, D, \delta))_d$ QECC.

Definition 2.1. A $((n, D, \delta))_d$ QECC is a quantum error correction code that encodes a D-dimensional quantum state into n qudits of dimension d and has distance δ.

A quantum error correction code that can correct up to t errors must have at least distance $\delta = 2t + 1$. To recover an encoded quantum state after losing r qudits, where the location of the lost qudits is known, requires a distance of $\delta = s + 1$. Often we will consider codes where the encoded states are also a collection of m qudits, such that $D = d^m$, but this is not a requirement for general codes.

2.4 Experimental Realization of Entangled States

In addition to the above described theoretical development of quantum information theory, the techniques for experimental realization of entangled states have also seen tremendous progress in the last couple of decades.

Two of the most promising systems to experimentally implement multipartite entangled states and quantum information protocols are photonic systems and trapped ions. In this section, we will shortly review their ability to encode quantum information and how entangled states can be created in these systems.

2.4.1 Photons

Photons offer a variety of different methods to encode quantum information [100]. The most common way is to use the polarization degree of freedom to encode the quantum information. The polarization of a photon is described by a two-level quantum system, with the basis most commonly chosen to be horizontal and vertical polarization. A general polarization state is then given by $|\Phi\rangle = \alpha\,|H\rangle + \beta\,|V\rangle$. The polarization of a photon is easily manipulated with polarizing beam splitters, polarizers and wave plates.

Another option to encode quantum information onto a photon is by using its spatial degree of freedom. In this case, different spatial modes or paths are defined for the photon, each of which represents an orthogonal basis state, and the photon can be in any superposition state of these modes. Manipulations of states encoded in spatial modes can be performed with multiport interferometers, for which it has been shown that they can always be decomposed into a system of beam splitters and phase shifters [107]

Since, in principle, any number of different spatial modes can be defined, this method can be used to implement general d-level systems (qudits) with photons. Similarly, instead of actually defining different physical paths for the photon, the quantum information can be encoded onto the orbital angular momentum [87] or frequency [125] of the photon, or by defining different time-bins along one path such that different time-bins represent orthogonal basis states for the qudit [11, 43]. Furthermore, different encoding options can be combined to encode higher dimensional information onto one photon. This simultaneous entanglement in multiple degrees of freedom is also as *hyper-entanglement* [75]. The most prominent choice for this is to use the polarization as well as different spatial modes of one photon.

Spontaneous Parametric Down-Conversion (SPDC)

In a spontaneous parametric down-conversion (SPDC) process (see, e.g., Ref. [100] and references therein), a high energy photon from a pump laser source is converted in a nonlinear crystal into two lower energy photons, called "signal" and "idler". The energy and momentum of the pump photon and the signal and idler photons are correlated such that $\omega_0 \approx \omega_i + \omega_s$ and $\mathbf{k}_0 \approx \mathbf{k}_i + \mathbf{k}_s$, where the exact relation is given by the *phase matching* condition of the nonlinear crystal. This phase matching condition implies that the signal and idler photons are entangled in frequency and momentum. In particular, this means that the directions in which signal and idler photons emerge from the nonlinear crystal are entangled and hence the SPDC process can be used to create two photons whose spatial modes are entangled.

Regarding the polarization of the emitted photons, there are two different types of SPDC processes, a type-I process, where the signal and idler photons have the same polarization, and a type-II process, where signal and idler have opposite polarizations. The two polarizations correspond to the ordinary and extraordinary waves of the crystal and thus are generally emitted into different directions. However, by carefully choosing the photons that are emitted into directions that are allowed for both waves, the spatial and polarization information can be decoupled, and the two photons are indistinguishable, resulting in a polarization entangled EPR state.

Additionally, the SPDC process can also be used to create two-photon states that are simultaneously entangled in their polarization and spatial modes. This is accomplished by reflecting the pump laser after it passed through the nonlinear crystal the first time to let it pass through it a second time, resulting in the possibility of creating an entangled photon pair in the direction opposite to the pair of the first pass [26, 138, 6]. If the distance of the reflecting mirror is chosen appropriately, this results in a two-photon hyper-entangled state of the form $|\Psi\rangle = |\psi\rangle_{\text{pol}} \otimes |\psi\rangle_{\text{path}}$, where $|\psi\rangle_{\text{x}}$ is a maximally entangled EPR state in the polarization or spatial degree of freedom, respectively.

Multi-Photon Entanglement

With SPDC, we have at our hands a good source to create two-photon entanglement, and, with careful engineering, SPDC sources can even be used to create multi-photon entangled states. One option to accomplish this is to cascade two SPDC sources such that one photon of the first pair gets further down-converted in a second crystal to generate genuine multipartite entanglement between three photons, the one photon remaining from the first pair and the two photons created in the second crystal [65, 119]. Another option to create multi-photon entanglement is to first generate multiple two-photon entangled states with SPDC processes, and then superpose them on linear optical networks to create multi-photon entangled states. Currently, this is the method most commonly used for the creation of multi-photon entanglement.

One of the biggest challenges in this proposal is that for photons originating from different SPDC processes to be able to be superposed on a beam splitter, they have to be indistinguishable. In particular, this means that they have to arrive at the beam splitter at the same time and cannot carry any information in other degrees of freedom, e.g., their frequency, that could in principle reveal the source from which the photon originated. This implies that the photon has to be in a pure state; a requirement that is not satisfied if the down-converted photon pairs are entangled in any other degrees of freedom, like their frequency. Preventing the frequency degree of freedom to compromise the indistinguishability of the photons can either be achieved by spectral filtering [54, 52] of the photons before they interact at a beam splitter, or by engineering SPDC crystals that emit photon pairs only in one spectral mode [53, 93].

Another problem is that the SPDC process is a probabilistic process, so it is not known when photon pairs were created, and with current technology it is not possible to perform a non-demolition photon counting measurement in the SPDC output modes to check that. So what has to be done is to perform the experiment many times, and then *post-select* only the events that are in accordance with the creation of the required

number of photon pairs [142, 100].

Keeping these issues in mind, a four-photon entangled state can be created by pumping two SPDC crystals to create two photon pairs in the state $\frac{1}{\sqrt{2}}(|H_a, H_b\rangle + |V_a, V_b\rangle)$ in the output modes $(a, b) = (1, 3)$ and $(a, b) = (2, 4)$, respectively. Then, after the modes 2 and 3 are sent into the input ports of a polarizing beam splitter (PBS), the resulting state is given by [142]

$$\frac{1}{2}(|H_1, H_2, H_3, H_4\rangle + |V_1, V_2, V_3, V_4\rangle + |H_1, H_3, V_3, V_4\rangle + |V_1, V_2, H_2, H_4\rangle). \tag{2.26}$$

If measurements are performed in the four output modes, and the data is post-selected to only include those events where one photon had been present in each of the four modes, the collected data will be the same as if a four-photon GHZ state of the form $\frac{1}{\sqrt{2}}(|H_1, H_2, H_3, H_4\rangle + |V_1, V_2, V_3, V_4\rangle)$ had been created. Furthermore, one of the four photons can be used as a *trigger* to prepare the remaining three photons in a three-photon entangled state [142]. Again, one has to rely on post-selection in this scenario; in addition to the detection of the trigger photon, the measurement data has to be post-selected for the events where three more detection events occur to ensure that indeed two photon pairs were created and only one photon ended up in the trigger arm.

The method of creating multiple photon pairs via SPDC processes and combining them at beam splitters can be extended to more than two photon pairs and thus to create multi-photon entangled states with more than four photons. Recently, an entangled state of eight photons has been created in such a way [64, 139]. However, it should always be kept in mind that these multi-photon states cannot be created deterministically, but rely on post-selecting only the relevant data, and the probability for the occurrence of such events decreases drastically if more photon pairs are involved, which makes this approach not very promising with respect to scalability to large entangled photon numbers.

Another method to create multi-photon entanglement with SPDC sources is to use only one crystal and "wait" for two pairs to be created from two photons of the same pump pulse. This "waiting" is again performed via post-selection by splitting the down-converted photons into different paths, and if in the end four photons are detected at the same time, we know that two pairs were created. As in the case of two crystals, the two pairs are split into different paths by a network of (polarizing) beam splitters. By using one of the photons as a trigger, this method has been used in Refs. [99, 19] to create a three-photon GHZ state, and in Ref. [35] to create a three-photon W-state.

2.4.2 Trapped Ions

Another system to implement qubits are ions confined in an ion trap by oscillating electric fields [15]. There are two different degrees of freedom that can be used to encode quantum information onto ions stored in an ion trap. First, the internal states of the ions can be used, and second, the vibrational states of the ions in the harmonic trap potential can be used. In most of today's experiments, the quantum information is stored in the internal states of the ions, while the vibrational modes are used to implement interactions between different ions. These inter-ion interactions are needed to create entanglement between the internal states of different ions.

For internal states to be suitable for quantum information processing, they must be stable enough to provide sufficient time to perform single- and multi-ion operations before spontaneous decay affects the qubit state of the ions. This means that in addition to the ground state of the ion, we seek metastable states that have lifetimes that are in the order of magnitude of seconds. Furthermore, additional, less stable energy levels are required for preparation and measurement of the qubit state, as will be discussed below. The two leading groups in current ion trap experiments are the group of Rainer Blatt at the University of Innsbruck, and the group of David Wineland at the National Institute of Standards and Technology (NIST) in Boulder [15]. In the following, we will describe the physics of trapped ions by using the $^{40}Ca^{+}$ ion, which is used in Innsbruck [111, 91]. The group of David Wineland at NIST uses $^{9}Be^{+}$ ions. The relevant energy levels of the $^{40}Ca^{+}$ ion with their transition wavelengths are depicted in Figure 2.1 [91].

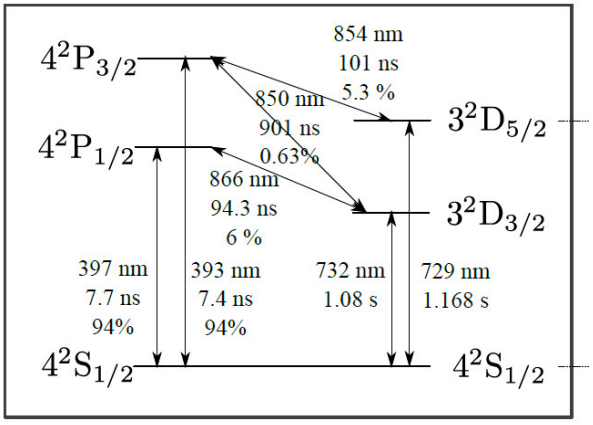


Figure 2.1: Relevant energy levels of the $^{40}Ca^{+}$ ion in an ion trap (Figure 4.1 from Ref. [91]).

The qubit encoding is done in the $|1\rangle = |S\rangle = |S_{1/2}\rangle = |4^2S_{1/2}(m = -1/2)\rangle$ and

$|0\rangle = |D\rangle = |D_{5/2}\rangle = |3^2D_{5/2}(m = -1/2)\rangle$ levels of each ion.[3] Unitary single-qubit operations can be performed by narrow laser light with wavelength 729 nm, tightly focused onto individual ions. The lifetime of $\tau \approx 1$ s of the metastable $|D_{5/2}\rangle$ state is sufficiently long to perform state manipulation and detection of the ions before the spontaneous decay introduces significant errors.

Non-unitary state preparation of the ions in the $S_{1/2}$ level is achieved by pumping the ions with laser light of wavelength 854 nm. This excites the ion from the $D_{5/2}$ state to the $P_{3/2}$ state, from which it will mostly decay to the $S_{1/2}$ state. With a small probability it will decay back into the $D_{5/2}$ level, or the $D_{3/2}$ level, from which it can be depleted by exciting it with a 866 nm laser to the $P_{1/2}$ state, from which it will decay to the $S_{1/2}$ state.

State detection is performed by shining laser light with wavelength 397 nm onto an ion. If the ion is in the $S_{1/2}$ state, it gets excited into the $P_{1/2}$ state, from which it decays back into the $S_{1/2}$ while emitting a photon of 397 nm, which can be detected as fluorescence light. If the ion is in the $D_{5/2}$ state, no such light occurs. Thus shining the 397 nm laser to the ion collapses the qubit either into the $|1\rangle = |S_{1/2}\rangle$ or $|0\rangle = |D_{5/2}\rangle$ state, and the collapsed state is detected by the presence or absence of fluorescent light.

The complete quantum state of N ions in an ion trap has to be described by the combined Hilbert space of the N qubits and the vibrational modes of the ions in the trap. In the following, we will only make use of the center-of-mass (COM) vibrational mode, and will therefore only include the COM mode in the state description. For example, a quantum state of $N = 4$ ions in the trap could be given by $|\Psi\rangle = |SDDS\rangle \otimes |n\rangle = |SDDS, n\rangle$, where the first four values describe the state of the four qubits, and n represents the number of phonons in the COM vibrational mode.

Preparation of the vibrational states in the ground state can be achieved by Doppler cooling and sideband cooling [124, 134, 33], on the $S_{1/2} \leftrightarrow P_{1/2}$ and $S_{1/2} \leftrightarrow D_{5/2}$ transition, respectively.

Single-Qubit Operations

As already mentioned above, single-qubit transitions between the $S_{1/2}$ and the $D_{5/2}$ levels can be achieved with a laser beam at wavelength 729 nm focused on the desired ion. By choosing appropriate durations and phases for the laser pulses, arbitrary unitary transformations on the qubit can be performed, while the other qubits and the vibrational

[3] For simplicity in notation we introduced the short-hand notations $|S_{1/2}\rangle$ and $|D_{5/2}\rangle$, respectively, and we will in general omit the principal quantum number and the Zeeman sublevel label. Furthermore, when we refer to the qubit states directly, we will mostly simply call them $|S\rangle$ and $|D\rangle$.

mode are not affected [111, 91].

By increasing (decreasing) the laser frequency by the energy of a COM phonon ω, unitary operations between the states $|S,n\rangle \leftrightarrow |D,n+1\rangle$ ($|S,n\rangle \leftrightarrow |D,n+1\rangle$) can be implemented. Here we only included the addressed ion and the COM vibrational mode in the notation, as the states of the other ions are still unaffected. This operation is generally referred to as a blue (red) sideband transition. It couples the internal states of one ion to the vibrational mode, and since the vibrational mode is shared between all ions, this can be used to realize interactions between two ions.

Cirac-Zoller Two-Ion Gate

With the single-qubit operations and their sideband variants, it is now possible to create entanglement between two ions, while only always addressing one ion at the same time. This idea was first proposed by Cirac and Zoller [29], and can be realized as follows. First a blue sideband transition on the first ion is used to move the qubit state of that ion to the vibrational COM mode. Since the vibrational mode is shared by all ions, the information of the first qubit is now available to the second ion. Thus, by only addressing the second ion while making use of sideband transitions, we can perform a quantum operation that involves both the first and the second qubit. After that operation, the state of the first qubit is moved back to the first ion by a sideband transition on the first ion. This idea can be used to create entanglement between the two ions.

The implementation of this gate requires that the vibrational COM mode is in the $n = 0$ state at the start of the protocol. Then a blue sideband transition can be applied that performs the transformation $|S,0\rangle \rightarrow |D,1\rangle$. The blue sideband laser does not couple to the $|D,0\rangle$ state since no $|S,-1\rangle$ state exists. Thus this transformation moves the qubit state from the ion to the vibrational mode:

$$(\alpha\,|S\rangle + \beta\,|D\rangle) \otimes |0\rangle \rightarrow |D\rangle \otimes (\alpha\,|1\rangle + \beta\,|0\rangle). \tag{2.27}$$

After that transformation, the combined states of the second ion and the COM mode is a superposition of the states $\{|D,0\rangle, |D,1\rangle, |S,0\rangle, |S,1\rangle\}$. Again, the blue sideband laser does not couple to the $|D,0\rangle$ state, but only to the other three. Thus, by appropriately choosing a sequence of blue sideband laser pulses, an operation can be implemented that adds a negative phase to all states except the $|D,0\rangle$ state. This operation is called a controlled-phase gate between the two qubits and can be used to transform separable states into maximally entangled states and vice versa. As a final step of the Cirac-Zoller gate, the state of the first qubit is moved back onto the internal states of the first ion via

a blue sideband transition.

The Cirac-Zoller gate has successfully been implemented to create entanglement between two-ions [115, 114], and has also found its use in more involved quantum information protocols, like the implementation of a teleportation protocol with trapped ions [110, 109].

Mølmer-Sørensen Gate

The Cirac-Zoller gate is a versatile gate that can be used for entangling operations between arbitrary ions in the ion trap. It has, however, also a few drawbacks, most notably that the vibrational COM mode has to be initialized in its ground state, which is a major source of errors and requires careful laser cooling of the motional states of the ions. Mølmer and Sørensen (MS) [90, 121, 122] proposed an inter-ion gate that is less sensitive to the phonon number of the vibrational mode.

In the MS proposal, the ions are not addressed individually by the laser, but instead a bichromatic laser field with frequencies $\nu \pm \omega \mp \delta$ is globally applied to all ions. Here ν is the energy difference between the internal $|S\rangle$ and $|D\rangle$ states, ω is the energy of one phonon of the vibrational COM mode, and δ is a small detuning from the sideband transitions. This detuning ensures that the transitions of the internal states of the ions only occur pairwise. The intermediate states, in which only the state of one ion is changed, exist only virtually. The trick in this scheme is that different paths, leading to the same final state through different virtual intermediate steps, interfere in such a way that the dependence on the vibrational phonon number cancels out [90]. If the interaction time of the bichromatic laser field is chosen appropriately, a maximally entangled state between two ion qubits can be created from an initial state with both ions in the ground state. This operation has been used to create two-ion entangled state with a fidelity of 99.3% [10].

Multi-Ion Entanglement

While the Cirac-Zoller gate can in principle be used to successively entangle arbitrarily many ions, it is the Mølmer-Sørensen gate that excels at creating multi-ion entanglement. This stems from the fact that the MS gate addresses all ions simultaneously and thus can also entangle all ions simultaneously. In fact, if the bichromatic laser field of the MS gate is applied to N ions, the resulting state is a GHZ state of the form [90]

$$|\Psi\rangle = \frac{1}{\sqrt{2}} \left(e^{i\phi_g} |SS\cdots S\rangle + e^{i\phi_e} |DD\cdots D\rangle \right). \tag{2.28}$$

Experimentally the multi-ion MS gate has been used to create GHZ states with up to 14 ions [92].

The idea of using a global beam provides a very elegant way to create multi-particle entanglement between all the ions in the trap, because the number of required operations does not depend on the number of ions in the trap. A global beam can also be used to create other kinds of multipartite entangled states. For instance, a W-state can be created by first preparing the system in the $|D\cdots D,1\rangle$ state and then applying a global blue sideband laser pulse, which performs the transition $|D,1\rangle \rightarrow |S,0\rangle$. Since the beam is applied globally, it cannot be known which ion went through this transition and thus the created state is the W-state $\frac{1}{\sqrt{N}}(|D\cdots DS,0\rangle + |D\cdots DSD,0\rangle + \cdots + |SD\cdots D,0\rangle)$ [91]. This has been implemented in Ref. [91] for two and four ions, and by using a similar approach in Ref. [66] for two ions. Earlier W-state preparation with single-ion addressing has been implemented for up to eight ions [55].

Chapter 3

Bounds on the Probability of Transformations between Multipartite Pure States

For a tripartite pure state of three qubits, it is well known that there are two inequivalent classes of genuine tripartite entanglement, namely the GHZ-class and the W-class. Any two states within the same class can be transformed into each other with stochastic local operations and classical communication (SLOCC) with a non-zero probability. The optimal conversion probability, however, is only known for special cases. Here, we derive new lower and upper bounds for the optimal probability of transformation from a GHZ-state to other states of the GHZ-class. A key idea in the derivation of the upper bounds is to consider the action of the LOCC protocol on a different input state, namely $1/\sqrt{2}[|000\rangle - |111\rangle]$, and demand that the probability of an outcome remains bounded by 1. We also find an upper bound for more general cases by using the constraints of the so-called interference term and 3-tangle. Moreover, we generalize some of our results to the case where each party holds a higher-dimensional system. In particular, we found that the GHZ state generalized to three qutrits, i.e., $|\mathrm{GHZ}_3\rangle = 1/\sqrt{3}[|000\rangle + |111\rangle + |222\rangle]$, shared among three parties can be transformed to *any* tripartite 3-qubit pure state with probability 1 via LOCC. Some of our results can also be generalized to the case of a multipartite state shared by more than three parties. This chapter is largely based on Ref. [32].

3.1 Introduction

Entanglement is the most peculiar feature that distinguishes quantum physics from classical physics and lies at the heart of quantum information theory. Thus it is important to get a good understanding of entanglement properties of quantum states. These properties are well understood for bipartite pure states. In the standard distant laboratory paradigm, suppose two distant parties, Alice and Bob, shared a bipartite entangled state. They may apply local operations and classical communications (LOCC) to convert it into another partite state. Bennett et al [12] has answered the question for the rate of LOCC transformation between bipartite pure states. It is quantified by the von Neumman entropy of a reduced density matrix. For the single-copy case, the optimal conversion probabilities are known for any pure state transformation [81, 95, 131]. For an LOCC transformation protocol, if it can succeed with probability 1, we call it deterministic, if it can only succeed with a nonzero probability smaller than 1, we call it stochastic, or SLOCC (Stochastic Local Operators and Classical Communications). For mixed states, the question of what the optimal rate of transformations is between them is still largely open.

For multipartite states, however, the problem is much more complicated. There exist different types of entanglement and therefore the transformations are rather involved. For the case of tripartite pure three qubit states, a characterization into six different entanglement classes, of which two contain true tripartite entanglement, exists [34]. One is the GHZ class state, which can always be transformed by local unitary operations to a state of the form

$$|\phi_{GHZ}\rangle = \sqrt{K}(c_\delta |0\rangle |0\rangle |0\rangle + s_\delta e^{i\varphi} |\varphi_A\rangle |\varphi_B\rangle |\varphi_C\rangle), \tag{3.1}$$

where

$$|\varphi_A\rangle = \; c_\alpha |0\rangle + s_\alpha |1\rangle , \tag{3.2}$$
$$|\varphi_B\rangle = \; c_\beta |0\rangle + s_\beta |1\rangle , \tag{3.3}$$
$$|\varphi_C\rangle = \; c_\gamma |0\rangle + s_\gamma |1\rangle , \tag{3.4}$$

and K=$(1 + 2c_\delta s_\delta c_\alpha c_\beta c_\gamma c_\phi)^{-1} \in [\frac{1}{2}, \infty)$, $c_\delta = \cos\delta, s_\delta = \sin\delta$, the same for $\alpha, \beta, \gamma, \phi$. The range for the parameters are $\delta \in (0, \frac{\pi}{4}]$, $\alpha, \beta, \gamma \in (0, \frac{\pi}{2}]$ and $\varphi \in [0, 2\pi)$.

The other one is the W class state, which is a state that is unitarily equivalent to

$$|\phi\rangle = (\sqrt{c}\,|0\rangle + \sqrt{d}\,|1\rangle)\,|00\rangle + |0\rangle\,(\sqrt{a}\,|01\rangle + \sqrt{b}\,|10\rangle), \tag{3.5}$$

with $c + d + a + b = 1$.

A transformation between any two states of the same class is always possible with non-zero probability. However, the optimal conversion between the states within the same class of genuine tripartite entangled states is *not* known. Incidentally, a similar characterization into nine different classes exists for four qubits [130]. In 2000, the optimal rate of distillation of a GHZ state from any GHZ-class state was found [2]. Recently, a necessary and sufficient condition for deterministically (i.e., with probability 1) transforming multipartite qubit states with Schmidt rank 2 [37] have been given [127].

In this chapter, we present new upper and lower bounds for multipartite entanglement transformations. In particular, we focus on transformations among states with the same Schmidt rank [37]. While we put an emphasis on the transformation from a GHZ state to a GHZ-class state, our upper bound can also be generalized to general transformations from one GHZ class state to another. Furthermore, some of the results are derived for the more general case of higher dimensions and more than three parties. In particular, we find that all tripartite pure three qubit states can be transformed from qutrit GHZ state, $\frac{1}{\sqrt{3}}(|000\rangle + |111\rangle + |222\rangle)$, with probability one, which is a new result. Moreover, some general theorems for deterministic transformation are also derived.

This chapter is structured as follows. In Section 3.2, we derive upper bounds for the transformation of the GHZ-state to any other state in the GHZ-class. The upper bounds are only non-trivial for a subclass of the GHZ-class. Thus Section 3.3 and 3.4 use a different approach that results in upper bounds for a wider class of states. More specifically, for any GHZ class state which does not have a known way to be transformed from the GHZ state with probability one, we can find a nontrivial upper bound for the probability of this transformation. Our upper bound can also be effective for the transformation from a GHZ class state to a large class of other GHZ class states. Lower bounds for the transformation of higher dimensional GHZ-states distributed among three or more parties to states with the same Schmidt rank are given in Section 3.5.

3.2 Upper Bound for the Conversion from GHZ state to a GHZ class state

In this section, we derive an upper bound for the conversion of the GHZ-state to any other state of the GHZ-class via LOCC. This upper bound will be nontrivial (i.e., smaller

than 1) for $\varphi \in (\frac{1}{2}\pi, \frac{3}{2}\pi)$. The transformation under consideration is given by

$$\begin{aligned} |\mathrm{GHZ}\rangle &= \tfrac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \\ \overset{\mathrm{LOCC}}{\longrightarrow} |\Psi\rangle &= \sqrt{K}(c_\delta |0\rangle |0\rangle |0\rangle + s_\delta e^{i\varphi} |\varphi_A\rangle |\varphi_B\rangle |\varphi_C\rangle), \end{aligned} \tag{3.6}$$

with the parameters defined in introduction.

The LOCC operation is represented by Kraus operators $\{O_i = A_i \otimes B_i \otimes C_i\}$. In the following we will refer to different Kraus operators of the LOCC protocol as different *branches*. Furthermore, a branch $O_i |\mathrm{GHZ}\rangle = |\Phi\rangle$ is called a *success branch* if $|\Phi\rangle \propto |\Psi\rangle$, and a *failure branch* if there exists no LOCC-operation that can transform $|\Phi\rangle$ into $|\Psi\rangle$ with a non-zero probability. If a branch is neither a success nor a failure, we call it an *undecided branch*. An optimal protocol only consists of success and failure branches.

For the following analysis we first recall two known results from Refs [34, 2]

Lemma 3.1. *For a GHZ-class state $|\Psi\rangle$ we have:*

a) The Schmidt rank of $|\Psi\rangle$ is 2 [34]. This means that the minimum number of product states necessary to write $|\Psi\rangle$ as a superposition of them is 2:

$$|\Psi\rangle = \sum_{i=1}^{2} \alpha_i |a_i b_i c_i\rangle , \tag{3.7}$$

with $\alpha_i \in (0,1)$ and $\langle a_i b_i c_i | a_i b_i c_i \rangle = 1$.

b) This product state decomposition, i.e., the set $\{(\alpha_1, |a_1 b_1 c_1\rangle), (\alpha_2, |a_2 b_2 c_2\rangle)\}$ is unique [1].

This result leads to

Lemma 3.2. *For a successful LOCC operation within the GHZ-class,*

$$\begin{aligned} |\Psi\rangle &= \alpha_1 |a_1 b_1 c_1\rangle + \alpha_2 |a_2 b_2 c_2\rangle \\ \overset{LOCC}{\longrightarrow} |\Psi'\rangle &= \alpha_1' |a_1' b_1' c_1'\rangle + \alpha_2' |a_2' b_2' c_2'\rangle , \end{aligned} \tag{3.8}$$

described by the operator O_1, we must either have the mapping

$$O_1 |a_1 b_1 c_1\rangle = o_1 \frac{\alpha_1'}{\alpha_1} |a_1' b_1' c_1'\rangle \tag{3.9}$$

$$O_1 |a_2 b_2 c_2\rangle = o_1 \frac{\alpha_2'}{\alpha_2} |a_2' b_2' c_2'\rangle \tag{3.10}$$

or

$$O_1 \left|a_1 b_1 c_1\right\rangle = o_1 \frac{\alpha_2'}{\alpha_1} \left|a_2' b_2' c_2'\right\rangle \tag{3.11}$$

$$O_1 \left|a_2 b_2 c_2\right\rangle = o_1 \frac{\alpha_1'}{\alpha_2} \left|a_1' b_1' c_1'\right\rangle \tag{3.12}$$

with some proportionality constant o_1, which can be chosen to be real. See Figure 3.1, Figure 3.2.

