# Absolutely Maximally Entangled states in small system sizes

Master Thesis

Theoretical Quantum Physics

Albert Rico

Supervisor: Prof. Dr. Barbara Kraus
Co-supervisor: Dr. Martin Hebenstreit
Institute for Theoretical Physics

University of Innsbruck
September 2020

*A la Barbara, una referent científica i humana.*
*Al Pare, la Mare i el Ferran.*

# Acknowledgements

First of all, I want to thank Barbara Kraus for her engagement, for her support and for all I could learn from her accurate, rigorous and meaningful advice. I am also very grateful to Martin Hebenstreit and Matthias Englbrecht for their help and for their discussions. In a more general context, I want to thank the whole research group for the warm and knowledge-sharing atmosphere to which all the members contribute. Furthermore, I am very grateful to Felix Huber and Zahra Raissi for their discussions. Last but not least, I wish to thank my family for their constant and unconditional support.

# Abstract

Absolutely Maximally Entangled (AME) states are pure multipartite quantum states which maximize the entanglement entropy across any possible bipartition. AME states have applications in multipartite quantum teleportation, quantum secret sharing, quantum error correction and toy models for the holographic principle. Determining for which system sizes AME states exist is an open problem in quantum information theory. The simplest case which existence is currently open is a hypothetical AME state shared among 4 parties in 6 local dimensions and it is called AME(4,6).

In this thesis we review the main results in the literature about the existence and applications of AME states. Inspired by those results and by current literature on related topics in quantum information, we investigate the existence and constructions of AME states via two approaches which are motivated to either prove or disprove the existence of AME(4,6). First, we provide a numerical algorithm which leads to 4-partite pure states having a high entanglement entropy across any possible bipartition. The algorithm converges to AME states for certain choices of the local dimensions. However, it does not lead to an AME(4,6). Second, we provide specific analytic constructions for AME states shared among a small number of parties and we study possible reformulations of the necessary and sufficient conditions for the existence of 4-partite AME states.

# Contents

# Chapter 1

# Introduction

## 1.1 Basic concepts in quantum information

Quantum Mechanics gives a mathematical framework to develop physical theories for quantum systems. It is based on few assumptions known as the *Postulates of Quantum Mechanics* connect such mathematical description with physical systems. Quantum information theory is the theory in quantum mechanics which describes how quantum information is processed, stored and transmitted. In this section we will introduce a selection of basic concepts in quantum information theory which will be needed for our purposes.

### Pure states and Hilbert spaces

Associated to any physical system, there is a *Hilbert space* $\mathcal{H}$, which is a complex vector space with a inner product. Such product among any two elements $|\psi\rangle, |\phi\rangle \in \mathcal{H}$ is denoted as $\langle\psi|\,\phi\rangle$. According to the first postulate of Quantum Mechanics, any isolated physical system can be fully described by a *pure quantum state*, which is a normalized vector of the corresponding Hilbert space,

$$|\psi\rangle \in \mathcal{H}: \quad \langle\psi|\,\psi\rangle = 1. \tag{1.1.1}$$

As an example, the spin of an electron is fully determined by a two-dimensional Hilbert space $\mathcal{H}_2 = \mathbb{C}_2$. Being $\{|0\rangle, |1\rangle\}$ an orthonormal basis of $\mathcal{H}_2$, such system is characterized by the pure state

$$|\psi\rangle = a_0\,|0\rangle + a_1\,|1\rangle\,, \tag{1.1.2}$$

where the complex coefficients $a_0$ and $a_1$ satisfy $|a_0|^2 + |a_1|^2 = 1$. The pure state given in equation (1.1.2) is called *qubit* and its associated Hilbert space has dimension $d = 2$. Pure states of a Hilbert space $\mathcal{H}_d = \mathbb{C}^d$ with $d > 2$ are called *qudits*. Often, a qudit $|\psi\rangle$ is written in an orthonormal basis of $\mathcal{H}_d$, $\{|i\rangle\}$ with $i \in \mathbb{Z}_d$, called *computational basis*:

$$|\psi\rangle = \sum_{i=0}^{d-1} a_i\,|i\rangle\,, \tag{1.1.3}$$

with $\sum_{i=0}^{d-1} |a_i|^2 = 1$.

Classically, states corresponding to binary systems (e.g., the outcome of flipping a coin) are described by *bits*, which can be *either* $|0\rangle$ *or* $|1\rangle$. Hence, qubits differ from bits because they allow for *superposition*, i.e., linear combination of elements of the computational

basis (1.1.2). This holds naturally for systems in dimension $d > 2$. The phenomenon of superposition is within the core of Quantum Mechanics, and one of the main distinctions among classical and quantum systems.

### Measurement

Any state $|\psi\rangle$ contains all the information of the system. For an external observer to obtain such information, a *measurement* must be done. According to the postulates of Quantum Mechanics, any measurable quantity corresponds to a set of operators $\{M_m\}$ acting on the Hilbert space associated to the physical system, satisfying the condition

$$\sum_m M_m^\dagger M_m = \mathbb{1}. \tag{1.1.4}$$

The set of positive operators $\{M_m^\dagger M_m\}$ is called *positive operator-valued measurement (POVM)*. Each index $m$ is associated to a measurement outcome $a_m$, and the probability $p(a_m)$ of obtaining $a_m$ reads

$$p(a_m) = \langle\psi| M_m^\dagger M_m |\psi\rangle . \tag{1.1.5}$$

According to the so-called *Copenhagen interpretation*, once a system in a state $|\psi\rangle$ is measured resulting in an outcome $a_m$, the state changes instantaneously as

$$|\psi\rangle \to \frac{M_m |\psi\rangle}{\sqrt{\langle\psi| M_m^\dagger M_m |\psi\rangle}}. \tag{1.1.6}$$

This phenomenon is known as the *collapse* of the state $|\psi\rangle$.

A *projective measurement* is the special case in which the operators $\{M_m\}$ are orthogonal projectors, so that we have

$$M_m^\dagger M_n = M_m \delta_{m,n}. \tag{1.1.7}$$

Such a measurement can also be described by an hermitian operator $O = \sum_m a_m M_m$. Here, $\{a_m\}$ denote the possible outcomes of the measurement. Given a system associated to a Hilbert space $\mathcal{H} = \mathbb{C}^d$ in dimension $d$ and $\{a_i, |\phi_i\rangle\}$ the set of eigenvalues and eigenstates of an operator $O$ acting on $\mathcal{H}$, the so-called *spectral decomposition* of $O$ reads

$$O = \sum_{i=0}^{d-1} a_i |\phi_i\rangle \langle\phi_i| , \tag{1.1.8}$$

where the eigenvalues $\{a_i\}$ can be degenerated. In quantum information, we typically use the term $\{|\phi_i\rangle\}$-*measurement* to refer to a measurement of an operator with eigenbasis $\{|\phi_i\rangle\}$ and non degenerated eigenvalues, and the term $O$-*measurement* to refer to a measurement of the operator $O$.

### Unitary evolution and gates

The evolution in time of a closed quantum system is described by a *unitary transformation*. That is, the state of a system at time $t_1$, $|\psi(t_1)\rangle$, is related to the state of such system at

time $t_2$, $|\psi(t_2)\rangle$, by a unitary operator $U$ which depends only on the times $t_1$ and $t_2$. Namely,

$$|\psi(t_2)\rangle = U\,|\psi(t_1)\rangle\,. \tag{1.1.9}$$

In the language of quantum computation, unitary operators $U$ which affect one or two qudits are usually called *quantum gates*, in the sense that the operation $U\,|\psi\rangle$ does a specific -desired or undesired- change to the state $|\psi\rangle$. Particularly interesting unitary and hermitian operators for qubits are the elements (up to phases) of the so-called *Pauli group* $\mathcal{P} = \{\pm 1, \pm i\} \times \{\mathbb{1}, X, Z, Y\} \in SU(2)$,

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \tag{1.1.10}$$

where $i$ is the imaginary unit and $\mathbb{1}$ is the identity operator. $\mathcal{P}$ has two generators, say $X$ and $Z$. In the language of quantum computation, $X$ is called *bit flip* and $Z$ is called *phase flip*.

A generalization of the Pauli group for $d$-dimensional systems is as follows. Using the same notation as [1] we define the multiplicative group $\mathcal{P}_d = \{D_{\mu,\nu}\} \in SU(d)$ with $1 \leq \lambda, \mu, \nu \leq d$, by defining its generators

$$\begin{aligned} X_d &= \sum_{l=0}^{d-1} |l \oplus 1\rangle \langle l| \\ Z_d &= \sum_{l=0}^{d-1} \omega^l\, |l\rangle \langle l|\ , \end{aligned} \tag{1.1.11}$$

with $\omega = e^{i\frac{2\pi}{d}}$ and where $\oplus$ denotes addition $mod(d)$. The elements of the group are

$$D_{\mu,\nu} = e^{i\frac{\pi\mu\nu}{d}} X_d^\mu Z_d^\nu = e^{i\frac{\pi\mu\nu}{d}} \sum_{l=0}^{d-1} \omega^{l\nu}\, |l \oplus \mu\rangle \langle l| \quad \forall \lambda, \mu, \nu \in \{0, ..., d-1\}\,. \tag{1.1.12}$$

The elements $\{D_{\mu,\nu}\}$ are in general not hermitian and they satisfy the following properties,

$$\begin{aligned} &D_{\mu,\nu} = e^{i\pi\nu} D_{\mu+d,\nu} = e^{i\pi\mu} D_{\mu,\nu+d} \\ &D_{\mu,\nu}^\dagger = D_{-\mu,-\nu} = e^{i\pi(\mu+\nu+d)} D_{\mu,\nu+d} \\ &D_{\mu,\nu} D_{\alpha,\beta} = \omega^{\nu\alpha-\mu\beta} D_{\alpha,\beta} D_{\mu,\nu} = \omega^{(\nu\alpha-\mu\beta)/2} D_{\nu+\alpha,\mu+\beta}. \end{aligned} \tag{1.1.13}$$

Usually, we will refer to the elements of $\mathcal{P}_d$ up to phases.

### Mixed states

So far we considered quantum systems described by pure states. However, non isolated systems can be described by a statistical ensemble $\{p_i, |\psi_i\rangle\}$, meaning that the system is in the state $|\psi_i\rangle$ with probability $p_i$. Then we describe such system with a *density operator*

$$\rho = \sum_i p_i\, |\psi_i\rangle \langle\psi_i| \in \mathcal{B}(\mathcal{H}), \tag{1.1.14}$$

where $\mathcal{B}(\mathcal{H})$ is the set of bounded operators acting on the Hilbert space $\mathcal{H}$ containing $\{|\psi_i\rangle\}$. A density operator is defined so that it fulfills the following properties.

- It is *self-adjoint*, $\rho^\dagger = \rho$
- It is *positive-semidefinite*, that is, all its eigenvalues are real and nonnegative.
- It is normalized with respect to the trace norm, $tr(\rho) = 1$.

A density operator $\rho$ describes a pure state, $\rho = |\psi\rangle\langle\psi|$, iff $tr(\rho^2) = 1$. Similarly as for pure states, the outcome of a measurement described by the operators $\{M_m\}$ is as follows,

$$p(m) = tr(M_m^\dagger M_m \rho) \tag{1.1.15}$$

and the state of the system collapses after obtaining a measure outcome $m$ to

$$\rho \to \frac{M_m \rho M_m^\dagger}{tr(M_m^\dagger M_m \rho)}. \tag{1.1.16}$$

## 1.2 Quantum entanglement

Let $\{\mathcal{H}_r\}$ with $1 \leq r \leq N$ be $N$ Hilbert spaces in arbitrary dimensions, each of which corresponds to a system labeled by $r$. Then the tensor product $\mathcal{H}^{\otimes N} = \bigotimes_{r=1}^{N} \mathcal{H}_r$ is also a Hilbert space and it corresponds to a composite system with the $N$ subsystems which are labeled by $\{r\}$. A system is said to be *homogeneous* if all the Hilbert spaces corresponding to its $N$ subsystems have the same dimension $d$, and *inhomogeneous* otherwise. A state $\rho \in \mathcal{B}(\mathcal{H}^{\otimes N})$ is called *$N$-partite* in the sense that it is shared among $N$ different physical systems, called *local parties*. Systems with $N > 2$ are called *multipartite*.

For $N \geq 2$, in general the information about the whole system is stored nonlocally. This phenomenon is known as *entanglement*. In this section we will first consider bipartite entanglement, and then we will move to multipartite entanglement.

### 1.2.1 Bipartite entanglement

We consider states describing a system composed by two subsystems $A$ and $B$ which has associated a Hilbert space $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$. Note that such consideration includes systems of two local parties $A$ and $B$, but also multipartite systems composed by $N$ local parties for which we consider the bipartition among a set $A$ of $|A|$ local parties and its complementary set $B$ with $|B|$ local parties, so that $|A| + |B| = N$. We will first consider the general case, namely bipartite entanglement in mixed states, and then focus on the particular case of pure states.

Consider a density operator $\rho$ acting on $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$. The state which describes the subsystem $A$, $\rho_A$, is given by the partial trace of $\rho$ with respect to the subsystem $B$,

$$\rho_A = tr_B(\rho) = \sum_{i=0}^{d-1} (\mathbb{1} \otimes \langle i|_B)\rho(\mathbb{1} \otimes |i\rangle_B). \tag{1.2.1}$$

The density operator $\rho_A$ is denoted as the *reduced density operator* corresponding to the subsystem $A$. An analogous description defines the reduced density operator $\rho_B$.

Suppose $\rho$ can be written as a tensor product,

$$\rho = \sum_j \alpha_j \sigma_A^{(j)} \otimes \sigma_B^{(j)}, \tag{1.2.2}$$

where $\alpha_j \geq 0$ and $\{\sigma_A^{(j)}\}$ and $\{\sigma_B^{(j)}\}$ are density operators acting respectively on the subspaces $\mathcal{H}_A$ and $\mathcal{H}_B$. Then $\rho$ is *separable* with respect to the bipartition $A|B$. Otherwise, $\rho$ is *entangled* with respect to such bipartition, or equivalently, the subsystem $A$ is entangled with the subsystem $B$. If $\rho$ describes a system with more than two local parties, then we can define some particular cases of separable states. $\rho$ is *biseparable* if it is separable with respect to a given bipartition. $\rho$ is *fully separable* if it is separable with respect to all the possible bipartitions,

$$\rho = \sum_j \alpha_j \bigotimes_{r=1}^{N} \sigma_r^{(j)}, \tag{1.2.3}$$

where $\{\sigma_r^{(j)}\}$ are density operators acting respectively on the Hilbert space $\mathcal{H}_r$ and $0 \leq \alpha_j \in \mathbb{R}$.

Let us now move to the case of pure states. Consider the pure state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$. If $|\psi\rangle$ can be written as a tensor product,

$$|\psi\rangle = |\phi\rangle_A \otimes |\varphi\rangle_B , \tag{1.2.4}$$

where $|\phi\rangle_A \in \mathcal{H}_A$ and $|\varphi\rangle_A \in \mathcal{H}_B$ are pure states, then $|\psi\rangle$ is *separable* with respect to the bipartition $A|B$. Otherwise, $|\psi\rangle$ is entangled with respect to such bipartition. Similarly as for mixed states, a $N$-partite state $|\psi\rangle$ is fully separable if it can be written as

$$|\psi\rangle = \bigotimes_{r=1}^{N} |i_r\rangle , \tag{1.2.5}$$

where $\{|i_r\rangle \in \mathcal{H}_r\}$ are pure states.

### 1.2.2 Entanglement as a physical resource

States which are shared among parties which are spatially separated can only be manipulated by means of *local operations assisted by classical communication*, either deterministic ($LOCC$) or stochastic ($SLOCC$). Here we will introduce this set of operations, which play a central role in understanding both entanglement foundations and in its applications. Furthermore, aside from being separable or entangled, a state $\rho \in \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_B)$ can be more or less entangled. That is, entanglement can be quantified, despite in general there is not a unique measure of the amount of entanglement present in quantum states. Here we will introduce the concept of entanglement as a resource, that is, as a physical quantity which can not increase under LOCC.

#### Local operations assisted by classical communication (LOCC)

Let $A$ and $B$ be two spatially separated quantum systems which can not interact classically and share a quantum state $\rho \in \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_B)$. Let Alice and Bob hold the local systems $A$ and $B$ respectively. The set of *local operations* is the set of quantum operations that Alice and

Bob can do in such scenario without classically communicating. The set of *local operations assisted by classical communication (LOCC)* is the set of operations which can be done by Alice and Bob when classical communication between them is allowed. This set of operators has the form

$$\{M_m \otimes \mathbb{1}\} \bigcup \{\mathbb{1} \otimes M_n\}, \tag{1.2.6}$$

being $\{M_n \in \mathcal{B}(\mathcal{H}_A)\}$ and $\{M_n \in \mathcal{B}(\mathcal{H}_B)\}$ arbitrary operators fulfilling the completeness relation. In contrast, a *joint operation* is an operation acting nontrivially on both $\mathcal{H}_A$ and $\mathcal{H}_B$. In LOCC, classical communication allows Alice and Bob to take into account the measurement outcomes of both parties to choose appropriately the subsequent measurements of the form (1.2.6) in order to achieve a given quantum task. A very special subset of LOCC is the set of *local unitaries (LU)*, which is the subset of local operations in which Alice and Bob apply respectively unitary operators $U_A$ and $U_B$,

$$\rho \to \sigma = (U_A \otimes U_B)\, \rho\, (U_A^\dagger \otimes U_B^\dagger). \tag{1.2.7}$$

LU operations are the only operations in LOCC which are invertible,

$$(U_A^\dagger \otimes U_B^\dagger)\, \sigma\, (U_A \otimes U_B) = \rho. \tag{1.2.8}$$

Two states $\rho_1$ and $\rho_2$ are said to be equivalent up to *LU* operations (or LU-equivalent) iff they can be transofmed into each other by means of local unitaries,

$$\rho_1 = (U_A \otimes U_B)\, \rho_2\, (U_A^\dagger \otimes U_B^\dagger). \tag{1.2.9}$$

A *LU-equivalence class* is the set of states which are interconvertible by means of LU operations.

There is a particular set of operations which Alice and Bob can do being spatially separated, called *stochastic local operations assisted by classical communication (SLOCC)*. The set of SLOCC is the set of operations which can be done by means of locally manipulating the quantum systems and classically communicating, so that Alice and Bob convert a state $\rho \in \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_B)$ into another state $\sigma_k \in \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_B)$ probabilistically, that is, with a non-vanishing probability of success $p_k$,

$$\rho \to \{\sigma_k, p_k\}, \tag{1.2.10}$$

with $\sum_k p_k = 1$. If two quantum states $\rho$ and $\sigma$ are interconvertible by means of SLOCC, then they are said to be in the same *SLOCC-equivalence class*.

### Quantifying bipartite entanglement. Bell states

If Alice and Bob share a separable state $\rho \in \mathcal{B}(\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B)$, then they cannot convert it into an entangled state by means of LOCC. This motivates the following definition, considering pure states. An *entanglement measure* is a map $E : \mathcal{B}(\mathcal{H}) \to \mathbb{R} \geq 0$ which can not increase under LOCC and vanishes for separable states. That is, consider two states $\rho \in \mathcal{B}(\mathcal{H})$ and $\sigma \in \mathcal{B}(\mathcal{H})$. If $\rho$ can be converted into $\sigma$ via LOCC, then $E(\rho) \geq E(\sigma)$. The fact that entanglement cannot increase under LOCC means that entanglement is a physical resource to manipulate quantum systems locally. Since entanglement cannot increase under LOCC and the operations in LU are invertible, it follows that the amount entanglement is

invariant under LU operations.

Given a bipartite pure state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$, the *entropy of entanglement* $E_E(|\psi\rangle)$ is the most commonly used entanglement measure and it reads

$$E_E(|\psi\rangle) = S(\rho_A). \tag{1.2.11}$$

Here $S(\rho_A)$ is the *Von Neumann entropy* of $\rho_A$,

$$S(\rho_A) = tr(\rho_A \log_2 \rho_A) = -\sum_k \lambda_k \log_2 \lambda_k, \tag{1.2.12}$$

where $\{\lambda_k\}$ are the eigenvalues of $\rho_A$ and $\log_2$ is the logarithm in base 2. We say that a bipartite state is *maximally entangled* if it maximizes $E_E$ over all the possible states of its Hilbert space. For two qubits, an orthonormal basis of states which are maximally entangled is the *Bell basis* and its elements are the so-called *Bell states*,

$$\begin{aligned}
\left|\Phi^+\right\rangle &= \frac{1}{\sqrt{2}}\big(\,|0\rangle\,|0\rangle + |1\rangle\,|1\rangle\,\big) \\
\left|\Phi^-\right\rangle &= \frac{1}{\sqrt{2}}\big(\,|0\rangle\,|0\rangle - |1\rangle\,|1\rangle\,\big) \\
\left|\Psi^+\right\rangle &= \frac{1}{\sqrt{2}}\big(\,|0\rangle\,|1\rangle + |1\rangle\,|0\rangle\,\big) \\
\left|\Psi^-\right\rangle &= \frac{1}{\sqrt{2}}\big(\,|0\rangle\,|1\rangle - |1\rangle\,|0\rangle\,\big),
\end{aligned} \tag{1.2.13}$$

where we used the shorthand notation $|a\rangle\,|b\rangle = |a\rangle \otimes |b\rangle$. For systems of larger dimension $d$, one generalization of the Bell basis reads [2]

$$\big\{\,|\phi_{k,l}\rangle\,\big\} \quad \forall\,|\phi_{k,l}\rangle = D_{l,k} \otimes \mathbb{1}\left|\phi_d^+\right\rangle = \frac{1}{\sqrt{d}} \sum_{r=0}^{d-1} \omega^{kr}\,|r \oplus l\rangle\,|r\rangle\,, \tag{1.2.14}$$

with $\left|\phi_d^+\right\rangle = \frac{1}{\sqrt{d}} \sum_{r=0}^{d-1} |r\rangle\,|r\rangle$, where the elements of $\mathcal{P}_d$ are taken up to phases.

For mixed states, there are different entanglement measures motivated by different physical scenarios. One example of entanglement measure for a mixed state $\rho$ acting on $\mathcal{H}_A \otimes \mathcal{H}_B$ is the *negativity* $N(\rho)$ [3],

$$N(\rho) = \frac{1}{d}\big(||\rho^{T_A}||_1 - 1\big), \tag{1.2.15}$$

with $||\sigma||_1 = tr\sqrt{\sigma\sigma^\dagger}$, $d$ being the dimension of $\mathcal{H}_A$ and $T_A$ denoting the partial transpose on the system $A$. That is, $\rho^{T_A} = (T \otimes \mathbb{1})(\rho)$, where $T$ denotes the transposition operator. If the negativity is nonzero, then $\rho$ is entangled, but the converse is not necessarily true. Under certain conditions, the negativity bounds how useful is a mixed state $\rho$ for certain tasks [4].

For two qubits, another entanglement measure is the *concurrence* $C(\rho)$ [5]. Consider

$$R = \sqrt{\sqrt{\rho}(Y \otimes Y)\rho^*(Y \otimes Y)\sqrt{\rho}}, \tag{1.2.16}$$

where $\rho^*$ is the complex conjugated of $\rho$ in the computational basis. Let the (real) eigenvalues

of $R$ be $\{\lambda_1, \lambda_2, \lambda_3, \lambda_4\}$ sorted in decreasing order. The concurrence is given by [5]

$$C(\rho) = max\{0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4\}. \tag{1.2.17}$$

This measure will become important in section 1.2.3.