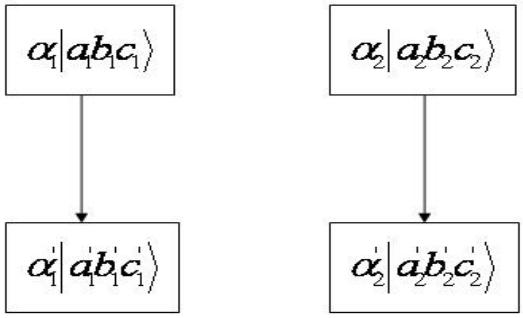


Figure 3.1: Option 1 for a successful mapping in Lemma 3.2

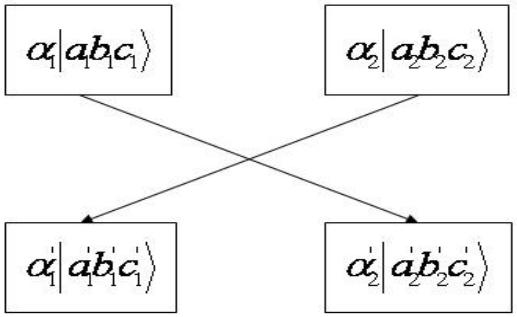


Figure 3.2: Option 2 for a successful mapping in Lemma 3.2

Proof. Since a LOCC Kraus operator is always of the form $O_1 = A_1 \otimes B_1 \otimes C_1$, a product state is always transformed into a product state. With that observation and the fact that the two-term product decomposition of a tripartite GHZ-class state is unique (see Lemma 3.1), Lemma 3.2 follows. □

Theorem 3.3. *An upper bound for the conversion probability for the transformation*

$$\begin{aligned} |\mathrm{GHZ}\rangle &= \tfrac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \\ \longrightarrow |\Psi\rangle \quad &= \sqrt{K}(c_\delta |000\rangle + s_\delta e^{i\varphi} |\varphi_A\varphi_B\varphi_C\rangle), \end{aligned} \tag{3.13}$$

where the parameters are defined in Equation (3.6)*, is given by*

$$p \leq \min\left\{1, \frac{1 + 2c_\delta s_\delta c_\alpha c_\beta c_\gamma c_\varphi}{1 - 2c_\delta s_\delta c_\alpha c_\beta c_\gamma c_\varphi}\right\} \tag{3.14}$$

Idea of the Proof. From Lemma 3.2 we know that, for a success branch and the input and output state in the form of Equation (3.13), each product state of the input states has to be mapped to a product state of the output state. This allows us to infer how the same LOCC protocol acts on the phase flipped GHZ state, $\frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)$. From the requirement that for this transformation, the sum of the probabilities for the output states also have to sum to 1, we can derive a bound for the parameters arising in the original transformation. This results in an upper bound on the successful transformation probability.

Proof. Assume that the optimal LOCC strategy is given by the Kraus operators $\{O_i = A_i \otimes B_i \otimes C_i\}$. According to Lemma 3.2, there are two possibilities to have a successful branch. They are

$$O_i |000\rangle = o_i c_\delta |000\rangle \tag{3.15}$$

$$O_i |111\rangle = o_i e^{i\varphi} s_\delta |\varphi_A\varphi_B\varphi_C\rangle \tag{3.16}$$

for $i = 1, \ldots, n_1$, and

$$O_i |000\rangle = o_i e^{i\varphi} s_\delta |\varphi_A\varphi_B\varphi_C\rangle \tag{3.17}$$

$$O_i |111\rangle = o_i c_\delta |000\rangle \tag{3.18}$$

for $i = n_1 + 1, \ldots, n_1 + n_2$. Both cases give the desired transformation

$$O_i |\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}} o_i (c_\delta |000\rangle + e^{i\varphi} s_\delta |\varphi_A\varphi_B\varphi_C\rangle) = \frac{o_i}{\sqrt{2K}} |\Psi\rangle \tag{3.19}$$

for $i = 1, \ldots, n_1 + n_2$. The successful conversion probability is then given by

$$p = \frac{1}{2K} \sum_{i=1}^{n_1+n_2} o_i^2. \tag{3.20}$$

To get an upper bound for $\sum_{i=1}^{n_1+n_2} o_i^2$, we consider how

$$\frac{1}{\sqrt{2}}(|000\rangle - |111\rangle) \tag{3.21}$$

behaves when put through the same protocol, described by the Kraus operators $\{O_i\}$. We have

$$\begin{aligned} & O_i \tfrac{1}{\sqrt{2}}(|000\rangle - |111\rangle) \\ = \; & \tfrac{1}{\sqrt{2}} o_i (c_\delta |000\rangle - e^{i\varphi} s_\delta |\varphi_A \varphi_B \varphi_C\rangle) = \tfrac{o_i}{\sqrt{2K'}} |\Psi'\rangle \end{aligned} \tag{3.22}$$

with

$$|\Psi'\rangle = \sqrt{K'}(c_\delta |000\rangle - e^{i\varphi} s_\delta |\varphi_A \varphi_B \varphi_C\rangle), \tag{3.23}$$

where $K' = 1/(1 - 2c_\delta s_\delta c_\alpha c_\beta c_\gamma c_\varphi)$, for $i = 1, \ldots, n_1 + n_2$, up to an overall minus sign for $i = n_1 + 1, \ldots n_1 + n_2$. Thus the conversion probability for this process is given by $\frac{1}{2K'} \sum_{i=1}^{n_1+n_2} o_i^2$. Being a probability, this has to be bounded by 1, giving $\sum_{i=1}^{n_1+n_2} o_i^2 \leq 2K'$. This, together with Equation (3.20), gives the upper bound

$$p \leq \frac{K'}{K} = \frac{1 + 2c_\delta s_\delta c_\alpha c_\beta c_\gamma c_\varphi}{1 - 2c_\delta s_\delta c_\alpha c_\beta c_\gamma c_\varphi} \tag{3.24}$$

for the process described by Equation (3.13). □

Special Case: For the case, where we have $|\varphi_A\rangle = |\varphi_B\rangle = |\varphi_C\rangle$, $c_\alpha = c_\beta = c_\gamma = \lambda_a$, $\varphi = 0$, and $c_\delta = s_\delta = \frac{1}{\sqrt{2}}$, i.e.,

$$|\Psi\rangle = \frac{1}{\sqrt{2}\sqrt{1 - \lambda_a^3}}(|000\rangle - |aaa\rangle), \tag{3.25}$$

we get

$$p \leq \frac{1 - \lambda_a^3}{1 + \lambda_a^3}. \tag{3.26}$$

Theorem 3.3 gives a non-trivial upper bound for the transformation from the GHZ-state to a GHZ-class state for all values of φ with $\cos\varphi < 0$, i.e., $\phi \in (\frac{\pi}{2}, \frac{3\pi}{2})$. This nicely shows that, contrary to the bipartite case, where the maximally entangled EPR-state can be tranformed into any other pure two qubit state with probability one, the GHZ-state, which exhibits maximal genuine tripartite entanglement as it maximizes the 3-tangle [31] and tracing out one qubit results in a totally mixed state, cannot be transformed to all other states in the same class with probability one.

3.3 Failure Branch

Theorem 3.3 of the last section gives a trivial bound for the case $\phi \in (\frac{\pi}{2}, \frac{3\pi}{2})$. Here, we will derive a useful bound for a larger class of states. We will derive a nontrivial upper bound for all cases except $\phi = \frac{\pi}{2}$, $\frac{3\pi}{2}$ and $\langle 000|\varphi_A\varphi_B\varphi_C\rangle = 0$. In fact, it was shown that for these cases the transformation can succeed with probability 1 [127]. Our proof has two important ingredients. First, the conservation of a new quantity defined as the "*interference term*" under positive operator valued measures (POVMs), and second that the three tangle is an entanglement monotone, which we will discuss in detail in the following.

The idea of the derivation is the following. As described above, the protocol is split into multiple branches. For each branch we will introduce two values, the "*interference term*", defined in Defintion 3.5, and the "*normalization*", defined in Definition 3.7, and we will show that the weighted summation over all branches has to be constant for both values at any step of the transformation. In Section 3.4, we show that the three tangle is bounded by the interference term. After that, we consider the whole process from the weak measurement viewpoint. This means, we divide the whole process into many infinitesimal steps, each of which changes the state very little, i.e., the change of the state can be viewed as continuous. We then stop in the middle and investigate whether a new upper bound can be found. Interestingly, we find there are some new upper bounds and these upper bounds will still be effective in the following steps, even when we reach the end. Hence it can be used to derive a new upper bound for the supremum success probability of the whole LOCC protocol. A more detailed discussion will be provided in Section 3.4.

Theorem 3.4. *For the transformation from GHZ to GHZ-class state $|\phi\rangle$, failure branches end with a state with at least one party's reduced matrix having rank 1.*

Proof. Suppose we want to get the GHZ-class state $|\phi\rangle = \sqrt{K}(c_\delta |0\rangle |0\rangle |0\rangle + s_\delta e^{i\varphi} |\varphi_A\rangle |\varphi_B\rangle |\varphi_C\rangle)$, where $|0_A\rangle$ is linearly independent of $|\varphi_A\rangle$, the same for B and C. For a state whose reduced density matrices for all parties have full rank, $|\phi\rangle = \sqrt{K'}(c'_\delta |0\rangle |0\rangle |0\rangle + s'_\delta e^{i\varphi'} |\varphi'_A\rangle |\varphi'_B\rangle |\varphi'_C\rangle)$, where $|0_A\rangle$ is linearly independent of $|\varphi'_A\rangle$, the same for B and C, it is easy to see that the equations

$$O_A |0\rangle = |0\rangle , \tag{3.27}$$

$$O_A |\varphi'_A\rangle = |\varphi_A\rangle , \tag{3.28}$$

and the same for B and C, always have non-trivial solution. That means we can always

transform this state into $|\phi\rangle$ with nonzero probability. Thus such a state can never be the end of a failure branch. □

3.3.1 Conservation of the Interference Term

To go further, we want to use the following property of the LOCC Kraus operators. For a complete set of Kraus operators $\{O_i = A_i \otimes B_i \otimes C_i\}$, we have $\sum O_i^\dagger O_i = \mathbb{1}$.

Suppose that a Kraus operator O satisfies

$$O\,|000\rangle = \alpha\,|a_1b_1c_1\rangle \tag{3.29}$$

$$O\,|111\rangle = \beta\,|a_2b_2c_2\rangle \tag{3.30}$$

with $\langle a_1b_1c_1|a_1b_1c_1\rangle = \langle a_2b_2c_2|a_2b_2c_2\rangle = 1$.

Then it can transform $|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}}(|000\rangle+|111\rangle)$ into $|\psi\rangle = \frac{1}{\sqrt{2p}}(\alpha\,|a_1b_1c_1\rangle+\beta\,|a_2b_2c_2\rangle$, where $\frac{1}{\sqrt{2p}}$ is the normalization factor, and p is exactly the probability of getting $|\psi\rangle$. From here we define the *interference term* and the *normalization* in the following:

Definition 3.5 (Interference Term)**.** For a normalized GHZ-class state $|\gamma\rangle$, where $\langle\gamma|\gamma\rangle = 1$, written in the form $|\gamma\rangle = \frac{1}{\sqrt{2}}(\alpha\,|a_1b_1c_1\rangle + \beta\,|a_2b_2c_2\rangle)$, we define the interference term I as

$$I = \mathrm{Re}(\alpha^*\beta k), \tag{3.31}$$

where $k = \langle a_1b_1c_1|a_2b_2c_2\rangle$.

It is easy to see, if an operator O transforms $|\mathrm{GHZ}\rangle$ to a state $|\psi\rangle$, the interference term of $|\psi\rangle$ is in fact the real part of $\frac{1}{p}\langle 000|O^\dagger O|111\rangle$, where p is the probability of the branch corresponding to operator O.

Remark 3.1. In fact, one can find $I = 1 - \frac{1}{2}(|\alpha|^2 + |\beta|^2)$.

Remark 3.2. Note also that $-\infty < I \leq 1$. In other words, it can be unbounded below. This fact will become important in our discussion in Section 3.4.

Remark 3.3. Notice that a failure branch gives a state that is *outside* the GHZ class. For such a state, the actual value of interference term depends not only on the state itself, but also on the particular Kraus operator, O_i, and the initial state, ϕ_i, used to reach the state. So, when we talk about the interference term of failure branches of an SLOCC transformation, we need to be careful: We are not talking about the interference term of the state given by the failure branches, but the interference term determined by the whole transformation protocol leading to that state.

Theorem 3.6 (Conservation of the Interference Term)**.** *For a complete set of Kraus operators $\{O_i\}$ of a LOCC protocol which transforms the GHZ state to other states, $\{O_i |\mathrm{GHZ}\rangle\}$, the weighted sum of the interference terms of all the branches is zero.*

$$0 = \sum p(O_i |\mathrm{GHZ}\rangle) I(O_i |\mathrm{GHZ}\rangle) \tag{3.32}$$

where $p(O_i |\mathrm{GHZ}\rangle)$ is the probability of the branch corresponding to the Kraus operator O_i, and $I(O_i |\mathrm{GHZ}\rangle)$ denotes the interference term I for the state $O_i |\mathrm{GHZ}\rangle$.

Proof. Suppose the corresponding complete set of Kraus operators consists of $\{O_i = A_i \otimes B_i \otimes C_i\}$. Then we have $\sum O_i^\dagger O_i = \mathbb{1}$. So, we should have

$$\begin{aligned} 0 &= \langle 000|111\rangle = \langle 000|\mathbb{1}|111\rangle \\ &= \langle 000| \sum O_i^\dagger O_i |111\rangle \\ &= \sum \langle 000|O_i^\dagger O_i|111\rangle \\ &= \sum p(O_i |\mathrm{GHZ}\rangle) \frac{\langle 000|O_i^\dagger O_i|111\rangle}{p(O_i |\mathrm{GHZ}\rangle)}. \end{aligned} \tag{3.33}$$

From the definition of the interference term I, we know the real part of the right hand side of Equation (3.33) is exactly the weighted sum of I of each branch. As the right hand side of Equation (3.33) is equal to zero, its real part should also be zero. Hence for a transformation from the GHZ-state to other states, the average value of the interference terms of all the states we get in each branch should be zero. We call this the *conservation of the interference term.* □

3.3.2 Conservation of the Normalization

Definition 3.7 (Normalization)**.** For a two-term tripartite state $|\gamma\rangle$, written in the form $|\gamma\rangle = \frac{1}{\sqrt{2}}(\alpha |a_1 b_1 c_1\rangle + \beta |a_2 b_2 c_2\rangle)$, we call $\frac{1}{2}(|\alpha|^2 + |\beta|^2)$ the normalization of $|\gamma\rangle$.

It is easy to see, if an operator O transforms $|\mathrm{GHZ}\rangle$ to the state $|\psi\rangle$, the normalization of $|\psi\rangle$ is in fact $\frac{1}{2p}(\langle 000|O^\dagger O|000\rangle + \langle 111|O^\dagger O|111\rangle)$, where $p = \langle GHZ|O^\dagger O|GHZ\rangle$. Additionally, since O is a positive operator, the normalization is always non-negative.

Now suppose that the corresponding complete set of Kraus operators consists of $\{O_i = A_i \otimes B_i \otimes C_i\}$. Then $\sum O_i^\dagger O_i = \mathbb{1}$, and we have

$$
\begin{aligned}
1 =& \langle GHZ|GHZ\rangle \\
=& \frac{1}{2}(\langle 000| + \langle 111|)(|000\rangle + |111\rangle) \\
=& \frac{1}{2}(\langle 000|000\rangle + \langle 111|111\rangle) \\
=& \frac{1}{2}(\sum \langle 000|O_i^\dagger O_i|000\rangle + \sum \langle 111|O_i^\dagger O_i|111\rangle) \\
=& \sum p(O_i\,|\mathrm{GHZ}\rangle)\frac{\langle 000|O_i^\dagger O_i|000\rangle + \langle 111|O_i^\dagger O_i|111\rangle}{2p(O_i\,|\mathrm{GHZ}\rangle)}
\end{aligned} \tag{3.34}
$$

From the definition of the normalization, we know that this is exactly the weighed sum of the normalization of each branch. In other words, for a transformation from $|\mathrm{GHZ}\rangle$ to other states, the average value of the normalization of all the states we get in each branch should be 1. Recall that the normalization cannot be less than zero. Hence each term in the summation cannot be larger than 1, which means that for each branch, the product of its probability and the normalization of the state it gets cannot be larger than 1.

In fact, the conservation of the normalization can be derived from the conservation of the interference term. However, the conservation of the normalization also gives the following. For each branch, the product of its probability and the normalization of the state it gets should be no larger than 1. This fact is also useful in determining the upper bound of the transformation probability.

The basic idea is that if we know the state we want and the state the failure branch gives, Equations (3.33) and (3.34), combined with the fact that the summation of probability should be one, can give us some implication about the supremum success probability. For example, we have the following theorem:

Theorem 3.8. *Consider a transformation protocol from the GHZ state to a GHZ-class state $|\phi\rangle$, with interference term $x > 0$ ($x < 0$). If there exists a $y > 0$, such that the interference term of all the failure branches are larger than $-y$ (smaller than y), we have the following upper bound for its successful probability:*

if $x > 0$:

$$p_s \leq p^U(-y) = \frac{y}{x+y}. \tag{3.35}$$

if $x < 0$:

$$p_s \leq p^U(y) = -\frac{y}{x-y}. \tag{3.36}$$

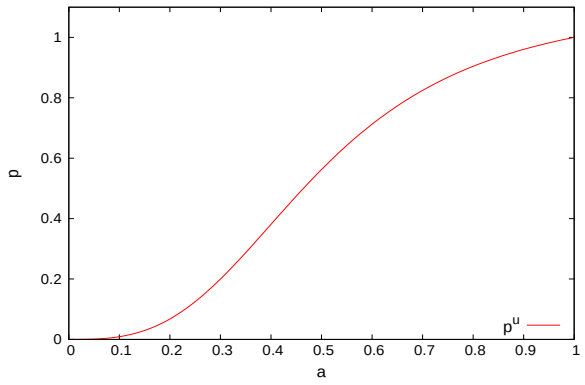


Figure 3.3: The value of p^U as a function of a. In this figure, $a = (\frac{y}{y-1})^{\frac{1}{3}}$. So when a goes from 0 to 1, y goes from 0 to ∞. Note that as y goes to infinity, a goes to 1. We express the value as a function of a because this will make it easier for us to combine different graphs into one graph later.

Proof. Take $x > 0$, suppose there are n failure branches, whose probabilities are $p_{f_1}, p_{f_2}, \cdots, p_{f_n}$, and the corresponding interference terms are $-y_1, -y_2, \cdots, -y_n$. Then we have

$$p_s x - \sum p_{f_i} y_i = 0 \tag{3.37}$$

$$p_s + \sum p_{f_i} = 1 \tag{3.38}$$

Rewriting it in the following form,

$$p_s x - p_{ft} y' = 0 \tag{3.39}$$

$$p_s + p_{ft} = 1 \tag{3.40}$$

where $p_{ft} = \sum p_{f_i}$ and $y' = \frac{\sum p_{f_i} y_i}{p_{ft}}$, gives the solution

$$p_s = \frac{y'}{x + y'}. \tag{3.41}$$

As the interference term of all the failure branches are larger than $-y$, we have $y' < y$. Hence we get

$$p_s < p^U(-y) = \frac{y}{x + y}. \tag{3.42}$$

The discussion for the case when $x < 0$ is similar. □

Remark 3.4. Recall that the range of I can be $-\infty < I \leq 1$, which means that I can be unbounded below. Then in the $x > 0$ case, if I of the failure branch goes to $-\infty$, or we can

say y goes to ∞, we will have $p^U(-y)$ arbitrary close to 1. Therefore, Theorem 3.8 alone is not enough for establishing a non-trivial upper bound. To derive a non-trivial upper bound, we need to find some additional constraints which are related to the interference term. In fact, this is what we will do in Section 3.4.

3.4 Upper Bound for a General Case

In this section, we will find an upper bound in a more general case. Recall the problem of Theorem 3.8 is that the interference can be unbounded below. So we would like to find an additional constraint. It turns out that the fact that the 3-tangle, a measure of tripartite entanglement introduced in [31], is an entanglement monotone (i.e., it cannot increase on average under LOCCs) is precisely what we need [34].

Our strategy is that, for any possible transformation protocol, we would like to construct a new protocol that has the following two properties: 1. It has an upper bound for the maximal successful probability of transformation which is obviously smaller than one; 2. We can reconstruct the original protocol from this new protocol, which means the successful probability of this new protocol can be no less than the original one. The way we construct such a protocol is given in Subsection 3.4.2 and the bound of it will be given in Subsection 3.4.3, in which we deal with a special example: the transformation from GHZ state to a special GHZ class state $|\phi\rangle = \gamma(|000\rangle + |aaa\rangle)$. In Subsection 3.4.4, we will generalize this bound to more general cases, where we find for any transformation from one GHZ-class state $|\phi\rangle$ to another GHZ-class state $|\psi\rangle$ with different interference terms, we can find an nontrivial upper bound for the successful probability.

3.4.1 Interference Term and the Maximal Value of the 3-tangle of a GHZ-Class State

Now consider such a question: Suppose we have an unknown GHZ class state $|\phi_{GHZ}\rangle = \sqrt{K}(c_\delta |0\rangle |0\rangle |0\rangle + s_\delta e^{i\varphi} |\varphi_A\rangle |\varphi_B\rangle |\varphi_C\rangle)$ with a given interference term f, what is the maximal value of the 3-tangle τ_{ABC} [34] ?

Theorem 3.9. *For a GHZ class $|\phi_{GHZ}\rangle$, if its interference term is I, then the maximal value of its 3-tangle is $\frac{(1-a^2)^3}{(1+a^3)^2}$, where $a = (\frac{f}{1-f})^{\frac{1}{3}}$.*

The proof will be given in the appendix.

3.4.2 "Stop and Reconstruct" Procedure

From [97], we know every measurement can be seen as constructed by many infinitesimal steps of weak measurement, that is, a measurement which only slightly changes the original state. From this view, to get a better understanding of the transformation protocol, we would like to try to reduce the case where a failure branch gives an $I > I_0$ (some prescribed value) to the case where an undecided branch has $I = I_0$. That is to say, we are using a reduction idea. First we need to answer the following question: Can we stop at some intermediate point and reconstruct the original measurement? It turns out that the answer is yes. In fact, from [97], the following theorem follows easily.

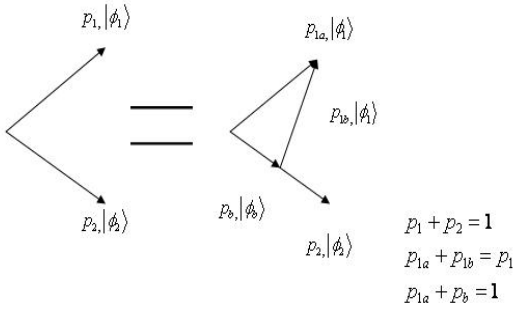


Figure 3.4: "stop and reconstruct" for a two-outcome measurement

Theorem 3.10. *A two-outcome measurement* $\{M_1, M_2\}$ *can be reconstructed by stopping at an immediate step* $\{\sqrt{1-e^{-2x}}M_1', \sqrt{1+e^{-2x}}M'(x)\}$ *and a reconstructing measurement* $\{M'(x,+\infty), M'(x,-\infty)\}$*, where* $M_1' = \sqrt{M_1^\dagger M_1}$ *and*

$$M'(x,+\infty) = \sqrt{\frac{1+\tanh(x)}{I+\tanh(x)(M_2'^2-M_1'^2)}}M_2', \tag{3.43}$$

$$M'(x,-\infty) = \sqrt{\frac{1-\tanh(x)}{I+\tanh(x)(M_2'^2-M_1'^2)}}M_1' \tag{3.44}$$

See Figure 3.4 for a graphical description.

Proof. Firstly, from polar decomposition we have $M_1 = U_1 M_1', M_2 = U_2 M_2'$, where U_1 and U_2 are unitary, $M_2' = \sqrt{M_2^\dagger M_2}$. Then $\{M_1', M_2'\}$ is also a measurement. As M_1' and M_2' are positive, it can be reconstructed from infinitesimal steps .[97] Secondly, instead of measure $\{M_1', M_2'\}$, we stop at $M'(x) = \sqrt{\frac{I+\tanh(x)(M_2'^2-M_1'^2)}{2}}$ before we reach M_2', that is to say, we perform measurement $\{\sqrt{1-e^{-2x}}M_1', \sqrt{1+e^{-2x}}M'(x)\}$. The effect is we still got $M_1'\rho M_1'^\dagger/p_1$ but the probability become $\sqrt{1-e^{-2x}}p_1$, but instead of get $M_2'\rho M_2'^\dagger/p_2$,

we get $M'(x)\rho M'^{\dagger}(x)/p(x)$ where $p(x) = Tr(M'(x)\rho M'^{\dagger}(x))$. Thirdly, we do nothing to the M'_1 branch, but do a POVM $\{M'(x,+\infty), M'(x,-\infty)\}$.

On the $M'(x)$ branch, it is easy to prove that,

$$\begin{aligned} M'(x,\infty)M'(x) &= e^{-x}M'_1, \\ M'(x,-\infty)M'(x) &= M'_2. \end{aligned} \tag{3.45}$$

So in total, we perform a POVM $\{\sqrt{1-e^{-2x}}M'_1, e^{-x}M'_1, M'_2\}$, that is just the same as $\{M'_1, M'_2\}$. Finally, if we get the result of measurement $M'_1(M'_2)$, perform a unitary transformation $U_1(U_2)$, we can reconstruct $\{M_1, M_2\}$ with a stop in the middle. □

However, a protocol may contain many measurements and measurements with more than two outcomes, can we still use this method to stop in the middle and reconstruct everything?

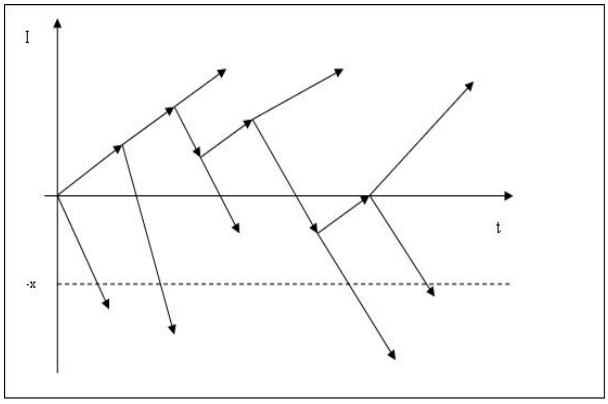


Figure 3.5: The original protocol written in the many two-outcome measurements form

The answer is yes. To show this, first we need to rewrite every measurement in the protocol into a sequence of two-outcome measurements [3], see Figure 3.5. Then the protocol consists of only two-outcome measurements. So the "stop and reconstruct" can work for each of them. The only thing is that, now, each two-outcome measurement may be related to many other two-outcome measurements, so during the "stop and reconstruct" process, many measurements might be affected. How can we be sure we can reconstruct everything? For this problem, notice that these two-outcome measurements are all in order. Then when we do the "stop and reconstruct", the principle is that we should always stop at the earlier two-outcome measurement first. Moreover, we need to reconstruct the earlier ones first. See Figure 3.6.

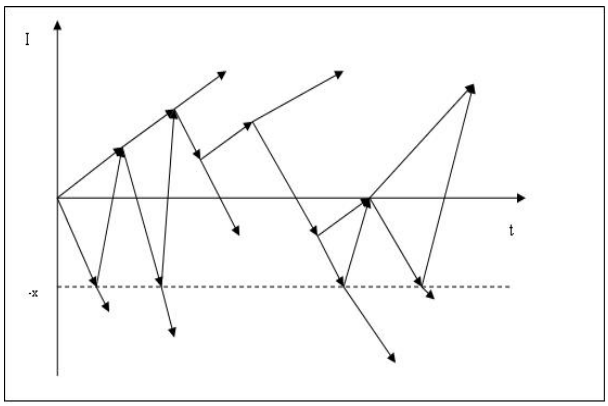


Figure 3.6: "Stop and reconstruct" method for the general protocol, I stands for the interference term

3.4.3 Example: $|\mathrm{GHZ}\rangle \to |\phi\rangle = \gamma(|000\rangle + |aaa\rangle)$

Now, we want to find an upper bound for the success probability of the transformation.

Theorem 3.11. *Suppose we have a SLOCC transformation protocol from* $|\mathrm{GHZ}\rangle$ *to* $|\phi\rangle = \gamma(|000\rangle + |aaa\rangle)$*, where* $|a\rangle = c\,|0\rangle + \sqrt{1-c^2}\,|1\rangle$ *and* $c \in (0, 1]$*. Suppose the successful probability is* p_m*. Then we can always find a protocol consisting of only successful and failure branches which has a successful probability no less than* p_m*.*

Proof. If the protocol is in that form, we do nothing. If the protocol has some branches which are neither successful nor failure. Then we do nothing to the successful or failure branches. However, for the undecided branches, from the definition of it we know we can always find a POVM that can transform it into the desired state with nonzero probability δ_p. Then the total successful probability is $p_m + \delta_p$, which is higher than p_m. In all, we can always find a protocol consisting of only successful and failure branches which have a successful probability no less than p_m. □

Now modify the protocol we get in the first step in the following way:

Suppose we can find at least one failure branch that have interference term smaller than -y, where $y \geq 0$. then we can find a x, where $0 \leq x \leq y$. As our initial interference term is zero, now we can use the weak measurement idea to let all the branches stop if its interference term reaches -x and do nothing to the branches which never reach -x. And we can get a new protocol in Figure 3.7

Remark 3.5. Note that to make this new protocol work, we have applied the intermediate value theorem. That is to say, we implicitly assume that the interference terms, I, of the two intermediate states specified in Theorem 3.9, are continuous functions of x. This assumption works because, from [97], we know $M(x, \delta x)$ changes the state given

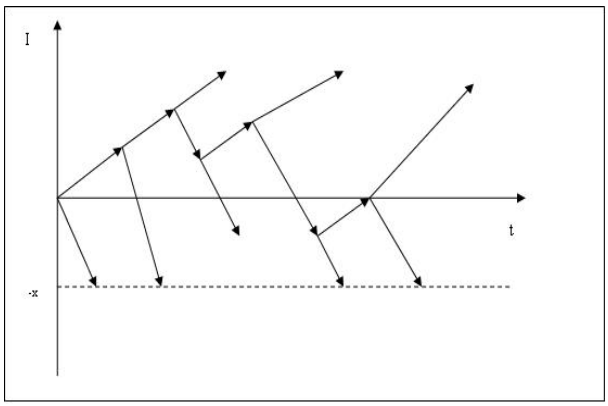


Figure 3.7: The new protocol, which can reconstruct the original one.

by $M(x)\,|\mathrm{GHZ}\rangle$ very little, or we can say it is a weak measurement. While from the expression of interference term Equation (A.1) in Appendix, we know interference term is a continuous function of the parameters of the state. Then, as the state changes very little under the weak measurement, the interference term also changes continuously.

Then we get a new protocol. It has two properties:

1) There are three kinds of branches: failure branches with interference term larger than or equal to -x, successful branches and the branches neither successful nor failure with interference term -x.

2) From the "stop and reconstruct" part, we know we can reconstruct the original protocol by performing LOCCs (may be a sequence of measurements) just on these branches which have interference term -x and do nothing on other branches. That is to say, just do LOCCs on the -x branches, we can get a total successful probability no less than the original one. So, if we have an upper bound of successful probability for the new protocol, that should also be an upper bound for the original one.

Then we can find the upper bound for this new protocol. Now, the protocol consists of three kinds of branches: successful branches, failure branches with interference term larger than or equal to -x, and undecided branches with interference term -x. The total successful probability of this protocol consists of two probability: the already existing successful branches' total probability p_{se} and the probability we can transform from the -x branches to the states we want.

Theorem 3.12. *As in Theorem 3.11, we consider a SLOCC transformation from* $|\mathrm{GHZ}\rangle$ *to* $|\phi\rangle = \gamma(|000\rangle + |aaa\rangle)$*. For all the possible new protocols shown in Figure 3.7, there is an upper bound for the success probability,*

$$\bar{p_s}(-x) = p_{as}(-x) + p_u(-x) * p_m(s| - x), \tag{3.46}$$

where $p_{as}(-x)$ are the already successful branches in this condition, while $p_u(-x)$ is the probability of the undecided branches with interference term $-x$, and $p_m(s|-x)$ is the maximal probability to transform a GHZ-class state with interference term $-x$ into the destination state ϕ_s. We get

$$p_{as} = \frac{\frac{a^3}{1-a^3}}{\frac{c^3}{1+c^3} + \frac{a^3}{1-a^3}}, \qquad p_u(-x) = 1 - p_{as}, \tag{3.47}$$

$$p_m(s|-x) = \min\left(\frac{\max(\tau_{ABC}(\phi|I(\phi) = -x))}{\tau_{ABC}(\phi_s)}, 1\right), \tag{3.48}$$

where a is the solution of the equation $x = \frac{a^3}{1-a^3}$, and τ_{ABC} stands for the 3-tangle.

We firstly consider the case that there exists no failure branches with interference term larger than -x, later we will show the other case can only give an upper bound smaller than in this case.

Lemma 3.13. *If the new protocol shown in Figure 3.7 consists of only successful branches and branches with interference term $-x$ (no failure branches with interference term larger than $-x$), it has an upper bound*

$$\bar{p_s}(-x) = p_{as}(-x) + p_u(-x)p_m(s|-x) \tag{3.49}$$

where the parameters are defined in Theorem 3.12.

Proof. For the already existing successful branches, the total probability is determined by -x and the conservation of interference term. As $x = \frac{a^3}{1-a^3}$, we have

$$p_{as}(-x)I(|\phi_s\rangle) - p_u(-x)x = 0 \tag{3.50}$$

$$p_{as}(-x) + p_u(-x) = 1 \tag{3.51}$$

Solving Equations (3.50) and (3.51), we can find

$$p_{as}(-x) = \frac{\frac{a^3}{1-a^3}}{\frac{c^3}{1+c^3} + \frac{a^3}{1-a^3}}. \tag{3.52}$$

For the maximum value of $p_s(-x)$, using the 3-tangle idea, we know it is bounded by

$p_u(-x)p_m(s|-x)$ where

$$p_m(s|-x) = \min\left(\frac{\max(\tau_{ABC}(\phi|I(\phi)=-x))}{\tau_{ABC}(\phi_s)}, 1\right) \tag{3.53}$$

Then we find an upper bound for the successful probability of this new protocol when there is no failure branch having interference term larger than $-x$:

$$\bar{p_s}(-x) = p_{as}(-x) + p_u(-x)p_m(s|-x) \tag{3.54}$$

□

Remark 3.6. To show it is really an upper bound for the successful probability for the new protocol, we need to show if there is any other failure branch with interference term larger than -x, we can only get a successful probability smaller than this.

Proof of Theorem 3.12. To prove this theorem, we just need to prove the following: If the new protocol contains a failure branch which has an interference term larger than -x, it has an upper bound for the success probability smaller than what we get in Lemma 3.13.

Consider the conservation of interference term, now we have:

$$p'_{as}(-x)I(|\phi_s\rangle) + \sum p_{fi}I(|\phi_{f_i}\rangle) - p'_u(-x)x = 0 \tag{3.55}$$
$$p'_{as}(-x) + \sum p_{fi} + p'_u(-x) = 1 \tag{3.56}$$

which can be rewritten as from Corollary 3.15

$$p'_{as}(-x)I(|\phi_s\rangle) - p"(-x')x' = 0 \tag{3.57}$$
$$p'_{as}(-x) + p"(-x') = 1 \tag{3.58}$$

where

$$x' = \frac{\sum p_{fi}I(|\phi_{f_i}\rangle) - p'_u(-x)x}{\sum p_{fi} + p'_u(-x)} \tag{3.59}$$
$$p"(-x') = \sum p_{fi} + p'_u(-x) \tag{3.60}$$

As $I(|\phi_{f_i}\rangle) > -x$, we know $-x' > -x$, so $p'_{as}(-x) < p_{as}(-x)$. Let the difference between $p'_{as}(-x)$ and $p_{as}(-x)$ be δ_s, then we have $\delta_s = p_{as}(-x) - p'_{as}(-x)$, so $\delta_s > 0$ and

$p"(-x') = p_u(-x) + \delta_s$. As $\sum p_{fi} > 0$, we have $p'(-x) < p"(-x') = p_u(-x) + \delta_s$. So the total successful probability in this case is

$$\begin{aligned} & \bar{p'_s} = p'_{as}(-x) + p'(-x) * p(s|-x) \\ \leq \quad & p'_{as}(-x) + p'(-x) * p_m(s|-x) \\ < \quad & p_{as}(-x) - \delta_s + (p_u(-x) + \delta_s) * p_m(s|-x) \\ < \quad & p_{as}(-x) + p_u(-x) * p_m(s|-x) \\ & +\delta_s(p_m(s|-x) - 1) \\ \leq \quad & p_{as}(-x) + p_u(-x) * p_m(s|-x) \\ = \quad & \bar{p_s}(-x) \end{aligned} \tag{3.61}$$

Here, in the second last step, we have used the fact that $p_m(s|-x)$ cannot be larger than one. So we know it is really an upper bound for the successful probability for the new protocol, which should also be an upper bound for the successful probability for the original protocol, and an upper bound for the transformation protocols which contains at least on failure branch which has interference term smaller than -x (or we can say it passes -x). So we have $\bar{p'_s} < \bar{p_s}(-x)$, which means $\bar{p_s}(-x)$ is an upper bound for the new protocol. □

Corollary 3.14. *As in Theorem 3.11, we consider a SLOCC transformation from* $|\mathrm{GHZ}\rangle$ *to* $|\phi\rangle = \gamma(|000\rangle + |aaa\rangle)$. *If a protocol contains at least one failure branch whose interference term is smaller than -y, its successful probability should be bounded by all the* $\bar{p_s}(-x)$, *where* $0 \leq x \leq y$.

Proof. If we see every branch from the weak measurement idea. We will find the interference term should change continuously, so we can stop at any point between 0 and -y. For each point we choose, we can get an upper bound. And all the upper bounds should be the upper bounds of the original branch. □

Corollary 3.15. *For a LOCC transformation protocol from* $|\mathrm{GHZ}\rangle$ *to* $|\phi\rangle = \gamma(|000\rangle + |aaa\rangle)$, *if the minimum interference term of all the failure branches is -z, then its successful probability should be bounded by*

$$p_{bound}(-z) = \min(p^U(-z), \bar{p}_{\tau_{ABC}}(-z)) \tag{3.62}$$

where $\bar{p}_{\tau_{ABC}}(-z)) = \min_{0 \leq x \leq z}(\bar{p_s}(-x))$.

Proof. If the minimum interference term is -z, then from Theorem 3.8, we know there is an upper bound $p^U(-z) = \frac{z}{I(|\phi_s\rangle)+z}$, which is in fact $p_{as}(-z)$. As it is bounded by all the $\bar{p_s}(-x)$, where $0 \leq x \leq z$, we can find another upper bound $\bar{p}_{\tau_{ABC}}(-z)) = \min_{0\leq x\leq z}(\bar{p_s}(-x))$. See Figure 3.8 for the relation between $\bar{p_s}$ and $\bar{p}_{\tau_{ABC}}$. Then the minimum of these two bounds is also an upper bound, which we call $p_{bound}(-z)$. □

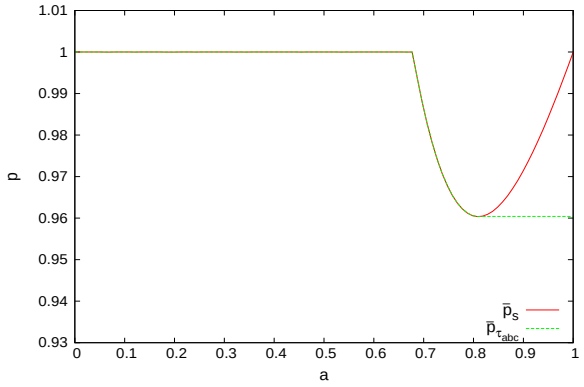


Figure 3.8: The relation between $\bar{p_s}$ and $\bar{p}_{\tau_{ABC}}$

Theorem 3.16. *An upper bound of LOCC transformation from GHZ state to a specific GHZ class state* $|\phi\rangle = \gamma(|000\rangle + |aaa\rangle)$ *is the maximum value of* $p_{bound}(-z)$ *where* $z \in [0, +\infty)$. *And it is in fact the minimum value of* $\bar{p_s}(-z)$, *where* $z \in [0, +\infty)$.

Proof. The basic picture of our proof can be represented in Figure 3.9.

Now we consider all the possible transformation protocols. Then the value of the minimum interference term -z may vary from 0 to ∞. (We can always find a protocol giving a very small value of -z, while its successful probability is still bounded.) Easy to see an upper bound is the maximum value of $p_{bound}(-z)$ for all the possible values of z, where $z \in [0, \infty)$. In fact, we can find the upper bound we get for this transformation is the minimum value of $\bar{p_s}(-z)$, where $z \in [0, +\infty)$. □

Put $\tau_{ABC}(\phi) = \frac{(1-c^2)^3}{(1+c^3)^2}$, in to the equation, we can get the upper bound. The analytic value is hard to get, if we put c=0.5. The minimum value of $\bar{p_s}(-x) = p_{as}(-x) + p_u(-x) * p_m(s| - x)$ is 0.9604 at x=1.13062, which is less than 1.

3.4.4 The General Case

In the above, we have considered an upper bound for the special case of $|\text{GHZ}\rangle \to |\phi\rangle = \gamma(|000\rangle + |aaa\rangle)$ to find the upper bound for it. Now, we will consider two more general

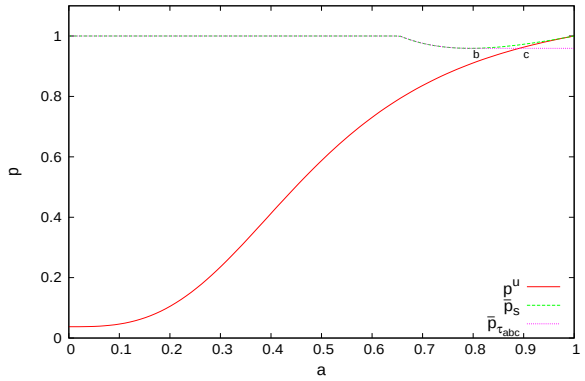


Figure 3.9: The upper bound for the transformation. In this figure, $a = (-\frac{x}{x-1})^{\frac{1}{3}}$. So when a goes from 0 to 1, x goes from 0 to ∞. The dashed line is the plot of $\bar{p_s}$ as a function of -x, the dot line is the plot of $\bar{p}_{\tau_{ABC}}$, the solid line is the plot of p^U. Notice that point b corresponds to the minimum value of $\bar{p_s}$, before b, $\bar{p_s}$ decreases monotonically. So before b, $\bar{p}_{\tau_{ABC}}$ is the same as $\bar{p_s}$, while after b, $\bar{p}_{\tau_{ABC}}$ remains to be the value of $\bar{p_s}$ at b. Another thing is that before c, p^U is smaller than $\bar{p}_{\tau_{ABC}}$, while after c, $\bar{p}_{\tau_{ABC}}$ is smaller than p^U. So the final plot we get for the upper bound is the solid line before c and the dot line after c, which we call upper bound line. The meaning of this upper bound line is that, for a given transformation protocol, if the smallest interference term of all the failure branches is -y, let $k = (-\frac{y}{y-1})^{\frac{1}{3}}$, the success probability cannot be larger than the corresponding point in the upper bound line. Consider all of the possible protocols (a goes from 0 to 1), the upper bound of the transformation probability is the largest value of the points on the upper bound line, which is just the minimum value of $\bar{p_s}$

cases. First, we will consider the transformation $|\text{GHZ}\rangle \to |\phi_{GHZ}\rangle = \sqrt{K}(c_\delta |0\rangle |0\rangle |0\rangle + s_\delta e^{i\varphi} |\varphi_A\rangle |\varphi_B\rangle |\varphi_C\rangle)$, which is the general GHZ class state; Second, we will consider a general GHZ class state to another general GHZ class state.

1. $|\text{GHZ}\rangle \to |\phi_{GHZ}\rangle = \sqrt{K}(c_\delta |0\rangle |0\rangle |0\rangle + s_\delta e^{i\varphi} |\varphi_A\rangle |\varphi_B\rangle |\varphi_C\rangle)$. In this case, we just need to change the expression for the interference term and 3-tangle of the destination state into

$$Interference\ term : I(\phi_s) = \frac{2c_\alpha c_\beta c_\gamma s_\delta c_\delta c_\varphi}{(1+2c_\alpha c_\beta c_\gamma s_\delta c_\delta)} \tag{3.63}$$

$$3-tangle : \tau_{ABC}(\phi_s) = \frac{4s_\alpha^2 s_\beta^2 s_\gamma^2 s_\delta^2 c_\delta^2}{(1+2c_\alpha c_\beta c_\gamma s_\delta c_\delta)^2} \tag{3.64}$$

Then we can use the similar process, except changing the corresponding value of Interference term and 3-tangle, see the following for details.

Firstly, using the "stop and reconstruct" method to get the new protocol with only successful branches and undecided branches with interference term x. We have

$$p_{as}(x) I(|\phi_s\rangle) + p_u(x) x = 0 \tag{3.65}$$

$$p_{as}(x) + p_u(x) = 1 \tag{3.66}$$

We have

$$p_{as}(x) = \frac{x}{x - I(|\phi_s\rangle)} = 1 - p_u(x) \tag{3.67}$$

$$p_m(s|x) = \min\left(\frac{max(\tau_{ABC}(\phi | I(\phi) = x))}{\tau_{ABC}(\phi_s)}, 1\right) \tag{3.68}$$

Then, the supremum success probability of this new protocol should be bounded by

$$\bar{p_s}(x) = p_{as}(x) + p_u(x) * p_m(s|x) \tag{3.69}$$

Consider all possible protocols, we find the minimum of $\bar{p_s}(x)$ where $x \in [0, \frac{1}{2}]$ if $I(|\phi_s\rangle) < 0$ and $x \in (-\infty, 0]$ if $I(|\phi_s\rangle) > 0$ is an upper bound of the success probability of this transformation.

Remark 3.7. Suppose we want to transform a GHZ state to a GHZ-class state $|\phi_{GHZ}\rangle = \sqrt{K}(c_\delta |0\rangle |0\rangle |0\rangle + s_\delta e^{i\varphi} |\varphi_A\rangle |\varphi_B\rangle |\varphi_C\rangle)$. If $I(|\phi_{GHZ}\rangle) \neq 0$, we can always find a nontrivial upper bound. However, for the case where $I(|\phi_{GHZ}\rangle) = 0$, we will get a trivial upper bound 1. This condition consists of 2 possibilities: 1. $\langle 000 | \varphi_A \varphi_B \varphi_C \rangle = 0$; 2. $\varphi = \frac{\pi}{2}$ or $\frac{3\pi}{2}$. In fact, in the paper [127], they have provided a protocol for such a transformation

with success probability 1.

2. A general GHZ class state to another general GHZ class state. In this case, the interference term is still conserved, but the initial value should be the interference term of the initial state.

$$p_{as}(x)I(|\phi_s\rangle) + p_u(x)x = I_{initial} \tag{3.70}$$
$$p_{as}(x) + p_u(x) = 1 \tag{3.71}$$

We have

$$p_{as}(x) = \frac{I_{initial}-x}{I(|\phi_s\rangle)-x} = 1 - p_u(x) \tag{3.72}$$
$$p_m(s|x) = \min(\frac{max(\tau_{ABC}(\phi|I(\phi)=x))}{\tau_{ABC}(\phi_s)}, 1) \tag{3.73}$$

Then, the supremum success probability of this new protocol should be bounded by

$$\bar{p_s}(x) = \bar{p_s}(x) + p_u(x) * p_m(s|x) \tag{3.74}$$

Consider all possible protocols, we find the minimum of $\bar{p_s}(x)$ where $x \in [I_{initial}, \frac{1}{2}]$ if $I(|\phi_s\rangle) < I_{initial}$ and $x \in (-\infty, I_{initial}]$ if $I(|\phi_s\rangle) > I_{initial}$ is an upper bound of the success probability of this transformation.

Example 3.17. An upper bound for the transformation from $|\phi\rangle = \gamma(|000\rangle + |abc\rangle)$ where $\langle 0|a\rangle = 0.1$, $\langle 0|b\rangle = 0.2$, $\langle 0|c\rangle = 0.2$, to $|\psi\rangle = \gamma'(|000\rangle + |a'b'c'\rangle)$ where $\langle 0|a'\rangle = 0.4$, $\langle 0|b'\rangle = 0.5$, $\langle 0|c'\rangle = 0.6$ is 0.9593. See Figure 3.10.

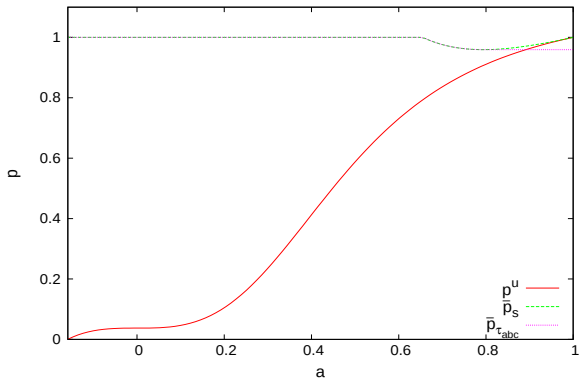


Figure 3.10: Upper bound for the transformation probability from $|\phi\rangle$ to $|\psi\rangle$.

Lemma 3.18. *For a transformation from a tripartite state $|\phi_i\rangle$ to another tripartite state $|\phi_s\rangle$, if the interference term of $|\phi_i\rangle$ is not equal with $|\phi_s\rangle$, we can get an upper bound for the supremum of the successful probability which is less than 1.*

Proof. If the interference term is not equal, put into the Equation (3.70), we know the maximal successful probability $p_{as}(x)$ cannot reach one. Otherwise the conservation of interference term will be violated. In fact, as the magnitude of the interference term of branches where we stop become larger and larger, $p_{as}(x)$ gets closer and closer to one. However, at the same time the maximal 3-tangle of these branches will go to zero. As the destination state is in GHZ class, its 3-tangle is not zero. So we can always find one $|x|$, when the magnitude square of the interference term reaches it, $\max(\tau_{ABC}(\phi||I(\phi)| = |x|)) < \tau_{ABC}(\phi_s)$, then it will give an upper bound for this transformation which is smaller than 1. □

Remark 3.8. One may naturally ask a question: If the interference terms of two states are the same, can we give an upper bound for the transformation probability? In this case, the above lemma cannot give a nontrivial upper bound. However, we can still use other entanglement monotones, such as 3-tangle, to give an upper bound for the transformation from one to another.

Example 3.19. Consider the transformation from $|\phi\rangle = \gamma(|000\rangle + |abc\rangle)$ where $\langle 0|a\rangle = 0.2$, $\langle 0|b\rangle = 0.4$, $\langle 0|c\rangle = 0.8$, to $|\psi\rangle = \gamma'(|000\rangle + |a'b'c'\rangle)$ where $\langle 0|a'\rangle = 0.4$, $\langle 0|b'\rangle = 0.4$, $\langle 0|c'\rangle = 0.4$. One can check that $I(|\phi\rangle) = I(|\psi\rangle) = 0.0602$. So naively we can only get a trivial upper bound for the transformation between them. However, notice that $\tau_{ABC}(|\phi\rangle) = 0.2564$ and $\tau_{ABC}(\psi) = 0.5235$, we can get an upper bound for the transformation from $|\phi\rangle$ to $|\psi\rangle$ which is

$$\frac{\tau_{ABC}(|\phi\rangle)}{\tau_{ABC}(|\psi\rangle)} = \frac{0.2546}{0.5235} = 0.4863 < 1 \tag{3.75}$$

3.5 Lower Bound for the Transformation

After the discussions about the upper bound, the question arises, how tight are the derived upper bounds? To get an idea about the answer to that question, in this section we will derive a lower bound for the transformation probability from the GHZ state to a GHZ class state. In Ref. [28], a straightforward protocol was provided for the

transformation

$$\begin{aligned} |\mathrm{GHZ}\rangle &= \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \\ \xrightarrow{\mathrm{LOCC}} |\Psi\rangle &= \sqrt{K}(|000\rangle + |\varphi_A\rangle\,|\varphi_B\rangle\,|\varphi_C\rangle). \end{aligned} \tag{3.76}$$

It consists of Alice performing the measurement $\left\{\frac{A}{\|A\|}, \sqrt{\mathbb{1} - \frac{1}{\|A\|^2}A^\dagger A}\right\}$, where

$$A\,|0\rangle = |0\rangle\,, \qquad A\,|1\rangle = |\varphi_A\rangle\,, \tag{3.77}$$

and similarly for Bob and Charlie. Then the final successful probability is

$$p = \frac{(1 + c_\alpha c_\beta c_\gamma)^3}{(1 + c_\alpha)(1 + c_\beta)(1 + c_\gamma)}. \tag{3.78}$$

This protocol, however, was mostly designed to achieve a non-zero transformation probability, and no particular considerations were given towards optimizing the transformation probability.

In the following, we will provide a transformation protocol that can transform the GHZ-state, generalized to n parties and m dimensions, to other states with the same dimensions and Schmidt rank. This protocol will yield a success probability higher than the straightforward protocol . We will see, however, that there is still a gap between this lower bound and the previously derived upper bounds.

From the presented protocol, we will further derive the interesting result that all tripartite pure 3-qubit states can be transformed from the generalized GHZ-state for three qutrits by LOCC with probability 1, which was not known before.

The steps of the protocol are shown in Figure 3.11 for the transformation from the GHZ-state to the state $|\Psi\rangle = \gamma(\alpha\,|a_1 b_1 c_1\rangle + \beta\,|a_2 b_2 c_2\rangle)$. We call this protocol the *"four-step method"*, as it consists of four steps. In the first step, we transform the GHZ state into $|\mathrm{GHZ}'\rangle = \alpha\,|000\rangle + \beta\,|111\rangle$, which has the same coefficient as $|\Psi\rangle$. Next, we transform $|\mathrm{GHZ}'\rangle$ into $|\phi_{b1}\rangle = \alpha\,|0b_1 0\rangle + \beta\,|1b_2 1\rangle$. Then, we transform $|\phi_{b1}\rangle$ into $|\phi_{c1}\rangle = \alpha\,|0b_1 c_1\rangle + \beta\,|1b_2 c_2\rangle$. We will show that these first three steps can be done with probability 1. The final step, which transforms $|\phi_{c1}\rangle$ into $|\Psi\rangle$ can achieved with probability 1 if $\langle a_1|a_2\rangle = 0$, because then $|\phi_{c1}\rangle$ and $|\Psi\rangle$ are unitarily equivalent. For $\langle a_1|a_2\rangle \neq 0$, we can still get $|\Psi\rangle$ with a higher probability than the previous result in [28] by performing an appropriate measurement on $|\phi_{c1}\rangle$.

The first step is a generalization of Nielsen's majorization result [95] and Lo and Popescu's [81] result for the maximum probability of distilling a maximally entangled

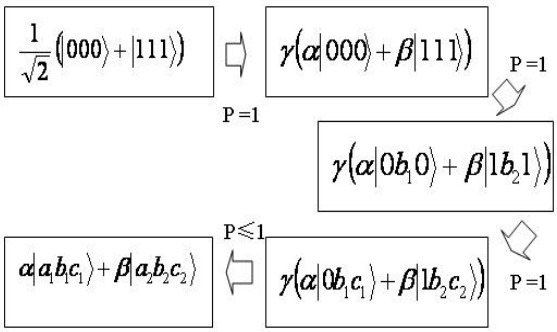


Figure 3.11: The four-step method to transform the GHZ-state into the state $\gamma(\alpha\,|a_1b_1c_1\rangle + \beta\,|a_2b_2c_2\rangle)$. The first three steps can be accomplished with probability 1. The overall success probability is thus determined by the fourth step, which is generally non-deterministic.

state. It has been noted previously in Ref. [137].

Definition 3.20. A GHZ-like (aka Schmidt decomposable) state is a tripartite state that can be written in the form

$$|\Psi\rangle = \sum_i \lambda_i\,|i\rangle\,|i\rangle\,|i\rangle \tag{3.79}$$

Theorem 1 of Lo-Popescu also holds for the GHZ-like states, because it gives an upper bound for the case where the Bob-Charlie alliance is allowed to perform any (non-local) operations, and when the allowed operations are restricted to the subclass of local operations, the upper bound still has to hold.

Theorem 2(a) of Lo-Popescu can in the same way be applied to GHZ-like (Schmidt decomposable) states, because all unitary transformations on Bob's side involve only a relabeling of the basis states ($|i\rangle \leftrightarrow |j\rangle$), and therefore extending it to GHZ-like states just changes this step to ($|i\rangle\,|i\rangle \leftrightarrow |j\rangle\,|j\rangle$), which can also be done by local unitaries only.

Theorem 2(b) generalizes to GHZ-like states as well, because here Alice performs all the operations and Bob either has to either perform no operation on his state at all (result "success"), or he has to discard it completely (result "failure"). Both operations can also be done if Bob's state is distributed among Bob and Charlie.

In Ref. [137], it was shown that Nielsen's majorization idea generalized to more par-

ties, can be applied to GHZ-like states, which means the transformation

$$\begin{aligned} |\mathrm{GHZ}_{mn}\rangle &= \frac{1}{\sqrt{m}} \sum_{i=1}^{m} |i\rangle_1 |i\rangle_2 ... |i\rangle_n \\ \rightarrow |\Psi\rangle &= \sum_{i=1}^{m} \alpha_i |i\rangle_1 |i\rangle_2 ... |i\rangle_n \end{aligned} \tag{3.80}$$

can be performed deterministically.

For the second and third step, we use the following lemma.

Lemma 3.21 ([127]). *The GHZ state can be transformed to* $|\Psi\rangle = \gamma(\alpha |a_1b_1c_1\rangle + \beta |a_2b_2c_2\rangle)$, *where* $\langle\Psi|\Psi\rangle = 1$ *and* $\alpha^2 + \beta^2 = 1$, *with probability 1, if* $|a_1b_1c_1\rangle$ *and* $|a_2b_2c_2\rangle$ *are orthogonal to each other.*

Proof. Suppose $|a_1\rangle$ and $|a_2\rangle$ are orthogonal to each other. If we choose the basis in which $|a_1b_1c_1\rangle = |000\rangle$, then we can write $|\phi\rangle = \gamma(\alpha |000\rangle + \beta |1\rangle_A (d_1 |0\rangle + d_2 |1\rangle)_B (e_1 |0\rangle + e_2 |1\rangle)_C)$, where $|d_1|^2 + |d_2|^2 = 1$ and $|e_1|^2 + |e_2|^2 = 1$. In this case we can see that $\gamma = 1$, and we can do the transformation in the following way.

First, use the result of the first step to transform $|\mathrm{GHZ}\rangle$ into $|\mathrm{GHZ}'\rangle = \alpha |000\rangle + \beta |111\rangle$ with probability 1.

Next, Bob performs a POVM

$$M_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & d_1 \\ 0 & d_2 \end{pmatrix}, \qquad M_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -d_1 \\ 0 & -d_2 \end{pmatrix}. \tag{3.81}$$

Then, with probability $\frac{1}{2}$, we get $|\phi_{b1}\rangle = \alpha |000\rangle + \beta |1\rangle_A (d_1 |0\rangle + d_2 |1\rangle)_B |1\rangle_C$, and with probability $\frac{1}{2}$ we get $|\phi_{b2}\rangle = \alpha |000\rangle - \beta |1\rangle_A (d_1 |0\rangle + d_2 |1\rangle)_B |1\rangle_C$. If we get $|\phi_{b2}\rangle$, Alice performs the unitary transformation

$$U_A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{3.82}$$

to also get $|\phi_{b1}\rangle$ in this case. So, with probability 1, we get $|\phi_{b1}\rangle$.