### Decompositions of bipartite pure states

A general description of a pure bipartite state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$, where the Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ have dimension $d_A$ and $d_B$ respectively, reads

$$|\psi\rangle = \sum_{i=0}^{d_A-1} \sum_{j=0}^{d_B-1} a_{i,j} |i\rangle |j\rangle , \tag{1.2.18}$$

where $\{|i\rangle\}$ and $\{|j\rangle\}$ denote the computational basis in dimension $d_A$ and $d_B$ respectively. Assuming $d_A > d_B$ and defining the $d_B \times d_A$ matrix $A = \sum_{i,j} a_{i,j} |i\rangle \langle j|$ with $0 \leq i \leq d_A - 1$ and $0 \leq j \leq d_B - 1$, we can generally write

$$|\psi\rangle = A \otimes \mathbb{1} \sum_{k=0}^{d_B-1} |k\rangle |k\rangle . \tag{1.2.19}$$

Having $|\psi\rangle$ written in this way and using that

$$A \otimes \mathbb{1} \sum_{k=0}^{d_B-1} |k\rangle |k\rangle = \mathbb{1} \otimes A^T \sum_{k=0}^{d_B-1} |k\rangle |k\rangle , \tag{1.2.20}$$

where $A^T$ is the transpose of $A$, we have that the reduced density operators of $|\psi\rangle$ read

$$\begin{aligned} \rho_A &= AA^\dagger \\ \rho_B &= A^T A^*. \end{aligned} \tag{1.2.21}$$

The so-called *singular value decomposition (SVD)* of $A$ reads

$$A = U\Sigma V^\dagger, \tag{1.2.22}$$

where $U$ is a $d_A \times d_A$ unitary matrix and $V$ is a $d_B \times d_B$ unitary matrix. $\Sigma$ is a $d_B \times d_A$ diagonal matrix where the last rows $\{d_B + 1, ..., d_A\}$ are 0 and the diagonal elements $\{\lambda_i\}$ are real and nonnegative and fulfill

$$\sum_{i=0}^{d_B-1} \lambda_i^2 = 1, \tag{1.2.23}$$

since physical states must be normalized. Let $\{|u_i\rangle \in \mathcal{H}_A\}$ be the first $d_B$ column vectors of $U$ and $\{|v_i\rangle \in \mathcal{H}_B\}$ the ($d_B$) column vectors of $V$. Note that both $\{|u_i\rangle\}$ and $\{|v_i\rangle\}$ form a basis for $\mathbb{C}^{d_B}$. Then, we can write $|\psi\rangle$ in the so-called *Schmidt decomposition*,

$$|\psi\rangle = \sum_{i=0}^{d_B-1} \lambda_i |u_i\rangle |v_i\rangle . \tag{1.2.24}$$

The coefficients $\{\lambda_i\}$ are called the *Schmidt coefficients* and $d_B$ is the *Schmidt rank*. Note that applying local unitaries to $|\psi\rangle$ will only change the local bases $\{|u_i\rangle\}$ and $\{|v_i\rangle\}$.

Regarding the Schmidt decomposition, the reduced density operators of $|\psi\rangle$ read

$$\begin{aligned} \rho_A &= \sum_{i=0}^{d_B-1} \lambda_i^2 \, |u_i\rangle \langle u_i| \\ \rho_B &= \sum_{i=0}^{d_B-1} \lambda_i^2 \, |v_i\rangle \langle v_i| \, . \end{aligned} \tag{1.2.25}$$

The Schmidt decomposition is a very important tool in quantum information. As a reason for that, it allows us to directly compute the amount of bipartite entanglement of a state $|\psi\rangle$ written as in (1.2.24). In particular, from equation (1.2.25) it is straightforward to see that the entanglement (entropy) among the subsystems $A$ and $B$ reads

$$E_E(|\psi\rangle) = -\sum_{i=0}^{d_B-1} \lambda_i^2 \log(\lambda_i^2). \tag{1.2.26}$$

### 1.2.3 Multipartite entanglement in pure states

So far we have introduced the concept of entanglement in bipartite states (or multipartite states for which we consider only one bipartite splitting). This case is well understood and the tools required for its analysis are usually the ones presented above. However, the structure of multipartite entanglement is much more complicated and presents a much richer phenomenology [6, 7, 8], exhibiting different SLOCC classes [8]. Here, we will note the fundamental difference among bipartite and multipartite entanglement by considering the particular case of three qubit systems, which is the simplest mutlipartite system which exhibits a different behaviour than bipartite systems. To shorten the notation, we will usually denote the reduced density operator corresponding to one local subsystem as *local reduction*.

#### SLOCC classes for three qubits

The rich structure of multipartite entanglement was first introduced in [8], where it was shown that for systems of four qubits, there exist already infinitely many inequivalent SLOCC classes, while for three qubit systems, there are two SLOCC classes.

One of those classes is the *GHZ class*. By convention, its representative is the *GHZ state* $|GHZ\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$,

$$|GHZ\rangle = \frac{1}{\sqrt{2}}\big( |0\rangle\,|0\rangle\,|0\rangle + |1\rangle\,|1\rangle\,|1\rangle \big). \tag{1.2.27}$$

The $GHZ$ state has the property that any local reduction is maximally mixed, i.e.,

$$\rho_A = \rho_B = \rho_C = \mathbb{1}, \tag{1.2.28}$$

from which some particular properties follow. For example, a Bell state can be obtained in any two of the three parties sharing the $GHZ$ state by means of LOCC [8]. It has also

the property that any bipartite reduction $\rho_{XY}$, with $X$ and $Y$ denoting two different parties within the set $\{A, B, C\}$, is a separable state. Therefore, it is fragile against an undesired measurement or loss of any of the three qubits.

The other distinguished class for 3-qubit systems is the *W class*. By convention, its representative is the *W state* $|W\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$,

$$|W\rangle = \frac{1}{\sqrt{3}}\big( |1\rangle |0\rangle |0\rangle + |0\rangle |1\rangle |0\rangle + |0\rangle |0\rangle |1\rangle \big). \tag{1.2.29}$$

The reduction to any two qubits $X$ and $Y$ of the $W$ state reads

$$\rho_{XY} = \frac{2}{3} \left|\Psi^+\right\rangle \left\langle\Psi^+\right| + \frac{1}{3} |00\rangle \langle 00| . \tag{1.2.30}$$

It can be shown that the state $\rho_{XY}$ given above maximizes several entanglement measures for bipartite mixed states [8] over the set of two-qubits mixed states. Therefore, in contrast to $GHZ$ state, $W$ state is robust against a measurement of a local party.

**Monogamy of entanglement**

Let us illustrate another fundamental difference among bipartite and multipartite entanglement with the following example. Let $A$, $B$ and $C$, share a three-partite pure state $|\psi\rangle$. The so-called *no-cloning Theorem* implies that if a pure bipartite state shared among parties $A$ and $B$ maximizes a bipartite entanglement measure, then a pure bipartite state shared among $B$ ($A$) and $C$ must be separable [9].

This fact is a particular case of a phenomenon called *monogamy of entanglement* which arises when we consider more than two parties. Following [10], we will introduce this concept for three qubits. To that end, we first define the *tangle*, an entanglement measure for bipartite mixed states which corresponds to the square of the concurrence. That is, given a mixed state $\rho$ describing two qubits, the tangle $\tau(\rho)$ reads

$$\tau(\rho) = C(\rho)^2. \tag{1.2.31}$$

Consider now a system of three qubits in which a pure state $|\psi\rangle$ is shared among the local parties $A$, $B$ and $C$. We define $\tau_{A|B} := \tau(\rho_{AB})$, where $\rho_{AB}$ is the reduction to parties $A$ and $B$ of the state $|\psi\rangle$. Since $|\psi\rangle$ is a pure state, $\rho_{BC}$ has has at most two nonzero eigenvalues. Taking those two values and the two eigenvalues of $\rho_A$, we can define the concurrence for those four values [11] and hence we can define its square, $\tau_{A|BC}$. With those definitions, in [10] it was shown that

$$\tau_{A|BC} \geq \tau_{A|B} + \tau_{A|C}. \tag{1.2.32}$$

If party $A$ is maximally entangled with party $B$, then we have $\tau_{A|BC} = \tau_{A|B} = 1$ and hence $\tau_{A|C} = 0$, which is the particular case stated above and can be derived from the no-cloning Theorem.

Following [11], we will finish this section connecting the two discussions above by means of understanding a bit better how the tangle describes the different types of entanglement in systems of three qubits. Considering a pure state $|\psi\rangle$ shared among three qubits $A$, $B$ and

$C$, let us define the following quantities,

$$\begin{aligned}\tau_1(|\psi\rangle) &= \frac{1}{3}\big(\tau_{A|BC} + \tau_{B|AC} + \tau_{C|AB}\big)\\ \tau_2(|\psi\rangle) &= \frac{1}{3}\big(\tau_{A|B} + \tau_{B|C} + \tau_{C|A}\big)\\ \tau_3(|\psi\rangle) &= \frac{1}{3}\big(\tau_{A|BC} - \tau_{A|B} - \tau_{A|C}\big)\end{aligned} \tag{1.2.33}$$

$\tau_1(|\psi\rangle)$ measures the mean entanglement across each of the bipartitions, and it is maximized by the $GHZ$ state. $\tau_2(|\psi\rangle)$ measures the mean entanglement within pairs of local parties, and it is maximized by the $W$ state. It can be shown that [10]

$$\tau_1(|\psi\rangle) \geq \tau_2(|\psi\rangle). \tag{1.2.34}$$

$\tau_3(|\psi\rangle)$, called *residual entanglement* or *3-tangle*, measures the fraction of entanglement which can not be described by considering only bipartite reductions.

As we will see in section 1.3, in this thesis we are interested in states which have a peculiar kind of entanglement. In the particular case of three qubits, we are interested in the states within the $GHZ$-class, which has the properties

$$\tau_1(|GHZ\rangle) = 1, \quad \tau_3(|GHZ\rangle) = 1. \tag{1.2.35}$$

For three qubits, more monogamy relationships and their link to a tradeoff between classical and quantum correlations have been derived in [12]. The generalization of equation (1.2.32) for $N$ qubits has been derived in [7]. It was shown that given a quantum system of $N$ qubits $\{1, ..., N\}$, and defining the tangle in a similar way as above, the following condition must hold,

$$\tau_{1|2,...,N} \geq \tau_{1|2} + \cdots + \tau_{1|N}. \tag{1.2.36}$$

Monogamy relations for other entanglement measures have been studied (see [13, 14] and references therein). In particular, monogamy relations for nonbinary systems have been proposed in [15] and [9].

## 1.3 k-uniform states and Absolutely Maximally Entangled (AME) states

In the previous section we discussed that multipartite entanglement has a much richer and more complicated structure than the bipartite entanglement by considering the example of three qubits. In this thesis, we are interested in one specific type of multipartite entanglement, which is the amount of entanglement present within all bipartitions of the whole system. More precisely, we are interested in the states that maximize this entanglement, called *k-uniform* states. Here we will introduce those states, with special emphasis on a particular set of states called *AME* states. We will also review some applications of AME states in quantum information and related fields.

### 1.3.1 Definition of k-uniform states and AME states

Consider a system of $N$ qudits described by a pure state $|\psi\rangle \in \mathbb{C}^{d^{\otimes N}}$. Consider a subset $S$ of $k \leq \lfloor N/2 \rfloor$ qudits and its complementary subset $S^c$ of $N-k$ qudits. Let $\rho_S$ be the reduced density operator describing the subset $S$. The entanglement between $S$ and $S^c$ can be computed by the Von Neumann entropy of the operator $\rho_S$, which is maximal if

$$\rho_S = \frac{1}{d^k}\mathbb{1}. \tag{1.3.1}$$

We say that $|\psi\rangle$ is *k-uniform* if for any subsystem $S$ of size $k \leq \lfloor N/2 \rfloor$, equation (1.3.1) is fulfilled. An entanglement measure which is efficient to compute and particularly useful to verify whether or not a given pure state $|\psi\rangle$ is $k$-uniform is the *average linear entropy* $Q_k(|\psi\rangle)$ [16]. Considering all the subsystems $\{S\}$ with $k$ or less parties, we have

$$Q_k(|\psi\rangle) = \frac{d^k}{d^k-1}\left(1 - \frac{k!(N-k)!}{N!}\sum_{|S|=k} tr(\rho_S^2)\right), \tag{1.3.2}$$

which is 1 iff $|\psi\rangle$ is $k$-uniform and 0 iff $|\psi\rangle$ is fully separable. $Q_k(|\psi\rangle)$ measures the average entanglement across all the possible bipartitions in which one of the subsystems is composed by $k$ or less local parties.

An *AME state* shared among $N$ parties in local dimension $d$, $AME(N,d)$, is a $k$-uniform state with $k = \lfloor N/2 \rfloor$. It follows from its definition that all the possible bipartitions are maximally entangled. Let us give two important equivalent definitions of AME states.

1. Consider a quantum state $|\Psi\rangle$ shared among $N$ parties in local dimension $d$. Let us consider a *balanced bipartition* of the $N$ local parties, namely a bipartition $S|S^c$ having the associated Hilbert spaces $\mathcal{H}_S = \mathbb{C}^{d^{\otimes \lfloor \frac{N}{2} \rfloor}}$ and $\mathcal{H}_{S^c} = \mathbb{C}^{d^{\otimes \lceil \frac{N}{2} \rceil}}$. $|\Psi\rangle$ is an AME state if for any choice of $S$, the state $|\Psi\rangle$ can be written as

$$|\Psi\rangle = \frac{1}{\sqrt{d^{\lfloor \frac{N}{2} \rfloor}}} \sum_{i_1,\ldots,i_{\lfloor N/2 \rfloor}=0}^{d-1} |i_1\rangle \cdots |i_{\lfloor N/2 \rfloor}\rangle |\psi_{i_1,\ldots,i_{\lfloor N/2 \rfloor}}\rangle, \tag{1.3.3}$$

   with $|i_1\rangle \cdots \left|i_{\lfloor N/2 \rfloor}\right\rangle \in \mathcal{H}_S$ and $|\psi_{i_1,\ldots,i_{\lfloor N/2 \rfloor}}\rangle \in \mathcal{H}_{S^c}$ being normalized.

2. Let us consider a general quantum state

$$|\Psi\rangle = \sum_{i_1,\ldots,i_N=0}^{d-1} a_{i_1,\ldots,i_N} |i_1\rangle \cdots |i_N\rangle . \tag{1.3.4}$$

   Let $a$ be the tensor with entries $\{a_{i_1,\ldots,i_N}\}$. Let $S$ be a chosen subset of $k \leq \lfloor N/2 \rfloor$ indices and its complementary set $S^c$ of $N-k$ indices. $|\Psi\rangle$ is an $AME(N,d)$ state if for any arbitrary choice of $S$, the tensor $a$ is a map from $\mathcal{H}_S$ to $\mathcal{H}_{S^c}$ which preserves the scalar product. If this condition holds, then $a$ is called a *perfect tensor*.

The question of whether or not an AME state exists given an arbitrary dimension $d$ and number of parties $N$ is currently an open question [17, 18]. As an example, an $AME(4,2)$ does not exist [19]. In general, for any number of parties $N$ there is a local dimension $\tilde{d}$ so

that for all $d \geq \tilde{d}$, an $AME(N,d)$ exists [20]. Let us give some simple examples of specific constructions. For binary systems in local dimension $d$, there is one AME state up to local unitaries, which can be written as

$$\left|\phi_d^+\right\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle\,|i\rangle\,. \tag{1.3.5}$$

For 3-partite systems with local dimension $d$, an example of AME state reads

$$|GHZ_d\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle\,|i\rangle\,|i\rangle\,. \tag{1.3.6}$$

For larger systems, it is in general not obvious whether or not AME states exist. An example of $AME(4,3)$ state reads [21]

$$|AME(4,3)\rangle = \sum_{i,j=0}^{2} |i\rangle\,|j\rangle\,|i+j\rangle\,|i+2j\rangle \tag{1.3.7}$$

and an example of $AME(4,4)$ state reads [22]

$$|AME(4,4)\rangle = \sum_{i,j,k,l=1}^{4} a_{i,j,k,l}\,|i,j,k,l\rangle\,,\ a_{i,j,k,l} = \begin{cases} 1 \text{ if } (i,j,k,l) \ \in E.P.(1,2,3,4) \\ 0 \text{ otherwise} \end{cases}, \tag{1.3.8}$$

where we denote as $E.P.(1,2,3,4)$ the set of even permutations of the digits $\{1,2,3,4\}$. The simplest putative AME state which existence is still open is the state $AME(4,6)$ [23].

### 1.3.2 Applications of AME states

The fact that $k$-uniform states, and in particular AME states, have the property that all reductions to $k$ or less parties are maximally mixed means that by measuring any $k$ qudits one cannot obtain any information *at all* about the original state. This property is in the core of a field of quantum information called *quantum error correction* (see section 2). The link in between $k$-uniform states and quantum codes will be explained in section 5. In addition, the ability of storing information nonlocally has some other applications. Here we will give a short review on the most prominent ones, which are *multipartite teleportation*, *entanglement swapping*, *quantum secret sharing* and *holography*.

#### Multipartite teleportation

Let $A$ and $B$ be two spatially separated local parties. The information stored in an unknown quantum state in $A$ can be reproduced in $B$ by means of LOCC if entanglement is used. This is called *teleportation* and requires sharing a maximally entangled state. The key points of the protocol are presented as follows.

Consider a Bell state $|\phi_{A_1B}\rangle \in \mathcal{H}_{A_1} \otimes \mathcal{H}_B$ shared among two parties, Alice and Bob, who are spatially separated. Suppose Alice has access to the system $A_1$ and to an additional qubit in an *unknown* quantum state $|a\rangle \in \mathcal{H}_{A_2}$, and Bob has access to the system $B$. In [2]

it was shown that Alice and Bob can perform deterministically the transformation

$$|a\rangle \in \mathcal{H}_{A_2} \rightarrow |a\rangle \in \mathcal{H}_B \tag{1.3.9}$$

by means of LOCC. For that, Alice does a measurement in the Bell basis in the subsystems $A_1$ and $A_2$. Since Alice and Bob share a Bell state, this operation will also collapse the state of the subsystem $B$. The outcome of the measurement, which Alice communicates classically to Bob, contains the information of the local operations that Bob needs to do to obtain the state $|a\rangle$ in his subsystem. Such protocol is known as *quantum teleportation*, and it requires sharing a maximally entangled state.

In [21, 22], two protocols which generalize the idea of teleportation to more than two nonbinary parties were designed, using the fact that in AME states all the possible bipartitions are maximally entangled. One type of those protocols is called *parallel teleportation*, and the other is called *open destination teleportation*. Let us introduce them.

*Parallel teleportation.* Consider $N$ local parties sharing a quantum state $|\Psi\rangle$. Consider the bipartition $S|S^c$ and the corresponding Hilbert subspaces $\mathcal{H}_S$ and $\mathcal{H}_{S^c}$ respectively, were the spatially separated subsystems $S$ and $S^c$ are composed by $k$ and $N-k$ parties respectively. Despite the fact that the whole explanation can be done considering arbitrary integer values of $k \geq 1$, and hence the protocol can be done considering $k$-uniform states, we will consider the case $k = \lfloor N/2 \rfloor$, which requires that $|\Psi\rangle$ is an AME state. Teleportation among $S$ and $S^c$ can be done as follows.

Let us write the shared AME state $|\Psi\rangle$ as

$$|\Psi\rangle = \frac{1}{\sqrt{d^{\left\lfloor \frac{N}{2} \right\rfloor}}} \sum_{i_1,...i_k=0}^{d-1} |i_1, ..., i_k\rangle \, |\psi_{i_1,...,i_k}\rangle \,, \tag{1.3.10}$$

with $|i_1, ..., i_k\rangle \in \mathcal{H}_S$ and $|\psi_{i_1,...,i_k}\rangle \in \mathcal{H}_{S^c}$. For simplicity, we use the notation $|a, b\rangle := |a\rangle \otimes |b\rangle$. It is clear that if the parties in $S^c$ perform a joint quantum operation to do the transformations

$$\begin{aligned} |\psi_{i_1,...,i_k}\rangle &\rightarrow U^\dagger_{S|S^c} \, |\psi_{i_1,...,i_k}\rangle = |i_1\rangle \cdots |i_k\rangle \, |0\rangle \quad (N \text{ odd}) \\ |\psi_{i_1,...,i_k}\rangle &\rightarrow U^\dagger_{S|S^c} \, |\psi_{i_1,...,i_k}\rangle = |i_1\rangle \cdots |i_k\rangle \quad (N \text{ even}), \end{aligned} \tag{1.3.11}$$

where $U^\dagger_{S|S^c}$ is the unitary operator

$$U_{S|S^c} = \sum_{i_1,...i_k=0}^{d-1} |\psi_{i_1,...,i_k}\rangle \, \langle i_1, ..., i_k| \tag{1.3.12}$$

each local party in $S$ shares the generalized Bell state $\left|\phi^+_d\right\rangle$ with a local party in $S^c$ and the protocol is reduced to the bipartite teleportation protocol.

*Open destination teleportation.* Let $|\Psi\rangle$ be an AME state shared among $N$ parties. Let us consider the bipartition $S|S^c$, where the subsets $S$ and $S^c$ have $k = \lfloor N/2 \rfloor$ and $N - k$ parties respectively. One of the parties in $S$, called the *dealer*, has access to an ancillary system in the state $|a\rangle = \sum_{r=0}^{d-1} |a_r\rangle \in \mathbb{C}^d$. The dealer teleports the state $|a\rangle$ by performing

a Bell measurement among her ancillary system and the system which is part of the AME state $|\Psi\rangle$. This operation does the transformation

$$|a\rangle\,|\Psi\rangle \to |\Phi'\rangle = \frac{1}{\sqrt{d^{\lfloor \frac{N}{2} \rfloor}}} \sum_{i,s_1,\ldots,s_{k-1}=0}^{d-1} b_{pq,i}\,|s_1\rangle_{S_1} \cdots |s_{k-1}\rangle_{s_{k-1}}\,|\phi(k,i)\rangle_{S^c}\,, \tag{1.3.13}$$

where $\{S_1,...,S_{k-1}\}$ represents the local parties in $S$, $S_k$ denotes the dealer, and $b_{pq}$ labels the outcome of the Bell measurement, which is communicated by classical communication to all the parties. $\{|\phi(k,i)\rangle\}$ belong to the Hilbert space of the dealer. Such operation teleports the information about the state $|a\rangle$ to the subset $S^c$, but none of the local parties has the state $|a\rangle$ in her system. This fact gives the name "open destination teleportation" to the protocol. As a next step, the parties in $S^c$ decide which party $S_i \in S$ will receive the state $|a\rangle$. Then they perform a unitary operation similarly as in (1.3.11) so that only Bell states are shared among parties in $S$ and parties in $S^c$, followed by a Bell measurement among qudits $S_k$ and $S_i$, which outcome $(r,s)$ is made public. Then, the state of $S_i$ reads

$$(Z^r X^s)^\dagger (Z^p X^q)^\dagger\,|a\rangle\,. \tag{1.3.14}$$

Since the outcomes $(r,s)$ and $(p,q)$ have been made public, $S_i$ can recover the state $|a\rangle$ with local operations.