Finally, Charlie performs the POVM

$$M_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & e_1 \\ 0 & e_2 \end{pmatrix}, \qquad M_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -e_1 \\ 0 & -e_2 \end{pmatrix}. \tag{3.83}$$

Then, with probability $\frac{1}{2}$, we get $|\phi_{c_1}\rangle = \alpha |000\rangle + \beta |1\rangle_A (d_1 |0\rangle + d_2 |1\rangle)_B (e_1 |0\rangle + e_2 |1\rangle)_C$, which is exactly the state $|\phi\rangle$ we want to get, and with probability $\frac{1}{2}$ we get $|\phi_{c_2}\rangle =$

$\alpha|000\rangle - \beta|1\rangle_A(d_1|0\rangle + d_2|1\rangle)_B(e_1|0\rangle + e_2|1\rangle)_C$. If we get $|\phi_{c_2}\rangle$, again, Alice can perform the unitary transformation

$$U_A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{3.84}$$

to get $|\phi_{c1}\rangle$, too. So with probability 1 we can get $|\phi_{c1}\rangle$. Then we can get $|\Psi\rangle = \alpha|a_1b_1c_1\rangle + \beta|a_2b_2c_2\rangle$ with certainty. □

Hence, we have shown that the first three steps can be done with probability 1. For the last step, we have the following theorem.

Theorem 3.22. *For $|\Psi\rangle = \gamma(\alpha|a_1b_1c_1\rangle + \beta|a_2b_2c_2\rangle)$, where $\alpha^2 + \beta^2 = 1$ and γ is a normalization factor, if $\langle a_1|a_2\rangle = \lambda_a$, $\langle b_1|b_2\rangle = \lambda_b$, $\langle c_1|c_2\rangle = \lambda_c$, then there exists a SLOCC transformation protocol from the GHZ state to $|\psi\rangle$ such that the probability of success is at least $\frac{1+2\alpha\beta\lambda_a\lambda_b\lambda_c}{1+\lambda_m}$, where $\lambda_m = \min(\lambda_a, \lambda_b, \lambda_c)$.*

Proof. First, note that we can write $|\psi\rangle$ as

$$|\psi\rangle = \gamma(\alpha|000\rangle + \beta(\lambda_a|0\rangle + \sqrt{1-\lambda_a^2}|1\rangle)_A(\lambda_b|0\rangle + \sqrt{1-\lambda_b^2}|1\rangle)_B(\lambda_c|0\rangle + \sqrt{1-\lambda_c^2}|1\rangle)_C),$$

where $\gamma = \frac{1}{\sqrt{1+2\alpha\beta\lambda_a\lambda_b\lambda_c}}$. From Lemma 3.21, we know that we can transform the GHZ state to $|\xi\rangle = \alpha|000\rangle + \beta|1\rangle_A(\lambda_b|0\rangle + \sqrt{1-\lambda_b^2}|1\rangle)_B(\lambda_c|0\rangle + \sqrt{1-\lambda_c^2}|1\rangle)_C$ with probability 1. Then, from $|\xi\rangle$, Alice can do the POVM

$$M_1 = \frac{1}{\sqrt{1+\lambda_a}} \begin{pmatrix} 1 & \lambda_a \\ 0 & \sqrt{1-\lambda_a^2} \end{pmatrix}, \tag{3.85}$$

$$M_2 = \frac{\sqrt{\lambda_a}}{\sqrt{1+\lambda_a}} \begin{pmatrix} 1 & -1 \\ 0 & 0 \end{pmatrix}. \tag{3.86}$$

So with probability $p = \frac{1+2\alpha\beta\lambda_a\lambda_b\lambda_c}{1+\lambda_a}$, we get $|\psi\rangle$, while the other branch will give a state in which the rank of ρ_a is 1, so that the probability to get $|\psi\rangle$ from it is zero. Thus, the total probability is $\frac{1+2\alpha\beta\lambda_a\lambda_b\lambda_c}{1+\lambda_a}$. However, we can do a permutation of A, B and C so that the probability can also be $\frac{1+2\alpha\beta\lambda_a\lambda_b\lambda_c}{1+\lambda_b}$ or $\frac{1+2\alpha\beta\lambda_a\lambda_b\lambda_c}{1+\lambda_c}$. And the maximum probability corresponds to $\min(\lambda_a, \lambda_b, \lambda_c)$. □

Example 3.23. Again, we use the transformation from $|\text{GHZ}\rangle$ to $|\phi\rangle = \gamma(\frac{1}{\sqrt{2}}|000\rangle + \frac{1}{\sqrt{2}}|aaa\rangle)$, where $|a\rangle = c|0\rangle + \sqrt{1-c^2}|1\rangle$ and $c \in (0, 1]$, as an example. Using the protocol we provided, we can get a successful probability of $p = \frac{1+c^3}{1+c}$. Let $c = 0.5$, then we have $p_s = 0.75$. In comparison, the upper bound we got in Section 3.4 was 0.9604. There is still a gap between these two values. How to reduce it is still an open problem.

Now we will generalize the result of Lemma 3.21 to higher dimensions and more parties. Suppose we are concerned with the transformation from the GHZ-state, generalized to n parties and m dimensions, $|\mathrm{GHZ}_{mn}\rangle = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} |i\rangle_1 |i\rangle_2 ... |i\rangle_n$, to $|\psi\rangle = \gamma(\sum_{i=1}^{m} \alpha_i |k_{1_i} k_{2_i} ... k_{n_i}\rangle)$. The basic idea of our protocol can be divided into three steps. First, we want to transform $|\mathrm{GHZ}_{mn}\rangle$ into $|\Psi\rangle = \sum_{i=1}^{m} \alpha_i |i\rangle |i\rangle |i\rangle$, which is called a GHZ-like (or Schmidt decomposable) state. Then, we transform $|\Psi\rangle$ into $|\psi_n\rangle = \sum_{i=1}^{m} \alpha_i |i_1 k_{2_i} k_{i_3} ... k_{i_n}\rangle$. We will show that these two steps can be done with probability 1. Finally, if for at least $m-1$ terms of $|\psi\rangle$, there is at least one party with a state that is orthogonal to this party's state in every other term, we show that we can transform $|\mathrm{GHZ}_{mn}\rangle$ into $|\psi\rangle$ with probability 1. In other cases, the transformation can still be done with a probability higher than what has been known before. The following theorem treats the case where the above criteria for the third step is met.

Theorem 3.24. *The GHZ-state, generalized to n parties and m dimensions,* $|\mathrm{GHZ}_{mn}\rangle = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} |i\rangle_1 |i\rangle_2 ... |i\rangle_n$, *can be transformed to* $|\psi\rangle = \sum_{i=1}^{m} \alpha_i |k_{1_i} k_{2_i} ... k_{n_i}\rangle$ *with probability 1, if for all but at most one* $i \in \{1, \cdots, m\}$, *there exists a party p such that* $\langle k_{p_i} | k_{p_j} \rangle = 0$ *for all* $j \neq i$. *This means that for at least* $m-1$ *terms, there is at least one party with a state that is orthogonal to this party's state in every other term.*

Proof. The basic idea is that we first make the coefficient of each term equal to the corresponding terms of the destination state. Then, we let party 2 perform a POVM that results in states that have the desired target state for party 2 in each term, however, depending on the outcome of the POVM, the coefficients might have picked up sign errors. The wrong signs can then be corrected by party 1. We proceed similarly for parties 3 through n. Finally, party 1 performs a similar POVM, which again may result in wrong signs for some terms. Then, if the requirements for the destination state are met, then there is at least one party for each term that can correct a wrong sign in its coefficient. The exact process is as follows.

Without loss of generality, we chose a basis for each party such that the target state $|\psi\rangle$ satisfies $|k_{q_i}\rangle = \sum_{j=1}^{i} a_{q_{ij}} |j\rangle_q$ for each party q. Then, as a first step, we use the result of Ref. [137] to get $|\mathrm{GHZ}'_{mn}\rangle = \gamma(\sum_{i=1}^{m} \alpha_i |i\rangle_1 |i\rangle_2 ... |i\rangle_n)$, where γ is a normalization

factor, from the initial $|\mathrm{GHZ}_{mn}\rangle$ state. Next, party 2 performs the POVM

$$
\begin{aligned}
M_0 &= \frac{1}{\sqrt{2^{m-1}}}\begin{pmatrix} 1 & a_{2_{10}} & \cdots & a_{2_{(m-1)0}} \\ 0 & a_{2_{11}} & \cdots & a_{2_{(m-1)1}} \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & a_{2_{(m-1)(m-1)}} \end{pmatrix}, \\
M_1 &= \frac{1}{\sqrt{2^{m-1}}}\begin{pmatrix} 1 & a_{2_{10}} & \cdots & -a_{2_{(m-1)0}} \\ 0 & a_{2_{11}} & \cdots & -a_{2_{(m-1)1}} \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & -a_{2_{(m-1)(m-1)}} \end{pmatrix}, \\
&\vdots \\
M_{2^{m-1}-1} &= \frac{1}{\sqrt{2^{m-1}}}\begin{pmatrix} 1 & -a_{2_{10}} & \cdots & -a_{2_{(m-1)0}} \\ 0 & -a_{2_{11}} & \cdots & -a_{2_{(m-1)1}} \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & -a_{2_{(m-1)(m-1)}} \end{pmatrix}.
\end{aligned}
\tag{3.87}
$$

This gives the state $|\psi_2\rangle = \sum_{i=1}^{m} \alpha_i |i_1 k_{i_2} i_3 ... i_n\rangle$ with probability $\frac{1}{2^{m-1}}$, and with the same probability we get other states that differ from $|\psi_2\rangle$ only in the signs of the coefficients α_i.

The wrong signs can be corrected with a unitary transformation by party 1, such that all branches now have the state $|\psi_2\rangle$. Then we can use the same method for parties $3, 4, \ldots, n$, so that we get the state $|\psi_n\rangle = \sum_{i=1}^{m} \alpha_i |i_1 k_{2_i} k_{3_i} ... k_{n_i}\rangle$ with probability 1.

After that, party 1 can perform a similar POVM and with probability $\frac{1}{2^{m-1}}$ we get $|\psi\rangle$ which is the state that we want, and with the same probability we get other states, which again differ from $|\psi\rangle$ only by the signs of the coefficients.

However, if for the jth term, there is at least one party p, with state $|k_{p_j}\rangle$ that is orthogonal to this party's state in every other term, then we can introduce a minus sign for the jth term by a unitary transformation of party p, which transforms $|k_{p_j}\rangle$ to $-|k_{p_j}\rangle$ and does nothing to all the other states orthogonal to $|k_{p_j}\rangle$. If such a party exists for at least $m-1$ terms, we can introduce a minus sign for these $m-1$ terms just by unitary transformations. For the only one term which possibly does not have this property (if it exists), we can introduce a minus sign for every other term and then introduce a global phase of -1. Hence, we can get $|\psi\rangle$ with probability 1. □

Remark 3.9. The condition we require in Theorem 3.24 is different from requiring that each term is orthogonal to the others. In fact, it is a stronger requirement than orthog-

onality. To see that, consider the following example: For the state $|\phi\rangle = \frac{1}{\sqrt{3}}[|000\rangle + |1\rangle(|0\rangle + |1\rangle)|0\rangle + (|0\rangle + |1\rangle)|0\rangle|1\rangle]$, it is easy to check that each term is orthogonal to the other ones in this state. But we do not know how to introduce a minus sign for any term, because the condition in Theorem 3.24 is not satisfied.

There is an open question: Is the condition in Theorem 3.24 also a necessary, or only a sufficient condition in higher dimensions? To determine if it is a necessary condition, there are two questions: *(i)* Is the form in which we write the state still unique in higher dimensions? We know, that for a 2-term tripartite state, in which each party has rank 2, if we write it in the form $|\psi\rangle = \gamma(\alpha|000\rangle + \beta(\lambda_a|0\rangle + \sqrt{1-\lambda_a^2}|1\rangle)_A(\lambda_b|0\rangle + \sqrt{1-\lambda_b^2}|1\rangle)_B(\lambda_c|0\rangle + \sqrt{1-\lambda_c^2}|1\rangle)_C)$, the result should be unique. It is also true for a 3-term tripartite state (the W-class state) [1]. However, similar results for higher dimensions have not been proved. *(ii)* Can a state in which all terms are orthogonal to each other be transformed from a GHZ-like state with probability 1? We know, our protocol can only work for a stronger requirement. However, that does not mean that no other protocol exists that works in this case, and no proof exists that shows that it cannot exist.

Corollary 3.25. *All tripartite pure three qubit states can be transformed from the 3-term GHZ state,* $|\mathrm{GHZ}_{33}\rangle = \frac{1}{\sqrt{3}}(|000\rangle + |111\rangle + |222\rangle)$*, with probability 1.*

Proof. From the Ref. [1], we know any tripartite pure state can be written as

$$\begin{aligned} |\Phi\rangle =& \lambda_0|000\rangle + \lambda_1 e^{i\phi}|100\rangle + \lambda_2|101\rangle \\ &+ \lambda_3|110\rangle + \lambda_4|111\rangle, \\ &\text{with } \lambda_i \geq 0,\ 0 \leq \phi \leq \pi,\ \mu_i \equiv \lambda_i^2,\ \sum \mu_i = 1 \end{aligned} \tag{3.88}$$

It was further shown in Ref. [1], that if Charlie introduces the unitary transformation

$$U = \frac{1}{\sqrt{\mu_1 + \mu_2}} \begin{pmatrix} \lambda_1 e^{-i\phi} & \lambda_2 e^{-i\phi} \\ \lambda_2 & -\lambda_1 \end{pmatrix}, \tag{3.89}$$

we can write $|\Phi\rangle$ in the form

$$\begin{aligned} |\Psi\rangle =& \frac{1}{\sqrt{\mu_1 + \mu_2}}[e^{-i\phi}\lambda_0\lambda_1|000\rangle + e^{-i\phi}\lambda_0\lambda_2|001\rangle \\ &+ (\lambda_1^2 + \lambda_2^2)|100\rangle + (\lambda_1\lambda_3 + \lambda_2\lambda_4)|110\rangle \\ &+ (\lambda_2\lambda_3 - \lambda_1\lambda_4)|111\rangle], \end{aligned} \tag{3.90}$$

which is unitarily equivalent with the state we want.

If we combine the first and second term into one term and do the same for the third and fifth term, we get

$$|\Psi\rangle = |00\rangle (a|0\rangle + b|1\rangle) + d|100\rangle + |11\rangle (c|0\rangle + e|1\rangle). \tag{3.91}$$

In this form, it is easy to see, that if we consider it as a 3-term state, it satisfies the condition we required for Theorem 3.24, so we can transform it from the generalized 3-term GHZ state, $|\mathrm{GHZ}_{33}\rangle$, with probability 1. □

Theorem 3.26. *For a general* $|\psi\rangle = \gamma(\sum_{i=1}^{m} \alpha_i |k_{1_i} k_{2_i} ... k_{n_i}\rangle)$, *where* $\sum_{i=1}^{m} \alpha_i^2 = 1$ *and* γ *is the normalization factor, there exists a SLOCC transformation protocol from the GHZ-state, generalized to n parties and m dimensions,* $|\mathrm{GHZ}_{mn}\rangle = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} |i\rangle_1 |i\rangle_2 ... |i\rangle_n$ *to* $|\psi\rangle$ *such that the probability of success is at least* $\max\left(\frac{1}{\gamma ||A_i||^2}\right)$, *where*

$$A_i = \frac{1}{\sqrt{2^{m-1}}} \begin{pmatrix} 1 & a_{i_{10}} & \cdots & a_{i_{(m-2)0}} & a_{i_{(m-1)0}} \\ 0 & a_{i_{11}} & \cdots & a_{i_{(m-2)1}} & a_{i_{(m-1)1}} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & a_{i_{(m-1)(m-1)}} \end{pmatrix} \tag{3.92}$$

Proof. From Theorem 3.24, we know that we can get $|\psi_n\rangle = \sum_{i=1}^{m} \alpha_i |i_1 k_{i_2} k_{i_3} ... k_{i_n}\rangle$ with certainty. Then, Alice performs the POVM $\left\{ \frac{A_1}{||A_1||}, \sqrt{1 - \frac{A_1^\dagger A_1}{||A_1||^2}} \right\}$, where

$$A_1 = \frac{1}{\sqrt{2^{m-1}}} \begin{pmatrix} 1 & a_{1_{10}} & \cdots & a_{1_{(m-2)0}} & a_{1_{(m-1)0}} \\ 0 & a_{1_{11}} & \cdots & a_{1_{(m-2)1}} & a_{1_{(m-1)1}} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & a_{1_{(m-1)(m-1)}} \end{pmatrix}. \tag{3.93}$$

The success probability for this POVM is $\frac{1}{\gamma ||A_1||^2}$. Similarly, we can choose any other party for the final step, and find the best one, which gives the maximum transformation probability. □

3.6 Summary and Concluding Remarks

In this chapter, we derived upper and lower bounds for the optimal transformation probability from the GHZ state to a GHZ-class state. In the derivation of the upper bounds, we first considered the action of the LOCC protocol on a different input state, namely $\frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)$, and demanded that the probability of an outcome remains bounded by

1. Then, by considering the constraints of the interference term and 3-tangle, we found an upper bound for more general cases. For the lower bound, we constructed a new transformation protocol, the "four-step method", to do the transformation. Before that, there was no nontrivial upper bound known for this transformation. The lower bound is generalized to higher dimension and more parties. As one application of the protocol that was used to find the lower bound, we discovered that all tripartite pure 3-qubit states can be transformed from the generalized GHZ state, $|\mathrm{GHZ}_{33}\rangle = \frac{1}{\sqrt{3}}(|000\rangle + |111\rangle + |222\rangle)$, with probability 1. This is a new result.

Chapter 4

Absolutely Maximal Entanglement and Quantum Secret Sharing

We study the existence of absolutely maximally entangled (AME) states in quantum mechanics and its applications to quantum information. AME states are characterized by being maximally entangled for all bipartitions of the system and exhibit genuine multipartite entanglement. With such states, we present a novel parallel teleportation protocol which teleports multiple quantum states between groups of senders and receivers. The notable features of this protocol are that (*i*) the partition into senders and receivers can be chosen after the state has been distributed, and (*ii*) one group has to perform joint quantum operations while the parties of the other group only have to act locally on their system. We also prove the equivalence between pure state quantum secret sharing schemes and AME states with an even number of parties. This equivalence implies the existence of AME states for an arbitrary number of parties based on known results about the existence of quantum secret sharing schemes. This chapter is largely based on Ref. [58].

4.1 Introduction

Entanglement is at the core of the power of quantum information processing and has been extensively studied for few qubits. The classification of entanglement classes for three and four qubits is well understood [34, 130, 59, 80, 85, 1, 21] and canonical forms of pure states under local unitary transformations of each local Hilbert space have also been analyzed [1, 74, 73]. As the number of local quantum degrees of freedom increases, our understanding of entanglement gets poorer. The number of independent invariants that classify entanglement grows exponentially and it is unclear which purpose each

category of entanglement serves [89, 41]. In recent years, there has been an important progress in the classification of the maximally multipartite entangled states composed of qubits [98, 22, 38, 47, 21]. Nevertheless, a complete understanding of the structure, classification and usefulness of quantum states with the largest possible entanglement for arbitrary dimension is still missing. Another motivation for studying multipartite entanglement is its connection to other apparently unrelated areas of physics, like string theory and black-holes [17, 18].

Quantum teleportation is one of the most intriguing utilizations of entanglement. It allows distant parties, who share a resource of entanglement, to transport a quantum state from one party to the other by only exchanging classical information and using up said entanglement. The first proposal of such a protocol used the resource of bipartite entanglement between two parties [13]. Later teleportation protocols using genuine multipartite entanglement between more than two parties were proposed theoretically for four qubit entanglement [140], and experimentally in the form of open-destination teleportation for five qubits [144].

This chapter is devoted to initiate the study of a class of states with genuine multipartite entanglement. These states, which we call absolutely maximally entangled (AME) states, are defined as having the strict maximal entanglement in all bipartitions of the system. Up until now, AME states have been thought to be a rather limited concept, because only few AME states exist for qubits, specifically no AME states exist for four, or eight and more qubits [38, 47, 104]. However, in this work, we consider the *qudit* problem, for which AME states exist for any number of parties for an appropriately chosen qudit dimension [57, 126]. A different approach, which has been investiged in Ref. [143], is to study the continuous variable regime instead of qubits.

The fact that AME states contain maximal entanglement makes them the natural candidates to implement novel multipartite communication protocols. Indeed, we shall here show how they can be used to implement novel parallel teleportation scenarios that postpone the choice of senders and receivers until after the state has been distributed. These protocols require that either the senders or receivers perform joint quantum operations, while the respective other parties only have to act locally on their systems. We further establish a one-to-one correspondence between pure state quantum secret sharing (QSS) schemes [30, 45] and even-party AME states. It should be mentioned that, while our parallel teleportation protocol is different from the aforementioned open-destination teleportation, it is also possible to implement open-destination teleportation with AME states [57].

4.2 Definition of AME States

An AME(n, d) state (absolutely maximally entangled state) of n qudits of dimension d, $|\psi\rangle \in \mathbb{C}_d^{\otimes n}$, is a pure state for which every bipartition of the system into the sets B and A, with $m = |B| \leq |A| = n - m$, is strictly maximally entangled such that

$$S(\rho_B) = m \log_2 d \,. \tag{4.1}$$

Consequently, every partition of m local degrees of freedom is represented by a reduced density matrix proportional to the identity

$$\rho_B = Tr_A |\psi\rangle\langle\psi| = \frac{1}{d^m} I_{d^m} \,, \qquad 1 \leq m \leq \frac{n}{2}. \tag{4.2}$$

In practice, to detect an AME state it is sufficient to check that all the $\binom{n}{\lfloor n/2 \rfloor}$ possible bipartitions of $\lfloor n/2 \rfloor$ qudits are maximally entangled, since all subsequent traces of the identity matrix are again identity matrices.

Furthermore, a state is an AME state iff it can be written as

$$|\mathrm{AME}\rangle = \frac{1}{\sqrt{d^m}} \sum_{k \in \mathbb{Z}_d^m} |k_1\rangle_{B_1} \cdots |k_m\rangle_{B_m} |\phi(k)\rangle_A \,, \tag{4.3}$$

with $\langle\phi(k)|\phi(k')\rangle = \delta_{kk'}$, for every partition into $m = |B| \leq |A| = n - m$ disjoint sets B and A. These equivalent characterizations of an AME state are summarized in the following definition.

Definition 4.1. An absolutely maximally entangled state is a pure state shared between n parties $P = \{1, \ldots, n\}$, each having a system of dimension d, i.e., $|\Phi\rangle \in \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n$ 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

$$|\Phi\rangle = \frac{1}{\sqrt{d^m}} \sum_{k \in \mathbb{Z}_d^m} |k_1\rangle_{B_1} \cdots |k_m\rangle_{B_m} |\phi(k)\rangle_A \,, \tag{4.4}$$

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, $\rho_A = d^{-\lfloor \frac{n}{2} \rfloor} \mathbb{1}_{d^{\lfloor \frac{n}{2} \rfloor}}$.

(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, $S(A) = |A| \log d$.

We denote such a state as an AME(n, d) state.

Two obvious examples of AME states are the Einstein-Rosen-Podolsky (EPR) and the Greenberger-Horne-Zeilinger (GHZ) states for two and three qubits, respectively. In both cases, the entanglement entropy is maximal for all their partitions. It has been proven that there are no absolutely maximally entangled states for four qubits [47]. AME states exist for five and six qubits [16], and a possible form for them will be given later in Example 4.4. No AME states exist for eight or more qubits [38, 47, 104]. The existence of an AME$(7, 2)$ state is still an open question, but it has been conjectured in Ref. [16] that no such state exists. By increasing the system dimension, AME states can be found for these cases in which no qubit AME states exist. For instance, there exists an AME state for four qutrits, which is given by

$$|\Phi\rangle = \frac{1}{\sqrt{9}} \sum_{i,j=0}^{2} |i\rangle\,|j\rangle\,|i+j\rangle\,|i+2j\rangle \tag{4.5}$$

We remark, however, that, although we will show that for each n, AME(n, d) states exist for some appropriate choice of d, finding the conditions for the existence of AME(n,d) states, depending on *n and d*, is generally a non-trivial problem. In the next chapter we will show that, interestingly, a special class of AME states can be constructed from certain classical error correcting codes, namely those that satisfy the Singleton bound [86].

4.3 Parallel Teleportation

The maximal entanglement property of an AME(n, d) state for any bipartition into the sets A and B can be used to teleport quantum states between those two sets. In contrast to the teleportation scenario where A and B share a maximally entangled state that is not an AME state, in the AME scenario the sets A and B do not have to be specified when the state is created, but instead can be chosen after the AME state has been distributed.

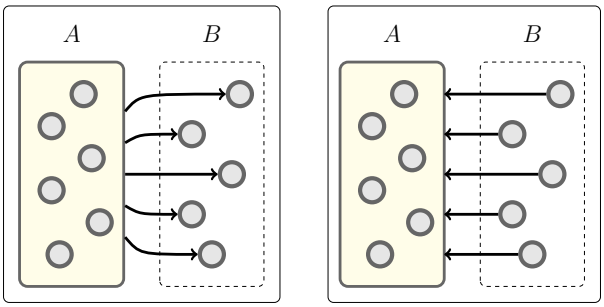


Figure 4.1: Parallel Teleportation scenarios of Theorem 4.2. Scenario (i) is on the left, and (ii) on the right. Parties in A perform joint quantum operations, parties in B only local quantum operations.

There are essentially three different ways in which the teleportation can be performed, depending on which parties can perform joint quantum operations, and which are separated and only able to perform local operations on their own quantum systems.

In the first case, the parties within each set, A and B, are able to perform joint quantum operations. A standard teleportation of an arbitrary d^m-dimensional state, where $m = \min(|A|, |B|)$, can be performed in either direction.

In the second case, the sending parties A can perform a joint quantum operation, but the parties in B are only able to perform local quantum operations. Additionally we require $m = |B| \leq |A| = n - m$. Then one qudit can be teleported from A to each of the parties in B, and thus in total m qudits are teleported from A to B. This is illustrated in the left hand side of Figure 4.1.

In the third and probably the most interesting case, the sending parties can only perform local operations, but the receiving parties can perform joint quantum operations. In this case, a teleportation is possible if the number of receiving parties is larger or equal $n/2$. Hence, sticking to our convention $m = |B| \leq |A|$, we now consider a teleportation from B to A. See the right hand side of Figure 4.1 for an illustration.

The first scenario is just a straightforward teleportation between maximally entangled parties. The second and third scenarios are presented in the following theorem.

Theorem 4.2. *Given an AME(n, d) state, and a bipartition of the n parties into the sets A and B such that $m = |B| \leq |A| = n - m$, then the following two parallel teleportation scenarios are possible*

(i) A can teleport one qudit to each party in B by performing a joint quantum operation and communicating two classical "dits" to each party in B. Each party in B can then locally recover their respective qudit with a local operation.

(ii) Each party in B can locally teleport one qudit to A. After receiving the measurement outcomes, consisting of two "dits" of classical information from each party in B, the parties in A are able to recover all m qudits by performing a joint quantum operation.

Proof. In both scenarios the parties in set A perform a joint quantum operation to transform the AME state into m d-dimensional EPR pairs. Then these pairs are used to teleport m qudits from the sending to the receiving parties. This is done by performing the joint unitary operation

$$U_A \left|\phi(k)\right\rangle_A = \left|k_1\right\rangle_{A_1} \cdots \left|k_m\right\rangle_{A_m} \left|0\right\rangle_{A'} . \tag{4.6}$$

on the initial AME(n, d) state

$$\left|\Phi\right\rangle = \frac{1}{\sqrt{d^m}} \sum_{k \in \mathbb{Z}_d^m} \left|k_1\right\rangle_{B_1} \cdots \left|k_m\right\rangle_{B_m} \left|\phi(k)\right\rangle_A , \tag{4.7}$$

with $\langle\phi(k)|\phi(k')\rangle = \delta_{kk'}$. This results in the state

$$U_A \left|\Phi\right\rangle = \left|\Psi\right\rangle_{B_1 A_1} \cdots \left|\Psi\right\rangle_{B_m A_m} \left|0\right\rangle_{A'} , \tag{4.8}$$

where $\left|\Psi\right\rangle = \sum \left|i\right\rangle \left|i\right\rangle$ are d-dimensional EPR pairs. These EPR pairs can now be used to teleport a qudit from A_i to B_i in case (i) (B_i to A_i in case (ii)). This requires A_i (B_i) to perform a generalized Bell measurement on her qudit and the qudit she wants to teleport, and communicate the measurement result to B_i (A_i). This amounts to sending the classical information of two "dits" for each EPR pair. Upon reception of the measurement result, B_i (A_i) can recover the teleported qudit by performing an appropriate unitary on his qudit. □

4.4 Quantum Secret Sharing

The last teleportation scenario suggests a close relationship between AME states and quantum secret sharing (QSS) schemes [30]. In a QSS protocol [30, 45], a dealer encodes a secret S in a quantum state that is shared among n players in such a way that only special subsets of players are able to recover the secret. The set of all subsets that are able to recover the secret form the access structure and the set of all subsets that can gain no information about the secret form the adversary structure. If the encoded state is a pure state, we call it a pure state QSS scheme. We are only interested in pure state

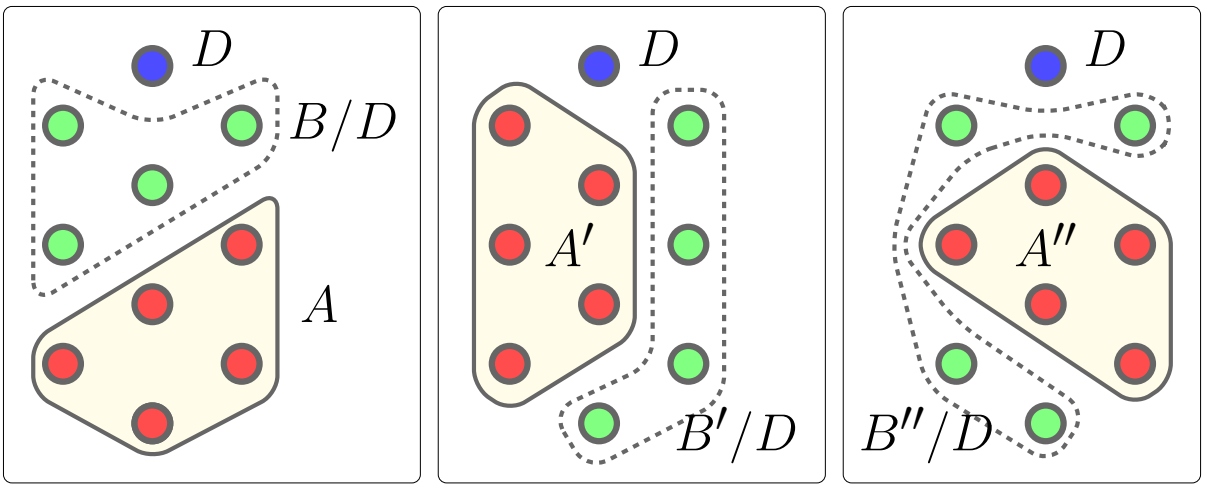


Figure 4.2: After D (blue) performs her teleportation operation, any set of m parties (red), A, A', A'' etc., can recover the teleported state. Any set of parties with $m-1$ or less parties (any set consisting only of green parties) cannot gain any information about the teleported state.

QSS schemes here.

Additionally, we restrict our attention to threshold QSS schemes [30], which means that the access structure is formed by all sets that contain k or more number of parties, while any set with less than k parties cannot obtain any information about the secret. Thus k is the threshold number of parties required to recover the secret. Such a QSS scheme is denoted as a $((k,n))$ threshold QSS scheme. For pure state threshold QSS schemes, n and k are always related by $n = 2k-1$ [30].

To see the relation between AME states and threshold QSS schemes, we consider an AME$(2m,d)$ state with an even number of parties and divide the parties into two sets $A = \{A_1,\ldots,A_m\}$ and $B = \{D, B_1,\ldots,B_{m-1}\}$ of equal size m. In set B we have singled out one party D, which will act as the dealer of the QSS scheme. Now we perform the protocol of Theorem 4.2 (ii), but only $D \in B$ performs the final teleportation operation. Also note that the unitary operation in Equation (4.6) and the Bell measurement by the dealer commute. Thus, D can first perform her Bell measurement, effectively encoding the teleported qudit onto the residual AME state, from which it can be recovered by the players in A.

Furthermore, instead of the bipartition into the sets A and B, we could have equally well chosen any other bipartition into two sets A' and B' of cardinality m with $D \in B'$. Then, without changing the operations that D has to perform, the parties in A' are able to recover the teleported qudit (see Figure 4.2 for an illustration).

Thus, any set of at least m of the residual $2m-1$ parties without D can recover

the teleported state, given that the measurement outcome is broadcasted to all parties. Furthermore, the no-cloning theorem guarantees that any set of less than m players cannot gain any information about the state [45]. Hence we constructed a $((m, 2m-1))$ threshold QSS scheme from an AME$(2m, d)$ state.

Before stating the theorem that formulates this observation concisely, we shortly review how a QSS protocol works. A secret of dimension d, $|S\rangle = \sum a_i |i\rangle$, is encoded into the state $\sum a_i |\Phi_i\rangle$ which is shared by the players such that each authorized set can deterministically recover $|S\rangle$ from its reduced state, while the reduced state of unauthorized sets is independent of the encoded secret. We call $|\Phi_i\rangle$ the basis states of the QSS scheme.

Theorem 4.3. *There is a one to one correspondence between AME$(2m, d)$ states and pure state $((m, 2m-1))$ threshold QSS schemes that have AME basis states, and share and secret dimensions d.*

Proof. AME to QSS: For any bipartition into parties $A = \{A_1, \ldots, A_m\}$ and $B = \{D, B_1, \ldots, B_{m-1}\}$, the AME$(2m, d)$ states has the form

$$|\Phi\rangle = \frac{1}{\sqrt{d^m}} \sum_{(i,k)\in\mathbb{Z}_d^m} |i\rangle_D |k_1\rangle_{B_1} \cdots |k_{m-1}\rangle_{B_{m-1}} |\phi(i,k)\rangle_A ,$$

with $\langle\phi(k,i)|\phi(k',j)\rangle = \delta_{kk'}\delta_{ij}$. We define the QSS basis states

$$\begin{aligned} |\Phi_i\rangle &= \sqrt{d}\ {}_D\langle i|\Phi\rangle \\ &= \frac{1}{\sqrt{d^{m-1}}} \sum_{k\in\mathbb{Z}_d^{m-1}} |k_1 \cdots k_{m-1}\rangle_B |\phi(k,i)\rangle_A . \end{aligned} \tag{4.9}$$

A secret encoded as

$$|a\rangle = \sum a_i |i\rangle \to \sum a_i |\Phi_i\rangle , \tag{4.10}$$

satisfies the requirement of a threshold QSS scheme, because the parties B have a completely mixed states, independent of the encoded secret. Additionally, the set A, which can be chosen to be any set of n players, can restore the secret $|a\rangle$ by performing the joint unitary operation

$$U_A |\phi(k,i)\rangle_A = |k_1\rangle_{A_1} \cdots |k_{m-1}\rangle_{A_{m-1}} |i\rangle_{A_m} . \tag{4.11}$$

QSS to AME: For any bipartition into m authorized parties $A = \{A_1, \ldots, A_m\}$ and $m-1$ unauthorized parties $B = \{B_1, \ldots, B_{m-1}\}$, the AME basis states of the QSS scheme

can be written in the form

$$|\Phi_i\rangle = \frac{1}{\sqrt{d^{m-1}}} \sum_{k \in \mathbb{Z}_d^{m-1}} |k_1\rangle_{B_1} \cdots |k_{m-1}\rangle_{B_{m-1}} |\phi(k,i)\rangle_A ,$$

where $\langle \phi(k,i)|\phi(k',i)\rangle = \delta_{kk'}$, because the states are AME states, and $\langle \phi(k,i)|\phi(k,j)\rangle = \delta_{ij}$, because the authorized parties can recover the secret deterministically. Thus,

$$\langle \phi(k,i)|\phi(k',j)\rangle = \delta_{kk'}\delta_{ij}. \tag{4.12}$$

From these basis states, define the state

$$\begin{aligned} |\Phi\rangle &= \frac{1}{\sqrt{d}} \sum_{i \in \mathbb{Z}_d} |i\rangle |\Phi_i\rangle \\ &= \frac{1}{\sqrt{d^m}} \sum_{(i,k) \in \mathbb{Z}_d^m} |i\rangle_D |k_1\rangle_{B_1} \cdots |k_{m-1}\rangle_{B_{m-1}} |\phi(k,i)\rangle . \end{aligned}$$

Because of Equation (4.12), $|\Phi\rangle$ is a maximally entangled state with respect to the bipartition $B \cup \{D\}$ vs. A. Since the original bipartition into A and B was arbitrary, $|\Phi\rangle$ is maximally entangled with respect to any bipartition into two cardinality m sets and thus is an AME$(2m, d)$ state. □

Example 4.4. In this example, we show how the five qubit code can be used to construct AME$(5,2)$ and AME$(6,2)$ states. From the five qubit code a $((3,5))$ threshold QSS scheme can be constructed [30]. The corresponding basis states are

$$\begin{aligned} |0_L\rangle = \frac{1}{4}(&|00000\rangle + |10010\rangle + |01001\rangle + |10100\rangle \\ &+ |01010\rangle - |11011\rangle - |00110\rangle - |11000\rangle \\ &- |11101\rangle - |00011\rangle - |11110\rangle - |01111\rangle \\ &- |10001\rangle - |01100\rangle - |10111\rangle + |00101\rangle), \end{aligned} \tag{4.13}$$

$$\begin{aligned} |1_L\rangle = \frac{1}{4}(&|11111\rangle + |01101\rangle + |10110\rangle + |01011\rangle \\ &+ |10101\rangle - |00100\rangle - |11001\rangle - |00111\rangle \\ &- |00010\rangle - |11100\rangle - |00001\rangle - |10000\rangle \\ &- |01110\rangle - |10011\rangle - |01000\rangle + |11010\rangle). \end{aligned} \tag{4.14}$$

These states are AME$(5,2)$ states as required. Following the recipe of Theorem 4.3, we

obtain the AME$(6,2)$ state

$$\begin{aligned}|\Phi\rangle =&\frac{1}{\sqrt{2}}[|0\rangle\,|0_L\rangle + |1\rangle\,|1_L\rangle]\\ =&\frac{1}{4}[|000\rangle\,(|+-+\rangle + |-++\rangle)\\ &+ |001\rangle\,(-|+--\rangle + |-++\rangle)\\ &+ |010\rangle\,(|++-\rangle - |--+\rangle)\\ &+ |011\rangle\,(-|+++\rangle - |---\rangle)\\ &+ |100\rangle\,(-|+++\rangle + |---\rangle)\\ &+ |101\rangle\,(-|++-\rangle - |--+\rangle)\\ &+ |110\rangle\,(-|+--\rangle - |-++\rangle)\\ &+ |111\rangle\,(-|+-+\rangle + |-+-\rangle)].\end{aligned} \tag{4.15}$$

4.5 Conclusion

In this chapter, we have introduced AME states, a class of highly entangled states, for n qudits shared among n locally separated parties. We have shown how they can be utilized in different parallel teleportation scenarios, which require some parties to perform joint quantum operations, while others' capabilities may be restricted to local operations. In those scenarios the advantage of AME states over less entangled states like a collection of EPR pairs lies in the fact that the partition into senders and receivers may be chosen after the state has been distributed.

Furthermore, we have investigated the relationship of AME states with QSS schemes and established a one-to-one correspondence between even party AME states and pure state threshold QSS schemes. In future work we further explore this very intuitive approach to develop new communication protocols from AME states as well as extending the range of QSS schemes that can be derived from AME states. For instance, instead of assigning the role of the dealer to only one of the parties in the AME state, we can imagine multiple dealers who encode independent secrets onto the residual AME states, resulting in QSS schemes with more involved access structures. The established connection to QSS schemes also confirms a relation between AME states and quantum error correction codes that was already suggested in Ref. [117]. A better understanding of this relation will allow us to construct new quantum error correction codes from AME states as well as deriving AME states from already known quantum codes. This might also shed light upon the open question of existence of AME states for a given number of parties

and system dimension.

Chapter 5

Absolutely Maximally Entangled States: Existence and Applications

In this chapter, we show the existence of AME states for any number of parties, given that the dimension of the involved systems is chosen appropriately. 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 properties for a wider class of ramp QSS schemes. We further show how AME states can be used as a valuable resource for open-destination teleportation protocols and to what extend entanglement swapping generalizes to AME states. This chapter is largely based on Ref. [57].

5.1 Introduction

In the previous chapter, we showed how AME states can be used for parallel teleportation protocols, where the parties are divided into a set of senders and receivers, and one set has to perform joint quantum operations, while the other set only needs to perform local quantum operations. These teleportation scenarios lead 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 [30, 45, 67]. 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 chapter, we will give an information-information theoretic proof of this equivalence of AME states and threshold QSS scheme, which shows that this 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 [120]. 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 [30]. We will then show two more applications for AME states. The first being the construction of a wider class of QSS schemes, the *ramp* QSS schemes, for which threshold QSS schemes are a special case. The other one is the utilization of AME states as resources for open-destination teleportation protocols [144]. Finally, we investigate to what extend entanglement can be swapped between two AME states.

This chapter is structured as follows. In Section 5.2 we show how AME states can be constructed from classical codes. In Section 5.3, we establish an equivalence between even party AME states and threshold QSS schemes, using an information theoretic approach to QSS. Section 5.4 shows how to share multiple secrets using AME states. In Section 5.5 we show that AME states can be used for open-destination teleportation.

5.2 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 $\mathcal{C}$ consists of M codewords of length n over an alphabet Σ of size d. For our purposes the alphabet is going to be $\Sigma = \mathbb{Z}_d$ and thus $\mathcal{C} \subset \mathbb{Z}_d^n$. The *Hamming distance* between two codewords is defined as the number of positions in which they differ, and the minimal distance δ of the code $\mathcal{C}$ as the minimal Hamming distance between any two codewords. For a given length n and minimal distance δ, the number of codewords M in the code is bounded by the *Singleton bound* [120, 86]

$$M \leq d^{n-\delta+1}. \tag{5.1}$$

Codes that satisfy the Singleton bound are referred to as maximum-distance separable (MDS) codes. They can be used to construct AME states:

Theorem 5.1(a). From a classical MDS code $\mathcal{C} \subset \mathbb{Z}_d^{2m}$ of length $2m$ and minimal distance

$\delta = m+1$ over an alphabet $\mathbb{Z}_d$, an AME$(2m, d)$ state can be constructed as

$$|\text{AME}\rangle = \frac{1}{\sqrt{d^m}} \sum_{c \in \mathcal{C}} |c\rangle \tag{5.2}$$

$$= \frac{1}{\sqrt{d^m}} \sum_{c \in \mathcal{C}} |c_1\rangle_1 \cdots |c_m\rangle_m |c_{m+1}\rangle_{m+1} \cdots |c_{2m}\rangle_{2m} . \tag{5.3}$$

Proof. The code $\mathcal{C}$ 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 (4.4) 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 5.1(b). From a classical MDS code $\mathcal{C} \subset \mathbb{Z}_d^{2m+1}$ 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

$$|\text{AME}\rangle = \frac{1}{\sqrt{d^m}} \sum_{c \in \mathcal{C}} |c\rangle \tag{5.4}$$

$$= \frac{1}{\sqrt{d^m}} \sum_{c \in \mathcal{C}} |c_1\rangle_1 \cdots |c_{m+1}\rangle_{m+1} |c_{m+2}\rangle_{m+2} \cdots |c_{2m}\rangle_{2m+1} . \tag{5.5}$$

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 (4.5) follows from the $[4, 2, 3]_3$ ternary Hammning code.

A wide class of MDS codes is given by the Reed-Solomon codes and its generalizations [108, 86, 118], which give MDS codes for $n = d-1$, $n = d$, and $n = d+1$, for $d = p^x$

being a positive power of a prime number p. From the Reed-Solomon codes, MDS codes can also be constructed for $n < d - 1$ [120]. 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 first paper on this subject [58], it has been brought to our attention by Gerardo Adesso that the results of this section have already been previously discovered by Ashish Thapliyal and coworkers, and were presented at a conference in 2003 [126], but remained unpublished.

5.3 Equivalence of AME states and QSS schemes

In the previous chapter, we showed that AME$(2m, d)$ 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 maximally entangled. B

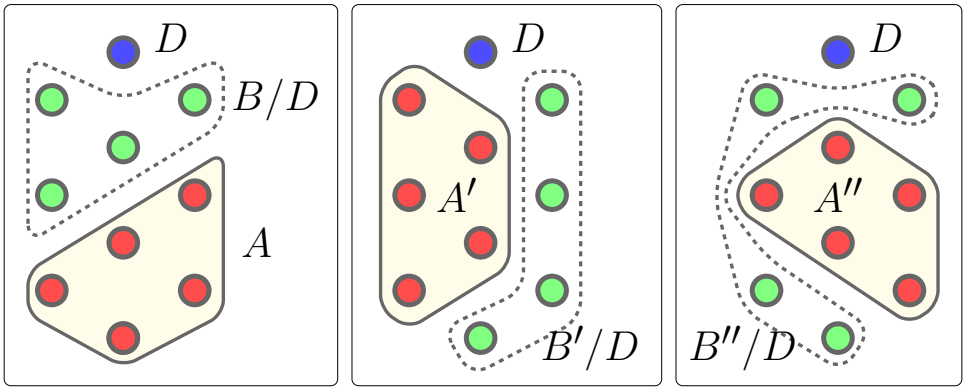


Figure 5.1: After D (blue) performs her teleportation operation, any set of m parties (red), A, A', A'' etc., can recover the teleported state. Any set of parties with $m - 1$ or less parties (any set consisting only of green parties) cannot gain any information about the teleported state.

We quickly review the information-theoretic framework for a pure state $((m, 2m-1))$ threshold QSS scheme [67]. 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

$$U_S : \mathcal{H}_S \to \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_{2m-1}. \tag{5.6}$$

The secret S is chosen randomly and thus is described by $\rho_S = 1/d \sum_i |i\rangle \langle i|$. We consider its purification by introducing a reference system R such that $|RS\rangle = 1/\sqrt{d} \sum_i |i\rangle |i\rangle \in \mathcal{H}_R \otimes \mathcal{H}_S$. Let ρ_{RA} denote the combined state of the reference system and a set of players $A \subseteq P$ after U_S has been applied to the secret. Then the players A can recover the secret, if there exists a completely positive map $T_A : \mathcal{H}_A \to \mathcal{H}_S$ such that [67, 116]

$$\mathbb{1}_R \otimes T_A(\rho_{RA}) = |RS\rangle . \tag{5.7}$$

This can be stated in terms of the mutual information

$$I(X : Y) = S(X) + S(Y) - S(X, Y) \tag{5.8}$$

as follows:

Definition 5.2. An isometry $U_S : \mathcal{H}_S \to \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_{2m-1}$ creates a $((m, 2m-1))$ threshold QSS scheme if and only if, after applying to the system S of the purification $|RS\rangle$, the mutual information between R and an authorized (unauthorized) set of players A (B) satisfies

$$I(R : A) = I(R : S) = 2S(S) \quad \text{if } |A| \geq m \tag{5.9}$$

$$I(R : B) = 0 \quad \text{if } |B| < m. \tag{5.10}$$

Here S is the von Neumann entropy, and because of $S(i) \geq S(S)$ [67], we have

$$S(S) = S(R) = S(i) = \log d. \tag{5.11}$$

From Equations (5.8) to (5.10) it immediately follows that

$$S(R, A) = S(A) - S(R) \quad \text{if } |A| \geq m \tag{5.12}$$

$$S(R, B) = S(B) + S(R) \quad \text{if } |B| < m. \tag{5.13}$$

Theorem 5.3. *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 (5.9) and (5.10) are satisfied, where R can be any of the $2m$ party. This follows directly from the definition of the mututal information, Equation (5.8), and Defintion 4.1(v).

$(ii) \rightarrow (i)$: 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 (5.12) we have

$$S(B, i, R) = S(B, i) - S(R) \tag{5.14}$$

On the other hand, using the Araki-Lieb inequality [96] $S(X, Y) \geq S(X) - S(Y)$ and Equation (5.13) gives

$$S(B, i, R) \geq S(B, R) - S(i) = S(B) + S(R) - S(i). \tag{5.15}$$

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

$$S(B, i) \geq S(B) + S(i), \tag{5.16}$$

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 [96]

$$S(X, Y) - S(Y) \geq S(X, Y, Z) - S(Y, Z) \tag{5.17}$$

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 5.4. *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.

5.4 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 5.3 shows the equivalence of AME states and QSS schemes, the actual protocol for the encoding and decoding operations has been presented in the previous chapter. 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($2m, d$) 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 [68, 42].

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 set 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* [14]. 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($2m, d$) state if more than one party assumes the role of the dealer.

Theorem 5.5. *Given an AME($2m, d$) state, a QSS scheme with secret dimension d^L and a $(m, L, 2m-L)$ 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 $2m$ 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 [13]

$$|\Psi_{qp}\rangle = \frac{1}{\sqrt{d}} \sum_j e^{2\pi i j q/d} |j\rangle |j+p\rangle \tag{5.18}$$

$$U_{qp} = \sum_j e^{2\pi i j q/d} |j\rangle \langle j+p| , \tag{5.19}$$

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

$$|\Phi_S\rangle = \frac{1}{\sqrt{d^{m-L}}} \sum_{k \in \mathbb{Z}_d^m} s_{\mathbf{qp},k_1 \cdots k_L} |k_{L+1}\rangle_{B_1} \cdots |k_m\rangle_{B_{m-L}} |\phi(k)\rangle_A . \tag{5.20}$$

Here

$$s_{\mathbf{qp},k_1 \cdots k_L} = \langle k_1 \cdots k_L | U^\dagger_{q_1 p_1} \otimes \cdots \otimes U^\dagger_{q_L p_L} | s \rangle , \tag{5.21}$$

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 5.20 can recover the secret. They can do so by applying the unitary operation

$$U = (U_{q_1 p_1} \otimes \cdots \otimes U_{q_L p_L} \otimes \mathbb{1}) V \tag{5.22}$$

with

$$V = \sum_{k \in \mathbb{Z}_d^m} |k_1\rangle \cdots |k_m\rangle \langle \phi(k)| , \tag{5.23}$$

to their system. This changes the state to

$$U\left|\Phi_S\right\rangle = \frac{1}{\sqrt{d^{m-L}}} \sum_{(k_{L+1},\ldots,k_m)\in\mathbb{Z}_d^{m-L}} \left|k_{L+1}\right\rangle_{B_1} \cdots \left|k_m\right\rangle_{B_{m-L}} \left|s\right\rangle_{A'} \left|k_{L+1}\right\rangle_{A_{L+1}} \cdots \left|k_m\right\rangle_{A_m} \tag{5.24}$$

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.

□

5.5 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 the previous chapter, 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 [144], 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 ancilla 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 $P\backslash A$ 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

$$|S\rangle |\Phi\rangle \to |\Phi_S\rangle = \frac{1}{\sqrt{d^m}} \sum_{(k,i)\in\mathbb{Z}_d^m} a_{pq,i} |k_1\rangle_{B_1} \cdots |k_{m-1}\rangle_{B_{m-1}} |\phi(k,i)\rangle_A , \tag{5.25}$$

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 (5.23) followed by a Bell measurement on qudits A_i 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 the previous chapter, 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.

Chapter 6

Absolutely Maximally Entangled Qudit Graph States

In this chapter, 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. This chapter is largely based on Ref. [56].

6.1 Introduction

In this chapter, 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 [20, 5]. 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 [105], error correction [113, 49, 82, 8], and quantum secret sharing [88, 69].

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 4.1(v).

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 Section 5.2 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 chapter provides a straightforward way to experimentally create qudit AME states. At this point, graph states have been experimentally created for up to six qubits [133, 84, 24, 40].

Quantum secret sharing (QSS) with qudits has already been investigated before [88, 69]. 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 [30], as well as for QSS schemes with a more general *ramp* access structure [14]. The connection between AME states and threshold QSS schemes has already been shown in the previous chapters, 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 Section 5.3 further show that AME graph states are the only graph states that result in threshold QSS schemes.

This chapter is structured as follows. In Section 6.2 we introduce qudit graph states and their representation as stabilizer states. In Section 6.3 we show two different methods for checking the bipartite entanglement in graph states. Section 6.4 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 6.5 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 6.6.

Notation: Throughout this chapter, 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.

6.2 Qudit Graph States

6.2.1 Generalized Pauli Operators

The generalized Pauli operators [101, 46, 7, 69] for qudits of dimension d are defined as

$$Z\left|k\right\rangle = \omega^k \left|k\right\rangle, \tag{6.1}$$

$$X\left|k\right\rangle = \left|k+1\right\rangle, \tag{6.2}$$

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

$$\mathsf{CZ}_{ij} = \sum_{k=0}^{d-1} \left|k\right\rangle\left\langle k\right|_i \otimes Z_j^k = \sum_{k,l=0}^{d-1} \omega^{kl} \left|k\right\rangle\left\langle k\right|_i \otimes \left|l\right\rangle\left\langle l\right|_j \tag{6.3}$$

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

$$F = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{kl} \left|k\right\rangle\left\langle l\right|, \tag{6.4}$$

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

$$\left|\bar{k}\right\rangle = F^\dagger \left|k\right\rangle = \frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} \omega^{-kl} \left|l\right\rangle. \tag{6.5}$$

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* $\mathcal{V} = \{v_i\}$, which are connected by *edges* $\mathcal{E} = \{e_{ij} = \{v_i, v_j\}\}$. 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 6.1. 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 $|G\rangle \in \mathcal{H}^{\otimes n}$, $\mathcal{H} \cong \mathbb{C}^p$ as

$$\left|G\right\rangle = \prod_{i>j} \mathsf{CZ}_{ij}^{A_{ij}} \left|\bar{0}\right\rangle^{\otimes n}. \tag{6.6}$$

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

$$|G_{\mathbf{z}}\rangle = Z^{\mathbf{z}} |G\rangle , \tag{6.7}$$

Here and in the following we use the notation

$$Z^{\mathbf{z}} = Z^{z_1} \otimes Z^{z_2} \otimes \cdots \otimes Z^{z_n}. \tag{6.8}$$

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.

6.2.3 Stabilizer States

Stabilizer states have first been introduced for qubits [44] and later generalized to qudits [4, 70]. The connection to qudit graph states has been made in Ref. [113, 5]. The *Pauli Group*, the group that is generated by the X and Z operators for qubits is defined as

$$\mathcal{G} = \{\alpha X^a Z^b; a, b \in \mathbb{Z}_2\}, \tag{6.9}$$

with $\alpha \in \{1, -1, i, -i\}$, and its generalization for the qudit Pauli operators of Equations (6.1) and (6.2) is

$$\mathcal{G} = \{\omega^c X^a Z^b; a, b, c \in \mathbb{Z}_p\}, \tag{6.10}$$

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

The *stabilizer code* is defined as the common eigenspace for eigenvalue one of a subgroup S of $\mathcal{G}_n$. The stabilizer code is non-trivial if S is abelian and does not contain any scalar multiples of the identity, except for $\mathbb{1}$ itself [70, 5]. Given such a subgroup and a minimal set of generators, $g_i = \omega^{c_i} X^{\mathbf{a_i}} Z^{\mathbf{b_i}}$, for the group, $S = \langle g_1, \ldots, g_k \rangle$, the *generator matrix* is defined as

$$M = \left(\begin{array}{c|c} \mathbf{a_1} & \mathbf{b_1} \\ \vdots & \vdots \\ \mathbf{a_k} & \mathbf{b_k} \end{array} \right). \tag{6.11}$$

The stabilizer code does not depend on the scalar coefficients ω^{c_i}, and is thus fully specified by the generator matrix M. The fact that S is abelian translates to $\mathbf{a_i} \cdot \mathbf{b_j} - \mathbf{b_i} \cdot \mathbf{a_j} = 0$ for two different rows of M. It has been shown in Ref. [5] 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

$$g_i = X_i \prod_j Z_j^{A_{ij}}. \tag{6.12}$$

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

$$M = (\mathbb{1}|A) \tag{6.13}$$

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. [63]). 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. [5].

Lemma 6.2 (Lemma 6 of Ref. [5])**.** *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*

$$Y = \begin{pmatrix} E & F \\ E' & F' \end{pmatrix}, \tag{6.14}$$

where

$$E = \mathrm{diag}(e_1, \ldots, e_n), \qquad F = \mathrm{diag}(f_1, \ldots, f_n) \tag{6.15}$$

$$E' = \mathrm{diag}(e'_1, \ldots, e'_n), \qquad F' = \mathrm{diag}(f'_1, \ldots, f'_n), \tag{6.16}$$

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 [5, 113, 49]. 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.

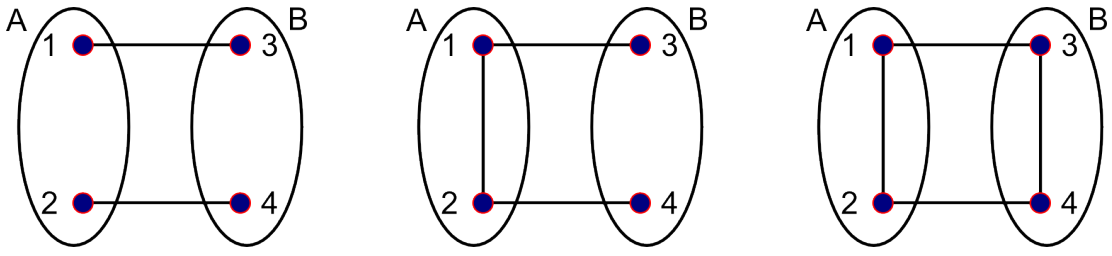
6.3 Entanglement in Graph States

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.

6.3.1 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 $|\bar{0}\rangle$ 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 $|\bar{0}\rangle$ 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 6.1(a).



(a) (b) (c)

Figure 6.1: 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.

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 6.1(b) and 6.1(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 6.1(a), 6.1(b), and 6.1(c), respectively. However, the entanglement for a different bipartition, for example between $C = \{1, 4\}$ and $D = \{2, 3\}$ in the graph of Figure 6.1(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 6.2. For graph states this lemma can be restated as operations on the graph [5]

Theorem 6.3 (Theorem 5 of Ref. [5])). *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*

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

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

A graphical representation of these operations, is given in Figures 1 and 2 of Ref. [5]. For qubits the $\circ$ operation is always the identity, and the $*$ 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 6.1(c), we can see that by applying the operations $(*_1 1,\ *_1 3,\ *_1 4)$, the graph is in fact local Clifford equivalent to the graph of Figure 6.1(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 6.4.