**Entanglement Swapping**

Let Alice, Bob and Carol be spatially separated. Alice has access to two physical systems $A_1$ and $A_2$, Bob has access to two physical systems $B_1$ and $B_2$ and Carol has access to two physical systems $C_1$ and $C_2$. Alice and Bob share a maximally entangled state $|\phi_{AB}\rangle \in \mathcal{H}_{A_1} \otimes \mathcal{H}_{B_1}$. Bob and Carol share a maximally entangled state $|\varphi_{BC}\rangle \in \mathcal{H}_{B_2} \otimes \mathcal{H}_{C_1}$.

In [24] it was shown that it is possible to create deterministically a maximally entangled state $|\psi_{AC}\rangle \in \mathcal{H}_{A_2} \otimes \mathcal{H}_{C_2}$ shared among Alice and Carol by means of LOCC. This is called *entanglement swapping* and it is possible only if $|\phi_{AB}\rangle$ and $|\varphi_{BC}\rangle$ are maximally entangled states.

In [22] it was shown that entanglement swapping can be generalized to multipartite settings by considering AME states. More precisely, the following corollary was proven.

**Corollary 1** ([22]). *Suppose each set of parties* $\{1,...,2k\},\{k+1,...,3k\},...,\{mk+1,...,(m+1)k\},...,\{Mk+1,...,(M+1)k\}$, *where* $m \in \mathbb{Z}_M$, *shares an* $AME(2k,d)$ *state*

$$|\Psi\rangle = \frac{1}{\sqrt{d^{\frac{N}{2}}}} \sum_{i_1,\ldots,i_k=0}^{d-1} |i_1,...,i_k\rangle\, U\,|i_1,...,i_k\rangle\,, \tag{1.3.15}$$

*which does not depend on* $m$, *with the peculiarity that* $U^M\,|i_1,...,i_k\rangle$ *is LU-equivalent to* $U\,|i_1,...,i_k\rangle$ *for all elements of the computational basis* $\{|i_1,...,i_k\rangle\}$ *up to permutations of local parties. Suppose also that each party holds an auxiliary quantum system. If each of the parties* $\{k+1,...,Mk\}$ *performs a Bell measurement on the system which shares* $|\Psi\rangle$ *and the auxiliary system, then the parties* $\{1,...,k,Mk+1,...,(M+1)k\}$ *will share an* $AME(2k,d)$ *state.*

Let us give the following example. Consider three sets of local parties, $\{A,B,C,D\}$, $\{C,D,E,F\}$ and $\{E,F,G,H\}$. Each party has access to two systems, labeled by 1 and 2.

Each of the three sets shares respectively the state $|\Psi\rangle_{A_1B_1C_1D_1}$, $|\Psi\rangle_{C_2D_2E_1F_1}$, $|\Psi\rangle_{E_2F_2G_1H_1}$, where $|\Psi\rangle$ is the state given in (1.3.8), i.e.,

$$|\Psi\rangle = \frac{1}{3}\sum_{i,j=0}^{2} |i,j\rangle\, U\, |i,j\rangle \tag{1.3.16}$$

with

$$U = \sum_{i,j=0}^{2} |i\oplus j, i\oplus 2j\rangle\, \langle i,j|\,. \tag{1.3.17}$$

By computing $U^2\,|i,j\rangle\ \forall i,j$, permuting the two parties of each resulting state and applying a unitary transformation which permutes $|1\rangle$ and $|2\rangle$ in the second party, it can be seen that $U^3\,|i,j\rangle$ is LU-equivalent to $U\,|i,j\rangle$ for all $i,j\in\mathbb{Z}_3$ up to permutations of parties [22]. Hence, if each of the parties $C$, $D$, $E$ and $F$ perform a Bell measurement in their two qutrits, then the parties $A$, $B$, $G$ and $H$ will share an $AME(4,3)$ state.

**Quantum secret sharing**

This application of AME states was discovered in [21] and it consists of a technique in quantum cryptography called *quantum secret sharing* which was introduced in [25].As a toy model to capture the essence of this technique, suppose we want to physically store an important secret password to prevent us from forgetting it. On one hand, there exists the danger of losing such information by means of physical processes. On the other hand, if a spy gets access to the physical setup where the password is stored, the information will not be secret anymore. To solve those two facts simultaneously, it might be useful to store our password in three different physical setups, in such a way that none of them contains the whole information, but any two of them together do. This is called *secret sharing*, and it is generally defined as sharing a secret among $N$ independent physical systems, so that only special subsets of them give access to the secret. If the physical systems where the information is stored are quantum, then we are allowed to store the information nonlocally by means of quantum entanglement, and the technique is called *quantum secret sharing (QSS)* [25]. Consider a quantum secret sharing protocol in which a quantum state $|\psi\rangle$ is shared among $N$ local parties in local dimension $d$, so that the special subsets which can reveal the whole information by means of measurements are all the possible subsets of $k+1$ or more parties. Let us assume also that any measurement which can be done on a subset of $k$ parties or less reveals absolutely no information about the state $|\psi\rangle$. This is a type of QSS protocol called *quantum (k,n) threshold scheme*. In [21, 22] it was shown that any $AME(2m,d)$ is equivalent to a quantum $(m, 2m-1)$ threshold scheme. Since this application for AME states is not simply the generalization of well known protocols for bipartite systems, let us illustrate this connection by introducing the following example of a quantum $(2,3)$ threshold scheme. We will use the word *qutrit* to refer to a 3-dimensional qudit and the notation $|abc\rangle := |a\rangle\otimes|b\rangle\otimes|c\rangle$.

Consider a message encoded in a qutrit,

$$|\Phi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle + \gamma\,|2\rangle\,, \tag{1.3.18}$$

with $\alpha,\beta,\gamma\in\mathbb{C}$ fulfilling the condition $|\alpha|^2+|\beta|^2+|\gamma|^2=1$. Let us store the information

of this qutrit in three parties $A$, $B$ and $C$ by means of the following mapping,

$$\begin{aligned} |0\rangle &\to |0_L\rangle = |000\rangle + |111\rangle + |222\rangle \\ |1\rangle &\to |1_L\rangle = |012\rangle + |120\rangle + |201\rangle \\ |2\rangle &\to |2_L\rangle = |021\rangle + |102\rangle + |210\rangle \ . \end{aligned} \tag{1.3.19}$$

Let us introduce the following notation. We call *logical qutrits* the states $\{|0_L\rangle, |1_L\rangle, |2_L\rangle\}$. We further define

$$|\Phi_L\rangle = \alpha\,|0_L\rangle + \beta\,|1_L\rangle + \gamma\,|2_L\rangle\,. \tag{1.3.20}$$

To see that each local party has no information about the information encoded in $|\Phi_L\rangle$, note that any two terms which belong to different logical qutrits are mutually orthogonal in exactly two local qutrits. Together with the fact that the logical qutrits are AME states, we have that any reduction to one party reads

$$\rho_A = \rho_B = \rho_C = \mathbb{1}, \tag{1.3.21}$$

independently of the coefficients $\alpha$, $\beta$ and $\gamma$, which is an equal mixture of $|0_L\rangle$, $|1_L\rangle$ and $|2_L\rangle$ and hence we gain no information about the original message encoded in $|\phi\rangle$.

Let us now show that the state $|\Phi\rangle$ can be obtained from two local parties. We will see that for parties $A$ and $B$, and a similar argument works for other pairs of parties.

Consider the state $|\Phi_L\rangle$ with the 3-partite terms $|0_L\rangle$, $|1_L\rangle$ and $|2_L\rangle$ written as in (1.3.19). Consider the reduction $\rho_{AB} = tr_C\big(\,|\Phi_L\rangle\,\langle\Phi_L|\,\big)$ and the unitary operation

$$\rho_{AB} \to \sigma_{AB} = (CX)_A (CX)_B\,\rho_{AB}\,(CX)_B^\dagger (CX)_A^\dagger, \tag{1.3.22}$$

where $(CX)_A = X^i \otimes \sum_{i=0}^2 |i\rangle\,\langle i|$ and $(CX)_B = \sum_{i=0}^2 |i\rangle\,\langle i| \otimes X^i$ are the so-called *control-X* gates. We are left with the separable state

$$\sigma_{AB} = \big(\alpha\,|0\rangle + \beta\,|1\rangle + \gamma\,|2\rangle\,\big)\big(\alpha\,\langle 0| + \beta\,\langle 1| + \gamma\,\langle 2|\,\big) \otimes \big(\,|0\rangle + |1\rangle + |2\rangle\,\big)\big(\,\langle 0| + \langle 1| + \langle 2|\,\big), \tag{1.3.23}$$

which recovers the original message $|\Phi\rangle\,\langle\Phi|$. By proceeding similarly for different pairs of parties, it can be seen that similar results hold for reduced density operators corresponding to the remaining pairs of parties [25].

### Perfect tensors for toy models for the AdS/CFT correspondence

The most prominent application of AME states was discovered in [26] and is related to *quantum gravity*, an area of Physics which aims to find a unified description of both quantum field theory and general relativity. Although quantum information provides some of the approaches by means of which this problem is tackled [27], a proper introduction requires several concepts which are unrelated to quantum information. Since introducing such background is inappropriate in this thesis, we will restrict ourselves to a small amount of such concepts which allows us to provide an intuitive idea of how AME states have an application in such field.

The current theory of gravity is based on the so-called *Einstein equations*. Those equations contain a real parameter $\Lambda$ called *cosmological constant*. For a certain subset of the solutions to Einstein equations, the sign of $\Lambda$ determines the sign of the curvature of the $D$-dimensional spacetime, $S \in \mathbb{R}^D$. Depending on the curvature, different possible spacetimes

have been proposed do describe our universe according to the following classification:

$$\begin{gathered}\Lambda > 0 \rightarrow \textit{de Sitter spacetime} \\ \Lambda < 0 \rightarrow \textit{Anti-de Sitter (AdS) spacetime} \\ \Lambda = 0 \rightarrow \textit{Minskowski spacetime}\end{gathered} \tag{1.3.24}$$

We will first give a property of the AdS spacetime. Then, we will give a property of the Minskowski spacetime. We will see that those two properties are isomorphic, which gives rise to the so-called *AdS/CFT* conjecture.

AdS spacetime is composed of a $(D-1)$-dimensional spacetime called *boundary* and the $D$-dimensional hypervolume enclosed by the boundary, called *bulk*. The solutions of Einstein equations are invariant under certain coordinate transformations, and those symmetries depend on the spacetime which we consider. In the case of an AdS spacetime $S_{AdS} \in \mathbb{R}^D$, they form a group which is called $SO(D-1,2)$ and is represented as

$$SO(D-1,2) = \{A \in \mathbb{R}_{(D+1)\times(D+1)} : AgA^T = g, \det(A) = 1\} \tag{1.3.25}$$

where $A^T$ is the transposition of $A$, $\det(A)$ is the determinant of $A$ and $g \in \mathbb{R}_{(D+1)\times(D+1)}$ is a diagonal matrix which is called *metric* and has $D-1$ entries equal to 1 and two entries equal to $-1$.

We will now focus on a Minskowski spacetime. Let two curves $f$ and $t$ of the same spacetime $S \in \mathbb{R}^D$ coincide in $z_0 \in S$. A certain coordinate transformation $\Gamma$ is called *locally conformal invariant in* $z_0$ if in the local coordinate $z_0$, (1) the angle among the tangent vectors of the two curves, $\vec{v}(f)_{z_0}$ and $\vec{v}(t)_{z_0}$, is preserved, and (2) both $\vec{v}(f)_{z_0}$ and $\vec{v}(t)_{z_0}$ are rescaled by the same factor $a$. Although a precise definition of conformal invariance involves more concepts, the conditions (1) and (2) are sufficient to provide an intuitive definition and we restrict ourselves to them for the sake of simplicity. A *conformal transformation* is a coordinate transformation which is conformal at all points of $S$. For a Minskowski spacetime $S_{Mink} \in \mathbb{R}^{D-1}$, the set of conformal transformations form the group $SO(D-1,2)$. A *conformal field theory (CFT)* is a quantum field theory so that the equations by which the phenomena are described are invariant under conformal transformations.

This coincidence gave rise to the conjecture that the phenomena which can occur according to a quantum gravity theory in an *AdS* spacetime of dimension $D$, namely the bulk, can be completely characterized by phenomena which can occur according to a conformal field theory in a Minskowski spacetime of dimension $D-1$, namely the boundary, and viceversa [28]. This conjecture is called *AdS/CFT correspondence* and it has been verified for certain theories of quantum gravity and certain quantum field theories. As its main applications, it provides a new formulation of a set of theories for quantum gravity called *string theories*, and it is used to study a phenomenon in quantum field theory called *strong coupling*.

The problem of mapping the phenomena in the bulk onto phenomena in the boundary is called *bulk reconstruction* and it has been tackled in [27] in the language of quantum error correction. More precisely, it was proposed that each local point in the bulk has associated a logical quantum state which code subspace belongs to the boundary. Thus, phenomena in the bulk are described by logical operations in the corresponding code subspaces in the boundary, and viceversa. In [26], the first toy model for this idea was developed by considering a special

type of codes called *holographic codes*, which are defined by considering perfect tensors to encode the physical qudits into the logical qudits. A good understanding of how such toy model was constructed would require introducing several concepts which are not in the scope of this thesis. Therefore, we will restrict ourselves to the intuitive idea that since perfect tensors are isometries from any set of indices to their complementary set, by considering perfect tensors for the mapping from the physical qudits to the logical qudits, that is, from the bulk to the boundary, we ensure that the information about phenomena in the bulk and inthe boundary is perfectly transferred in between those two spaces.

# Chapter 2

# Classical and quantum error correction

One of the main problems for developing real quantum computers is due to the fact that qubits interact with their environment and this leads to quantum errors. Therefore, correcting such errors is on the scope of current research in quantum information. Moreover, entanglement is needed for quantum error correction. We will explore the link among highly entangled states and quantum error correcting codes in section 5. In the current section we will provide a description of the basics in both classical and quantum error correction, with special emphasis on those concepts which are important for the study of entangled states.

We will first introduce classical error correction and then quantum error correction, which is fundamentally different. We will focus on an important type of codes, namely *stabilizer codes*, which are widely used in quantum information. We will also present *graph states* and *graph codes* as an example of stabilizer codes. Finally we will present *additive codes* and how they are used to construct stabilizer codes for non-binary systems.

## 2.1 Classical error correction

Classically, the only error which can occur is a bit flip error. To protect the information from this error, we need to encode our message in a longer message containing the original information and some redundancy. As an example, suppose we want to protect a binary message encoded in the single bit strings 0 and 1. We can encode the information in a *repetition code*, for instance

$$\begin{aligned} 0_L &= 000 \\ 1_L &= 111\,. \end{aligned} \tag{2.1.1}$$

The bit strings where the message is contained, which in the example (2.1.1) are $0_L$ and $1_L$, are called *logical* strings. They are encoded in *physical* strings or *codewords*, which in our example correspond to 000 and 111. If there is a bit flip on one of the three digits in the codewords of the example (2.1.1), the other two digits uniquelly determine the original codeword. This is called *majority vote* criteria, as we will explain later on. If there is an error on two or more of the three digits, any decoding procedure will flip the original logical string. This is called a *logical error*. Once the basic idea of error correction is introduced by this simple example, let us now present a more general approach to classical error correction.

### Classical codes

A classical linear code $C$, denoted $C[N,k,\delta]_d$, is a set of $d^k$ codewords $\{x\}$ of $N$ digits each encoding $d^k$ logical strings $\{x_L\}$ of $k$ digits each.

As we have seen in the example (2.1.1), we need redundancy to protect from errors, and therefore in general we need $N > k$. The *weight* of a classical codeword, $wt(x)$, is the number of nonzero digits in it. The *distance* among two codewords is the number of digits in which they differ, and the distance $\delta$ of a code $C$ is the minimal distance among the codewords in $C$. For bit strings, the distance among two codewords $x_1$ and $x_2$ reads $\delta(x_1,x_2) = wt(x_1 \oplus x_2)$, where $\oplus$ denotes addition $mod(2)$. If two codewords having distance $\delta$ suffer from an error of weight $t$ each, we will be able to correct from such error only if the two codewords remain orthogonal after the errors. Therefore, a code with distance $\delta = 2t+1$ allows us to correct up to $t$ bit flips.

Each classical code $C = \{x\}$ is defined by a *generator matrix* $G \in \mathbb{N}_d^{N\times k}$ such that

$$Gx_L = x, \tag{2.1.2}$$

$$Hx = 0 \quad \forall x \in C. \tag{2.1.3}$$

The *dual* $C^\perp$ of a code $C$ is a code with generator matrix $G^\perp := H^T$ and parity check matrix $H^\perp := G^T$, where the subindex $T$ stands for the transpose operation. A code $C$ is said to be *self-dual* iff $C = C^\perp$, and *weakly self-dual* or *self-orthogonal* iff $C \subset C^\perp$. A classical code $C$ is *pure* iff $C^\perp$ has no elements of weight less than the distance of the code $\delta$.

### Error syndrome to correct errors

Consider an error $e$ so that $x \to x' = x \oplus e$. Applying the parity check matrix to the corrupted codeword $x'$ leads to

$$Hx' = Hx + He = He, \tag{2.1.4}$$

which does not depend on the original codeword $x$ but only on $e$. In this sense $He$ is called the *error syndrome*.

One possible procedure to correct from $e$ is to search the codeword $x$ so that the distance to $x'$ is minimized, which will give us the codeword before the error happened iff $wt(e) \leq t$. This is called *majority vote* criteria and it requires calculating

$$wt(x - x') \quad \forall x \in C, \tag{2.1.5}$$

which leads to exponentially many calculations with respect to the size $k$ of the logical strings. A more efficient method uses the fact that each error syndrome $He$ uniquely defines the error $e$ up to a certain weight $t$ of $e$. Namely, among all the possible errors compatible with the syndrome $He$, we compute the one with minimal weight, say $e_{min}$, which is an efficient task [29]. As long as $wt(e) \leq t$ for a binary code with distance $\delta = 2t+1$, assuming that $e_{min}$ is the error that occurred is equivalent to assuming that $x$ is the closest codeword to $x'$. Thus, we can identify an error and correct it by computing $Hx'$ iff $wt(e) \leq t$.

Those are the very basics to correct bit flips, also called *classical errors*. However, if we want to protect information from quantum errors, we have more difficulties to overcome. First, the possibilities for quantum errors are continuous, because not only bit flip errors

are possible, but also phase flips and any combination in between a bit flip and a phase flip can occur. Second, quantum information cannot be cloned, which prevents from using repetition codes. Third, if we do a projective measurement in order to obtain information about the output of the channel as we do in classical error correction by applying the parity check matrix, we will in general destroy the information encoded within the superposition of states. Hence we need a new approach to deal with quantum errors.

## 2.2 Quantum channel

### CPTP map and error bases

Let us assume we prepare a pure quantum state $|\psi\rangle$, initially in a product state with its environment. Without loss of generality the environment is initially also in a pure state $|0\rangle_E$, so that the global state reads

$$|\psi\rangle_{global} = |\psi\rangle |0\rangle_E . \tag{2.2.1}$$

In the most general case, the system evolves under a global unitary $U$ and $|\psi\rangle_{global}$ becomes entangled. When we trace out the environment in $|\psi\rangle_{global}$ state after such evolution, the resulting state is generally described with a *quantum channel*, which is a completely positive and trace-preserving (CPTP) linear map

$$\mathcal{M} : |\psi\rangle \langle\psi| \to \rho = \sum_i M_i |\psi\rangle \langle\psi| M_i^\dagger, \tag{2.2.2}$$

with the completeness relationship

$$\sum_i M_i^\dagger M_i = \mathbb{1}. \tag{2.2.3}$$

This can be read as follows. Since $\mathcal{M}$ is trace preserving, $Tr(M_i |\psi\rangle \langle\psi| M_i^\dagger)$ can be read as the probability that an error $M_i$ occured, transforming the initial state into $|\psi\rangle \to \mathcal{N} M_i |\psi\rangle$, where $\mathcal{N}$ is a normalization factor.

In order to explain how errors can be corrected, we note that an error $M$ acting on $\mathbb{C}^{d^{\otimes N}}$ can be expanded in a basis of local operators, $\{\boldsymbol{A}_i = A_i^{(1)} \otimes A_i^{(2)} \otimes \dots A_i^{(N)}\}$ which are orthonormal under the Hilbert-Schmidt product, $tr(\boldsymbol{A}_i \boldsymbol{A}_j^\dagger) \propto \delta_{ij}$. Since $\mathcal{M}$ is linear, correcting a subset $S_A$ of $\{\boldsymbol{A}_i\}$ suffices to correct all the subspace $\varepsilon$ spanned by linear combinations of the elements in $S_A$. If the elements of such basis form a multiplicative group up to phases, which means that $\{\boldsymbol{A}_i\}$ contains the identity and therefore $tr\boldsymbol{A}_i = \delta_{\boldsymbol{A}_i,\mathbb{1}}$, then $\{\boldsymbol{A}_i\}$ is called a *nice error basis*. For qubits we will choose the $N$-qubit Pauli group up to phases, $\mathcal{P}^{\otimes N} = \{\sigma_x, \sigma_y, \sigma_z, \mathbb{1}\}^{\otimes N}$ [30]. For nonbinary systems we will consider the generalization $\mathcal{P}_d^{\otimes N}$ (1.1.12).

The following notation is analogous to the one in classical error correction. The set of parties to which an element $E \in \mathcal{P}^{\otimes N}$ acts nontrivially is the *support* of $E$, $supp(E)$. The number of such parties is called *weight*, $wt(E) = |supp(E)|$. According to the standard notation, a quantum error correcting code $C[\![N, k, \delta]\!]_d$ corresponds to the linear subspace spanned by a set of $d^k$ orthogonal states called *codewords* or *physical states* $\{|\psi_i\rangle\} \in \mathcal{H}_d^{\otimes N}$ encoding $d^k$ orthogonal states $\{|\psi_i\rangle\} \in \mathcal{H}_d^{\otimes k}$ called *logical states*. Similarly to the classical case, to correct errors we need $N > k$. If an operation on a codeword gives as a result a different codeword, then such operation is a *logical operation* and it leads to a *logical error*.

The *distance* of a quantum code $\delta$ is the minimal weight of an error in $\mathcal{P}^{\otimes N}$ needed to perform a logical operation.

**Knill-Laflamme Theorem**

In what follows we will present the *Knill-Laflamme condition*, which tells us whether or not a given set of errors can be corrected by a given quantum code. We will explain its proof and analyze its physical meaning.

[[31]] Let $C = \{|\psi_i\rangle\}$ be a quantum error correcting code. A set of errors $\varepsilon = \{M_m\}$ can be corrected by $C$ iff

$$\langle\psi_i| M_a^\dagger M_b |\psi_j\rangle = \delta_{i,j}\zeta_{a,b} \quad \forall M_a, M_b \in \varepsilon, \tag{2.2.4}$$

where $\zeta_{a,b}$ is independent of the codewords $|\psi_i\rangle$ and $|\psi_j\rangle$.

*Proof.* To correct an error $M_m$, we need a *recovery map* $\mathcal{R}$. That is, a CPTP map with the property that maps the corrupted state to the original codeword of the code $C$,

$$\mathcal{R} : \sum_m M_m |\psi_i\rangle \langle\psi_i| M_m^\dagger \to \sum_{r,m} R_r M_m |\psi_i\rangle \langle\psi_i| M_m^\dagger R_r^\dagger = |\psi_i\rangle \langle\psi_i| \in C. \tag{2.2.5}$$

We will first proof Theorem 2.2 assuming the existence of $\mathcal{R}$.

Recall that $\mathcal{M}$ is a linear map and hence any linear combination of correctable errors is also correctable. This implies that we need to consider only a representative set of Kraus operator $\{M_i\} = \varepsilon$ to study the correction properties of a given code. The set of Kraus operators $\{M_m\}$ can be chosen from the global unitary $U$ that governs the interaction among our system and its environment, a basis $\{|\mu_m\rangle\}$ for the environment and the initial state $|e\rangle$ of the environment, as [31]

$$\{M_m\} = \{(\mathbb{1} \otimes \langle\mu_m|_E) U (\mathbb{1} \otimes |e\rangle_E)\}. \tag{2.2.6}$$

From (2.2.5) it follows that given a quantum channel $\mathcal{M}$ and a linear combination of codewords $|\phi\rangle = \sum_{i=1}^k \alpha_i |\psi_i\rangle \in C$, a recovery map $\mathcal{R}$ will bring the (non-normalized) corrupted state $M_m |\phi\rangle$ to the correct state $|\phi\rangle$ iff

$$\forall M_m \in \mathcal{M}, R_r \in \mathcal{R} : \quad R_r M_m |\phi\rangle = \lambda_{r,m} |\phi\rangle . \tag{2.2.7}$$

Due to the linearity of $\mathcal{M}$ and $\mathcal{R}$, $\lambda_{r,m}$ can not depend on $|\phi\rangle$. Therefore, given two codewords $|\psi_i\rangle$ and $|\psi_j\rangle$, we have

$$\begin{gathered} \langle\psi_i| M_a^\dagger M_b |\psi_j\rangle = \langle\psi_i| M_a^\dagger \mathbb{1} M_b |\psi_j\rangle = \\ \sum_r \langle\psi_i| M_a^\dagger R_r^\dagger R_r M_b |\psi_j\rangle = \langle\psi_i|\psi_j\rangle \sum_r \lambda_{a,r}^* \lambda_{b,r} = \zeta_{a,b}\delta_{i,j} \end{gathered} \tag{2.2.8}$$

if and only if $\mathcal{R}$ exists and corrects $\mathcal{M}$.

To see that there always exists a recovery map $\mathcal{R}$ and a set of errors $\varepsilon$ it can correct, one needs to construct $\mathcal{R}$ [31]. □

It is convenient to introduce now some further notation. If the matrix $\zeta = (\zeta_{a,b})$ is not of full rank, the code is said to be *degenerate* with respect to the set of errors $\varepsilon$, and

*non-degenerate* otherwise.

As an overview, this Theorem tells us two conditions for error correction. First, the condition that any two corrupted codewords $|\tilde{\psi}_i\rangle = M_a |\psi_i\rangle$ and $|\tilde{\psi}_j\rangle = M_b|\psi_j\rangle$ must fulfill

$$\langle\tilde{\psi}_j|\tilde{\psi}_i\rangle \propto \delta_{i,j} \tag{2.2.9}$$

in order to correct $M_a$ and $M_b$ is equivalent to not suffering a logical error. This condition tells us that a QECC with distance $2t+1$ can correct errors of weight less or equal than $t$, similarly to the classical case. Second, the coefficients of $\zeta_{a,b}$ must be the same for any codeword: physically, a recovery operator must not reveal any information about the encoded message. The reason for that is that otherwise, learning information about the error would collapse the information contained in the superposition within the quantum codeword.

## 2.3 Stabilizer codes

As we discussed in the end of 2.1, the nature of Quantum Mechanics makes quantum error correction more challenging than classical error correction. The most used and best understood quantum error correcting codes are *stabilizer codes* and they are inspired by classical codes. In this section we will present this type of codes and we will explain how they arise from classical codes.

### Stabilizer formalism

Let us first introduce some notation. Given the N-qubit Pauli group $\mathcal{P}^{\otimes N} := \{\pm 1, \pm i\} \times \{\mathbb{1}, X, Y, Z\}^{\otimes N}$, let us consider an abelian subgroup $S$ with $N-k$ local generators $\{\boldsymbol{s_l}\} = \{\bigotimes_{n=1}^{N} s_l^{(n)}\}$ that does not contain any of the elements in $\{\pm i, -1\} \times \mathbb{1}$ and where $N-k > 0$. The *stabilizer code* defined by $S$ is the $d^k$-dimensional vector eigensubspace of $S$ with eigenvalue 1.

If $k = 0$, the code contains a single state and therefore it is not useful to encode information. States of this type are called *stabilizer states*. They can be highly entangled and they are useful for Quantum Computation tasks [32, 33, 34]. In 2.4 we will present an example of stabilizer codes and states which plays a very important role in quantum information, namely the *graph codes* and *graph states*.

### Quantum error correction for stabilizer codes

Once the stabilizer formalism and its importance in quantum information are introduced, we will explain the correction properties of stabilizer codes. To do so, let us recall that a linear combination of correctable errors is also correctable. Hence, we will restrict ourselves to consider errors in $\mathcal{P}^{\otimes N}$ and we will comment on the correction properties in the general case if it is required.

Let us suppose that a codeword $|\psi\rangle$ of a stabilizer code $C$ suffers from some error in the set $\varepsilon = \{E_i\} \subset \mathcal{P}^{\otimes N}$. We define $E := E_a^\dagger E_b$ with $E_a, E_b \in \varepsilon$.

1. If $E \in S$, the state $E|\psi_i\rangle = |\psi_i\rangle$ is not corrupted. This is the trivial case.

2. Another possibility is that $E \notin S$ and $E$ does *not* commute with all the elements in

$S$. Let us choose an element $\boldsymbol{s}_l \in S$ which anticommutes with $E$. (2.2.4) is fulfilled, as

$$\langle\psi_i| E |\psi_j\rangle = \langle\psi_i| \boldsymbol{s}_l E |\psi_j\rangle = -\langle\psi_i| E\boldsymbol{s}_l |\psi_j\rangle = -\langle\psi_i| E |\psi_j\rangle = 0. \tag{2.3.1}$$

This implies that a set of errors $\varepsilon \notin S$ anticommuting with at least one element in $S$ can be corrected. The procedure for such correction works in the following way.

To identify the error we measure each generator of $S$. For each $\boldsymbol{s_l} \in S$, the eigenvalue of each outcome will be

$$(-1)^{\prod_{n=1}^{N} f_{s_l}^{(n)}}, f_{s_l}^{(n)} = \begin{cases} 0, & \text{if } [s_l^{(n)}, E^{(n)}]=0 \\ 1, & \text{if } \{s_l^{(n)}, E^{(n)}\}=0 \end{cases}, \tag{2.3.2}$$

denoting the commutator as $[a,b] = ab-ba$ and the anticommutator as $\{a,b\} = ab+ba$. If an error occurs, the set of all the outcomes corresponding to the measurements of each generator of the stabilizer group will detect it. In this sense, the function (2.3.2) is called the error syndrome for stabilizer codes.

As we mentioned in the discussion of the Knill-Laflamme Theorem (2.2.4), a linear combination of elements in $\varepsilon$ that leads to a corrupted codeword $|\psi_i'\rangle = \sum_{j\in\varepsilon} \alpha_j E_j |\psi_i\rangle$ must also be correctable. In the case of stabilizer codes, this is particularly solved as follows. When we measure an operator which is a generator of the stabilizer group with the system in the state $|\psi_i'\rangle$, by the postulates of Quantum Mechanics we will collapse the state $|\psi_i'\rangle$ to a codeword which has been corrupted by a single error of the set $\varepsilon$, say, $E_k |\psi_k\rangle$. Once the state has collapsed, the rest of the procedure for error correction works as we have discussed previously.

3. The last scenario consists of errors in the so-called *normalizer* of $S$, $N(S) = \{E_i\} \notin S : [E_i, s_l] = 0 \ \forall i, l$. In this case the codewords are projected to the code subspace instead to an orthogonal subspace. The normalizer of $S$ is the set of logical operators for the code with stabilizer $S$, so that errors in $N(S)$ can not be detected.

**Parity check matrix for stabilizer codes**

We have seen that the generators of $S$ for stabilizer codes play the role of the parity check matrices for classical codes, in the sense that they give us the error syndrome. To deepen this analogy, consider a stabilizer code with $S = \langle \boldsymbol{s_1}, ..., \boldsymbol{s_L} \rangle$. We define a parity check matrix in the stabilizer formalism as a $L \times 2N$ matrix of the following form,

$$H(S) = (H(S)_X | H(S)_Z) = \left(\begin{array}{ccc|ccc} \tilde{s}_1^{(1)} & \dots & \tilde{s}_1^{(N)} & \tilde{s}_1^{(N+1)} & \dots & \tilde{s}_1^{(2N)} \\ \vdots & \ddots & & \vdots & \ddots & \\ \tilde{s}_L^{(1)} & & \tilde{s}_L^{(N)} & \tilde{s}_L^{(N+1)} & & \tilde{s}_L^{(2N)} \end{array}\right). \tag{2.3.3}$$

$\tilde{s}_l^{(n)}$ is 1 if $\boldsymbol{s_l} \in S$ acts with an $X$ to the qubit $n$, and 0 otherwise. Similarly, $\tilde{s}_l^{(N+n)}$ is 1 if $\boldsymbol{s_l} \in S$ acts with an $Z$ to the qubit $n$ and 0 otherwise. Given a generator $\boldsymbol{s_l}$ the action of a $Y$ on a qubit $n$ is represented with a 1 both in $\tilde{s}_l^{(n)}$ and $\tilde{s}_l^{(N+n)}$.

We note two interesting properties of $H(S)$:

1. *The elements $s_l$ are independent generators iff the rows $r(s_l)$ are linearly independent.* [35]. To see this note that, as Pauli matrices square to the identity, adding two rows $r(\boldsymbol{s_a}) \oplus r(\boldsymbol{s_b})$ is equivalent to multiplying the corresponding generators in $S$,

$r(\boldsymbol{s_a} \cdot \boldsymbol{s_b})$. Suppose now a set of $n \leq L$ rows is not linearly independent. We have $\sum_{i=1}^{n} r(s_i) = 0$ iff $\prod_{i=1}^{n} \boldsymbol{s_i} = \mathbb{1}$, which implies that $s_j = \prod_{i \neq j} s_i$ and therefore $\boldsymbol{s_l}$ is not an independent generator.

2. *S is abelian iff* $H(S)_X \cdot H(S)_Z^T = 0$ [36], with $\cdot$ denoting the scalar product in $mod(2)$ among the rows of $H(S)_X$ and the columns of $H(S)_Z$ over $\mathbb{Z}_2$. This can be easily seen by noting that $[\boldsymbol{s_a}, \boldsymbol{s_b}] = 0$ iff their local operators (1) are non-trivial and (2) differ in an even number of sites. This will happen iff the part of the vector $r(\boldsymbol{s_a})$ corresponding to $H(S)_X$ ($H(S)_Z$) and the part of the vector $r(\boldsymbol{s_b})$ corresponding to $H(S)_Z$ ($H(S)_X$) are orthogonal $mod(2)$. This must be true for all vectors, which is is equivalent to $H(S)_X \cdot H(S)_Z^T = 0$.

**Stabilizer and classical codes: CSS codes**

The stabilizer formalism leads to the historically first relation between classical codes and quantum codes, discovered in [37] and [38]. To see that, let us consider two classical codes $C_1[N, k_1] = \{x\}$ and $C_2[N, k_2] = \{y\}$ with $C_2 \subset C_1$ so that both $C_1$ and $C_2^{\perp}$ correct errors with weight $t$. We define a quantum code $CSS(C_1, C_2)[N, k_1 - k_2, 2t+1] = \{\sum_{y \in C_2} |x \oplus y\rangle\}$.

Let us suppose that an error $e_X$ producing at most $t$ bit flips and an error $e_Z$ producing at most $t$ phase flips occur, leading to the corrupted (non-normalized) state

$$\sum_{y \in C_2} (-1)^{(x \oplus y) \cdot e_z} |x \oplus y \oplus e_X\rangle . \tag{2.3.4}$$

To correct $e_x$ we add an ancilla, we perform controlled-not gates to have the state

$$\sum_{y \in C_2} (-1)^{(x \oplus y) e_z} |(x \oplus y) \cdot e_X\rangle |H(C_1) e\rangle \tag{2.3.5}$$

and we measure the ancilla to get the syndrome $H(C_1)e$. To correct $e_Z$, one can apply a Hadamard gate to each qubit to get the state

$$\sum_{z=1}^{2^N} \sum_{y \in C_2} (-1)^{(x \oplus y) \cdot (e_Z \oplus z)} |z\rangle . \tag{2.3.6}$$

Defining $z' := z \oplus e_Z$ we turn $e_Z$ into a bit flip and we see that only $\{z'\} \in C_2^{\perp}$ will contribute to the coefficients of the state, so that we can proceed as previously with the check matrix $H(C_2^{\perp})$.

Let us finally remark that, due to the two properties stated above and $C_2 \subset C_1$, the matrix $H(CSS) = (H(C_1)|H(C_2^{\perp}))$ defines a set of independent mutually commuting generators. That is, a $CSS$ code is a stabilizer code.

## 2.4 Graph codes and graph states

As an example of stabilizer states, we will introduce the *graph states*, which are particularly used in quantum information [39, 40] because they have an intuitive graphical representation. An important property of graph states is that that any stabilizer state is LU-equivalent to a graph state given in equation [41].

Consider a graph $G = (E, V)$ with a set of vertices $V$ connected by a set of edges $E$. The *adjacency matrix* $A$ of $G$ is the matrix with $|V|^2$ elements

$$A_{a,b} = \begin{cases} 1 & if \quad (a,b) \in E \\ 0 & if \quad (a,b) \notin E \end{cases} \quad \forall a, b \in V. \tag{2.4.1}$$

Each graph $G$ can be associated to a binary $|V|$-partite state $|G\rangle$, such that each vertex corresponds to a qubit and each edge corresponds to a quantum gate acting on the two corresponding connected qubits. A graph state is defined as

$$|G\rangle = \prod_{a,b \in E} CZ_{a,b} \, |+\rangle^{\otimes |V|}, \tag{2.4.2}$$

where $CZ_{a,b} := \frac{1}{2}\big(\mathbb{1} + Z_a \otimes \mathbb{1} + \mathbb{1} \otimes Z_b - Z_a \otimes Z_b\big) = diag(1, 1, 1, -1)$ is the controlled-$Z$ gate applied to the qubits $a$ and $b$ and $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.

To each vertex $a \in |V|$, we can associate a local operator

$$S_a = X^a \prod_{b \in N_a} Z^b, \tag{2.4.3}$$

where $N_a := \{b \in V | (a, b) \in E\}$ is the number of qubits connected to $a$ by an edge. $|G\rangle$ is the stabilizer state which is stabilized by the generators $\{S_a\}$. If such space has only $|V| - k$ generators, then the subspace stabilized by $\{S_a\}$ is a $[\![|V|, k, \delta]\!]$ quantum error correcting code called *graph code*, and it is uniquely defined by its corresponding graph $G$ [42].

As we have mentioned above, in [41] it was shown that each stabilizer code is equivalent to a graph code. In particular, each graph code $G$ characterized by the adjacency matrix $A$ corresponds to a stabilizer code $S$ with an associated parity check matrix $H(S) = (A|\mathbb{1})$. Furthermore, it was also shown in [41] that any stabilizer state is equivalent to a graph state up to local unitaries of the group $\{U_C^{(l)}\}$ that fulfill $U_C^{(l)} \mathcal{P}_d^{\otimes N} U_C^{(l)\,\dagger} = \mathcal{P}_d^{\otimes N}$. This group is called *Clifford group*.

## 2.5 Stabilizer codes from additive codes

The construction of CSS codes gave rise to further constructions of quantum codes and highly entangled quantum states from classical codes, for both binary and nonbinary systems [43, 44, 45, 46, 47, 36]. Here we will present two important tools for such constructions. First we will introduce the so-called *Galois fields* following [48], which will allow us to present a type of classical codes called *additive codes*. From additive codes, stabilizer codes for qudits can be constructed [46]. In particular, examples for $AME(9, 3)$ state and $AME(10, 3)$ state have been constructed in this way [49, 50], and such constructions led to the proof of their existence. Although we will not deepen the details of how such examples have been constructed, here we will illustrate the relation between self-dual additive codes and stabilizer codes which underlies such constructions by giving the example for qubits which was proposed in [47].

### Additive codes

We aim to introduce the definition of additive codes. To do that, we will first define Galois fields and then we will see how additive codes are constructed from Galois fields.

A *field* $\mathbb{F}_p$ is a set of a prime number $p$ of elements with the following properties:

- The elements in $\mathbb{F}_p$ form an abelian group under addition in module $p$, denoted as $\oplus$.
- The elements in $\mathbb{F}_p$ excluding the neutral element of the addition, 0, form an abelian group under multiplication in module $p$, denoted as $\cdot$.
- The distributive property is fulfilled, $(a \oplus b) \cdot c = a \cdot b \oplus a \cdot c \quad \forall a, b, c \in \mathbb{F}_p$.

$\mathbb{Z}_p$ is an example of $\mathbb{F}_p$ with respect to the standard sum and product $mod(p)$.

Given a natural number $m$, we denote by $\mathbb{F}_p^m(x)$ the set of all the polynomials of degree less or equal than $m$ having coefficients in $\mathbb{F}_p$. We denote as $g(x)$ a polynomial of degree $m$ which can not be factorized over $\mathbb{F}_p^m(x)$, namely which is *irreducible* over $\mathbb{F}_p^m(x)$. This means that $g(x)$ can not be factorized over $\mathbb{Z}_p$. We perform the sum $\oplus$ among elements in $\mathbb{F}_p^m(x)$ by summing the corresponding polynomial coefficients in $mod(p)$, and the product $\cdot$ as the multiplication among polynomials in $mod\big(g(x)\big)$.

A *Galois Field* $GF(p^m)$ is a field with $p^m$ elements which can be associated one to one to all the possible remainders arising from all the possible divisions among elements in $\mathbb{F}_p^m(x)$, considering the operations $\oplus$ and $\cdot$ as defined above.

We have introduced Galois Fields, which are the building blocks of additive codes. Now, let us introduce additive codes.

Given a field $GF(p^2)$, let us define the *trace*,

$$\begin{aligned} tr: \quad GF(p^2) \quad &\rightarrow \quad GF(p) \\ tr(x) = x^p \oplus x \quad &\forall x \in GF(p^2). \end{aligned} \tag{2.5.1}$$

Consider a concatenation of $N$ elements $\{x^{(n)}\} \in GF(p^2)$, $\boldsymbol{x} := x^{(1)}, ..., x^{(N)} \ \forall \ 1 \leq n \leq N$. Let us denote as $GF(p^2)^N := \{\boldsymbol{x}\}$ the additive group of all the possible such concatenations. An *additive code* of length $N$ over $GF(p^2)$ is an additive subgroup of $GF(p^2)^N$. Given two elements $\boldsymbol{x}, \boldsymbol{y} \in GF(p^2)^N$, we introduce the following inner product,

$$\mathbf{x} \cdot \mathbf{y} = \sum_{n=1}^{N} tr(x^{(n)} \bar{y}^{(n)}) \quad mod(p), \tag{2.5.2}$$

where $\bar{y} = y^p$ [44]. This allows us to define the dual $C^\perp$ of an additive code $C$ as the set of elements in $GF(p^2)^{\otimes N}$ which are orthogonal to $C$ under the inner product (2.5.2). $C^\perp$ is also an additive code.

### Stabilizer codes constructed from additive codes

Additive codes and the generalization of Pauli matrices $\mathcal{P}_d$ are two important tools used to construct quantum codes from classical codes [43, 44, 45, 47, 46, 36]. Here, we will illustrate this connection by giving a particular binary example.

First of all, let us now recall the generalization of the Pauli group given in section 1.2.2, $\mathcal{P}_d = \{\pm\omega^\lambda\} \times \{D_{\mu,\nu}\}$, with the definition

$$D_{\mu,\nu} = \sum_{l=0}^{d-1} \omega^{l\nu} \left|l \oplus \mu\right\rangle \left\langle l\right| \quad \forall\lambda,\mu,\nu \in \{0,...,d-1\} \tag{2.5.3}$$

with $\omega = e^{i\frac{2\pi}{d}}$. The elements $\{D_{\mu,\nu}\}$ form an orthonormal basis for operators of size $d \times d$. Therefore, they form a nice error basis. The notion of stabilizer code can be generalized to dimension $d$ as a vector subspace stabilized by an abelian subgroup $S_d \subset \mathcal{P}_d^{\otimes N}$.

We are now ready to explain how stabilizer codes can be constructed from additive codes. In particular, we will restrict ourselves to Pauli matrices for binary systems and $GF(4) = \{0, 1, \alpha, \alpha^2\}$ to give an example of such constructions [47]. Here $\oplus$ stands for the sum $mod(2)$. We define $\alpha^2 := \alpha \oplus 1$. Considering $GF(2) = \{0, 1\}$, the trace is now defined as

$$\begin{array}{rccc} tr: & GF(4) & \to & GF(2) \\ & tr(x) = x^2 \oplus x & \forall x \in GF(4)\,, & \end{array} \tag{2.5.4}$$

with the properties $tr(0) = tr(1) = 0$ and $tr(\alpha) = tr(\alpha^2) = 1$. In addition, we have $\bar{0} = 0$, $\bar{1} = 1$, $\bar{\alpha} = \alpha^2$ and thus $\bar{\alpha^2} = \alpha$.

Consider the following mapping from each element of $GF(4)$ to a Pauli matrix,

$$\begin{array}{c} 0 \to \mathbb{1} \\ \alpha \to X \\ \alpha^2 \to Z \\ 1 \to Y. \end{array} \tag{2.5.5}$$

Similarly, we map each element of $GF(4)^N$ to an element of the $N$-qubit Pauli group $\mathcal{P}^{\otimes N}$. The modular sum of elements in the additive group $GF(4)^N$ is mapped to the product of elements in the multiplicative group $\mathcal{P}^{\otimes N}$ up to phases, and thus the trace scalar product relations (2.5.2) in $GF(4)^N$ are analogous to the commutation relations in $\mathcal{P}^{\otimes N}$.

Let $C_A \in GF(4)^N$ be an additive code which is self-orthogonal under the inner product (2.5.2), that is, we have $C_A \subset C_A^\perp$, being $C_A^\perp$ the dual of $C_A$ defined by the inner product (2.5.2). Considering the map (2.5.5), the code $C_A$ is mapped to an abelian multiplicative subgroup of $\mathcal{P}^{\otimes N}$, which defines a stabilizer code. That is to say, *a self-orthogonal additive code in $GF(4)^N$ defines a stabilizer code of $N$ physical qubits.*

Similarly as for qubits, a stabilizer group for a non-binary system of prime dimension $p$ can be constructed from a self-orthogonal additive code in dimension $p^2$ by mapping each element $x \in GF(p^2)$ to an element of $\mathcal{P}_d$ [1],

$$\Phi_p: \quad GF(p^2) \quad \to \quad \{D_{\mu,\nu}\}, \tag{2.5.6}$$

where $\Phi_p(x)$ is an invertible function that depends on the dimension $p$ which uniquely determines a pair $(\mu,\nu)$ given $x$ and viceversa. In the case of qubits, the analogy (2.5.5) follows by choosing $\Phi_2(x) = \phi^{-1}(\mu,\nu)$, with $\phi(\mu,\nu) = \alpha\mu + \alpha^2\nu$.