6.3.2 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 6.4. 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 6.5. For an $n \times n$ adjacency matrix A, we denote the ith row of the matrix by A_i, so $A_i = (A_{i1}, \dots A_{in})$. Further for $K = \{k_1, k_2, \dots, k_m\}$, with $k_1, \dots, k_m$ between 1 and n, we define $A_i\backslash K$ to be the vector A_i with the entries $\{A_{ik_1}, \dots, A_{ik_m}\}$ removed. For instance,

$$A_i\backslash\{2,6\} = (A_{i1}, A_{i3}, A_{i4}, A_{i5}, A_{i7}, \dots, A_{in}). \tag{6.17}$$

First note that a Z-measurement[1] on the kth qudit of the graph

$$|G\rangle = \prod_{i>j} \mathsf{CZ}_{ij}^{A_{ij}} |\bar{0}\rangle^{\otimes n} \tag{6.18}$$

$$= \prod_{l\neq k} \sum_{m=0}^{p-1} |m\rangle\langle m|_k \otimes Z_l^{mA_{kl}} \prod_{\substack{i>j \\ i,j\neq k}} \mathsf{CZ}_{ij}^{A_{ij}} |\bar{0}\rangle^{\otimes n}, \tag{6.19}$$

with measurement outcome a gives

$${}_k\langle a|G\rangle = \frac{1}{\sqrt{p}} \prod_{l\neq k} Z_l^{aA_{kl}} \prod_{\substack{i>j \\ i,j\neq k}} \mathsf{CZ}_{ij}^{A_{ij}} |\bar{0}\rangle^{\otimes n-1} \tag{6.20}$$

$$= \frac{1}{\sqrt{p}} |G^{\backslash\{k\}}_{aA_k\backslash\{k\}}\rangle . \tag{6.21}$$

So this is a labeled graph state for the remaining $n-1$ qudits, with the label given by $A_k\backslash\{k\}$ with each componenet multiplied by the measurement outcome a. All measurement outcomes are equally likely, and given that $A_k\backslash\{k\} \neq 0$, meaning that the kth qudit in $|G\rangle$ is connected by at least one edge, the label is different for each possible

[1] Z is not technically an oberservable, what we mean by a Z-measurement is a projection onto the eigenstates with (complex) eigenvalues ω^k. For simplicity we then call the measurement result k.

measurement outcome. Since labeled graph states with different labels are orthogonal, the measurement outcome can be deduced from $|G^{\setminus\{k\}}_{aA_k\setminus\{k\}}\rangle$. 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

$$_{k_1,\ldots,k_m}\langle a_1, \ldots, a_m|G\rangle = \frac{1}{\sqrt{p^m}} |G^{\setminus K}_{\sum_i^k a_i B_{k_i}\setminus K}\rangle \,. \tag{6.22}$$

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:

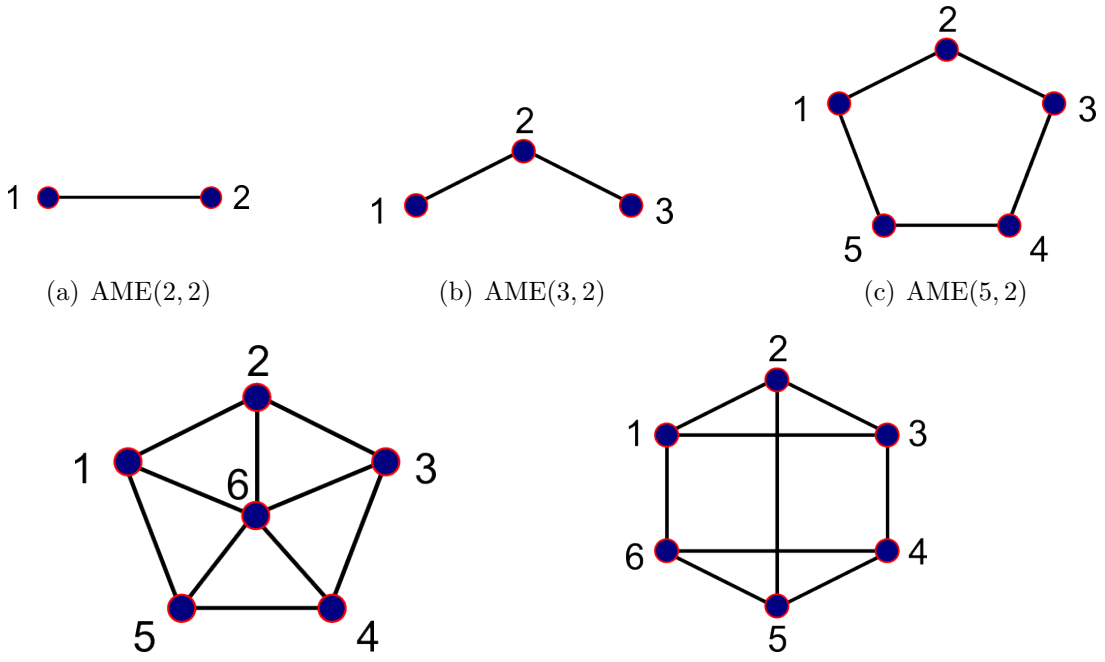
Theorem 6.6. *A graph state with adjacency matrix A is absolutely maximally entangled, if and only if for all sets $K = \{k_1, \ldots, k_m\}$ of size $m = \lfloor \frac{n}{2} \rfloor$, the vectors $A_{k_i}\setminus K$ are linearly independent in $\mathbb{Z}_p^{n-m}$. Here $A_{k_i}\setminus K$ denotes the k_i*th *row of the adjacency matrix with the entries $\{A_{k_ik_1}, \ldots, A_{k_ik_m}\}$ removed.*

As a concrete example, we take a look at the graph of Figure 6.1(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 $A_1\setminus\{1, 2\} = (1, 0)$ and $A_2\setminus\{1, 2\} = (0, 1)$. 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 maximally entanglement there. However, for the bipartition into $C = \{1, 4\}$ and $D = \{2, 3\}$, we get the vectors $A_1\setminus\{1, 4\} = (1, 1)$ and $A_4\setminus\{1, 4\} = (1, 1)$. 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.

6.4 Absolutely Maximally Entangled Graph States

6.4.1 Qubits, Qutrits, and Beyond

Recall 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 6.2. 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 6.2(c) and 6.2(d) for five and six qubits can be used for quantum secret sharing protocols [88], as will also be discussed in the next section. We also included a second graph for six qubits in Figure 6.2(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 $*_1 v$ operation) to the one in Figure 6.2(d).

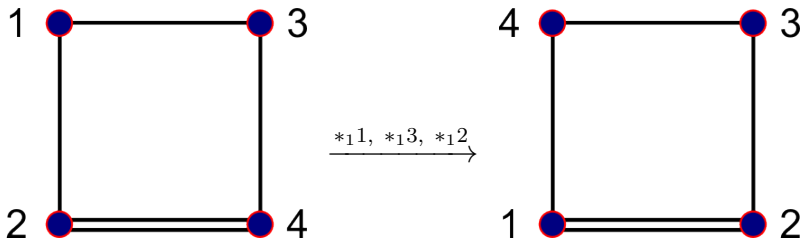


(a) AME(2, 2) (b) AME(3, 2) (c) AME(5, 2)

(d) AME(6, 2) (e) AME(6, 2)

Figure 6.2: 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 6.2(d) emphasizes the connection to the five qubit state, while the locally equivalent state of Figure 6.2(e) nicely demonstrates the maximal entanglement.

For four and more than eight qubits no AME states exists. For seven qubits no AME states are known, and and 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.



(a) AME(4, 3) (b) AME(4, 3)

Figure 6.3: 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 $\{1,4\}/\{2,3\}$.

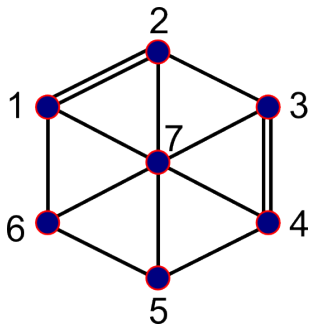


Figure 6.4: AME(7, 3) graph state. The use of double edges allows us to find an AME graph state for seven qutrits, while no such graph state exists for qubits.

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 6.1(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 6.3(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 $(*_1 1,\ *_1 3,\ *_1 2)$ to obtain the graph shown in Figure 6.3(b), from which we see that the C/D bipartition is also maximally entangled. Likewise, we could have considered the two vectors $A_1\backslash\{1,4\} = (1,1)$ and $A_4\backslash\{1,4\} = (2,1)$, to see that 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 6.3.2 for checking bipartite entanglement in graph states allowed us to find an AME$(7,3)$ graph state. It is displayed in Figure 6.4.

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 often works for more than one dimension. For instance the qubit graph states of Figure 6.2 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 6.3(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 6.5, 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 $\mathbb{Z}_7^2$.

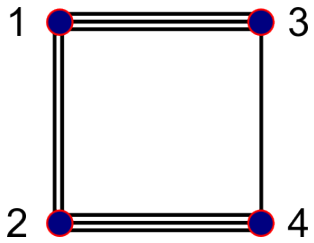


Figure 6.5: An AME state for one dimension is not neccessarily a graph state for a higher dimension. For instance, this graph states is absolutely maximally entangled for four qudits of dimension 5, but not for qudits of dimension 7.

6.4.2 AME Graph States from Classical Codes

By now we have seen AME graph states for system with up to seven parties. In Section 5.2, we showed 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 $\mathcal{C}$, which encodes k *dits* of information into n dits, is described by a *generator matrix* $G : \mathbb{Z}_p^k \to \mathbb{Z}_p^n$ such that the codewords $c \in \mathcal{C}$ are given by $G\mathbf{x}$ for $\mathbf{x} \in \mathbb{Z}_p^k$. An equivalent description of a linear code as the kernel of the *parity check* matrix H. For every linear code $\mathcal{C}$ one can define a parity check matrix $H : \mathbb{Z}_p^n \to \mathbb{Z}_p^{n-k}$ such that $c \in \mathcal{C}$ if and only if $Hc = 0$. From $HGx = 0$, it follows that the rows of H are orthogonal to the columns of G.

Recall that the *Hamming distance* between two codewords is defined as the number of positions at which the codewords differ. The *minimal distance* δ of a code is the minimum Hamming distance between any two codewords. The larger δ, the more robust the encoding is against errors. The minimal distance is bounded by the Singleton bound, $\delta \leq n - k + 1$ [120, 86]. 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 (see Theorem 5.1(a), Equation (5.2))

$$|AME\rangle = \frac{1}{\sqrt{d^k}} \sum_{\mathbf{x} \in \mathbb{Z}_p^k} |G\mathbf{x}\rangle \,. \tag{6.23}$$

Note that

$$\begin{aligned} X^{G\mathbf{y}} |AME\rangle &= \frac{1}{\sqrt{d^k}} \sum_{\mathbf{x} \in \mathbb{Z}_p^k} |G\mathbf{x} + G\mathbf{y}\rangle & (6.24)\\ &= \frac{1}{\sqrt{d^k}} \sum_{\mathbf{x} \in \mathbb{Z}_p^k} |G\mathbf{x}\rangle & (6.25)\\ &= |AME\rangle \,, & (6.26) \end{aligned}$$

where we have used that $\mathcal{C}$ 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 $X^{G\mathbf{y}}$ is a stabilizer to the AME state for all $\mathbf{y} \in \mathbb{Z}_p^k$. 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

$$Z^{\mathbf{y}} |AME\rangle = \frac{1}{\sqrt{d^k}} \sum_{\mathbf{x} \in \mathbb{Z}_p^k} \omega^{\mathbf{y}^T G\mathbf{x}} |G\mathbf{x}\rangle \,. \tag{6.27}$$

Thus $Z^{\mathbf{y}}$ is a stabilizer for the AME state if $\mathbf{y}$ is a linear combination of rows of the parity

check matrix H, $\mathbf{y}^T = \mathbf{z}^T H$. This gives us a full set of stabilizers that we can describe by the generator matrix

$$M = \left(\begin{array}{c|c} G^T & 0 \\ 0 & H \end{array}\right). \tag{6.28}$$

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 $\mathbf{a_i} \cdot \mathbf{b_j} - \mathbf{b_i} \cdot \mathbf{a_j} = 0$ 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 6.2 [5].

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 6.7. The generator matrix for the $[4, 2, 3]_3$ ternary Hamming code $\mathcal{C}$ is given by

$$G = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 2 & 1 \end{pmatrix}, \tag{6.29}$$

and the parity check matrix by $H = G^T$ ($\mathcal{C}$ is a self-dual code). Thus the generator matrix for the AME state $|AME\rangle = \frac{1}{3}\sum_{c\in\mathcal{C}} |c\rangle$ is

$$M = \left(\begin{array}{cccc|cccc} 1 & 0 & 1 & 2 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{array}\right) \tag{6.30}$$

Now we have to choose the matrices U and Y of Lemma 6.2 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 ith column of the second block to the ith 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

$$M \to MY = \left(\begin{array}{cccc|cccc} 1 & 0 & 1 & 2 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 2 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \end{array}\right). \tag{6.31}$$

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

$$U = \begin{pmatrix} 1 & 0 & 2 & 0 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 2 & 2 \\ 0 & 0 & 1 & 2 \end{pmatrix}, \tag{6.32}$$

which results in the generator matrix

$$M \to UMY = \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 2 & 0 & 2 & 1 \\ 0 & 1 & 0 & 0 & 0 & 2 & 2 & 2 \\ 0 & 0 & 1 & 0 & 2 & 2 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 2 & 0 & 1 \end{array}\right). \tag{6.33}$$

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 $e_i' = 0$, $e_i = f_i' = 0$, and $(e_1, e_2, e_3, e_4) = (1, 1, 2, 2)$. Thus we arrived at the graph state shown in Figure 6.6, which is an absolutely maximally entangled graph state for four qutrits.

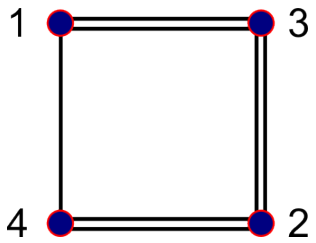


Figure 6.6: AME$(4, 3)$ graph state constructed from the $[4, 2, 3]_3$ ternary Hamming code

Notice that the procedure of constructing a stabilizer state from classical codes is reminiscent of the construction of Calderbank-Shor-Steane (CSS) codes [23, 123]. In fact we may interpret the AME states that are constructed in this form as one-dimensional generalized CSS codes $\mathrm{CSS}_p(\mathcal{C}, \mathcal{C})$.

6.4.3 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 $|\bar{0}\rangle$ 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 6.3. 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 6.3(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 the each 4-dimensional systems as consisting of two qubits and construct the graph state shown in Figure 6.7 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).

6.5 Quantum Secret Sharing

As was shown in the previous chapters, one application for AME states is to construct quantum secret sharing (QSS) protocols. Furthermore, describing quantum secret sharing protocols with the help of graph states has already been studied for qubit [88] and

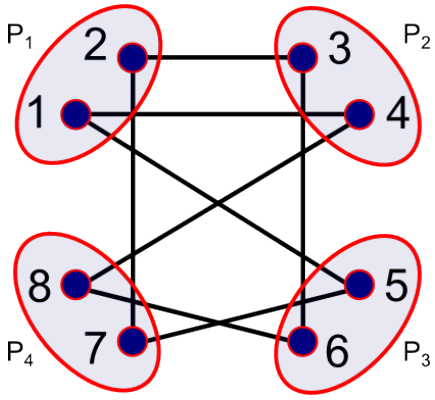


Figure 6.7: By grouping qudits together, we can construct AME graph states for non-prime dimensions. This figure shows eight qudits that are grouped into four 4-dimensional systems to form an AME$(4,4)$ graph state. This, however, is not an AME$(8,2)$ state if each qudit is regarded as a single party.

qudit graph states of prime dimension [69]. In these papers it was shown that threshold quantum secret sharing schemes can be constructed from the graph state shown in Figure 6.2(d) for 6 qudits of arbitrary prime dimension, and for the graph state shown in Figure 6.3(a) for four qudits of prime dimension $p \geq 3$. However, the question which graph states are generally suitable for quantum secret sharing remained an open question, which we will answer in this section.

6.5.1 Threshold QSS Schemes

In Chapters 4 and 5, we have already shown that there exists a one-to-one correspondence between pure state $((m, 2m-1))$ threshold QSS schemes and AME$(2m,d)$ states. 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$(2m,p)$ graph state $|G\rangle$, the role of the *dealer* D is assigned to one of the $2m$ 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 $2m-1$ players. He does that by performing a generalized Bell measurement, which is a projective measurement onto the basis

$$|\Psi_{gh}\rangle = \frac{1}{\sqrt{p}} \sum_j e^{2\pi i j g/p} |j\rangle |j+h\rangle , \tag{6.34}$$

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

$$|\Phi_S\rangle = \sum_{i=0}^{p-1} \beta_i \, |G^{\backslash D}_{iA_D\backslash\{D\}}\rangle \,, \tag{6.35}$$

where $\beta_i = \langle i|U^\dagger_{gh}|s\rangle$, with

$$U_{gh} = \sum_j e^{2\pi ijg/p} \, |j\rangle \langle j+h| \,, \tag{6.36}$$

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 $m-1$ parties $K = P\backslash B = \{k_1, \ldots, k_{m-1}\}$ gives

$$\begin{aligned}
\rho &= \mathrm{Tr}_K \, |\Phi_S\rangle \langle\Phi_S| && (6.37)\\
&= \sum_{i,j} \sum_{\mathbf{a}\in\mathbb{Z}_p^{m-1}} \beta_i \beta^*_j \, {}_{D,K}\langle i, a_1, \ldots, a_{m-1}|G\rangle \, \langle G|j, a_1, \ldots, a_{m-1}\rangle_{D,K} && (6.38)\\
&= \sum_{i,j} \sum_{\mathbf{a}\in\mathbb{Z}_p^{m-1}} \beta_i \beta^* \, |G^{\backslash\{D,K\}}_{iA_D+\sum_l a_l A_{k_l}\backslash\{D,K\}}\rangle \, \langle G^{\backslash\{D,K\}}_{jA_D+\sum_l a_l A_{k_l}\backslash\{D,K\}}| \,. && (6.39)
\end{aligned}$$

Since the vectors $\{A_D\backslash\{D,K\}, A_{k_1}\backslash\{D,K\}, \ldots, A_{k_{m-1}}\backslash\{D,K\}\}$ are linearly independent,

$$V : |G^{\backslash\{D,K\}}_{iA_D+\sum_l a_l A_{k_l}\backslash\{D,K\}}\rangle \to |i, a_1, \ldots, a_{m-1}\rangle \tag{6.40}$$

is a unitary operation on the qudits shared by the players in B. Applying it to ρ gives

$$V\rho V^\dagger = |s'\rangle \langle s'| \otimes \sum_{\mathbf{a}} |a_1, \ldots, a_{m-1}\rangle \langle a_1, \ldots, a_{m-1}| \,, \tag{6.41}$$

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.

6.5.2 Ramp QSS Schemes

A generalization of threshold secret sharing schemes are (m, L, n) *ramp secret sharing schemes* [14]. 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.

In Section 5.4, we showed 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 an 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

$$|\Phi_S\rangle = \sum_{i_1,\ldots,i_L} \alpha_{1,i_1} \cdots \alpha_{L,i_L} |G^{\setminus D}_{\sum_m i_m A_{d_m} \setminus D}\rangle . \tag{6.42}$$

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

$$\begin{aligned} \rho &= \mathrm{Tr}_K |\Phi_S\rangle \langle\Phi_S| && (6.43)\\ &= \sum_{\substack{i_1,\ldots,i_L \\ j_1,\ldots,j_L}} \sum_{\mathbf{a} \in \mathbb{Z}_p^{m-L}} \alpha_{1,i_1} \cdots \alpha_{L,i_L} \alpha^*_{1,j_1} \cdots \alpha^*_{L,j_L} && (6.44)\\ &\quad |G^{\setminus\{D,K\}}_{\sum_m i_m A_{d_m} + \sum_l a_l A_{k_l} \setminus \{D,K\}}\rangle \langle G^{\setminus\{D,K\}}_{\sum_m j_m A_{d_m} + \sum_l a_l A_{k_l} \setminus \{D,K\}}| . && (6.45) \end{aligned}$$

And applying V recovers the secrets:

$$V \rho V^\dagger = |s_1\rangle \langle s_1| \otimes \cdots \otimes |s_L\rangle \langle s_L| \otimes \sum_{\mathbf{a}} |a_1, \ldots, a_{m-L}\rangle \langle a_1, \ldots, a_{m-L}| \tag{6.46}$$

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 why 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 Section 5.4.

6.6 Conclusion and Open Questions

In this chapter, we have shown how the graph state formalism can be used to describe absolutely maximally entangled states. 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 [88, 69], but only two examples for threshold QSS schemes for 4 and 6 qudits, corresponding to the graph states in Figures 6.3 and 6.2(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.

Chapter 7

Entanglement in Quantum Error Correction Codes

7.1 Introduction

In the previous chapters, we investigated highly entangled multipartite states, the absolutely maximally entangled states and discovered a close relationship to quantum secret sharing protocols, in particular pure state threshold QSS schemes. A $((m, 2m-1))$ threshold QSS scheme is equivalent to a code for the quantum erasure channel (QEC) that can correct $m-1$ erasures, where the positions of the erasures are known [48, 30, 45]. This is easily seen since a $((m, 2m-1))$ threshold QSS scheme can recover the states if any $m-1$ qudits are missing, i.e., if $m-1$ known qudits are erased. The other way around, the encoded state can be recovered by any set with at least m parties because then we have at most $m-1$ erased qudits. Security then follows from the no-cloning theorem, which ensures that any set with $m-1$ or less parties has no information at all. Thus a $((m, 2m-1))$ threshold QSS scheme is equivalent to a code that corrects $m-1$ erasure, which in turn is equivalent to a $((2m-1, d, m))_d$ quantum error correction code [48].

Similarly, we can argue that a $(m, L, 2m-L)$ ramp QSS scheme is equivalent to a code that corrects $m-L$ erasures, which is a $((2m-L, d^L, m-L+1))_d$ QECC. Both allow to recover the encoded state when at most $m-L$ qudits are lost, the no-cloning theorem forbids players that hold m or less qudits to gain any information, and partial information is available for any other sets as per the same argument used in the proof for Theorem 5.5.

So we know that from an AME$(2m, d)$ state, we can construct $((2m-L, d^L, m-L+1))_d$

QECCs for $1 \leq L \leq m$, but for the opposite direction, we only know that going from a $((2m-L, d^L, m-L+1))_d$ QECC to an AME$(2m, d)$ state works for the case where the QECC corresponds to a threshold QSS scheme, i.e., for $L = 1$. So the question arises if there exists a similar equivalence between QECCs and AME states for the cases where $L \neq 1$, and if not, what other conclusions can be drawn about the entanglement in these QECCs. This question is answered in this chapter by deriving the necessary and sufficient entanglement conditions for such codes.

First, we will generalize the equivalence statement of Theorem 5.3 for AME states and threshold QSS schemes to give necessary and sufficient conditions for the entanglement required to construct $(m, L, 2m-L)$ ramp QSS schemes. Due to the equivalence of the ramp QSS schemes and $((2m-L, d^L, m-L+1))_d$ QECCs, we can then quickly follow that the same entanglement conditions must hold for these codes. We will consider the case where the involved states are graph states, and the codes are graph codes. We will establish a connection to stabilizer codes and derive existence conditions for certain stabilizer codes based on the existence of an associated graph state. Finally, some more discussion and examples will be provided.

7.2 Entanglement in Ramp Secret Sharing Schemes

We start by generalizing the methods used in Section 5.3 that were used to prove the equivalence of AME states and QSS schemes in Theorem 5.3 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,

$$U_S : \mathcal{H}_S \to \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_{2m-L}, \tag{7.1}$$

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 $|RS\rangle = 1/\sqrt{d}\sum_i |i\rangle|i\rangle \in \mathcal{H}_R \otimes \mathcal{H}_S$, i.e., $|\Phi\rangle = \mathbb{1}_R \otimes U_S |RS\rangle$. A set of players $A \subset P$ shares the state $\rho_{RA} = \mathrm{Tr}_{P\setminus A}|\Phi\rangle$ with the reference system. A is authorized, if there exists a completely positive map $T_A : \mathcal{H}_A \to \mathcal{H}_S$ such that [67, 116]

$$\mathbb{1}_R \otimes T_A(\rho_{RA}) = |RS\rangle\,. \tag{7.2}$$

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

$$I(R:A) = I(R:S) = 2S(S) \quad \text{if } |A| \geq m, \tag{7.3}$$

and for a forbidden set, we must have

$$I(R:B) = 0 \quad \text{if } |B| \leq m - L. \tag{7.4}$$

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

Since any set of players $C \subset P$ with $|C| = L$ can change some forbidden set into an authorized set, we have $S(C) \geq S(S)$ [67] for all sets with L players. And because $S(S)$ is maximal and equal to $S(R)$,

$$S(S) = S(R) = S(C) = L \log d. \tag{7.5}$$

Equations (7.3) and (7.4) can be rewritten to give

$$S(R, A) = S(A) - S(R) \quad \text{if } |A| \geq m \tag{7.6}$$

$$S(R, B) = S(B) + S(R) \quad \text{if } |B| \leq m - L. \tag{7.7}$$

This sums up the changes in the lead-up to Theorem 5.3 in Section 5.3, 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 7.1. *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.

Proof. $(i) \to (ii)$: 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 (7.3) and (7.4) while using the definition of the mutual information (Equation 5.8), 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 (7.6) we have

$$S(B, C, R) = S(B, C) - S(R) \tag{7.8}$$

On the other hand, using the Araki-Lieb inequality [96] $S(X, Y) \geq S(X) - S(Y)$ and Equation (7.7) gives

$$S(B, C, R) \geq S(B, R) - S(C) = S(B) + S(R) - S(C). \tag{7.9}$$

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

$$S(B, C) \geq S(B) + S(C), \tag{7.10}$$

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 [96]

$$S(X, Y) - S(Y) \geq S(X, Y, Z) - S(Y, Z) \tag{7.11}$$

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 $P \backslash A \cup R$, which contains all L reference qudits, and thus is maximally entangled for any bipartition where all reference qudits are in the same set. □

Note that AME states are special states that fulfill the requirement, as they exceed the requirement. They possess more entanglement than minimally required for $L > 1$.

Furthermore, also the protocol presented in the proof of Theorem 5.5 works for states that are maximally entangled for any bipartition with the reference qudits in one set. It only uses the maximal entanglement for such bipartitions where all dealers are in the same set.

7.3 Entanglement in Quantum MDS Codes

For QECCs, a quantum analogue to the classical Singleton bound that gives an upper bound on the number of encoded qudits exists [103]:

Theorem 7.2 (Quantum Singleton Bound)**.** *For a $((n, K, \delta))_d$ QECC, the amount of encoded information K is restricted by*

$$K \leq d^{n-2\delta+2}. \tag{7.12}$$

As in the classical case, we call codes that saturate this bound *quantum MDS codes*. A comparison with the $((2m - L, d^L, m - L + 1))_d$ codes mentioned in the introduction that are equivalent to $(m, L, 2m-L)$ ramp QSS schemes shows that these are exactly the codes that saturate the Singleton bound. Thus we have an equivalence between quantum MDS codes and pure state ramp QSS schemes, and Theorem 7.1 can be restated to give the entanglement in quantum MDS codes.

Theorem 7.3. *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 $((2m - L, d^L, m - L + 1))_d$ QECC.

Corollary 7.4. *A d^L dimensional state encoded with a $((2m - L, d^L, m - L + 1))_d$ MDS QECC into $2m - L$ qudits is maximally entangled for any bipartition of the qudits into sets A and B with $|A| \geq m$.*

7.4 Graph Codes

Graphs are a very powerful tool to construct quantum error correction codes. A lot of good quantum codes, in particular any stabilizer code, can be described in terms of graphs. To understand how graph codes work, let us recall the definition of labeled graph

states, Definition 6.1. Given a graph state $|G\rangle$ over n qudits of dimension p, a labeled graph state $|G_{\mathbf{z}}\rangle$ with $\mathbf{z} = (z_1, \ldots, z_n) \in \mathbb{Z}_p^n$ is defined as

$$|G_{\mathbf{z}}\rangle = Z^{\mathbf{z}} |G\rangle . \tag{7.13}$$

Labeled graph states with different labels are orthogonal and thus the collection of all labeled graph states for any graph $|G\rangle$ form a Hilbert space basis.

A quantum code is defined by a mapping $U : \mathcal{H}_s \to \mathcal{H}_e$ of a D-dimensional Hilbert space $\mathcal{H}_s$ into a D-dimensional subspace of a larger Hilbert space $\mathcal{H}_e$. If $\mathcal{H}_e$ is the space of n qudits of dimension p, i.e., $\mathcal{H}_e$ has dimension $p^n > D$, we can define a quantum code via a mapping from the D basis states in $\mathcal{H}_s$ to D different labeled graph states. This mapping, described by a classical code $\mathcal{C}$, together with the graph $|G\rangle$ defines a *quantum code*.