# Chapter 3

# AME states of minimal support

Consider a $N$-qudit state,

$$|\psi\rangle = \sum_{i_1,...,i_N=0}^{d-1} t_{i_1,...,i_N} |i_1, ..., i_N\rangle . \tag{3.0.1}$$

The *support* of $|\psi\rangle$ is the number of nonzero coefficients, $t_{i_1,...,i_N} \neq 0$, when $|\psi\rangle$ is written in a product basis as in (3.0.1).

A $k$-uniform state has at least support $d^k$, which is its Schmidt rank for any bipartition among $k$ and $N-k$ parties. $k$-uniform states with only $d^k$ coefficients are called of *minimal support* and they are specially easy to study because they can be constructed from classical linear codes. Naturally, a $k$-uniform state which is LU-equivalent to a state which has support $d^k$ is considered to be of minimal support (up to LU operations). In this section we will explore this kind of states, with special emphasis on AME states. In particular, we will see how a special type of classical linear codes called *maximum distance separable* codes and a certain class of combinatorial designs called *mutually orthogonal latin hypercubes* are equivalent to $k$-uniform states of minimal support, and in particular to AME states of minimal support.

For the rest of this thesis, we introduce the shorthand notation $AME(N,d)_{min}$ to denote a $N$-partite AME state of $d$-level systems which is of minimal support.

## 3.1 AME states and maximum distance separable (MDS) codes

AME states of minimal support are equivalent to a certain type of classical linear codes called *MDS* codes [22, 51]. Here we will define this type of codes and explain why they are equivalent to $AME(N,d)_{min}$. Such equivalence is important because it provides a systematic constructions for $AME$ states [43].

Consider a classical linear code $C[N,k,\delta]_d$. The number of codewords $M$ which such code can have is upper bounded by the *Singleton Bound*,

$$M \leq d^{N-\delta+1}. \tag{3.1.1}$$

A classical linear code is *maximum-distance separable (MDS)* if it saturates the Singleton

Bound, i.e., if it has distance $\delta = N - k + 1$.

Consider a MDS code $C_k[N, k, N-k+1]_d$ with $d^k$ codewords $\{x_l = i_1, ..., i_N\}$, $l \in (0, d^k - 1)$. We define a particular case of states written as in (3.0.1) in which each term of the state $|\psi\rangle$ corresponds to a codeword $x$ of $C_k$, and all the coefficients $t_l$ are equal. Such state reads

$$|\psi\rangle = \frac{1}{\sqrt{d^k}} \sum_{l=0}^{d^k-1} |x_l\rangle \,. \tag{3.1.2}$$

Let $\{S_i\}$ be all the possible subsets of $k \leq \lfloor N/2 \rfloor$ qudits. Consider the reduction to a subset $S_i$ of the state $|\psi\rangle$,

$$\rho_{S_i} = tr_{S_i^c} |\psi\rangle \langle\psi| = \frac{1}{d^k} \sum_{l,l'=0}^{d^k-1} tr_{S_i^c} |x_l\rangle \langle x_{l'}| \,, \tag{3.1.3}$$

where $S_i^c$ denotes the complementary subset of $S_i$. First of all, note that since the distance between any two codewords is $N - k + 1$, any two terms $|x_l\rangle$ and $|x_{l'}\rangle$ with $l \neq l'$ are orthogonal in at least $N - k + 1$ components, which implies that

$$tr_{S_i^c} |x_l\rangle \langle x_{l'}| = 0 \quad \forall\, l \neq l'. \tag{3.1.4}$$

This means that the off-diagonal terms in equation (3.1.3) vanish. Second, consider the following notation for the partial traces of $\{|x_l\rangle \langle x_l|\}$,

$$\{tr_{S_i^c} |x_l\rangle \langle x_l|\} = \{\left|x_l^{S_i}\right\rangle \left\langle x_l^{S_i}\right|\}. \tag{3.1.5}$$

Since any two terms $|x_l\rangle$ and $|x_{l'}\rangle$ with $l \neq l'$ have always at least $N - k + 1$ orthogonal components, we have that the set $\{\left|x_l^{S_i}\right\rangle\}$ forms an orthonormal basis for any value of $i$. Let us now recall that given $d^k$ vectors $\{|\psi_i\rangle\}$ with $1 \leq i \leq d^k$, we have

$$\sum_{i=1}^{d^k} |\psi_i\rangle \langle\psi_i| = \mathbb{1} \tag{3.1.6}$$

if and only if $\{|\psi_i\rangle\}$ form an orthonormal basis of $\mathbb{C}_d^k$. It is now straight forward to see that we have

$$\sum_{l=1}^{d^k} tr_{S_i^c} |x_l\rangle \langle x_l| = \mathbb{1}. \tag{3.1.7}$$

That is, the two observations above imply that *any reduction to k parties of the state* $|\psi\rangle$ *is maximally mixed.* This was first noted in [22].

Let us now show that the converse statement is also true. Consider a state $|\psi\rangle$ of the form (3.1.2), in which the distance among the codewords $\{x_l\}$ is $\delta < N - k + 1$. It is clear that there exist two codewords $x_l$ and $x_{l'}$, and a set of $k$ parties $S$, so that we have

$$tr_{S^c} |x_l\rangle \langle x_l'| \neq 0 \,, \tag{3.1.8}$$

where $S^c$ denotes the complementary set of $S$. This implies that there is a reduction to $k$ qudits in which not all the off-diagonal terms vanish. This fact represents a contradiction with the definition of $k$-uniform states, and therefore we see that $\delta \geq N - k + 1$ is a necessary condition for the state $|\psi\rangle$ to be $k$-uniform. This was first noted in [51].

This means that *a $k$-uniform state of minimal support shared among $N$ parties in dimension $d$ is equivalent to an MDS code $C_k[N, k, N-k+1]_d$. In particular, a state $AME(N,d)_{min}$ is equivalent to a MDS code with $k = \lfloor \frac{N}{2} \rfloor$.*

The dimension $d$ of a MDS code $C_{MDS}[N, \lfloor \frac{N}{2} \rfloor, \lceil \frac{N}{2} \rceil]_d$ is lower bounded by [51]

$$d \geq \left\lfloor \frac{N}{2} \right\rfloor + 1. \tag{3.1.9}$$

Hence, this leads to a necessary condition for the existence of a state $AME(N,d)_{min}$. For instance, this implies that a state $AME(5,2)$ can not be of minimal support.

## 3.2 MDS codes and mutually orthogonal latin hypercubes (MOLH)

Each MDS code is equivalent to a combinatorial design called *set of mutually orthogonal hypercubes (MOLH)* [52]. Therefore, AME states of minimal support are also equivalent to such objects. The equivalences among AME states of minimal support, MDS codes and mutually orthogonal latin hypercubes are summarized in [53]. The equivalence between AME states of minimal support and mutually orthogonal latin hypercubes is useful to determine the existence of such type of AME states, since mutually orthogonal latin hypercubes have been widely studied. A lot of effort has been done on finding new constructions [54, 55, 56, 57, 58, 59], as well as on studying their existence [60, 61, 62]. Specific constructions of $AME$ states from MOLHs can be found in [23].

The goal of this section is to explain that MDS codes and MOLHs are equivalent [52], and hence AME states of minimal support are equivalent to MOLHs. First we will give some definitions, starting from an instructive example of MOLHs of order two, called *mutually orthogonal latin squares (MOLS)*, to further move to the most general and abstract case. MOLS are particularly interesting to determine the existence of $AME_{min}(4,d)$.

### Mutually orthogonal latin squares (MOLS)

A *latin square* $T$ is a square matrix of dimension $d$ so that each entry $T_{ij} \in \{0, ..., d-1\}$ appears only once in every row and column. For instance, for $d = 3$, the object

$$\begin{array}{ccc} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{array} \tag{3.2.1}$$

is a latin square.

Two latin squares, $T^{(1)}$ and $T^{(2)}$, of the same dimension $d$ are *orthogonal* when, once they are superimposed creating a 2-tuple of latin squares, every ordered pair of entries appears exactly once.

More generally, $s$ latin squares $\{T^{(1)}, ..., T^{(s)}\}$ are mutually orthogonal latin squares (MOLS) iff the condition $(T^{(a)}_{i,j}, T^{(b)}_{i,j}) \neq (T^{(a)}_{l,m}, T^{(b)}_{l,m}) \iff (i,j) \neq (l,m)$ holds when they are superimposed creating an $s$-tuple of latin squares. Equivalently, iff when we superimpose them creating an $s$-tuple, all possible $d^s$ combinations of $s$ entries appear.

To give some examples, let us write explicitly $s = 2$ superimposed orthogonal Latin squares of dimension $d = 3$,

$$\begin{array}{ccc} 00 & 11 & 22 \\ 12 & 20 & 01, \\ 21 & 02 & 10 \end{array} \tag{3.2.2}$$

and $s = 3$ mutually orthogonal latin squares of dimension $d = 5$,

$$\begin{array}{ccccc} 000 & 432 & 314 & 241 & 123 \\ 111 & 043 & 420 & 302 & 234 \\ 222 & 104 & 031 & 413 & 340. \\ 333 & 210 & 142 & 024 & 401 \\ 444 & 321 & 203 & 130 & 012 \end{array} \tag{3.2.3}$$

### Mutually orthogonal latin hypercubes (MOLH)

A hypercube generalizes the idea of a square to larger orders $k > 2$. A *latin hypercube of order $k$ and dimension $d$* is an array $T_{i_1,...,i_k}$ of $k$ coordinates $\{i_1, ..., i_k\} \in \mathbb{Z}_d^k$ so that, fixing all indices except for one of them, no entries are repeated. For instance, fixing all but the last coordinate $i_k$, we have $T_{i_1,...i_{k-1},i_k} \neq T_{i_1,...,i_{k-1},j_k}$ $\forall i_k \neq j_k$. A latin square is an example of latin hypercube with $k = 2$, and its coordinates are classified into rows and columns.

Similarly as before, $s \geq 2$ latin $k-$hypercubes $T^{(1)}, ..., T^{(s)}$ are *mutually orthogonal latin hypercubes (MOLHs)* iff, fixing all the coordinates but two, no pairs are repeated in the $s$-tuple arrays formed by concatenating the entries of the hypercubes: $(T^{(a)}_{i_1,...,i_k}, T^{(b)}_{i_1,...,i_k}) \neq (T^{(a)}_{j_1,...,j_k}, T^{(b)}_{j_1,...,j_k})$ whenever $\{i_1, ..., i_k\}$ and $\{j_1, ..., j_k\}$ differ in 2 or less digits. Equivalently, all $s$ latin squares created by fixing all but two coordinates of the hypercubes are mutually orthogonal.

To illustrate the definition of MOLHs, let us give the following example of $s = 3$ MOLHs of order $k = 3$ and dimension $d = 4$, which is taken from [23].

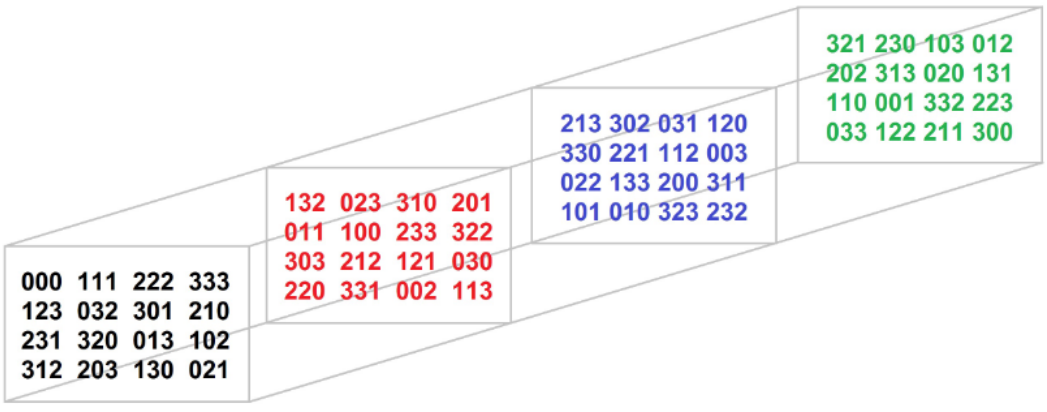


**Figure 3.2.1:** Example of $s = 3$ MOLHs of order $k = 3$ and dimension $d = 4$. The order of the layers along the axis which we can not represent in a two dimensional picture is represented by the order of the different squares, from down-left to up-right.

**MOLHs, MDS codes and $k$-uniform states**

In previous parts of the current section we have defined MDS codes and MOLHs. Now, we will see that those two objects are in fact equivalent. Given that MDS codes and AME states are also equivalent, our derivations will show that MOLHs, MDS and $k$-uniform states of minimal support are mutually equivalent objects.

First of all, we will see that MOLHs define MDS codes. Let us consider $s$ latin $k-$hypercubes $\{T^{(1)},...,T^{(s)}\}$, each of them having $k$ coordinates $\{i_1,...,i_k\}$. We superimpose them creating $d^k$ arrays of $s$ digits, $\{(T^{(1)}_{i_1,...,i_k},...,T^{(s)}_{i_1,...,i_k})_{i_1,...,i_k}\}$. Let us write those $d^k$ arrays as $d^k$ vectors $\{(i_1,...,i_k,T^{(1)}_{i_1,...,i_k},...,T^{(s)}_{i_1,...,i_k})\}$ of $k+s$ components each, so that the first $k$ components correspond to the coordinates that determine each vector.

Let us consider two of those vectors,

$$\begin{aligned}&(i_1,...,i_k,T^{(1)}_{i_1,...,i_k},...,T^{(a)}_{i_1,...,i_k})\\&(j_1,...,j_k,T^{(1)}_{i_1,...,i_k},...,T^{(a)}_{i_1,...,i_k})\,.\end{aligned}\tag{3.2.4}$$

Since $T^{(1)},...,T^{(s)}$ are latin hypercubes, fixing all the coordinates to be equal except for one (e.g. the last one, $i_k\neq j_k$), we have $T^{(a)}_{i_1,...,i_k}\neq T^{(a)}_{i_1,...,j_k}\ \forall 1\leq a\leq s$. This means that in this case the distance among the two vectors $(i_1,...,i_k,T^{(1)}_{i_1,...,i_k},...,T^{(a)}_{i_1,...,i_k})$ and $(j_1,...,j_k,T^{(1)}_{i_1,...,i_k},...,T^{(a)}_{i_1,...,i_k})$ given in (3.2.4) is $s+1$.

Consider now the set of $d^2$ vectors of the form $(i_1,...,i_k,t^{(1)},...,t^{(s)})$ resulting from fixing an arbitrary set of $k-2$ coordinates. Due to the fact that every two latin hypercubes $T^{(a)}$ and $T^{(b)}$ are orthogonal, each pair $(t^{(a)},t^{(b)})$ can not be repeated in any two of those vectors. Therefore, the $d^2$ vectors corresponding to such freedom have the property that each pair $(t^{(a)},t^{(b)})$ spans all the $d^2$ possible combinations with two numbers in $\mathbb{Z}_d$. This means that any pair $(t^{(a)},t^{(b)})$ can play the role of the two non fixed coordinates, and those coordinates can play the role of $(t^{(a)},t^{(b)})$.

The argument can be extended to $r$-tuples $\{(t^{(1)},...,t^{(r)})\}$ of as follows. Let us fix $k-r$ of the coordinates. Instead of a pair $(t^{(a)},t^{(b)})$, we consider now any $r$-tuple array of entries of $r$ different hypercubes, e.g. $(t^{(1)},...,t^{(r)})$. The fact that all pairs of latin squares are orthogonal implies that each set of $d^r$ $r$-tuple arrays of the form $(t^{(1)},...,t^{(r)})$ spans all the $d^r$ possibilities of permuting $r$ numbers in $\mathbb{Z}_d$. Similarly to before, such set of $d^r$ arrays $\{(t^{(1)},...,t^{(r)})\}$ can play the role of $r$ coordinates and the $r$ coordinates which are not fixed, and viceversa. For instance, fixing all but the first $k$ coordinates, the set $\{i_1,...,i_k\}$ can play the role of the corresponding entries of $k$ mutually orthogonal latin hypercubes and viceversa.

This tells us that, given a vector $(i_1,...,i_k,t^{(1)},...,t^{(s)})$, any $k$ components can be regarded as coordinates, such that the remaining $s$ components are the corresponding entries of $s$ mutually orthogonal latin hypercubes. Therefore, if we fix any $k-1$ entries in the set of vectors $\{(i_1,...,i_k,t^{(1)},...,t^{(s)})\}$, the non-fixed $s+1$ elements must be different. This implies that any two vectors of the form (3.2.4) have distance $\delta=s+1$, and hence $\{(i_1,...,i_k,t^{(1)},...,t^{(s)})\}$ defines an MDS code $C_k[N,k,N-k+1]_d$.

The converse statement is also true. That is, given a MDS code $C_k[N,k,N-k+1]_d$, taking any $k$ digits of the codewords (say, the first $k$ digits) as coordinates, the remaining $s$ digits are the entries of $s$ hypercubes of order $k$. This can be seen by noting that the fact that the distance among the different codewords is $\delta=s+1$ implies that (1) fixing all the first $k$ entries except for one, the remaining $s$ are all different and (2) fixing all of

them except for 2, only one of the remaining $s$ can coincide, which means that no pairs are repeated. Therefore a MDS code $C_k[N, k, N-k+1]_d$ defines a set of $s$ mutually orthogonal latin hypercubes of order $k$ in dimension $d$.

We are now ready to state the following Theorem, which was given in [53]. [[53]] Any set of $s$ MOLHs of dimension $d$ and order $k$ defines a MDS code $C_k[N, k, N-k+1]_d$, and viceversa. Both an MDS code $C_k[N, k, N-k+1]_d$ and $s$ MOLHs of dimension $d$ and order $k$ define a $k$-uniform state of support $k$ shared among $N = s+r$ parties of $d$ levels each, and viceversa. In particular, such state is an AME state of minimal support for $\lfloor \frac{N}{2} \rfloor = k$.

The equivalence between MOLHs and AME states of minimal support sheds some light in both the existence of AME states of minimal support and their construction. As an example, the 2 MOLS $T^{(1)}$ and $T^{(2)}$ (3.2.2) allow us to construct the state given in equation [23]

$$|\Psi\rangle = \frac{1}{3}\sum_{i,j=0}^{d-1} |i,j\rangle\, |T^{(1)}_{i,j}\rangle |T^{(2)}_{i,j}\rangle = \frac{1}{3}\sum_{i,j=0}^{d-1} |i,j\rangle\, |i+j\rangle |i+2j\rangle, \tag{3.2.5}$$

which is exactly equivalent to the construction (1.3.8). A more general construction for 2-uniform states of minimal support is also given in [23],

$$|\Phi\rangle = \frac{1}{d}\sum_{i,j=0}^{d-1} |i,j\rangle \bigotimes_{m=1}^{\mathcal{N}(d)} |T^{(m)}_{i,j}\rangle, \tag{3.2.6}$$

where $T^{(m)}_{i,j}$ is the entry of the latin square $T^{(m)}$ in the coordinates $(i,j)$ and $\mathcal{N}(d)$ is the maximal number of MOLS in dimension $d$. Let us mention that for non prime dimensions, only lower bounds for $\mathcal{N}(d)$ are known [60].

Note that the existence of a state $AME(4,d)_{min}$ is equivalent to the existence of two MOLS in dimension $d$. The problem of whether or not 2 MOLS in dimension $d$ exist is known as *Euler's conjecture* and it took two centuries to be completely solved. For instance, in [54] it was shown that 2 MOLS exist for $d = 10$, giving a negative answer to the so-called *Euler's conjecture*. In general, 2 MOLS exist for any dimension except for $d = 2$ and $d = 6$ [63]. This implies that $AME(4,d)_{min}$ exist for all $d \neq 2, 6$. For $d = 2$, no 4-partite AME state exists [19]. However, the existence of $AME(4,6)$ is still open. We will investigate this problem in sections 6 and 7.

# Chapter 4

# AME states from qudit graph states

## 4.1 Graph states which are AME states

AME states of $N$ parties in a prime dimension $p$ can be constructed from graph states in dimension $p$. In this section we define nonbinary graph states and explain how they can be used to construct AME states. We will follow the results of [45] and use the same notation as used therein.

**Qudit graph states**

We define a graph $G(V,E)_p$, as a set of vertices $V$ connected by a set of edges $E$ so that in between two vertices $a$ and $b$ there can be up to one edge, in which the edges have associated a parameter called *weight* which can take an integer value in between 0 and $p-1$. We will assume $p$ to be prime. The reason for this assumption is that otherwise the states given in (4.1.5) are not necessarily orthogonal and hence the results of [45] do not hold. $G(V,E)_p$ has associated an adjacency matrix $A$ with entries $A_{a,b} \in \mathbb{Z}_p$, which denote the weight of the corresponding edge. The graph $G(V,E)_p$ is represented with lines labeled as $A_{a,b}$ which connect the qudits $a$ and $b$. We denote each row of $A$ as $A_i = (A_{i1}, ..., A_{iN})$.

Consider the graph state defined by a graph $G(V,E)_p$,

$$|G\rangle = \prod_{a<b} CZ_{ab}^{A_{a,b}} |+\rangle^{\otimes |V|} \quad \forall a,b \in V. \tag{4.1.1}$$

Analogously as for qubit graph states (2.4.2), we define $|+\rangle = \frac{1}{\sqrt{p}} \sum_{r=0}^{p-1} |r\rangle$ and

$$CZ_{a,b} = \sum_{k=0}^{p-1} |k\rangle_a \langle k| \otimes Z_b^k = \sum_{k,l=0}^{p-1} \omega^{kl} |k\rangle_a \langle k| \otimes |l\rangle_b \langle l| . \tag{4.1.2}$$

Given a bipartition of a graph state, the entanglement among the two subsets is equal to the number of edges connecting both sets if each local party of one subset is connected to at most one party of the complementary subset, and viceversa. However, it is in general hard to write a graph state in such a form that this condition is fulfilled. An efficient method to know whether or not a given bipartition of a graph state is maximally entangled is described in the following part of this section. This will give rise to a necessary and sufficient condition for a graph state to be absolutely maximally entangled.

**Maximal entanglement in qudit graph states**

Let us first define a *labeled graph state* by attaching a label $\mathbf{z} = (z_1, ..., z_N)$ with $z_i \in \mathbb{Z}_p$ to a graph state $|G\rangle$ as

$$|G_{\mathbf{z}}\rangle = Z^{\mathbf{z}} |G\rangle , \tag{4.1.3}$$

defining $Z^{\mathbf{z}} = Z^{z_1} \otimes \cdots \otimes Z^{z_N}$. Te set $\{|G_{\mathbf{z}}\rangle = Z^{\mathbf{z}} |G\rangle\}$ is called *graph state basis*. In what follows, we will explain a method to detect maximal entanglement across specific bipartitions of a given graph state which is given in [45].

If in a graph $G(V, E)_p$ we remove a set of $m$ vertices, $K = \{k_1, ..., k_m\}$, and all the edges to which they are connected, we are left with another graph denoted as $G(V, E)_p^{\setminus K}$. Each row of the adjacency matrix of $G(V, E)_p^{\setminus K}$ is denoted as $A_i^{\setminus k}$, which is the row $A_i$ with entries $A_{ik_1}, ..., A_{ik_m}$ set to 0. We denote the corresponding graph state shared among $N-K$ parties as $\left|G^{\setminus K}\right\rangle$.

For any subset of qudits $K = \{k_1, ..., k_m\}$, we can write an $N$-partite graph state $|G\rangle$ as

$$|G\rangle = \prod_{l=1}^{N} \sum_{r=0}^{p-1} |r\rangle_1 \langle r| \otimes Z_l^{rA_{1,l}} \cdots \prod_{l=1}^{N} \sum_{r=0}^{p-1} |r\rangle_m \langle r| \otimes Z_l^{rA_{m,l}} \prod_{a<b;\ a,b\notin K} CZ_{ab}^{A_{a,b}} |+\rangle^{\otimes |V|} , \tag{4.1.4}$$

with $Z_l$ denoting the gate $Z$ applied to the qudit $l$. Note that $A_{r,l} = 0$ if $r = l$.

Consider now a $Z$-measurement on the set of qudits $K$ of $|G\rangle$, giving measurement outcomes $z_1, ..., z_m$. We denote a $Z$-measurement on the qudit $r$ as $Z_r$. The resulting state is

$$\begin{aligned} {}_{k_1,...,k_m}\langle z_1, ..., z_m |G\rangle &= \bigotimes_{l=1}^{N} Z_l^{z_1 A_{1,l}} \cdots \bigotimes_{l=1}^{N} Z_l^{z_m A_{m,l}} \prod_{a<b;\ a,b\notin K} CZ_{ab}^{A_{a,b}} |+\rangle^{\otimes |V|} \\ &= Z_1^{\sum_{s=1}^{m} z_s A_{s,1}} \otimes \cdots \otimes Z_m^{\sum_{s=0}^{m} z_s A_{s,m}} \prod_{a<b;\ a,b\notin K} CZ_{ab}^{A_{a,b}} |+\rangle^{\otimes |V|} = \frac{1}{\sqrt{p}} \left|G_{\mathbf{z}}^{\setminus K}\right\rangle , \end{aligned} \tag{4.1.5}$$

where we define

$$\mathbf{z} = \left( \sum_{s=1}^{m} z_s A_{s,1}, ..., \sum_{s=1}^{m} z_s A_{s,m} \right) = \sum_{s=1}^{m} z_s A_s \setminus K. \tag{4.1.6}$$

Each combination of outcomes $z = (z_1, ..., z_m)$ defines a resulting graph state. If all those possible resulting states are mutually orthogonal, then we can uniquely determine the outcomes $(z_1, ..., z_m)$ by knowing $|G_{\mathbf{z}}^{\setminus K}\rangle$, which means that the $N - m$ parties sharing $|G_{\mathbf{z}}^{\setminus K}\rangle$ were maximally entangled with the other $m$ parties before the measurement.

Consider now two different vectors corresponding to two possible sets of outcomes of the measures and having $m$ components each, $z = (z_1, ..., z_m)$ and $z' = (z'_1, ..., z'_m)$. The corresponding graph state labels $\mathbf{z}$ and $\mathbf{z}'$ will be different if each component of $z$ ($z'$) defines an independent component in $\mathbf{z}$ ($\mathbf{z}'$), which will happen if all the rows $\{A_s\}$ are linearly independent in $\mathbb{Z}_p$. If we consider the $d^m$ possible outcome sets $\{z\}$, this condition becomes also necessary. Hence, the states $\{|G_{\mathbf{z}}^{\setminus K}\rangle\}$ will be orthogonal iff the rows $\{A_s \setminus K\}$ are linearly independent.

This leads to the following observation. Let $|G\rangle$ be a $N$-partite graph state in (prime) dimension $p$. The rows of its adjacency matrix $A$ are $\{A_s\}$. Consider a subset $K$ of $m$ parties. The parties in $K$ are maximally entangled with the remaining $N - m$ iff the rows of $A$ corresponding to the set which is complementary to $K$, namely the rows $\{A_s \setminus K\}$, are

linearly independent in $\mathbb{Z}_p$.

This leads to a Theorem that tells us whether a given graph state is an AME state or not.

[[45]] Let $|G\rangle$ be a $N$-partite graph state in (prime) dimension $p$. The rows of its adjacency matrix $A$ are $\{A_s\}$. $|G\rangle$ is an AME state iff for any subset $K$ of $\lfloor \frac{N}{2} \rfloor$ parties, the corresponding rows $\{A_s \setminus K\} \quad \forall s \in K$ are linearly independent in $\mathbb{Z}_p$.

## 4.2 AME graph states constructed from classical MDS codes

We have explained a method to detect maximal entanglement across given bipartitions of a graph state. Now, we are interested in constructing graph states which are absolutely maximally entangled. We will do that by considering MDS codes, following the steps of [45]. In fact we will see that every AME state of minimal support is a stabilizer state and hence it can be converted into a graph state by applying local operators in the so-called *Clifford group*.

Consider an AME state $|\psi\rangle$ of minimal support constructed from a MDS code $C[N, \lfloor \frac{N}{2} \rfloor, \lfloor \frac{N}{2} \rfloor + 1]_p = \{x\}$ with a generator matrix $G$ so that $\{x\} = \{Gx_L\}$, as explained in chapter 2. Such state reads

$$|\psi\rangle = \frac{1}{\sqrt{p^{\lfloor \frac{N}{2} \rfloor}}} \sum_{x_L \in \mathbb{Z}_p^{\lfloor N/2 \rfloor}} |Gx_L\rangle \,. \tag{4.2.1}$$

Following the notation introduced in 4.1, given an operator $A$ we denote $A^{a_1} \otimes \cdots \otimes A^{a_M}$ as $A^a$, with $a = (a_1, ..., a_M)$. Since $C$ is a classical linear code, given any string $y_L \in \mathbb{Z}_p^{\lfloor N/2 \rfloor}$ we have

$$X^{Gy_L} |\psi\rangle = \frac{1}{\sqrt{p^{\lfloor \frac{N}{2} \rfloor}}} \sum_{x_L \in \mathbb{Z}_p^{\lfloor N/2 \rfloor}} |Gx_L + Gy_L\rangle = |\psi\rangle \,. \tag{4.2.2}$$

Therefore, $|\psi\rangle$ has $p^{\lfloor \frac{N}{2} \rfloor}$ symmetries, namely $X^{Gx_L} \; \forall x_L \in \mathbb{Z}_p^{\lfloor N/2 \rfloor}$. A generator for $\{x\}$ is given by the set of columns of $G$. Therefore, each column of $G$ defines an independent stabilizer for $|\psi\rangle$.

With similar definitions, note that

$$Z^{Gy} |\psi\rangle = \frac{1}{\sqrt{p^{\lfloor \frac{N}{2} \rfloor}}} \sum_{x_L \in \mathbb{Z}_p^{\lfloor N/2 \rfloor}} \omega^{y^T G x_L} |Gx_L\rangle \,. \tag{4.2.3}$$

If $y_L$ is in the kernel of $G$, then $Z^{Gy}$ is a stabilizer of $|\psi\rangle$, because $y^T G x_L = z H G x_L = 0$ for some $z \in \mathbb{Z}_d^{\lfloor \frac{N}{2} \rfloor}$. A generator for the kernel of $G$ is given by the rows of $H$.

Therefore, $|\psi\rangle$ is a stabilizer state and its stabilizer group can be described with the check matrix

$$H(S) = \left( \begin{array}{c|c} G^T & 0 \\ 0 & H \end{array} \right) . \tag{4.2.4}$$

Using the two properties of $H(S)$ described in 2.3, we see that (1) the generators described in (4.2.4) are independent because the columns of $G$ are independent as well as the rows of $H$, and (2) the stabilizers described by (4.2.4) commute since the rows of $H$ are orthogonal to

the columns of $G$. Since the rows of $H$ are a basis for the kernel of $G$, the number of rows of $H$ plus the number of columns of $G$ sum up to $N$. This proves that *each AME state of minimal support is a stabilizer state which parity check matrix $H(S)$ is given by* (4.2.4). Since stabilizer states are LU-equivalent to graph states under elements of the Clifford group [64], by applying operations of the local Clifford group we can transform any AME state of minimal support into a qudit graph state. The operations that lead to the graph state are those that transform $H(S)$ into the form $H(S) = (\mathbb{1}|A)$, and $A$ will be the adjacency matrix of the corresponding graph. Those results were given in [45].

Note that this procedure to construct graph states from classical codes is analogous to the construction of CSS codes explained in section 2.3. In that sense, we can interpret a graph AME state constructed from an AME of minimal support as a CSS code with a single codeword.

## 4.3 Related constructions for non prime dimensions

The construction of graph states which are absolutely maximally entangled given above can be done for prime dimensions. However, it gives rise to constructions for AME states of non prime local dimensions as follows.

Consider an AME state of $N$ parties in dimension $d_1$

$$|\psi(N,d_1)\rangle = \sum_{i_1,\ldots,i_N \in \mathbb{Z}_{d_1}} t_{i_1,\ldots,i_N} |i_1\rangle \cdots |i_N\rangle \tag{4.3.1}$$

and an AME state of $N$ parties in dimension $d_2$,

$$|\psi(N,d_2)\rangle = \sum_{j_1,\ldots,j_N \in \mathbb{Z}_{d_2}} t_{j_1,\ldots,j_N} |j_1\rangle \cdots |j_N\rangle \,. \tag{4.3.2}$$

Consider now the following $2N$-partite tensor product,

$$\begin{aligned} |\psi(N,d_1\cdot d_2)\rangle &= |\psi(N,d_1)\rangle \otimes |\psi(N,d_2)\rangle \\ &= \sum_{i_1,\ldots,i_N \in \mathbb{Z}_{d_1} j_1,\ldots,j_N \in \mathbb{Z}_{d_2}} t_{i_1,\ldots,i_N} t_{j_1,\ldots,j_N} |i_1\rangle |j_1\rangle \cdots |i_N\rangle |j_N\rangle \\ &= \sum_{k_1,\ldots,k_N \in \mathbb{Z}_{d_1\cdot d_2}} t_{k_1,\ldots,k_N} |k_1\rangle \cdots |k_N\rangle \,, \end{aligned} \tag{4.3.3}$$

where the tensors $\{t_{k_1,\ldots,k_N}\}$ arise from the definition

$$\begin{aligned} |i_1\rangle |j_1\rangle &= |k_1\rangle \in \mathcal{H}_{d_1\cdot d_2} \\ &\vdots \\ |i_N\rangle |j_N\rangle &= |k_N\rangle \in \mathcal{H}_{d_1\cdot d_2} \end{aligned} \tag{4.3.4}$$

It is clear that any reduction $\rho_k$ of the state $|\psi(N,d_1\cdot d_2)\rangle$ to $k$ parties, e.g. the parties $\{1,\ldots,k\}$, is maximally mixed, and therefore $|\psi(N,d_1\cdot d_2)\rangle$ is a state $AME(N,d_1\cdot d_2)$. This gives the following sufficient condition for the existence of some AME states of non prime

local dimensions. If there exists a prime decomposition $d = \prod_l d_l$ so that for all those dimensions $d_l$ there exists a state $AME(N, d_l)$, then a state $AME(N, d)$ exists and can be constructed as above.

However, not all AME states in non-prime dimensions can be constructed in this way. As a counter example, note that there exists a state $AME(4, 4)$ while there does not exist a state $AME(4, 2)$.

# Chapter 5

# AME states and quantum codes

AME states of minimal support are characterized by classical linear codes, as we have seen in 3.1. Despite there is no generalization of such characterization for quantum codes, there are some connections among quantum codes and AME states of non minimal support. As an example, consider the quantum error correcting code $C[\![5,1,3]\!]_2 = \{|0_L\rangle, |1_L\rangle\}$ [65], with the (unnormalized) quantum codewords

$$\begin{aligned} |0_L\rangle &= +|00\rangle(|000\rangle+|111\rangle)-|11\rangle(|100\rangle+|011\rangle)+|10\rangle(|110\rangle+|001\rangle) \\ &\quad +|01\rangle(|010\rangle+|101\rangle) \\ |1_L\rangle &= -|11\rangle(|000\rangle-|111\rangle)-|00\rangle(|100\rangle-|011\rangle)+|01\rangle(|110\rangle-|001\rangle) \\ &\quad -|10\rangle(|010\rangle-|101\rangle). \end{aligned} \tag{5.0.1}$$

A state $AME(5,2)$ can be constructed by superposing the codewords of $C$, namely [23, 66]

$$AME(5,2) = \frac{1}{\sqrt{2}}\big(|0_L\rangle + |1_L\rangle\big). \tag{5.0.2}$$

This state has support 8. In fact, an $AME(5,2)$ of minimal support (namely, of support 4) does not exist [23].

AME states can be constructed from quantum error correcting codes, but also particularly useful quantum error correcting codes can be constructed taking AME states as codewords [43]. Connections among quantum error correcting codes and highly entangled states are not surprising, since the principle of quantum error correction lies on the fact that information is stored non locally. As one could expect, this fact is also related to the features of QSS schemes, introduced in section 1.3.2. More precisely, QSS schemes were shown to be equivalent to certain quantum codes in [25]. In this section we will review the relation between maximal entanglement and quantum error correction.

## 5.1 Non-degenerate codes and $t$-uniform states

Following the lines of Chapter 7 in [67], we will review here that the codewords of a quantum code $C[\![N,k,t+1]\!]_d$ with $\zeta_{a,b} = \delta_{a,b}$ are $t$-uniform states, where $\delta_{a,b}$ is the Kronecker delta and $\zeta_{a,b}$ is defined in section 2.2. As we will see, this follows trivially from the Knill-Laflamme condition introduced in section 2.2.

Consider a quantum non-degenerated code $C[\![N,k,t+1]\!]_d = \{|\psi_i\rangle\}$ having $\zeta_{a,b} = \delta_{a,b}$ with respect to the set of correctable errors $\varepsilon$. Given $E$ an element of $\mathcal{P}_d^{\bigotimes N}$ with weight less or equal than $t$, any codeword $|\psi_i\rangle \in C$ must fulfill

$$\langle\psi_i| E |\psi_i\rangle = 0. \tag{5.1.1}$$

Let us denote as $\rho_i^{(t)}$ the partial trace of $\rho_i = |\psi_i\rangle\langle\psi_i|$ over $N-t$ parties. Similarly, we will denote as $E^{(t)}$ the partial trace of $E$ over any $N-t$ parties where $E$ acts trivially. Developing (5.1.1), we see that

$$\langle\psi_i| E |\psi_i\rangle = tr\big(\rho_i E\big) = tr\big(\rho_i^{(t)} E^{(t)}\big) = 0. \tag{5.1.2}$$

Let us define the vectors $\boldsymbol{\mu} = (\mu_1, ..., \mu_N)$ and $\boldsymbol{\nu} = (\nu_1, ..., \nu_N)$, so that the elements of $\mathcal{P}_d^{\bigotimes N}$ read

$$\mathcal{D}_{\boldsymbol{\mu},\boldsymbol{\nu}} = D_{\mu_1,\nu_1} \otimes \cdots \otimes D_{\mu_N,\nu_N}. \tag{5.1.3}$$

Let us denote as $\mathcal{D}^{(t)}_{\boldsymbol{\mu},\boldsymbol{\nu}}$ the elements of $\mathcal{P}^{\otimes t<N}$. In this notation, the vectors $\boldsymbol{\mu}$ and $\boldsymbol{\nu}$ have only $t$ components. Note that $E^{(t)}$ is also in $\mathcal{P}^{\otimes t}$. In order to stress this fact but also distinguish $E^{(t)}$ from the rest of elements in $\mathcal{P}^{\otimes t}$, we will use the notation $E^t := \mathcal{D}^{(t)}_{\boldsymbol{\alpha},\boldsymbol{\beta}}$. Expanding $\rho_i^{(t)}$ in the elements of $\mathcal{P}^{\bigotimes t}$,

$$\rho_i^{(t)} = \mathbb{1} + \sum_{\mathcal{D}^{(t)}_{\boldsymbol{\mu},\boldsymbol{\nu}} \neq \mathbb{1}} \boldsymbol{c}_{\boldsymbol{\mu},\boldsymbol{\nu}} \mathcal{D}^{(t)}_{\boldsymbol{\mu},\boldsymbol{\nu}}\,, \tag{5.1.4}$$

and recalling that all the elements in $\mathcal{P}_d$ different from the identity are traceless, we conclude

$$\langle\psi_i| \mathcal{D}^{(t)}_{\boldsymbol{\alpha},\boldsymbol{\beta}} |\psi_i\rangle = tr\big(\mathcal{D}^{(t)}_{\boldsymbol{\alpha},\boldsymbol{\beta}} + \sum_{\mathcal{D}^{(t)}_{\boldsymbol{\mu},\boldsymbol{\nu}} \neq \mathbb{1} \boldsymbol{c}_{\boldsymbol{\mu},\boldsymbol{\nu}}} \mathcal{D}^{(t)}_{\boldsymbol{\mu},\boldsymbol{\nu}} \mathcal{D}^{(t)}_{\boldsymbol{\alpha},\boldsymbol{\beta}}\big) = \boldsymbol{c}_{\boldsymbol{\alpha},\boldsymbol{\beta}}. \tag{5.1.5}$$

Since $C$ must correct any error in $\mathcal{P}^{\otimes t}$, (5.1.5) will vanish iff all the coefficients $\{\boldsymbol{c}_{\boldsymbol{\mu},\boldsymbol{\nu}}\}$ vanish. Therefore we have

$$\rho_i^{(t)} = \frac{1}{d^t}\mathbb{1}, \tag{5.1.6}$$

which means that the codewords $\{|\psi_i\rangle\} \in C$ are $t$-uniform states.

## 5.2 Pure quantum codes and $t$-uniform states

Here we will define a type of quantum codes called *pure* [1]. We will see that the codewords of any pure quantum code which has distance $t+1$ are $t$-uniform states. We will follow the derivation in [1], which is a reformulation of the results in [68]. As we will see in the following section, this connection is useful because it implies that all the necessary conditions for the existence of pure quantum codes are also necessary conditions for the existence of $t$-uniform states, and of AME states in particular.

Before that, let us comment on the notation of quantum error correcting codes. In 2.2 we introduced the notation $[\![N,k,\delta]\!]_d$ to denote a quantum code encoding $k$ logical qudits, and therefore having $K = d^k$ codewords. Although this is the most natural notation for most of the practical applications of quantum codes, here we will consider a more general case in which the number of codewords $K$ is not necessarily a power of the dimension $d$. Namely,

in general we will consider a quantum code $C$ with $K$ codewords in $\mathbb{C}^{d^N}$ having distance $\delta$. We will denote such code as $C((N,K,\delta))_d$.

A quantum code $C((N,K,\delta))_d$ is *pure* with respect to the set of quantum errors

$$\varepsilon = \left\{ E = E_a E_b^\dagger : wt(E_a), wt(E_b) \leq \frac{\delta - 1}{2} \right\} \tag{5.2.1}$$

if the following relationship is fulfilled,

$$\langle \psi_i | E | \psi_j \rangle = \frac{1}{d^N} tr(E) \delta_{i,j} \quad \forall \, |\psi_i\rangle, |\psi_j\rangle \in C. \tag{5.2.2}$$

Using the language of the Knill-Laflamme condition given in Theorem 2.2 and choosing the error basis spanned by $\mathcal{P}_d$ defined in equation (1.1.11), if $C$ is pure we have that

$$\langle \psi_i | \mathcal{D}_{\boldsymbol{\mu},\boldsymbol{\nu}} | \psi_j \rangle = \zeta_{\boldsymbol{\mu},\boldsymbol{\nu}} \delta_{i,j} \quad \forall (\mathcal{D}_{\boldsymbol{\mu},\boldsymbol{\nu}}) \leq \delta - 1, \tag{5.2.3}$$

with $\zeta_{\boldsymbol{\mu},\boldsymbol{\nu}} = \delta_{\boldsymbol{\mu},0}\delta_{\boldsymbol{\nu},0}$.

Following the lines of [1], let us show that the codewords of pure codes with distance $t+1$ are $t$-uniform states. Let $C((N,1,\delta))_d$ be a quantum code and let $\{|\psi_i\rangle\}$ be its codewords. The distance $\delta$ of $C$ is now defined so that for any local error $E$ with $wt(E) \leq \delta - 1$, we have the condition

$$\langle \psi_i | E | \psi_i \rangle = \zeta(E) \quad \forall \, |\psi_i\rangle \in C. \tag{5.2.4}$$

Recalling the notation of section 2.2, $C$ is pure if $\zeta(E) = \frac{1}{d^N} tr(E)$ for any $E$ with $wt(E) \leq \delta - 1$. Considering a pure quantum code $C((N,1,t+1))_d$ and one of its codewords $|\psi_i\rangle \in C$ and expanding $|\psi_i\rangle\langle\psi_i|$ in the basis $\mathcal{P}_d^{\otimes N}$, we have that

$$|\psi_i\rangle\langle\psi_i| = \frac{1}{d^N}\mathbb{1} + \sum_{1 \leq wt(\mathcal{D}_{\boldsymbol{\mu},\boldsymbol{\nu}}) \leq t} c_{\boldsymbol{\mu},\boldsymbol{\nu}} \mathcal{D}_{\boldsymbol{\mu},\boldsymbol{\nu}} + \sum_{t+1 \leq wt(\mathcal{D}_{\boldsymbol{\mu},\boldsymbol{\nu}}) \leq N} c_{\boldsymbol{\mu},\boldsymbol{\nu}} \mathcal{D}_{\boldsymbol{\mu},\boldsymbol{\nu}}. \tag{5.2.5}$$

In order for $C$ to have distance $t+1$, the coefficients $c_{\boldsymbol{\mu},\boldsymbol{\nu}} = \langle \psi_i | \mathcal{D}_{\boldsymbol{\mu},\boldsymbol{\nu}} | \psi_i \rangle$ must vanish in the first sum. Therefore, since the operators $\mathcal{D}_{\boldsymbol{\mu},\boldsymbol{\nu}}$ different from the identity are traceless, we have that the reduction of $|\psi_i\rangle$ to $t$ parties or less reads

$$\rho^{(t)} = \frac{1}{d^t}\mathbb{1}, \tag{5.2.6}$$

so that $|\psi\rangle$ is $t$-uniform.

Conversely, if $|\psi_i\rangle$ is $t$-uniform, then for any displacement operator with $wt\big(\mathcal{D}_{\boldsymbol{\mu},\boldsymbol{\nu}}\big) \leq t$ we have

$$\langle \psi_i | \mathcal{D}_{\boldsymbol{\mu},\boldsymbol{\nu}} | \psi_i \rangle = tr\big( |\psi_i\rangle\langle\psi_i| \mathcal{D}_{\boldsymbol{\mu},\boldsymbol{\nu}} \big) = \frac{1}{d^N} tr\big(\mathcal{D}_{\boldsymbol{\mu},\boldsymbol{\nu}}\big) = \delta_{(\boldsymbol{\mu},\boldsymbol{\nu}),(0,0)}, \tag{5.2.7}$$

recalling from section 2 that $D_{0,0} = \mathbb{1}$ and hence $\mathcal{D}_{\mathbf{0},\mathbf{0}} = \mathbb{1}^{\otimes N}$. Therefore, if all the codewords $\{|\psi_i\rangle\}$ are $t$-uniform and they have mutual distance $t+1$, then they define a pure quantum code $C[\![N, 0, t+1]\!]_d$.