Definition 7.5. Given a classical code $\mathcal{C} : \mathbb{Z}_D \to \mathbb{Z}_p^n$ and a graph state $|G\rangle \in \mathcal{H}^{\otimes n}$, where $\mathcal{H} \cong \mathbb{C}^p$, a $((n, D, \delta))_p$ graph code is defined by the encoding

$$U |i\rangle = |G_{\mathcal{C}(i)}\rangle . \tag{7.14}$$

The distance δ of the code is defined as the smallest value for which an operator Q exists that acts on δ qudits non-trivially and violates the Knill-Laflamme condition [72] $\langle G_{\mathcal{C}(i)}|Q|G_{\mathcal{C}(j)}\rangle = f(Q)\delta_{ij}$ (see Section 2.3.3 and Refs. [72, 44, 96, 82]). The graph code is fully described by specifying the graph $|G\rangle$ and the classical code $\mathcal{C}$. Thus we denote such a graph code by $\mathcal{Q} = (G, \mathcal{C})$.

If the classical code $\mathcal{C}$ is a linear code, then the graph code is a stabilizer code [82]. Moreover, any stabilizer code is local Clifford equivalent to such a graph code [113, 49]. Furthermore, for graph codes of that form, we can find purifications that are graph states.

Lemma 7.6. *For a $((n, p^k, \delta))_p$ graph code $\mathcal{Q} = (G, \mathcal{C})$, where $\mathcal{C}$ is a linear code, described by a generator matrix $M : \mathbb{Z}_p^k \to \mathbb{Z}_p^n$, there exists a purification of the code that is a graph state, $|\mathcal{G}\rangle$, described by the adjacency matrix*

$$B = \left(\begin{array}{c|c} A & M \\ M^T & 0 \end{array} \right), \tag{7.15}$$

where A is the adjacency matrix of the graph $|G\rangle$.

Proof. The codespace of the graph code is $\mathcal{Q} = (G, \mathcal{C})$ is spanned by the p^k graph states

$|G_{M\mathbf{a}}\rangle$, with $a \in \mathbb{Z}_p^k$. [1] Hence

Performing a Z-measurement on the k qudits of the reference system R of the purification, i.e., the last k qudits of the graph state $|\mathcal{G}\rangle$, with measurement outcomes $\mathbf{a} = (a_1, \ldots, a_k)$ results in the labeled graph state state (see Section 6.3.2)

$$ {}_R\langle a_1, \ldots, a_k|G\rangle = \frac{1}{\sqrt{p^k}} |\mathcal{G}^{\setminus R}_{\sum_{i=1}^k a_i B_{n+i} \setminus R}\rangle = \frac{1}{\sqrt{p^k}} |G_{\sum_{i=1}^k a_i M_i^T}\rangle , \tag{7.16}$$

where M_i^T is the ith row of the transpose of the generator matrix, M^T. For an explanation of the notation, see Definitions 6.4 and 6.5. Hence

$$|\mathcal{G}\rangle = \frac{1}{\sqrt{p^k}} \sum_{a \in \mathbb{Z}_p^k} |a_1, \ldots, a_k\rangle \, |G_{\sum_{i=1}^k a_i M_i^T}\rangle \tag{7.17}$$

$$= \frac{1}{\sqrt{p^k}} \sum_{a \in \mathbb{Z}_p^k} |\mathbf{a}\rangle \, |G_{M\mathbf{a}}\rangle , \tag{7.18}$$

which shows that $|\mathcal{G}\rangle$ is a purification of the graph code $\mathcal{Q} = (G, \mathcal{C})$. □

We can now restate Theorem 7.3 for graph codes, which have the huge advantage that the entanglement of in graph codes can easily be checked with the methods derived in Section 6.3.

Theorem 7.7. *The graph state $|G\rangle$ of a $((2m-L, d^L, m-L+1))_p$ graph code $\mathcal{Q} = (G, \mathcal{C})$, i.e., a graph code that satisfies the quantum Singleton bound, is maximally entangled for any bipartition into sets A and B if $|A| \geq m$.*

Proof. This follows directly from Corollary 7.4 □

The observations that graph codes with linear classical codes are equivalent to stabilizer codes and that purifications can be found that are graph states can be combined in the following theorem

Theorem 7.8. *A $[[n, k, \delta]]_p$ stabilizer code that satisfies the Quantum Singleton bound, $k = n - 2\delta + 2$, exists if and only if there exists a graph state $|G\rangle$ for $n+k$ qudits, divided into two sets P and R with $|P| = n$ and $|R| = k$, that is maximally entangled for all bipartitions where the k qudits in R are in the same set.*

[1] To not clutter up the notation even more, we do not distinguish between row and column vectors in the graph label.

7.5 Further Discussions and Illustrations

A state that is the purification of a $((2m-L, d^L, m-L+1))_d$ QECC also trivially satisfies the entanglement condition that the purification of a $((2m-L', d^{L'}, m-L'+1))_d$ code, with $L' > L$, has to satisfy. Thus, from a $((2m-L, d^L, m-L+1))_d$ QECC we can always construct a $((2m-L', d^{L'}, m-L'+1))_d$ QECC with $L' > L$. The opposite, however, is generally not true, as can be easily seen from qubit examples, for which quantum MDS codes exist for $n = 2m \geq 8$ parties for some parameter sets with $L > 1$ [50], but no AME states with $n \geq 8$ exist, and hence also no quantum MDS codes can exist for $L = 1$ or $L = 0$ with $n = 2m \geq 8$. Note that a $L = 0$ MDS code is equivalent to an AME state, a fact that has been noted before, e.g., in Ref. [102]. Thus these codes are of considerable value, although they only "encode" a 0-dimensional state and one might therefore at first wonder what they are good for.

In the following, we will illustrate our results of this chapter on a graph code for six qutrits.

Example 7.9 (Cycle Graphs)**.** One set of graphs that have been shown to be a good candidate for the construction of graph codes are *cycle graphs* [82], which are graphs where the qudits form a circle that is made of edges with non-zero weight. See Figure 7.1 for an illustration for six qudits.

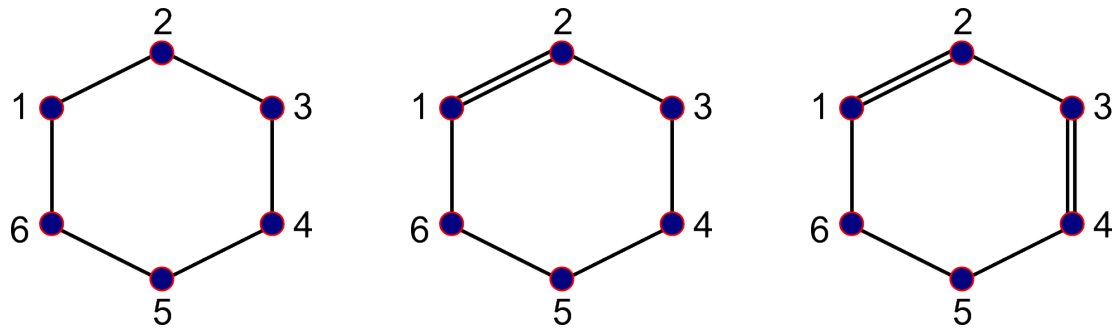


Figure 7.1: Cycle graphs for six qudits. All edges must have non-zero weight. They may all have weight 1 as in Figure (a), but may as well contain edges with a different non-zero weight as in Figures (b) and (c).

It can easily be checked with the methods shown in Section 6.3, that all cycle graph states for n qudits are maximally entangled for any bipartition into sets with 2 and $n-2$ parties, respectively, and are not maximally entangled for bipartitions into two sets that both contain more than two qudits. Hence, we know from Theorem 7.7 that these graph

states can potentially be used to construct MDS graph codes with $\delta \leq 3$, but will never produce MDS graph codes with $\delta > 3$.

One example of where this works successfully is the 5-qubit code, where the cycle graph given in Figure 6.2(c) can be used to construct a $((5, 2, 3))_2$ QECC. MDS graph codes for qutrits with a cycle graph and $\delta = 3$ have been found for up to ten qutrits [82].

In the following, we will provide an example for constructing a $((6, 3^2, 3))_3$ QECC for qutrits from a cycle graph.

Example 7.10. We can try to find a $((6, 3^2, 3))_3$ graph code by attaching two more qutrits to a cycle graph and check if the resulting graph is maximally entangled for all bipartition where the two added qutrits are in the same set. Then, from Theorem 7.8, we know that the graph is equivalent to a $[[6, 2, 3]]_3$ stabilizer code, i.e., a $((6, 3^2, 3))_3$ graph code with a linear classical code.

The number of possible 8 qutrit graph states constructed this way is small enough that we can do an exhaustive computer search. This computer search showed that no graph state with the required entanglement conditions exist based on the graph of Figure 7.1(a), which contains only edges with weight 1. However, using the graph in Figure 7.1(b) proved to be more successful and numerous suitable graphs were found. One of them, with the least number of edges, is depicted in Figure 7.2. This graph state gives a $((6, 3^2, 3))_3$ graph code $\mathcal{Q} = (G, \mathcal{C})$ with the graph G of Figure 7.1(b), and the a linear code $\mathcal{C}$ given by the generator matrix $M : \mathbb{Z}_3^2 \to \mathbb{Z}_3^6$,

$$M = \begin{pmatrix} 1 & 1 \\ 1 & 0 \\ 1 & 1 \\ 0 & 2 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{7.19}$$

We have also done an exhaustive search of all 8 qutrits graph states based on any cycle graph of 6 qutrits to look for an AME$(8, 3)$ state, but no such AME state could be found. Thus, this provides an example where a $((6, 3^2, 3))_3$ code exists from which no $((7, 3^1, 4))_3$ or $((8, 3^0, 5))_3$ code can be constructed.

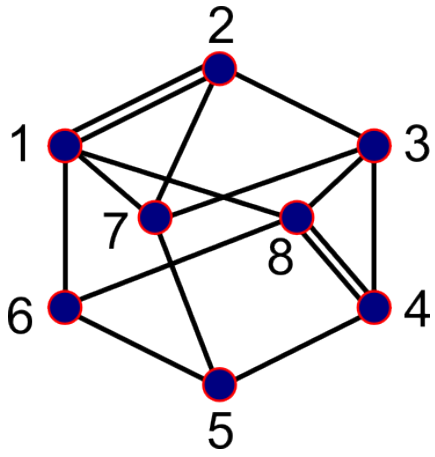


Figure 7.2: Graph state to construct a $((6, 3^2, 3))_3$ graph code. This graph state is maximally entangled for all bipartitions for which qutrits 7 and 8 are in the same set.

7.6 Conclusion

This chapter provided a treatment of codes that correct quantum erasures from an entanglement perspective. The general idea of treating quantum erasures goes back to the parallel teleportation protocol introduced in Section 4.3, which provides us with sufficient entanglement conditions to correct quantum erasures by providing a way to encode a quantum state such that it is robust against losses, if the state used for encoding satisfies the entanglement conditions stated in Theorem 7.3.

To show that these entanglement conditions are also necessary, we first generalized the previously derived results regarding the relationship between AME states and threshold QSS schemes to derive necessary and sufficient condition for $(m, L, 2m - L)$ ramp QSS schemes. Since QSS schemes are fundamentally very similar to codes for the QEC, as erasing qudits belonging to a forbidden set does not prevent us from recovering an encoded state, we were able to use these results to derive equivalent necessary and sufficient entanglement conditions for codes for the QEC, and thus QECCs, that satisfy the quantum Singleton bound.

A popular tool to investigate QECC are graph codes. They consist of a graph state and a classical code, which together fully describe the QECC. The subset of graph codes with a linear classical code coincide with the stabilizer codes. This connection and the previously derived entanglement conditions for quantum MDS codes, allowed us to formulate an existence criterion for MDS stabilizer codes in terms of the existence of highly entangled graph states.

It should be noted, that the occurrence of entanglement in QECCs has been noted before for special cases, in particular, it has been noted before [102], that $((2n, 1, n+1))_d$

QECCs or $[[2n, 0, n+1]]_d$ stabilizer codes, i.e., MDS codes that only contain one state, are absolutely maximally entangled. An example of that actually already occurred in Section 6.4.2, where we saw that the construction of AME states from classical MDS codes is equivalent to the construction of CSS codes that are $[[2n, 0, n+1]]_d$ stabilizer codes. However, a more general analysis of entanglement conditions for QECCs has been missing. Additionally, our treatment of the QEC via the parallel teleportation protocol does not rely on previous results from quantum error correction and should instead be viewed as an alternative approach to the QEC purely based on entanglement.

Chapter 8

Conclusion and Outlook

The goal of this thesis was to broaden our understanding of multipartite entanglement in quantum information processing tasks. First, we investigated transformations among multipartite entangled states, specifically for the transformation from the GHZ state to another multipartite entangled three qubit state of the GHZ class. For this transformation, we derived new upper and lower bounds. The lower bound is derived by giving a specific protocol that provides this transformation probabilities. For a certain class of target states, this protocol can also be extended to higher dimensional GHZ states shared among more parties.

The focus was then shifted to a special kind of multipartite entangled states, which we call absolutely maximally entangled (AME) states. These are pure multipartite states shared among n parties, each with a d-dimensional system, such that for every bipartition of the n parties, the state is maximally entangled. We showed that such states exist for any number of parties, if the system dimensions are chosen appropriately.

We demonstrated how this high degree of entanglement can be used for novel parallel teleportation protocols. A closer look at these parallel teleportation protocols revealed that threshold quantum secret sharing (QSS) schemes follow naturally from AME states. Furthermore, AME states are not only a sufficient, but also a necessary resource for the implementation of pure state threshold QSS schemes. The same idea that was used to construct a threshold QSS scheme, can also be used to produce more general QSS schemes, namely ramp QSS schemes. For these QSS schemes, the necessary entanglement properties of the utilized state can be slightly loosened, and we derived the necessary and sufficient entanglement properties.

Sharing quantum secrets is fundamentally very similar to protecting information against losses, which is generally modeled as a quantum erasure channel (QEC). The ramp QSS schemes we treated refer to codes for the QEC that are optimal in the sense

that they satisfy the quantum Singleton bound. Hence our method, based on the parallel teleportation protocol, also provides an intuitive approach to the protection of quantum information against losses, which is solely based on the entanglement of the state used for encoding the information. Moreover, the entanglement properties are not only sufficient, but also necessary for protection against losses in optimal codes for QECs. Since codes for QEC and quantum error correction codes (QECC) are equivalent, the results also give necessary and sufficient entanglement properties in optimal (i.e., those that satisfy the quantum Singleton bound) QECCs.

A particularly nice framework to describe highly entangled multipartite states is the graph states formalism. We showed how bipartite entanglement can efficiently be checked in graph states, which was then used to find various graph AME states, among them AME graph states for all previously known qubit and qutrit cases, as well as a new AME state for seven qutrits. Existence of AME graph states for any number of parties was shown, and the derivation of threshold and ramp QSS schemes from AME states was formulated entirely within the graph state formalism. The graph state approach to AME states should also prove helpful in future considerations for experimental implementations of AME states, as they are also valuable resources in quantum error correction and quantum computing, which means there is ample interest in progressing their implementation.

8.1 Open Problems

By deriving quantum secret sharing schemes, and thus protocols that protect quantum information against losses, from the parallel teleportation protocol, we were able to develop a very intuitive approach to quantum error correction that solely relies on the entanglement of the involved states.

There are, however, still two missing parts to understand all aspects of quantum error correction from a purely entanglement based point of view. First, at the moment, we can only give necessary and sufficient entanglement conditions for QECCs that satisfy the quantum Singleton bound. Thus, one question is how the generalization of these conditions look like for arbitrary QECCs.

The second open problem is that we, in fact, only derived the construction of codes for the QEC from our entanglement based approach, and then used known results about the equivalence of codes that can correct erasures, and codes that can detect and correct errors [72, 48] to argue that these conditions must hold for QECCs. Thus, it would be desirable to design a method that can also *detect* and then correct errors in the encoded states, by only using the knowledge about the entanglement used to encode the state.

8.1.1 Experimental Prospect

In addition to the theoretical challenges, there is also the task of experimentally realizing AME states to implement the presented protocols. The fundamental building blocks to implement AME states are an appropriate system to represent the qudits, and entangling operations between the qudits. With photonic systems and trapped ions we have already introduced two different approaches of implementing entangled states in Section 2.4.

As discussed in Section 2.4.1, there are various ways to encode quantum information onto photons. Qubits can be encoded onto the polarization degree of freedom, while general qudits can, for instance, be encoded onto the path, time-bin or frequency of the photons, or by creating a hyper-entangled state that is entangled in more than one of these degrees of freedom. The entanglement in experiments with photons is generally created by spontaneous parametric down-conversion (SPDC). This method of creating entangled states is non-deterministic; we have to post-select the final data for those events, where the probabilistic SPDC pair creation was successful and the photons ended up in the desired paths.

For trapped ions, we have only discussed the qubit case in Section 2.4.2, because that is what current experiments focus on. However, there is no fundamental obstacle to using more than one metastable internal state in addition to the ground state, to implement higher dimensional qudits with ions. Also the vibrational mode, which is described by a harmonic oscillator, can contain any number of excitations, and can thus represent any higher dimensional qudit as well. Furthermore, various different entangling operations exist, most notably the Cirac-Zoller and Mølmer-Sørensen gates that have been introduced in Section 2.4.2.

Hence, even though photonic and trapped ion systems are not quite at the technological level where AME states can actually be created, the fundamental building blocks are already available. To give an idea at what stage current experimental implementations are at, we will shortly describe the current technological state of three areas that have been shown in this thesis to be closely related to AME states: graph state generation, quantum error correction and quantum secret sharing. Given the recent efforts to create multipartite entangled states in the laboratory, we might not be too far away from actually implementing AME states other than the EPR and GHZ state. The first candidates for implementation will likely be the AME$(6, 2)$, AME$(4, 3)$ and AME$(4, 4)$ states, whose graph state representations are shown in Figures 6.2, 6.3 and 6.7, respectively.

It should be noted that although we only provide a quick overview of the possibility of experimental implementation with photons and trapped ions, there are also other promising systems that can be used to for implementing quantum information protocols,

like nuclear magnetic resonance (NMR) systems and superconductors. An overview of the currently developed systems, with their advantages and shortcomings, can be found in Ref. [76].

Graph States

Graph states find application in numerous quantum information processing task, most notably in quantum error correction and quantum computing, where it has been shown that cluster states, a special class of graph states, form a universal resource for measurement-based quantum computing (MBQC) [105]. This fact has sparked interest in experimental implementations of graph states, and with recent technological advances ever more sophisticated graph and cluster states have been created.

As mentioned in Section 2.4.1, the maximum number of photons that have been entangled by using networks of SPDC crystals and linear optical elements (beam splitters, phase shifters, etc.) are eight photons, and both of these implementations are indeed graph states. One of the created states was an eight photon GHZ state, which is a graph state [64], and the other one the graph state shown in Figure 8.1, with $N = 8$ [139]. In both experimental setups, four photon pairs were created via SPDC, and then further superposed on polarizing beam splitters to create the desired state. The experiments relied on post-selection, i.e., the states were not created deterministically, but instead, only the data where eight-fold coincidence in the desired paths was registered were kept, while the rest had to be discarded. Both experiments used the polarization of the photons to encode the quantum information. Experiments that use the idea of hyper-entanglement [75] to encode two qubits onto certain photons, one in the polarization degree of freedom and one in the spatial degree of freedom, have also been implemented to create graph states of six [40] and seven [78] qubits encoded onto four photons. In these experiments, two photon pairs were created via SPDC and further superposed on (polarizing) beam splitters to create the hyper-entanglement in polarization and path.

For trapped ions, the largest entangled state that has been created is a 14 ion GHZ-state [92], which is a graph state. It was created by applying a global Mølmer-Sørensen (MS) gate [90] to all 14 ions in the trap. More involved cluster and graph states have just recently been successfully implemented with up to seven ions [77]. One of the states was a 2D cluster state consisting of four ions, and the others were graph states of the form of Figure 8.1 with $N = \{3, 5, 7\}$ qubits. The graph states were implemented by global MS gates to create large scale entanglement between the ions, supplemented by single-ion operations.

As a final remark, when talking about large-scale cluster states, it should be mentioned

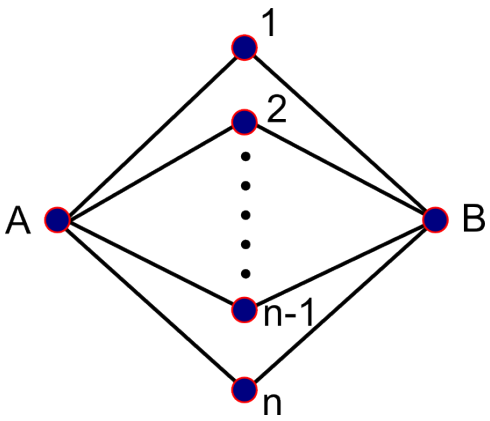


Figure 8.1: Cluster state for $N = n+2$ qubits used for topological error correction against up to $(n-1)/2$ phase flip errors.

that just recently a continuous-variable cluster state of more than 10 000 entangled modes has been created [141]. The modes were wave packets of light, multiplexed in the time domain. The implementation being in the continuous-variable setting makes it not immediately applicable for the discrete-variable AME states discussed in this thesis. There exists, however, a theoretical proposal of how to encode qubits in continuous-variable systems [46], which gives hope that these large-scale continuous-variable cluster states might also be useful for the implementation of the AME states discussed in this thesis.

Quantum Error Correction

For photons, in addition to errors that change the state of the encoded qubit, another common error source is the complete loss of a photon. This is described by the quantum erasure channel discussed in the last chapter. It is an error that is easier to correct, because it is already known which photon was lost. Experimentally, a system to encode one qubit onto four photons such that the information is protected against the loss of one of the four photons has been implemented in Ref. [83]. The entangled four photon state to encode the qubit was generated by creating two photon pairs via SPDC followed by a linear optical network. To test the system, three different input states were used and a photon loss was simulated, after which the initial state could be reconstructed with a fidelity between 74% and 83%, dependent on the input state.

For trapped ions, quantum error correction has been implemented by encoding one qubit onto three ions [27, 112] by using Mølmer-Sørensen type entangling operations [90, 79]. Since the minimum amount of qubits required to correct an arbitrary error is five [96], these implementations are not able to correct arbitrary errors, but instead

can only correct either bit-flip [27] or phase-flip errors [112]. Currently no experimental implementation with trapped ions exists that can correct bit-flip as well as phase flip errors, however, a laser pulse sequence that would implement a five qubit code to correct any error on one of the five ions has already been proposed [94].

Additionally, for both systems, photons and trapped ions, topological error correction [71, 106] can be performed with a cluster state of the type of Figure 8.1, which has been created for $N = 8$ photons [139] and $N = \{3, 5, 7\}$ ions [77]. In this scheme, the left and right qubits are the input and output qubits, respectively, while the state is encoded onto the middle $n = N - 2$ qubits. Hence these are the ones that experience the errors. The error encoding can correct phase-flip errors occurring on up to $(n - 1)/2$ of the qubits. This has been successfully simulated with $n = 6$ photons, by introducing an error on one of the six photons, and for the trapped ions by introducing an error on one ion for $n = 3$, and two errors for $n = 5$. Furthermore, in both cases, all n qubits were randomly subjected to an error with probability p, and the error observed in the output state was in agreement with the expected theoretical value. .

Quantum Secret Sharing

For quantum secret sharing, photons are the most suitable system, as the information has to be distributed over greater distances, which works well for photons due to their weak coupling to the environment. So far, QSS schemes where parties actually share a quantum secret, as discussed in this thesis, have not been implemented, yet. However, multipartite entangled quantum states also provide a resource for sharing classical secrets [61], which is easier to implement experimentally.

The simplest implementation to share a classical secret requires a GHZ state shared between three parties [61]. This allows one party to distribute a key such that the other two parties can only access the key if they cooperate. This has been implemented in Ref. [25], where two photon pairs were created via SPDC and then further superposed on PBS to create a four photon GHZ state. This four photon GHZ state was then transformed into a three photon GHZ state by measuring one photon, similar to the method described in Section 2.4.1. After correcting the introduced error via error correction (EC) and privacy amplification (PA) techniques widely used in quantum cryptography protocols [43], a secret key could successfully be established. Additionally, they implemented a third-man cryptography protocol [145] that allows two parties to share a secret key if the third party assists them.

By using all four photons emitted by a second-order SPDC process, also a four party secret sharing scheme has been implemented [39]. The four photons were distributed

between four parties. One of them acted as a dealer, while the other three were able to recover the secret when they collaborated. In the employed scheme, depending on the measurement outcomes, two parties were sometimes able to deduce a secret bit without the help of the third party, while one party alone was never able to gain any information. Introduced errors were again corrected with EC and PA protocols.

Appendix A

A.1 Proof of Theorem 3.9

Theorem 3.9. For a GHZ class $|\phi_{GHZ}\rangle$, if its interference term is I, then the maximal value of its 3-tangle is $\frac{(1-a^2)^3}{(1+a^3)^2}$, where a = $(\frac{f}{1-f})^{\frac{1}{3}}$.

Proof. From the formula of the two quantity:

$$I = \frac{2c_\alpha c_\beta c_\gamma s_\delta c_\delta c_\varphi}{1+2c_\alpha c_\beta c_\gamma s_\delta c_\delta c_\varphi} \tag{A.1}$$

$$I^2 = \frac{4c_\alpha^2 c_\beta^2 c_\gamma^2 s_\delta^2 c_\delta^2 c_\varphi^2}{(1+2c_\alpha c_\beta c_\gamma s_\delta c_\delta c_\varphi)^2} \tag{A.2}$$

$$\tau_{ABC} = \frac{4s_\alpha^2 s_\beta^2 s_\gamma^2 s_\delta^2 c_\delta^2}{(1+2c_\alpha c_\beta c_\gamma s_\delta c_\delta c_\varphi)^2} \tag{A.3}$$

$$\tag{A.4}$$

We have

$$\begin{aligned}\tau_{ABC} &= I^2 \frac{s_\alpha^2 s_\beta^2 s_\gamma^2}{c_\alpha^2 c_\beta^2 c_\gamma^2 c_\varphi^2} \\ &= I^2 \frac{(1-c_\alpha^2)(1-c_\beta^2)(1-c_\gamma^2)}{c_\alpha^2 c_\beta^2 c_\gamma^2 c_\varphi^2}\end{aligned} \tag{A.5}$$

We consider the condition when $I > 0$ at first.

Firstly, we consider the condition when $s_\delta = c_\delta = \frac{\sqrt{2}}{2}, c_\varphi = 1$. In this case, we have $c_\alpha c_\beta c_\gamma = \frac{I}{1-I}$. let $\frac{I}{1-I} = a^3$ where $a = (\frac{I}{1-I})^{\frac{1}{3}}$. Then we have

$$\begin{aligned}\tau_{ABC} &= I^2 \frac{(1-c_\alpha^2)(1-c_\beta^2)(1-c_\gamma^2)}{c_\alpha^2 c_\beta^2 c_\gamma^2} \\ &= I^2 \frac{(1-c_\alpha^2)(1-c_\beta^2)(1-\frac{a^6}{c_\alpha^2 c_\beta^2})}{a^6}\end{aligned} \tag{A.6}$$

Take partial derivation of c_α and c_β we can find this expression reaches its maximum

value when $c_\alpha = c_\beta = c_\gamma = a$ and the corresponding maximum value of 3-tangle is $\tau_{ABC_0} = ((1-I)^{\frac{2}{3}} - I^{\frac{2}{3}})^3 = \frac{(1-a^2)^3}{(1+a^3)^2}$.

Now we will show in other cases when $s_\delta \neq c_\delta or c_\varphi < 1$, we can only get a 3-tangle smaller than τ_{ABC_0}.

If $s_\delta \neq c_\delta$, we will have $s_\delta c_\delta < \frac{1}{2}$, then from the expression of I we can find $c_\alpha c_\beta c_\gamma c_\varphi > \frac{I}{1-I} = a^3$, then as $c_\varphi \leq 1$, we also have $c_\alpha c_\beta c_\gamma = b^3 > a^3$. And also take the partial derivation of $(1-c_\alpha^2)(1-c_\beta^2)(1-c_\gamma^2)$ we can find its maximum value is $(1-b^2)^3 < (1-a^2)^3$. Finally we have

$$\begin{aligned} \tau_{ABC} = & \quad I^2 \frac{(1-c_\alpha^2)(1-c_\beta^2)(1-c_\gamma^2)}{c_\alpha^2 c_\beta^2 c_\gamma^2 c_\varphi^2} \\ < & \quad I^2 \frac{(1-a^2)^3}{a^6} = \frac{(1-a^2)^3}{(1+a^3)^2} = \tau_{ABC_0} \end{aligned} \tag{A.7}$$

That is to say, when $s_\delta \neq c_\delta$, τ_{ABC} is always smaller than τ_{ABC_0}. Now let us consider the case when $s_\delta = c_\delta = \frac{\sqrt{2}}{2}$, but $c_\varphi < 1$.

Then again we have $c_\alpha c_\beta c_\gamma c_\varphi = \frac{I}{1-I} = a^3$. But as $c_\varphi < 1$, we still have $c_\alpha c_\beta c_\gamma = d^3 > a^3$. And also take the partial derivation of $(1-c_\alpha^2)(1-c_\beta^2)(1-c_\gamma^2)$ we can find its maximum value is $(1-d^2)^3 < (1-a^2)^3$. So we have

$$\begin{aligned} \tau_{ABC} = & \quad I^2 \frac{(1-c_\alpha^2)(1-c_\beta^2)(1-c_\gamma^2)}{c_\alpha^2 c_\beta^2 c_\gamma^2 c_\varphi^2} = I^2 \frac{(1-d^2)^3}{a^6} \\ < & \quad I^2 \frac{(1-a^2)^3}{a^6} = \frac{(1-a^2)^3}{(1+a^3)^2} = \tau_{ABC_0} \end{aligned} \tag{A.8}$$

Then we show, for the interference term $I > 0$, we have

$$max(\tau_{ABC}(\phi | I(\phi) = I > 0)) = \frac{(1-a^2)^3}{(1+a^3)^2} \tag{A.9}$$

When $I \leq 0$, the discussion is almost the same. Except that, we need to consider the condition $s_\delta = c_\delta = \frac{\sqrt{2}}{2}, c_\varphi = -1$ first and find $c_\alpha c_\beta c_\gamma = -\frac{I}{1-I} = a'^3 > 0$. Then easy to find the corresponding maximum value is $\frac{(1-a'^2)^3}{(1-a'^3)^2}$. And use the same tricks one can show it is the maximum value of the 3-tangle.