That is, we have seen that (1) the codewords of pure quantum codes with distance $t+1$ are $t$-uniform and (2) a subspace of orthogonal $t$-uniform states form a pure quantum code. By considering pure quantum codes with $K = 1$, namely pure quantum codes of a single

codeword, it is clear that any $t$-uniform state shared amont $N$ parties in local dimension $d$ is equivalent to a pure quantum code $C((N, 1, t+1))_d$. As we will see next, this connection is useful because it implies that all the necessary conditions for the existence of pure quantum codes are also necessary conditions for the existence of $t$-uniform states, and of AME states in particular.

Similarly as classical codes, quantum codes satisfy the *quantum Singleton bound*. That is, given a quantum code $C((N, K, \delta))_d$, we have the inequality

$$K \leq d^{N-2(\delta-1)}. \tag{5.2.8}$$

A quantum code saturating (5.2.8) is called a *quantum maximum distance separable (QMDS) code*. It has been proven that any QMDS code is a pure quantum code (see [20] and references therein). Hence, a QMDS code $C[\![N, k = N-2(\delta-1), \delta]\!]_d$ is equivalent to a subspace spanned by $d^{N-2(\delta-1)}$ $(\delta-1)$-uniform states. This connection is important because most of the results for $(\delta-1)$-uniform states have implications for QMDS codes of distance $\delta$.

## 5.3 System sizes for which AME states can exist

As we mentioned in section 1, the existence of AME states of arbitrary dimension $d$ and number of parties $N$ is non trivial and no general necessary and sufficient nontrivial conditions are known. In this section we will present the two most important necessary conditions for their existence, which are reviewed in [18]. Most of those bounds have been derived in [69] for quantum codes and firstly applied to AME states in [1, 18].

### An analytic bound for the existence of AME states

We will follow the derivation of [1] to obtain an upper bound of the number of parties $N$, given a local dimension $d$, for the existence of an $AME(N, d)$ state. This bound is systematic, in the sense that it can be expressed in a close formula for all $N$ and $d$.

Let $O$ and $P$ be two positive semi-definite hermitian operators acting on $\mathbb{C}^{d^{\otimes N}}$. Given a local error basis $\varepsilon = \{E\}$, we define the *Shor-Laflamme weight enumerators* [70],

$$\begin{aligned} A_j(O, P) &= \sum_{E:wt(E)=j} tr(EO)tr(E^\dagger P) \\ B_j(O, P) &= \sum_{E:wt(E)=j} tr(EOE^\dagger P)\,. \end{aligned} \tag{5.3.1}$$

Those enumerators are independent of the chosen local basis $\varepsilon$ and they are an important tool in quantum information theory. As an example, they can be interpreted as a decomposition of the trace of the operators $O$ and $P$. In particular, it can be seen that [18]

$$\begin{aligned} tr(OP) &= d^{-N} \sum_{j=1}^{N} A_j(O, P) \\ tr(O)tr(P) &= d^{-N} \sum_{j=1}^{N} B_j(O, P)\,. \end{aligned} \tag{5.3.2}$$

Consider now a quantum error correcting code $C((N,K,\delta))_d$ and the projector onto its codespace $\Pi_C = \sum_i |\psi_i\rangle\langle\psi_i| \ \forall\ |\psi_i\rangle \in C$. We will refer to the definitions above associated to $C$ by setting $O = P = \Pi_C$. The code $C$ exists if and only if $A_j(\Pi_C,\Pi_C)$ and $B_j(\Pi_C,\Pi_C)$ are nonnegative and

$$\begin{aligned} &KB_0(\Pi_C,\Pi_C) = A_0(\Pi_C,\Pi_C) = K^2 \\ &KB_j(\Pi_C,\Pi_C) \geq A_j(\Pi_C,\Pi_C)\,, \end{aligned} \tag{5.3.3}$$

with equality in the second equation for $j < \delta$ [69, 18]. It is shown in [1] that for pure codes, we have $A_j(\Pi_C,\Pi_C) = B_j(\Pi_C,\Pi_C) = 0\ \forall\ 0 \leq j \leq \delta$, and in particular AME states fulfill [18]

$$\begin{aligned} &A_j(\Pi_C,\Pi_C) = 0 \quad \text{and} \\ &A_j = B_j\ \forall\, j\,. \end{aligned} \tag{5.3.4}$$

for any $0 \leq j \leq \lfloor N/2 \rfloor + 1$. Shor-Laflamme enumerators (5.3.1) are important to describe quantum codes and entangled states [69]. As an example, for stabilizer codes, $A_j(\Pi_C,\Pi_C)$ is the number of elements with weight $j$ in the stabilizer and $B_j(\Pi_C,\Pi_C)$ is the number of elements with weight $j$ in the normalizer. For a code with a single codeword $|\psi\rangle$, $\{A_j(\rho)\}$ contain the information about the entanglement among qudits within subsets of size $j$.

Requiring the conditions (5.3.3) and the nonnegativity of $A_{\lfloor N/2 \rfloor+2}$ for $AME(N,d)$ states and solving the subsequent equations, the following *necessary* was derived in [1],

$$N \leq \begin{cases} 2(d^2-1) & \forall N \in \mathbb{N}_{even} \\ 2d(d+1)-1 & \forall N \in \mathbb{N}_{odd} \end{cases}\,. \tag{5.3.5}$$

For most of the system sizes in which an AME state does not exist, the non existence of such corresponding AME state is a direct consequence of this bound. In what follows we will present a further bound which was derived in [18].

### One more bound for the existence of AME states

In [18], another necessary condition for the existence of AME states was given by using the results in [69]. Here, we will present this condition. Although this bound is not systematic in the sense that it does not give a closed formula which bounds the number of parties $N$ given any possible dimension $d$ (or viceversa) of the correspondig $AME(N,d)$ state, it is used to disprove the existence of several AME states by exploration.

Let $S$ be a subset of $k \leq N$ parties and $S^c$ its complementary subset. Let $O$ and $P$ be two operators acting on $\mathcal{H}_d^{\otimes N}$. Following [18], we first define the following operator,

$$\mathcal{A}'_S(O,P) = tr_S\big(tr_{S^c} O tr_{S^c} P\big). \tag{5.3.6}$$

We further define

$$S_j(O,P) = \sum_{|T|=j} \sum_{S \subseteq \{1,\ldots,N\}} (-1)^{|S\cap T^c|} \mathcal{A}'_S(O,P), \tag{5.3.7}$$

summing over all the subsets $T \subseteq \{1,...,N\}$ of cardinality $j$. $\{S_j(O,P)\}$ are the coefficients of the following polynomial *Shadow enumerator*

$$S_{O,P}(x,y) = \sum_{j=0}^{N} S_j(O,P) x^{N-j} y^j\,, \tag{5.3.8}$$

called *Shadow enumerator*. Aside from the conditions that lead to the bounds (5.3.5), another *necessary* condition for a hypothetical quantum error correcting code (or AME state in particular) to exist is as follows. Let $|\psi\rangle$ be a pure quantum state and $\rho = |\psi\rangle\langle\psi|$ its corresponding density operator. In order for $|\psi\rangle$ to be an AME state, by setting $O = P = \rho$ it was shown in [69] that all the coefficients of the Shadow enumerator (5.3.8) must be nonnegative.

Several examples of hypothetical AME states have been proven not to exist by computing the coefficients $\{S_j(\rho,\rho)\}$ [18] of the corresponding Shadow enumerator. One of those examples is the $AME(4,2)$ state, which existence was already disproven in [19].

## 5.4 An AME state of seven qubits can not exist

Despite the bounds presented in 5.3, the existence of some AME states of relatively small number of particles and dimensions is still an open problem. A particularly interesting case is the seven qubits case, which was recently solved [71]. Here we will present how its existence was disproven. To that end, we will first introduce two properties which are general for any AME state. Then we will see that in the case of seven qubits, they lead to a contradiction.

Let $|\psi\rangle$ be an $AME(N,d)$ state. Consider a subsystem $A$ of $k \geq \lfloor N/2 \rfloor + 1$ parties and its complementary subsystem, which we call $B$. By computing the corresponding Schmidt decomposition of $|\psi\rangle$, one can see that if the reduction $\rho_B$ is maximally mixed, then $\rho_A$ is proportional to a projector and

$$(\rho_A)^2 = d^{-(N-k)}\rho_A. \tag{5.4.1}$$

Also by computing the Schmidt decomposition of $|\psi\rangle$ corresponding to the bipartition between the subsets $A$ and $B$, one can see that

$$\rho_A \otimes \mathbb{1}^{\otimes(N-k)} |\psi\rangle = d^{-(N-k)} |\psi\rangle . \tag{5.4.2}$$

The two conditions (5.4.1) and (5.4.2) are general for any local dimension $d$. From now on, we will restrict ourselves to qubits, i.e. $d = 2$, so that $|\psi\rangle$ is a state $AME(N,2)$.

Consider the reduction to $k$ qubits of the state $|\psi\rangle$, $\rho_{(k)}$. Expanding $\rho_{(k)}$ into the elements of $\mathcal{P}^{\otimes N}$ and separating the sum in several sums containing terms of the same weight, we have

$$\rho_{(k)} = \frac{1}{d^N}\big(\mathbb{1}^{\otimes k} + \sum_{j=1}^{k}\sum_{V:|V|=j} P_j^V = \frac{1}{d^N}\big(\mathbb{1}^{\otimes k} + \sum_{j=1}^{k} P_j\big), \tag{5.4.3}$$

with $P_j = \sum_{V:|V|=j} P_j^V$, denoting as $P_j^V = \{\alpha_i^V \Sigma_i^V\}_j$ each subset of elements $\Sigma_i^V \in \mathcal{P}^{\otimes N}$ acting nontrivially on each subsystem $V$ of size $j$ with their respective coefficients $\{\alpha_i^V\}_j$. Note that for AME states, we have $P_j^V = \{0\}\ \forall\ j \leq \lfloor N/2 \rfloor$. Considering the set of the first $k$ qubits $V = 1, ..., k$, from (5.4.2) we obtain the equation

$$P_k^{1,...,k} \otimes \mathbb{1}^{\otimes(N-k)} |\psi\rangle = \begin{cases} 3\,|\psi\rangle & N \in \mathbb{N}_{even} \\ 1\,|\psi\rangle & N \in \mathbb{N}_{odd} \end{cases} . \tag{5.4.4}$$

Assume now there exists a state $AME(7,2)$ $|\phi\rangle$. For the reduction to the first five qubits

$\rho_{1,\dots,5}$, we have

$$\rho_{1,\dots,5}^2 = \frac{1}{4}\rho_{1,\dots,5}. \tag{5.4.5}$$

Considering the bipartitions $\{1,2,3,4|5,6,7\}$ and $\{1,2,3,4,5|6,7\}$, we have

$$\rho_{1,2,3,4}\mathbb{1}^{\otimes 3}\left|\phi\right\rangle = \frac{1}{8}\left|\phi\right\rangle \tag{5.4.6}$$

and

$$\rho_{1,2,3,4,5}\mathbb{1}^{\otimes 2}\left|\phi\right\rangle = \frac{1}{4}\left|\phi\right\rangle. \tag{5.4.7}$$

Expanding $\rho_{1,2,3,4}$ and $\rho_{1,2,3,4,5}$ in elements of $\mathcal{P}^{\otimes 7}$, we have

$$\rho_{1,2,3,4} = \frac{1}{2^4}\big(\mathbb{1} + P_4\big), \tag{5.4.8}$$

$$\rho_{1,2,3,4,5} = \frac{1}{2^5}\big(\mathbb{1} + \sum_{j=1}^{5} P_4^{(V_j)} \otimes \mathbb{1}_j + P_5\big), \tag{5.4.9}$$

with $V_j = \{1,2,3,4,5\}\setminus j$ denoting each of the five possible terms acting nontrivially on four parties out of five, namely all except for $j$. Here we denote as $\mathbb{1}_j$ the idenetity acting on the party $j$. With this notation, equations (5.4.6) and (5.4.7) read

$$P_4^{(V_j)}\mathbb{1}^{\otimes 3}\left|\phi\right\rangle = 1\left|\phi\right\rangle \tag{5.4.10}$$

and

$$P_5\mathbb{1}^{\otimes 2}\left|\phi\right\rangle = 2\left|\phi\right\rangle. \tag{5.4.11}$$

Let us now recall the following property [71]. Let $O$ and $P$ be two hermitian operators acting on $\mathbb{C}_2^{\otimes N}$. Assume that each of them is proportional to an element of $\mathcal{P}^{\otimes N}$ and that they act non trivially on $o$ and $p$ qubits respectively. Then, their anticommutator either vanishes, or the parity of its weight, which we denote as $|\{O,P\}|$, fulfills

$$|\{O,P\}| = o \oplus p, \tag{5.4.12}$$

with $\oplus$ denoting the sum in modulo 2. As usual, we define the *parity* of an integer $n \in \mathbb{N}$ as 0 if $n$ is even, and 1 if $n$ is odd. That is, $|\{O,P\}| = 0$ if $\{O,P\}$ has even weight, and $|\{O,P\}| = 1$ if $\{O,P\}$ has odd weight. This property implies that, expanding as in (5.4.9) both sides of equation (5.4.5), not all the terms in the left hand side can contribute. Instead, the property (5.4.12) implies that some of them sum up to zero. Aggrupating the terms in a convenient way and collecting the terms which sum does not vanish, one can see that

$$\Big\{P_5, \sum_{j=1}^{5} P_4^{(V_j)} \otimes \mathbb{1}_j\Big\} = 6P_5, \tag{5.4.13}$$

and therefore we have

$$\Big\{P_5, \sum_{j=1}^{5} P_4^{(V_j)} \otimes \mathbb{1}_j\Big\} \otimes \mathbb{1}^{\otimes 2}\left|\phi\right\rangle = 6P_5 \otimes \mathbb{1}^{\otimes 2}\left|\phi\right\rangle, \tag{5.4.14}$$

which leads to the following contradiction,

$$(2 \cdot 5 \cdot 1 + 5 \cdot 1 \cdot 2) \left|\phi\right\rangle = 6 \cdot 2 \left|\phi\right\rangle , \tag{5.4.15}$$

and therefore the assumption that a state $AME(7,2)$ $\left|\phi\right\rangle$ exists is false.

## 5.5 Current knowledge on the existence of AME states. An overview

So far, in this thesis we have reviewed the main tools which have been used to both construct some AME states and disprove the existence of some other AME states. Here, we will summarize those results in table 5.1, which has been taken from [17]. Each cell can be understood by considering the following notation.

- The label "MDS" denotes that the corresponding AME state exists and it has been constructed by using MDS codes [23, 22] (see chapter 3).
- The label "Graph" denotes that the corresponding AME state exists and it has been constructed by means of a graph state given in equation [45] (see chapter 4).
- The label "GF(d)" denotes that the corresponding AME state exists and it is a stabilizer stated constructed by a self-orthogonal additive code over $GF(d)$ [46] (see section 2.5).
- The label "Scott" denotes that the existence of the corresponding AME state has been disproven by using the bounds derived in [1] (see section 5.3).
- The label "Shadow" denotes that the existence of the corresponding AME state has been disproven by the bounds derived in [18] (see section 5.3).
- The label "Huber" denotes that the existence of the corresponding AME state has been disproven by using a particular method proposed in [71] (see section 5.4).
- The label "?" denotes that the existence of the corresponding AME state is currently unknown.

In order to establish a general rule for the existence of AME states which system sizes are beyond table 5.1, let us note that the bound given in (5.3.5) implies that, for any arbitrary dimension $d$, there exists a number of parties $n$ so that for all $N \geq n$, an $AME(N,d)$ state can not exist. To give an example, for $d = 2$ we have $n = 12$.

| | $d=2$ | $d=3$ | $d=4$ | $d=5$ | $d=6$ | $d=7$ | $d=8$ | $d=9$ | $d=10$ |
|---|---|---|---|---|---|---|---|---|---|
| $N=2$ | MDS | MDS | MDS | MDS | MDS | MDS | MDS | MDS | MDS |
| $N=3$ | MDS | MDS | MDS | MDS | MDS | MDS | MDS | MDS | MDS |
| $N=4$ | Shadow | MDS | MDS | MDS | ? | MDS | MDS | MDS | MDS |
| $N=5$ | Graph | MDS | MDS | MDS | Graph | MDS | MDS | MDS | MDS |
| $N=6$ | Graph | Graph | MDS | MDS | Graph | MDS | MDS | MDS | MDS |
| $N=7$ | Huber | Graph | MDS | MDS | ? | MDS | MDS | MDS | MDS |
| $N=8$ | Scott | Shadow | ? | MDS | ? | MDS | MDS | ? | ? |
| $N=9$ | Shadow | GF(9) | MDS | MDS | ? | MDS | MDS | MDS | ? |
| $N=10$ | Scott | GF(10) | MDS | MDS | ? | MDS | MDS | MDS | ? |
| $N=11$ | Shadow | ? | ? | ? | ? | MDS | MDS | ? | ? |
| $N=12$ | Scott | Shadow | Shadow | ? | ? | MDS | MDS | ? | ? |
| $N=13$ | Scott | Shadow | MDS | ? | ? | MDS | MDS | ? | ? |
| $N=14$ | Scott | Shadow | MDS | ? | ? | MDS | MDS | ? | ? |
| $N=15$ | Scott | ? | ? | ? | ? | ? | ? | ? | ? |
| $N=16$ | Scott | Shadow | Shadow | ? | ? | ? | ? | ? | ? |
| $N=17$ | Scott | Shadow | ? | ? | ? | ? | ? | ? | ? |
| $N=18$ | Scott | ? | ? | ? | ? | ? | ? | ? | ? |
| $N=19$ | Scott | Shadow | ? | ? | ? | ? | ? | ? | ? |
| $N=20$ | Scott | Scott | Shadow | ? | ? | ? | ? | ? | ? |

**Table 5.1:** In this table we summarize the current knowledge on the existence and constructions of AME states. In each row we represent a different number of qudits $N$ among which the corresponding states are shared, and in each column we represent a different local dimension $d$ of the parties. Each cell is filled with the abbreviation of the method which has been used to construct the corresponding $AME(N,d)$ state or to disprove its existence. We use the following notation. "MDS" denotes that the corresponding AME state exists and it has been constructed by using MDS codes [23, 22]; "Graph" denotes that the corresponding AME state exists and it has been constructed by means of a graph state given in equation [45]; "GF($d$)" denotes that the corresponding AME state exists and it is a stabilizer stated constructed by a self-orthogonal additive code over the field $GF(d)$ [46]; "Scott" denotes that the existence of the corresponding AME state has been disproven by using the bounds derived in [1]; "Shadow" denotes that the existence of the corresponding AME state has been disproven by the bounds derived in [18] for pure quantum codes; "Huber" denotes that the existence of the corresponding AME state has been disproven by using a particular method proposed in [71]; "?" denotes that the existence of the corresponding AME state is unknown. Each method is depicted in a different color of the sake of clarity. As a general rule, green denotes that the corresponding state exists, red denotes that the corresponding state does not exist, and orange denotes that it is unknown whether or not the corresponding AME state exists. The results summarized in this table are directly taken from [17].

# Chapter 6

# An algorithm to find 4-partite AME states

4-partite AME states are the simplest cases in terms of number of parties which existence is nontrivial. In particular, it is unclear whether or not an $AME(4,6)$ state exists [17]. Aside from analytical approaches to analyze the structure of 4-partite AME states [72, 23], numerical approaches have been used to tackle this problem [66]. In this section we will present a particular numerical method to try to find 4-partite AME states and a hypothetical $AME(4,6)$ state in particular.

Our method is inspired by an algorithm described in [73] which structure is as follows. We choose an initial pure state $\rho^{(0)} = |\psi^{(0)}\rangle\langle\psi^{(0)}|$ and we apply locally certain local operators $\{A_i\} \in SL(d,\mathbb{C})$, where $SL(d,\mathbb{C})$ is the group of $d \times d$ complex matrices with determinant 1, in an iterative way so that the trace norm of the (non-normalized) state $\rho^{(r)} = |\psi^{(r)}\rangle\langle\psi^{(r)}|$ at an iteration $r$ is reduced with respect to the trace norm of the state $\rho^{(r-1)} = |\psi^{(r-1)}\rangle\langle\psi^{(r-1)}|$ at the previous iteration $r-1$, unless $\rho^{(r-1)}$ is 1-uniform. More precisely, if the SLOCC class of the initial state $|\psi^{(0)}\rangle$ contains a 1-uniform state, the algorithm will converge to a 1-uniform state. Otherwise, the algorithm will converge to a state which has trace norm arbitrarily close to 0.

Our approach works similarly. We choose randomly an initial 4-partite state and we apply iterativelly similar operations as in [73] which affect two qudits instead of one, so that the trace norm of the state $\rho^{(r)}$ at each iteration $r$ is reduced with respect to the previous one unless we reach a 2-uniform state, namely an $AME(4,d)$ state. Although this approach is different from [73] because we apply nonlocal operations, the final state of the algorithm is either a 2-uniform state (i.e., an AME state) or to a state with trace norm close to 0. Moreover, as we will see, some parameters of the states within the algorithm show a repetitive pattern after a certain number of iterations. Although this situation differs from the situation in which the algorithm converges to a specific state, both cases have some similarities. Due to this fact, we will call *convergence* the situation in which some parameters of the states within the algorithm show a repetitive pattern after a certain number of iterations.

The fact that we apply non-local iterations makes the analytical description of the algorithm we propose more complicated than in the original algorithm proposed in [73], which applies local operations. In particular, the conditions under which the algorithm we propose converges to a 2-uniform state are not given by the SLOCC class of the initial state but to more complicated mathematical properties of tensors which we are not able to describe. Therefore, we can only rely on the numerical approach of running the algorithm and

analyzing its results.

In this section, we will first present the algorithm proposed in [73] and the framework in which it is motivated. Once this is done, the motivation of our research will be clear and we will propose an algorithm with the aim of finding 4-partite AME states. Then, we will explain the results of running the algorithm starting from 4-partite states in local dimensions $d \in \{2, 3, 4, 5, 6\}$. Finally, we will give the results of choosing the initial states in a particular way which will give very specific results. For the whole section we will use the notation $|i, j, ...\rangle = |i\rangle \otimes |j\rangle \otimes \cdots$ and the definition

$$\left|\phi_d^+\right\rangle_{XY} = \sum_{i=0}^{d-1} |i, i\rangle \in \mathcal{H}_{X,Y}, \tag{6.0.1}$$

with $\mathcal{H}_{X,Y} = \mathcal{H}_X \otimes \mathcal{H}_Y = \mathbb{C}^d \otimes \mathbb{C}^d$.

## 6.1 An algorithm to find 1-uniform states

In this section we will introduce an algorithm proposed in [73] which converts an initial state $|\psi^{(0)}\rangle$ into a final state $|\psi^{(f)}\rangle$ which will be 1-uniform or not depending on whether or not in the SLOCC class of $|\psi^{(0)}\rangle$ there is a 1-uniform state.