One thing to notice is that, the expression of a' and a is just opposite to each other. So if we let $a = \frac{I}{1-I} = -a'$ when $I \leq 0$, we will get

$$max(\tau_{ABC}(\phi | I(\phi) = I \leq 0)) = \frac{(1-a'^2)^3}{(1-a'^3)^2} = \frac{(1-a^2)^3}{(1+a^3)^2} \tag{A.10}$$

Then in all we have

$$max(\tau_{ABC}(\phi|I(\phi) = I) = \frac{(1 - a'^2)^3}{(1 - a'^3)^2} = \frac{(1 - a^2)^3}{(1 + a^3)^2} \tag{A.11}$$

□

Bibliography

[1] A. Acín, A. Andrianov, L. Costa, E. Jané, J. I. Latorre, and R. Tarrach. Generalized Schmidt Decomposition and Classification of Three-Quantum-Bit States. *Phys. Rev. Lett.*, 85(7):1560–1563, Aug 2000.

[2] A. Acín, E. Jané, W. Dür, and G. Vidal. Optimal Distillation of a Greenberger-Horne-Zeilinger State. *Phys. Rev. Lett.*, 85(22):4811–4814, Nov 2000.

[3] Erika Andersson and Daniel K. L. Oi. Binary search trees for generalized measurement. *arXiv:0712.2665*, 2007.

[4] A. Ashikhmin and E. Knill. Nonbinary quantum stabilizer codes. *Information Theory, IEEE Transactions on*, 47(7):3065 –3072, nov 2001.

[5] Mohsen Bahramgiri and Salman Beigi. Graph States Under the Action of Local Clifford Group in Non-Binary Case. *arXiv:quant-ph/0610267*, 2006.

[6] M. Barbieri, C. Cinelli, P. Mataloni, and F. De Martini. Polarization-momentum hyperentangled states: Realization and characterization. *Phys. Rev. A*, 72:052110, Nov 2005.

[7] Stephen D. Bartlett, Hubert de Guise, and Barry C. Sanders. Quantum encodings in spin systems and harmonic oscillators. *Phys. Rev. A*, 65:052316, May 2002.

[8] Salman Beigi, Isaac Chuang, Markus Grassl, Peter Shor, and Bei Zeng. Graph concatenation for quantum codes. *Journal of Mathematical Physics*, 52(2):022201, 2011.

[9] J.S. Bell. On the Einstein Podolsky Rosen Paradox. *Physics*, 1:195, 1964.

[10] Jan Benhelm, Gerhard Kirchmair, Christian F. Roos, and Rainer Blatt. Towards fault-tolerant quantum computing with trapped ions. *Nat Phys*, 4(6):463–466, June 2008.

[11] Charles H. Bennett. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.*, 68:3121–3124, May 1992.

[12] Charles H. Bennett, Herbert J. Bernstein, Sandu Popescu, and Benjamin Schumacher. Concentrating partial entanglement by local operations. *Phys. Rev. A*, 53(4):2046–2052, Apr 1996.

[13] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.*, 70:1895–1899, Mar 1993.

[14] G. R. Blakley and Catherine Meadows. Security of Ramp Schemes. In *CRYPTO*, pages 242–268, 1984.

[15] Rainer Blatt and David Wineland. Entangled states of trapped atomic ions. *Nature*, 453(7198):1008–1015, June 2008.

[16] A Borras, A R Plastino, J Batle, C Zander, M Casas, and A Plastino. Multiqubit systems: highly entangled states and entanglement distribution. 40(44):13407, 2007.

[17] L. Borsten, D. Dahanayake, M. J. Duff, A. Marrani, and W. Rubens. Four-Qubit Entanglement Classification from String Theory. *Phys. Rev. Lett.*, 105:100507, Sep 2010.

[18] L. Borsten, M. Duff, A. Marrani, and W. Rubens. On the black-hole/qubit correspondence. *The European Physical Journal Plus*, 126:1–31, 2011.

[19] Dik Bouwmeester, Jian-Wei Pan, Matthew Daniell, Harald Weinfurter, and Anton Zeilinger. Observation of Three-Photon Greenberger-Horne-Zeilinger Entanglement. *Phys. Rev. Lett.*, 82:1345–1349, Feb 1999.

[20] Hans J. Briegel and Robert Raussendorf. Persistent Entanglement in Arrays of Interacting Particles. *Phys. Rev. Lett.*, 86:910–913, Jan 2001.

[21] S Brierley and A Higuchi. On maximal entanglement between two pairs in four-qubit pure states. 40(29):8455, 2007.

[22] I D K Brown, S Stepney, A Sudbery, and S L Braunstein. Searching for highly entangled multi-qubit states. *Journal of Physics A: Mathematical and General*, 38(5):1119–1131, 2005.

[23] A. R. Calderbank and Peter W. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A*, 54:1098–1105, Aug 1996.

[24] Raino Ceccarelli, Giuseppe Vallone, Francesco De Martini, Paolo Mataloni, and Adán Cabello. Experimental Entanglement and Nonlocality of a Two-Photon Six-Qubit Cluster State. *Phys. Rev. Lett.*, 103:160401, Oct 2009.

[25] Yu-Ao Chen, An-Ning Zhang, Zhi Zhao, Xiao-Qi Zhou, Chao-Yang Lu, Cheng-Zhi Peng, Tao Yang, and Jian-Wei Pan. Experimental Quantum Secret Sharing and Third-Man Quantum Cryptography. *Phys. Rev. Lett.*, 95:200502, Nov 2005.

[26] Zeng-Bing Chen, Jian-Wei Pan, Yong-De Zhang, Časlav Brukner, and Anton Zeilinger. All-Versus-Nothing Violation of Local Realism for Two Entangled Photons. *Phys. Rev. Lett.*, 90:160408, Apr 2003.

[27] J. Chiaverini, D. Leibfried, T. Schaetz, M. D. Barrett, R. B. Blakestad, J. Britton, W. M. Itano, J. D. Jost, E. Knill, C. Langer, R. Ozeri, and D. J. Wineland. Realization of quantum error correction. *Nature*, 432(7017):602–605, December 2004.

[28] Eric Chitambar, Runyao Duan, and Yaoyun Shi. Tripartite Entanglement Transformations and Tensor Rank. *Phys. Rev. Lett.*, 101(14):140502, 2008.

[29] J. I. Cirac and P. Zoller. Quantum Computations with Cold Trapped Ions. *Phys. Rev. Lett.*, 74:4091–4094, May 1995.

[30] Richard Cleve, Daniel Gottesman, and Hoi-Kwong Lo. How to Share a Quantum Secret. *Phys. Rev. Lett.*, 83:648–651, Jul 1999.

[31] Valerie Coffman, Joydip Kundu, and William K. Wootters. Distributed entanglement. *Phys. Rev. A*, 61(5):052306, Apr 2000.

[32] Wei Cui, Wolfram Helwig, and Hoi-Kwong Lo. Bounds on probability of transformations between multipartite pure states. *Phys. Rev. A*, 81:012111, Jan 2010.

[33] F. Diedrich, J. C. Bergquist, Wayne M. Itano, and D. J. Wineland. Laser Cooling to the Zero-Point Energy of Motion. *Phys. Rev. Lett.*, 62:403–406, Jan 1989.

[34] W. Dür, G. Vidal, and J. I. Cirac. Three qubits can be entangled in two inequivalent ways. *Phys. Rev. A*, 62(6):062314, Nov 2000.

[35] Manfred Eibl, Nikolai Kiesel, Mohamed Bourennane, Christian Kurtsiefer, and Harald Weinfurter. Experimental Realization of a Three-Qubit Entangled W State. *Phys. Rev. Lett.*, 92:077901, Feb 2004.

[36] A. Einstein, B. Podolsky, and N. Rosen. Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? *Phys. Rev.*, 47:777–780, May 1935.

[37] Jens Eisert and Hans J. Briegel. Schmidt measure as a tool for quantifying multiparticle entanglement. *Phys. Rev. A*, 64(2):022306, Jul 2001.

[38] Paolo Facchi, Giuseppe Florio, Giorgio Parisi, and Saverio Pascazio. Maximally multipartite entangled states. *Phys. Rev. A*, 77:060304, Jun 2008.

[39] S. Gaertner, C. Kurtsiefer, M. Bourennane, and H. Weinfurter. Experimental Demonstration of Four-Party Quantum Secret Sharing. *Phys. Rev. Lett.*, 98:020503, Jan 2007.

[40] Wei-Bo Gao, Ping Xu, Xing-Can Yao, Otfried Gühne, Adán Cabello, Chao-Yang Lu, Cheng-Zhi Peng, Zeng-Bing Chen, and Jian-Wei Pan. Experimental Realization of a Controlled-NOT Gate with Four-Photon Six-Qubit Cluster States. *Phys. Rev. Lett.*, 104:020501, Jan 2010.

[41] I.M. Gelfand, M.M. Kapranov, and A.V. Zelevinsky. *Discriminants, Resultants and Multidimensional Determinants*. Birkhauser, 1994.

[42] Vlad Gheorghiu. Generalized semiquantum secret-sharing schemes. *Phys. Rev. A*, 85:052309, May 2012.

[43] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Rev. Mod. Phys.*, 74:145–195, Mar 2002.

[44] Daniel Gottesman. *Stabilizer Codes and Qantum Error Correction*. PhD thesis, California Institute of Technology, 1997.

[45] Daniel Gottesman. Theory of quantum secret sharing. *Phys. Rev. A*, 61:042311, Mar 2000.

[46] Daniel Gottesman, Alexei Kitaev, and John Preskill. Encoding a qubit in an oscillator. *Phys. Rev. A*, 64:012310, Jun 2001.

[47] Gilad Gour and Nolan R. Wallach. All maximally entangled four-qubit states. *Journal of Mathematical Physics*, 51(11):112201, 2010.

[48] M. Grassl, Th. Beth, and T. Pellizzari. Codes for the quantum erasure channel. *Phys. Rev. A*, 56:33–38, Jul 1997.

[49] M. Grassl, A. Klappenecker, and M. Rotteler. Graphs, quadratic forms, and quantum codes. In *Information Theory, 2002. Proceedings. 2002 IEEE International Symposium on*, pages 45–, 2002.

[50] Markus Grassl. Bounds on the minimum distance of linear codes and quantum codes. Online available at `http://www.codetables.de`, 2007.

[51] Daniel M. Greenberger, Michael A. Horne, and Anton Zeilinger. *Going Beyond Bell's Theorem in Bell's Theorem, Quantum Theory, and Conceptions of the Universe*, pages 69–72. Kluwer, Dordrecht, 1989.

[52] W. P. Grice, R. Erdmann, I. A. Walmsley, and D. Branning. Spectral distinguishability in ultrafast parametric down-conversion. *Phys. Rev. A*, 57:R2289–R2292, Apr 1998.

[53] W. P. Grice, A. B. U'Ren, and I. A. Walmsley. Eliminating frequency and space-time correlations in multiphoton states. *Phys. Rev. A*, 64:063815, Nov 2001.

[54] W. P. Grice and I. A. Walmsley. Spectral information and distinguishability in type-II down-conversion with a broadband pump. *Phys. Rev. A*, 56:1627–1634, Aug 1997.

[55] H. Häffner, W. Hänsel, C. F. Roos, J. Benhelm, D. Chek-al kar, M. Chwalla, T. Körber, U. D. Rapol, M. Riebe, P. O. Schmidt, C. Becher, O. Gühne, W. Dür, and R. Blatt. Scalable multiparticle entanglement of trapped ions. *Nature*, 438(7068):643–646, December 2005.

[56] Wolfram Helwig. Absolutely Maximally Entangled Qudit Graph States. *arXiv:quant-ph/1306.2879*, 2013.

[57] Wolfram Helwig and Wei Cui. Absolutely Maximally Entangled States: Existence and Applications. *arXiv:quant-ph/1306.2536*, 2013.

[58] Wolfram Helwig, Wei Cui, José Ignacio Latorre, Arnau Riera, and Hoi-Kwong Lo. Absolute maximal entanglement and quantum secret sharing. *Phys. Rev. A*, 86:052335, Nov 2012.

[59] A. Higuchi and A. Sudbery. How entangled can two couples get? *Physics Letters A*, 273(4):213 – 217, 2000.

[60] Scott Hill and William K. Wootters. Entanglement of a Pair of Quantum Bits. *Phys. Rev. Lett.*, 78:5022–5025, Jun 1997.

[61] Mark Hillery, Vladimír Buzek, and André Berthiaume. Quantum secret sharing. *Phys. Rev. A*, 59:1829–1834, Mar 1999.

[62] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki. Quantum entanglement. *Rev. Mod. Phys.*, 81:865–942, Jun 2009.

[63] Erik Hostens, Jeroen Dehaene, and Bart De Moor. Stabilizer states and Clifford operations for systems of arbitrary dimensions and modular arithmetic. *Phys. Rev. A*, 71:042315, Apr 2005.

[64] Yun-Feng Huang, Bi-Heng Liu, Liang Peng, Yu-Hu Li, Li Li, Chuan-Feng Li, and Guang-Can Guo. Experimental generation of an eight-photon Greenberger-Horne-Zeilinger state. *Nat Commun*, 2:546–, November 2011.

[65] Hannes Hubel, Deny R. Hamel, Alessandro Fedrizzi, Sven Ramelow, Kevin J. Resch, and Thomas Jennewein. Direct generation of photon triplets using cascaded photon-pair sources. *Nature*, 466(7306):601–603, July 2010.

[66] D. B. Hume, C. W. Chou, T. Rosenband, and D. J. Wineland. Preparation of Dicke states in an ion chain. *Phys. Rev. A*, 80:052302, Nov 2009.

[67] 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.*, 5:068, 2005.

[68] M. Iwamoto and H. Yamamoto. Strongly secure ramp secret sharing schemes. In *Information Theory, 2005. ISIT 2005. Proceedings. International Symposium on*, pages 1221–1225, 2005.

[69] Adrian Keet, Ben Fortescue, Damian Markham, and Barry C. Sanders. Quantum secret sharing with qudit graph states. *Phys. Rev. A*, 82:062315, Dec 2010.

[70] A. Ketkar, A. Klappenecker, S. Kumar, and P.K. Sarvepalli. Nonbinary Stabilizer Codes Over Finite Fields. *Information Theory, IEEE Transactions on*, 52(11):4892 –4914, nov. 2006.

[71] E. Knill. Quantum computing with realistically noisy devices. *Nature*, 434(7029):39–44, March 2005.

[72] Emanuel Knill and Raymond Laflamme. Theory of quantum error-correcting codes. *Phys. Rev. A*, 55:900–911, Feb 1997.

[73] B. Kraus. Local unitary equivalence and entanglement of multipartite pure states. *Phys. Rev. A*, 82:032121, Sep 2010.

[74] B. Kraus. Local Unitary Equivalence of Multipartite Pure States. *Phys. Rev. Lett.*, 104:020504, Jan 2010.

[75] Paul G. Kwiat. Hyper-entangled states. *Journal of Modern Optics*, 44(11-12):2173–2184, 1997.

[76] T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe, and J. L. O/'Brien. Quantum computers. *Nature*, 464(7285):45–53, March 2010.

[77] B. P. Lanyon, P. Jurcevic, M. Zwerger, C. Hempel, E. A. Martinez, W. Dür, H. J. Briegel, R. Blatt, and C. F. Roos. Measurement-Based Quantum Computation with Trapped Ions. *Phys. Rev. Lett.*, 111:210501, Nov 2013.

[78] Sang Min Lee, Hee Su Park, Jaeyoon Cho, Yoonshik Kang, Jae Yong Lee, Heonoh Kim, Dong-Hoon Lee, and Sang-Kyung Choi. Experimental realization of a four-photon seven-qubit graph state for one-way quantum computation. *Opt. Express*, 20(7):6915–6926, Mar 2012.

[79] D. Leibfried, B. DeMarco, V. Meyer, D. Lucas, M. Barrett, J. Britton, W. M. Itano, B. Jelenkovic, C. Langer, T. Rosenband, and D. J. Wineland. Experimental demonstration of a robust, high-fidelity geometric two ion-qubit phase gate. *Nature*, 422(6930):412–415, March 2003.

[80] Péter Lévay. On the geometry of four-qubit invariants. *Journal of Physics A: Mathematical and General*, 39(30):9533, 2006.

[81] Hoi-Kwong Lo and Sandu Popescu. Concentrating entanglement by local actions: Beyond mean values. *Phys. Rev. A*, 63(2):022301, Jan 2001.

[82] Shiang Yong Looi, Li Yu, Vlad Gheorghiu, and Robert B. Griffiths. Quantum-error-correcting codes using qudit graph states. *Phys. Rev. A*, 78:042303, Oct 2008.

[83] Chao-Yang Lu, Wei-Bo Gao, Jin Zhang, Xiao-Qi Zhou, Tao Yang, and Jian-Wei Pan. Experimental quantum coding against qubit loss error. *Proceedings of the National Academy of Sciences*, 105(32):11050–11054, 2008.

[84] Chao-Yang Lu, Xiao-Qi Zhou, Otfried Guhne, Wei-Bo Gao, Jin Zhang, Zhen-Sheng Yuan, Alexander Goebel, Tao Yang, and Jian-Wei Pan. Experimental entanglement of six photons in graph states. *Nat Phys*, 3(2):91–95, February 2007.

[85] Jean-Gabriel Luque and Jean-Yves Thibon. Polynomial invariants of four qubits. *Phys. Rev. A*, 67:042303, Apr 2003.

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

[87] Alois Mair, Alipasha Vaziri, Gregor Weihs, and Anton Zeilinger. Entanglement of the orbital angular momentum states of photons. *Nature*, 412(6844):313–316, July 2001.

[88] Damian Markham and Barry C. Sanders. Graph states for quantum secret sharing. *Phys. Rev. A*, 78:042309, Oct 2008.

[89] A. Miyake and M. Wadati. Multipartite entanglement and hyperdeterminants. *Quant. Inf. & Comp.*, 2:540–555, 2002.

[90] Klaus Mølmer and Anders Sørensen. Multiparticle Entanglement of Hot Trapped Ions. *Phys. Rev. Lett.*, 82:1835–1838, Mar 1999.

[91] Thomas Monz. *Quantum information processing beyond ten ion-qubits*. PhD thesis, Leopold-Franzens-Universität Innsbruck, 2011.

[92] Thomas Monz, Philipp Schindler, Julio T. Barreiro, Michael Chwalla, Daniel Nigg, William A. Coish, Maximilian Harlander, Wolfgang Hänsel, Markus Hennrich, and Rainer Blatt. 14-Qubit Entanglement: Creation and Coherence. *Phys. Rev. Lett.*, 106:130506, Mar 2011.

[93] Peter J. Mosley, Jeff S. Lundeen, Brian J. Smith, Piotr Wasylczyk, Alfred B. U'Ren, Christine Silberhorn, and Ian A. Walmsley. Heralded Generation of Ultrafast Single Photons in Pure Quantum States. *Phys. Rev. Lett.*, 100:133601, Apr 2008.

[94] V. Nebendahl, H. Häffner, and C. F. Roos. Optimal control of entangling operations for trapped-ion quantum computing. *Phys. Rev. A*, 79:012312, Jan 2009.

[95] M. A. Nielsen. Conditions for a class of entanglement transformations. *Physical Review Letters*, 83:436, 1999.

[96] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. 2000.

[97] Ognyan Oreshkov and Todd A. Brun. Weak measurements are universal. *Physical Review Letters*, 95:110409, 2005.

[98] A. Osterloh and J. Siewert. Entanglement monotones and maximally entangled states for multipartite qubit systems. *Int. J. Quant. Inf.*, 4:531, 2006.

[99] Jian-Wei Pan, Dik Bouwmeester, Matthew Daniell, Harald Weinfurter, and Anton Zeilinger. Experimental test of quantum nonlocality in three-photon Greenberger-Horne-Zeilinger entanglement. *Nature*, 403(6769):515–519, February 2000.

[100] Jian-Wei Pan, Zeng-Bing Chen, Chao-Yang Lu, Harald Weinfurter, Anton Zeilinger, and Marek Żukowski. Multiphoton entanglement and interferometry. *Rev. Mod. Phys.*, 84:777–838, May 2012.

[101] 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*, 29(3):665–673, 1988.

[102] John Preskill. Lecture Notes on Quantum Information. chapter 7. 1999.

[103] E.M. Rains. Nonbinary quantum codes. *Information Theory, IEEE Transactions on*, 45(6):1827–1832, 1999.

[104] Eric M. Rains. Quantum codes of minimum distance two. *Information theory, IEEE Transactions on*, 45:266–271, 1999.

[105] Robert Raussendorf and Hans J. Briegel. A One-Way Quantum Computer. *Phys. Rev. Lett.*, 86:5188–5191, May 2001.

[106] Robert Raussendorf and Jim Harrington. Fault-Tolerant Quantum Computation with High Threshold in Two Dimensions. *Phys. Rev. Lett.*, 98:190504, May 2007.

[107] Michael Reck, Anton Zeilinger, Herbert J. Bernstein, and Philip Bertani. Experimental realization of any discrete unitary operator. *Phys. Rev. Lett.*, 73:58–61, Jul 1994.

[108] I. Reed and G. Solomon. Polynomial Codes Over Certain Finite Fields. *Journal of the Society for Industrial and Applied Mathematics*, 8(2):300–304, 1960.

[109] M Riebe, M Chwalla, J Benhelm, H Häffner, W Hänsel, C F Roos, and R Blatt. Quantum teleportation with atoms: quantum process tomography. *New Journal of Physics*, 9(7):211, 2007.

[110] M. Riebe, H. Häffner, C. F. Roos, W. Hänsel, J. Benhelm, G. P. T. Lancaster, T. W. Körber, C. Becher, F. Schmidt-Kaler, D. F. V. James, and R. Blatt. Deterministic quantum teleportation with atoms. *Nature*, 429(6993):734–737, June 2004.

[111] Mark Riebe. *Preparation of Entangled States and Quantum Teleportation with Atomic Qubits*. PhD thesis, Leopold-Franzens-Universität Innsbruck, 2005.

[112] Philipp Schindler, Julio T. Barreiro, Thomas Monz, Volckmar Nebendahl, Daniel Nigg, Michael Chwalla, Markus Hennrich, and Rainer Blatt. Experimental Repetitive Quantum Error Correction. *Science*, 332(6033):1059–1061, 2011.

[113] Dirk Schlingemann. Stabilizer codes can be realized as graph codes. *Quant. Inf. & Comp.*, 2:307, 2002.

[114] F. Schmidt-Kaler, H. Hffner, S. Gulde, M. Riebe, G.P.T. Lancaster, T. Deuschle, C. Becher, W. Hnsel, J. Eschner, C.F. Roos, and R. Blatt. How to realize a universal quantum gate with trapped ions. *Applied Physics B*, 77(8):789–796, 2003.

[115] Ferdinand Schmidt-Kaler, Hartmut Haffner, Mark Riebe, Stephan Gulde, Gavin P. T. Lancaster, Thomas Deuschle, Christoph Becher, Christian F. Roos, Jurgen Eschner, and Rainer Blatt. Realization of the Cirac-Zoller controlled-NOT quantum gate. *Nature*, 422(6930):408–411, March 2003.

[116] Benjamin Schumacher and M. A. Nielsen. Quantum data processing and error correction. *Phys. Rev. A*, 54:2629–2635, Oct 1996.

[117] A. J. Scott. Multipartite entanglement, quantum-error-correcting codes, and entangling power of quantum evolutions. *Phys. Rev. A*, 69:052330, May 2004.

[118] G. Seroussi and R.M. Roth. On MDS extensions of generalized Reed-Solomon codes. *Information Theory, IEEE Transactions on*, 32(3):349 –354, May 1986.

[119] L. K. Shalm, D. R. Hamel, Z. Yan, C. Simon, K. J. Resch, and T. Jennewein. Three-photon energy-time entanglement. *Nat Phys*, 9(1):19–22, January 2013.

[120] R. Singleton. Maximum distance q-nary codes. *Information Theory, IEEE Transactions on*, 10(2):116 – 118, apr 1964.

[121] Anders Sørensen and Klaus Mølmer. Quantum Computation with Ions in Thermal Motion. *Phys. Rev. Lett.*, 82:1971–1974, Mar 1999.

[122] Anders Sørensen and Klaus Mølmer. Entanglement and quantum computation with ions in thermal motion. *Phys. Rev. A*, 62:022311, Jul 2000.

[123] Andrew Steane. Multiple-Particle Interference and Quantum Error Correction. *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, 452(1954):2551–2577, 1996.

[124] Stig Stenholm. The semiclassical theory of laser cooling. *Rev. Mod. Phys.*, 58:699–739, Jul 1986.

[125] P. C. Sun, Y. Mazurenko, and Y. Fainman. Long-distance frequency-division interferometer for communication and quantum cryptography. *Opt. Lett.*, 20(9):1062–1064, May 1995.

[126] Ashish V. Thapliyal. Multipartite maximally entangled states, minimal entanglement generating states and entropic inequalitites. unpublished presentation (2003).

[127] S. Turgut, Y. Gul, and N. K. Pak. Deterministic Transformations of Multipartite Entangled States with Schmidt Rank 2. *arXiv:0907.3960v2*, 2009.

[128] Armin Uhlmann. Optimizing entropy relative to a channel or a subalgebra. *Open Sys. & Inf. Dyn.*, 5:209–227, 1998.

[129] V. Vedral, M. B. Plenio, M. A. Rippin, and P. L. Knight. Quantifying Entanglement. *Phys. Rev. Lett.*, 78(12):2275–2279, Mar 1997.

[130] F. Verstraete, J. Dehaene, B. De Moor, and H. Verschelde. Four qubits can be entangled in nine different ways. *Phys. Rev. A*, 65:052112, 2002.

[131] Guifré Vidal. Entanglement of Pure States for a Single Copy. *Phys. Rev. Lett.*, 83(5):1046–1049, Aug 1999.

[132] Guifré Vidal. Entanglement monotones. *Journal of Modern Optics*, 47(2-3):355–376, 2000.

[133] P. Walther, K. J. Resch, T. Rudolph, E. Schenck, H. Weinfurter, V. Vedral, M. Aspelmeyer, and A. Zeilinger. Experimental one-way quantum computing. *Nature*, 434(7030):169–176, March 2005.

[134] David J. Wineland and Wayne M. Itano. Laser Cooling. *Phys. Today*, 6:34, 1987.

[135] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, October 1982.

[136] William K. Wootters. Entanglement of Formation of an Arbitrary State of Two Qubits. *Phys. Rev. Lett.*, 80:2245–2248, Mar 1998.

[137] Yu Xin and Runyao Duan. Conditions for entanglement transformation between a class of multipartite pure states with generalized Schmidt decompositions. *arxiv:0707.1947*, 2007.

[138] Tao Yang, Qiang Zhang, Jun Zhang, Juan Yin, Zhi Zhao, Marek Żukowski, Zeng-Bing Chen, and Jian-Wei Pan. All-Versus-Nothing Violation of Local Realism by Two-Photon, Four-Dimensional Entanglement. *Phys. Rev. Lett.*, 95:240406, Dec 2005.

[139] Xing-Can Yao, Tian-Xiong Wang, Hao-Ze Chen, Wei-Bo Gao, Austin G. Fowler, Robert Raussendorf, Zeng-Bing Chen, Nai-Le Liu, Chao-Yang Lu, You-Jin Deng, Yu-Ao Chen, and Jian-Wei Pan. Experimental demonstration of topological error correction. *Nature*, 482(7386):489–494, February 2012.

[140] Ye Yeo and Wee Kang Chua. Teleportation and Dense Coding with Genuine Multipartite Entanglement. *Phys. Rev. Lett.*, 96:060502, Feb 2006.

[141] Shota Yokoyama, Ryuji Ukai, Seiji C. Armstrong, Chanond Sornphiphatphong, Toshiyuki Kaji, Shigenari Suzuki, Jun-ichi Yoshikawa, Hidehiro Yonezawa, Nicolas C. Menicucci, and Akira Furusawa. Ultra-large-scale continuous-variable cluster states multiplexed in the time domain. *Nat Photon*, 7(12):982–986, December 2013.

[142] Anton Zeilinger, Michael A. Horne, Harald Weinfurter, and Marek Żukowski. Three-Particle Entanglements from Two Entangled Pairs. *Phys. Rev. Lett.*, 78:3031–3034, Apr 1997.

[143] Jing Zhang, Gerardo Adesso, Changde Xie, and Kunchi Peng. Quantum Teamwork for Unconditional Multiparty Communication with Gaussian States. *Phys. Rev. Lett.*, 103:070501, Aug 2009.

[144] Zhi Zhao, Yu-Ao Chen, An-Ning Zhang, Tao Yang, Hans J. Briegel, and Jian-Wei Pan. Experimental demonstration of five-photon entanglement and open-destination teleportation. *Nature*, 430:54–58, 2004.

[145] M. Zukowski. Quest for GHZ States. *Acta Phys. Pol.*, 93:187, 1998.