Given two quantum states $|\psi\rangle |\phi\rangle \in \bigotimes_{k=1}^N \mathcal{H}_k$ with $\mathcal{H}_k = \mathbb{C}^{d_k}$, $|\phi\rangle$ is in the SLOCC class of $|\psi\rangle$, $SLOCC_{|\psi\rangle}$, if and only if there exists a set of local operators $\{A_k\}$ with $A_k \in SL(d_k, \mathbb{C})$ and a scalar $\lambda \in \mathbb{C}$ so that [74]

$$A_1 \otimes \cdots \otimes A_N |\psi\rangle = \lambda |\phi\rangle . \tag{6.1.1}$$

Therefore, any state in $SLOCC_{|\psi\rangle}$ can be attained by applying to $|\psi\rangle$ local operators in $SL(d_k, \mathbb{C})$.

Consider now a multipartite state $|\psi\rangle \in \bigotimes_{k=1}^N \mathcal{H}_k$. The so-called *trace norm* of $|\psi\rangle$ is given by $tr(|\psi\rangle \langle\psi|)$. Recalling some well-known notions of entanglement theory, $|\psi\rangle$ can be of one of the following types of states, depending on its SLOCC class.

- $|\psi\rangle$ is *ploystable* if there exists a critical state in $SLOCC_{|\psi\rangle}$. That is, in this case there exits a finite set of local operators $\{A_\alpha\}$ with $A_\alpha \in SL(d_k, \mathbb{C})$ so that $|\psi\rangle$ can be converted into a critical state by applying the sequence of operators defined by $\{A_\alpha\}$ taking $\alpha$ as a label for the sequential order.

- $|\psi\rangle$ is *strictly semistable* if there exits no critical state in $SLOCC_{|\psi\rangle}$ but there exists a sequence of local operators $\{A_\alpha\}$ with $A_\alpha \in SL(d_k, \mathbb{C})$ so that applying the elements in $\{A_\alpha\}$ to $|\psi\rangle$ with $\alpha$ tending to infinity, the resulting state tends to a critical state $|\varphi_{crt}\rangle$. Note that in this case $|\varphi_{crt}\rangle$ can not be exactly reached by acting with finitely many operators $\{A_\alpha\}$ on $|\psi\rangle$ because $SLOCC_{|\psi\rangle}$ and $SLOCC_{|\varphi_{crt}\rangle}$ are different classes by definition.

- $|\psi\rangle$ is in the *null cone* if there exists no critical state in $SLOCC_{|\psi\rangle}$, and also there exists no infinite sequence of local operators $\{A_\alpha\}$ with $A_\alpha \in SL(d_k, \mathbb{C})$ so that $|\psi\rangle$ can be converted into a critical state with arbitrary precision.

In [73], an algorithm which applies transformations of the kind (6.1.1) to an initial state $|\psi^{(0)}\rangle$ having all local reduced density operators full rank is proposed in order to (1) distinguish whether or not $|\psi^{(0)}\rangle$ is in the null cone, and (2) if $|\psi^{(0)}\rangle$ is not in the null cone, convert it into a 1-uniform state by means of SLOCC, either exactly if it is polystable or up to arbitrary precision if it is strictly semistable. Let us first describe such algorithm and then discuss why it has those properties.

**Algorithm 1** ([73]). *Consider a $N$-partite pure state $|\psi^{(r)}\rangle \in \bigotimes_{k=1}^{N} \mathcal{H}_k$, with $\mathcal{H}_k = \mathbb{C}^{d_k}$. $r \in \mathbb{N}$ will label the iteration of the algorithm to which $|\psi^{(r)}\rangle$ corresponds. We will denote the local reduced density operator of the state $|\psi^{(r)}\rangle$ corresponding to each party $k$ as $\rho_k^{(r)}$.*

1. *We choose an initial state $|\psi^{(0)}\rangle \in \bigotimes_{k=1}^{N} \mathcal{H}_k$ normalized by the trace norm which has all reduced density operators being full rank.*

2. *We compute $|\psi^{(1)}\rangle = |\det(\rho_1^{(0)})|^{\frac{1}{2d_1}} \rho_1^{(0)-\frac{1}{2}} \otimes \mathbb{1} \otimes \cdots \otimes \mathbb{1}|\psi^{(0)}\rangle$. We call this operation* applying $\rho_1^{(0)-\frac{1}{2}}$ to the first party of the state $|\psi^{(0)}\rangle$. *Note that (1) this is a local operation of the group $SL(d_1, \mathbb{C})$ and hence we have $|\psi^{(1)}\rangle \in SLOCC_{|\psi^{(0)}\rangle}$, (2) $|\psi^{(1)}\rangle$ is not normalized and (3) it has the property that $\rho_1^{(1)} = |\det(\rho_1^{(0)})|^{\frac{1}{d_1}} \frac{1}{d_1}\mathbb{1}$.*

3. *We proceed similarly applying $\rho_2^{(1)-\frac{1}{2}}$ to the party 2 of $|\psi^{(1)}\rangle$, resulting into a state $|\psi^{(2)}\rangle$ which has similar properties as (1) and (2) described in the previous iteration. Despite it has the property that $\rho_2^{(2)} = |\det(\rho_2^{(1)})|^{\frac{1}{d_2}} \frac{1}{d_2}\mathbb{1}$, the property (3) given above is in general not fulfilled at the current iteration. Then we repeat a similar operation for each local party until we apply $\rho_N^{(N-1)-\frac{1}{2}}$ to the party $N$ of the state $|\psi^{(N-1)}\rangle$, resulting into a state $|\psi^{(N)}\rangle$ with $\rho_N^{(N)} = |\det(\rho_N^{(N-1)})|^{\frac{1}{d_N}} \frac{1}{d_N}\mathbb{1}$ in which similar properties as (1) and (2) given above hold.*

4. *We repeat steps 2 and 3 iteratively a certain nuber of times $R$, so that the total number of iterations at the end of the algorithm will be $f = N \cdot R$.*

Let us now discuss the properties of algorithm1. Since both the trace and the determinant are invariant under unitary operations, by considering the diagonal forms of $\rho_1^{(1)}$ and $\rho_1^{(0)}$ and recalling that the geometric mean is always smaller or equal than the arithmetic mean, one can see that after step 2 we have the following condition,

$$tr(|\psi^{(1)}\rangle\langle\psi^{(1)}|) = tr(\rho_1^{(1)}) = d_1 |\det(\rho_1^{(0)})|^{\frac{1}{d_1}} \leq tr(\rho_1^{(0)}) = tr(|\psi^{(0)}\rangle\langle\psi^{(0)}|), \tag{6.1.2}$$

with equality iff $\rho_1^{(0)} = \frac{1}{d_1}\mathbb{1}$. A similar condition holds for the subsequent iterations of the algorithm. Together with the fact that the trace of positive definite operators has always a positive lower bound, this implies that the trace norm of the states within algorithm 1 will be always positive and it will decrease after each iteration unless a critical state is reached.

Furthermore, note that the trace norm of the initial state $|\psi^{(0)}\rangle$ can tend to 0 if and only if $SLOCC_{|\psi^{(0)}\rangle}$ is in the null cone. Therefore, if the initial state $|\psi^{(0)}\rangle$ is either stable or strictly semistable, then the algorithm will converge to a critical state which trace norm does not vanish. That is, algorithm 1 distinguishes whether or not the initial state is in the null cone and it converges to a critical state with finite trace norm if and only if the initial state $|\psi^{(0)}\rangle$ is not in a null cone. This convergence is exact if $|\psi^{(0)}\rangle$ is polystable and it has associated a certain numerical precision which depends on $f$ if $|\psi^{(0)}\rangle$ is semistable.

## 6.2 An algorithm to find 2-uniform states

Aside from its fundamental relevance in entanglement theory as a method to distinguish states which are in the null cone from states which are not, algorithm 1 can be understood as a numerical method which converges or not to a critical state depending on the features of the SLOCC class containing the initial state of the algorithm. This perspective provides an inspiration to try to find AME states by means of designing a similar algorithm which acts nonlocally and reduces the trace of the state at each iteration unless an AME state is reached. In particular, we are interested in exploring this idea to try to find an $AME(4,6)$ state.

In order to explain our approach, let us first write a 4-partite quantum state as

$$\begin{aligned} |\psi\rangle &= \sum_{i,j,k,l} a_{ijkl} |ijkl\rangle = (A^{AB} \otimes \mathbb{1}) \left|\phi_d^+\right\rangle_{AC} \left|\phi_{BD}^+\right\rangle \\ &= (A^{AC} \otimes \mathbb{1}) \left|\phi_{AD}^+\right\rangle \left|\phi_{CB}^+\right\rangle = \left(A^{AD} \otimes \mathbb{1}\right) \left|\phi_{AB}^+\right\rangle \left|\phi_{DC}^+\right\rangle, \end{aligned} \tag{6.2.1}$$

with $A^{AB} = \sum_{i,j,k,l=0}^{d-1} a_{ijkl} |ij\rangle \langle kl| \in \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_B)$ and similarly for $A^{AC}$ and $A^{AD}$. Note that $|\psi\rangle$ will be an AME state if and only if $A^{AB}$ and the permutations of its elements $A^{AC}$ and $A^{AD}$ are all unitary operators. This property of $A^{AB}$ is called *multi-unitarity* [23].

Being this notation introduced, we are ready for the following consideration. Suppose that in algorithm 1 we apply to the initial state $|\psi^{(0)}\rangle$ the inverse of the square root of a reduction to two or more parties, e.g.

$$|\det(\rho_{12}^{(0)})|^{\frac{1}{2d_1d_2}} \rho_{12}^{(0)-\frac{1}{2}} \mathbb{1} \otimes \cdots \otimes \mathbb{1} |\psi^{(0)}\rangle = |\psi^{(1)}\rangle. \tag{6.2.2}$$

Similarly as above, after this iteration we have

$$tr(|\psi^{(1)}\rangle\langle\psi^{(1)}|) \leq tr(|\psi^{(0)}\rangle\langle\psi^{(0)}|), \tag{6.2.3}$$

with equality iff $\rho_{12}^{(0)} = \frac{1}{d_1d_2}\mathbb{1}$. This means that by applying the nonlocal version of the algorithm 1 which is exemplified in equation (6.2.2) we preserve the property that the trace is reduced unless the corresponding reduction is maximally mixed. Note that this is the same mechanism by which algorithm 1 converges to a 1-uniform state under some conditions for the initial state. This fact motivates the exploration of a nonlocal version of algorithm 1 to find $k$-uniform states. In particular, we wish to focus on the simplest nontrivial case, namely 4-partite AME states of small local dimensions, with special emphasis on trying to find an AME(4,6) state because its existence is currently an open problem. For that purpose, let us define the following algorithm.

**Algorithm 2.** *First of all, we generate a random 4-partite initial state in local dimension $d$. We need the following definitions and notation.*

- *First, consider the hermitian matrix $Q = M + M^\dagger$, with $M$ a $d^2 \times d^2$ matrix which coefficients are of the form $a + bi$, where $i$ is the imaginary unit and $a, b \in \mathbb{R}$ are the outputs of a function which generates pseudo-random numbers sampled from a Gaussian distribution of mean 0 and variance 1.*

- *Defining the unitary matrix $U_Q = e^{i\epsilon Q}$, with $0 < \epsilon \leq 1$, we compute the state*

$$|\psi^{(0)}\rangle = U_Q \otimes \mathbb{1} |\phi\rangle \in \mathcal{H} \tag{6.2.4}$$

*with* $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C \otimes \mathcal{H}_D = \mathbb{C}^{d^{\otimes 4}}$, $U_Q \in \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_B)$ *and* $|\phi\rangle \in \mathcal{H}$ *an arbitrary state. This enables us to choose the initial state* $|\psi^{(0)}\rangle$ *to be close to a desired state* $|\phi\rangle$ *up to a precision* $\epsilon^{-1}$.

- *We denote as* random state *the choices* $|\phi\rangle = \left|\phi_d^+\right\rangle_{AC} \left|\phi_{BD}^+\right\rangle$ *and* $\epsilon = 1$. *This will be the choice of the initial state of the algorithm by default. In special cases, we will denote as* state close to $|\phi\rangle$ *the choices of an arbitrary state* $|\phi\rangle$ *and* $\epsilon << 1$. *Due to the way it has been generated, the subset of initial states* $|\psi^{(0)}\rangle$ *which have at least one reduction to two parties not being full rank is of measure 0.*

- *We denote the reduction of a state* $|\psi^{(r)}\rangle$ *to the parties* $X$ *and* $Y$ *as* ${\rho^{(r)}}_{XY}$.

*Now that this notation has been introduced, we are able to establish the steps of the algorithm we propose.*

1. *We start by choosing an initial random state* $|\psi^{(0)}\rangle$.

2. *We apply* $\rho_{AB}^{(0)\,-\frac{1}{2}} \otimes \mathbb{1} \left|\psi^{(0)}\right\rangle = |\psi^{(1)}\rangle$ *with* $\rho_{AB}^{(0)\,-\frac{1}{2}} \in \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_B)$, *so that we have* ${\rho^{(1)}}_{AB} = \frac{1}{d^2}\mathbb{1}$.

3. *We apply* ${\rho^{(1)}}_{AC}^{-\frac{1}{2}} \otimes \mathbb{1}|\psi^{(1)}\rangle = |\psi^{(2)}\rangle$ *with* $\rho_{AC}^{(1)\,-\frac{1}{2}} \in \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_C)$, *so that now we have* ${\rho^{(2)}}_{AC} = \frac{1}{d^2}\mathbb{1}$. *However, note that in general at this step we have* ${\rho^{(2)}}_{AB} \not\propto \mathbb{1}$.

4. *We apply* ${\rho^{(2)}}_{AD}^{-\frac{1}{2}} \otimes \mathbb{1}|\psi^{(2)}\rangle = |\psi^{(3)}\rangle$ *with* $\rho_{AD}^{(2)\,-\frac{1}{2}} \in \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_D)$, *which leads to similar results as the previous step.*

5. *We repeat steps 3, 4 and 5 iteratively a certain number of times. Each of those steps will be called an* iteration. *Note that therefore, the number of iterations will always be a multiple of 3.*

6. *After a certain number of iterations which depends on the local dimension* $d$, *we stop the algorithm and check whether or not the final state is an AME state.*

Due to inequality (6.2.3), in algorithm 2 the trace is reduced after each iteration unless we reach an AME state. However, note that by applying nonlocal operations we lose the property that any two states which belong to subsequent iterations are in the same SLOCC class and hence wan analytical description of operations of the type (6.2.2) is left for a further research line. Therefore, an empirical exploration of algorithm 2 must be done.

## 6.3 Results by choosing randomly the initial states

As we have seen, the results of implementing algorithm 2 are difficult to predict because it is not guaranteed that two states which belong to different iterations are in the same SLOCC class. Therefore, we need to use numerical tools to implement it and analyze its results a posteriori. In this section we will explain those results after implementing algorithm 2 for randomly chosen initial states having local dimension $2 \leq d \leq 6$. We will focus on both the evolution of the states within the algorithm and the probability of finding AME states for each choice of $d$, which we define as the fraction of AME states found out of the total number of instances tried. In order to see clearly the results of the algorithm, we will normalize the state within each iteration. This will prevent the states which do not converge to AME

states to have a vanishing norm at some iteration of the numerical implementation of the algorithm.

For such analysis, we will run the algorithm for $m$ different instances of random states labeled as $i \in \{1, ..., m\}$ for $f$ iterations each. Naturally, a state within the iteration $r$ of the algorithm which evolves from an initial state labeled by $i$ will be called $|\psi_i^{(r)}\rangle$. Furthermore, given a general 4-partite state $|\psi\rangle$ written as (6.2.1), we denote the singular value decomposition of $A^{XY}$ as $A^{XY} = U\Sigma V$, where $U$ and $V$ are unitaries and $\Sigma = diag(s_1, ..., s_{d^2})$ is the diagonal matrix of the Schmidt coefficients $\{s_l\}$ of $|\psi\rangle$ corresponding to the bipartition among parties $XY$ and the rest of the system.

As a tool to analyze the evolution of the states within the algorithm, consider the Von-Neumann entropy corresponding to the bipartition among parties $XY$ and the rest of the system of the state $|\psi_i^{(r)}\rangle$,

$$S_i^{XY}(r) = -\sum_{l=0}^{d^2-1} s_l^2 \log\left(s_l^2\right). \tag{6.3.1}$$

At each iteration we will analyze the quantity

$$S_i(r) = S_i^{AB}(r) + S_i^{AC}(r) + S_i^{AD}(r), \tag{6.3.2}$$

which can be understood as the average amount of bipartite entanglement among the three possible bipartitions of $|\psi_i^{(r)}\rangle$ (up to a factor 3). We denote as $\{S_i(r)\}_i$ the set of values of (6.3.2) along the iterations $\{r\}$ given an initial state $i$ and as $\{S_i(r)\}$ the set of all values of (6.3.2) along all the iterations $\{r\}$ given all the choices $\{i\}$ of initial states for which we run the algorithm.

For each dimension $2 \leq d \leq 6$, we will plot the curves defined by $\{S_i(r)\}$ as a function of the iterations. Each curve defined by $\{S_i(r)\}_i$ will be called a *trajectory* and it will be denoted as $S_i$. As we will see, $\{S_i\}$ can converge to a single value but they can also show a repetitive pattern among a set of different values of $S_i(r)$. Let us recall that we denote this situation as *convergence*. Suppose a set of different trajectories which reach convergence to the same set of three values of $S_i(r)$. We call such set of trajectories a *plateau*.

Now that the notation has been introduced, we are ready to analyze the numerical results of algorithm 2. This analysis will be done for each dimension $2 \leq d \leq 6$. For each value of $d$, we will give the relevant details about how the convergence is reached. That is, we will consider whether or not plateaus are formed, whether or not the trajectories are periodic along the iterations and on the probability of finding AME states within the instances we have sampled. The results explained below are summarized in Table 6.1.

- For $d = 2$, it is proven that no AME exists [19] and hence no AME state has been found with the algorithm within a sample of $10^3$ instances. The convergence is reached after approximately 150 iterations, and once the convergence is reached no plateaus have been found. The states $\{|\psi_i^{(r)}\rangle\}_i$ corresponding to each trajectory $S_i$ are periodic every 6 iterations.

- For $d = 3$ and $d = 4$ the trajectories reach convergence after 200 and 400 iterations respectively. Most of the trajectories which do not converge to AME states form plateaus (see Figure 6.3.1). In most of the cases, the corresponding trajectories are periodic every three iterations once the convergence is reached.

  For a sample generated by running the algorithm for $10^4$ different initial states which are randomly chosen for both $d = 3$ and $d = 4$, the output states are AME states in

| | $d=2$ | $d=3$ | $d=4$ | $d=5$ | $d=6$ |
|---|---|---|---|---|---|
| Prob(AME) | 0% | 90% | 20% | $10^{-4}$% | 0% |
| Rand Inst | $10^3$ | $10^4$ | $10^4$ | $10^6$ | $10^6$ |
| Plateaus | No | Yes | Yes | No | No |
| Iters needed | 150 | 200 | 400 | $3 \cdot 10^4$ | $10^5$ |
| Periodicity | 6 | 3 | 3 | 3 | 3 |

**Table 6.1:** In this table we show the results of the algorithm we propose according to the samples we have checked. Along the different rows we represent the probability of finding AME states, the number of instances which we have checked starting from randomly chosen states, whether or not plateaus are formed in our plots, the number of iterations needed to reach convergence and the number of iterations every which most of the trajectories are periodic once the convergence is reached. Each of those parameters is represented for the different local dimensions $2 \leq d \leq 6$, each of which corresponds to a column.

90% of the instances for $d = 3$ and in 15% of the instances for $d = 4$. However, the probability of finding AME states can be modified by choosing appropriately the initial states. As an example for $d = 3$, in a sample generated by running the algorithm for $10^3$ initial states close to

$$|\psi\rangle = \frac{1}{\sqrt{3}} \sum_{i=0}^{2} |i, i, i, i\rangle \tag{6.3.3}$$

up to a precision defined by $\epsilon = 10^{-30}$, 95% of the output states are AME states.

- For $d = 5$ and $d = 6$ the convergence is reached after approximately $3 \cdot 10^5$ and $10^6$ iterations respectively (see Figure 6.3.2), which are different orders of magnitude with respect to the cases discussed above. In addition, each initial state has associated a different trajectory and no plateaus are formed in the convergence. Similarly as for $d = 3$ and $d = 4$, in most of the trajectories the corresponding trajectories are periodic every 3 iterations (see Figure 6.3.2).

  Out of $10^6$ randomly chosen initial states, only one AME state has been found for $d = 5$ and no AME states have been found for $d = 6$. This clear drop of the probability of finding AME states with respect to the cases $d = 3$ and $d = 4$ might be related to the increment of the number of iterations needed to reach convergence and with the fact that no plateaus are formed for $d = 5$ and $d = 6$ in contrast to the cases $d = 3$ and $d = 4$.

As a general property, let us note that within the plateaus, the corresponding sates are periodic every 3 (for $3 \leq d \leq 6$) iterations or 6 (for $d = 2$) iterations, which is a multiple of 3. This is because algorithm 2 applies the corresponding operator on the same splitting every 3 iterations.

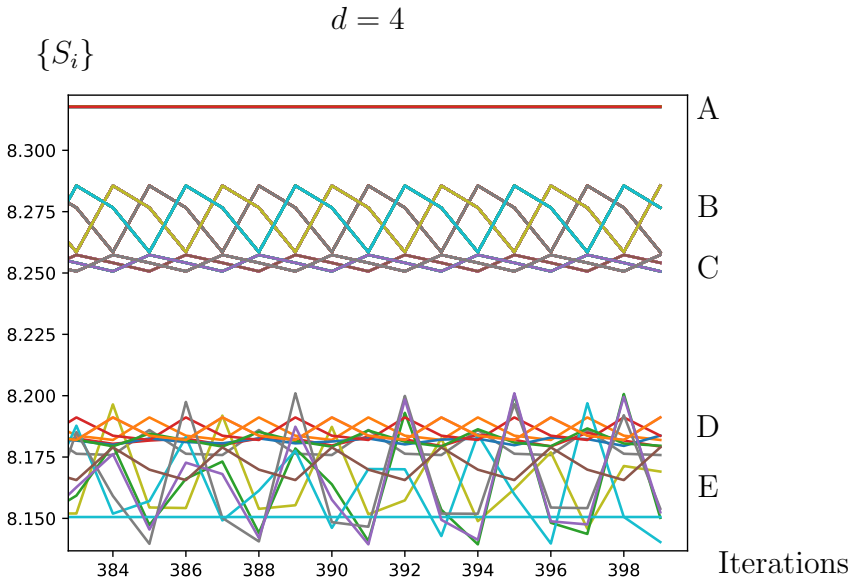


**Figure 6.3.1:** $\{S_i\}$ as a function of the last iterations corresponding to 200 initial states of local dimension $d = 4$. The initial states have been randomly chosen. We show this plot in order to illustrate the formation of plateaus. We see the convergence to AME states (A) and three plateaus (B, C and D), among other trajectories (E) which present more complicated patterns. For several instances we have noticed that the periodicity of the trajectories every three iterations coincides with the fact that the states are periodic every three iterations. However, our analysis is not complete enough to ensure that this coincidence holds as a general rule.

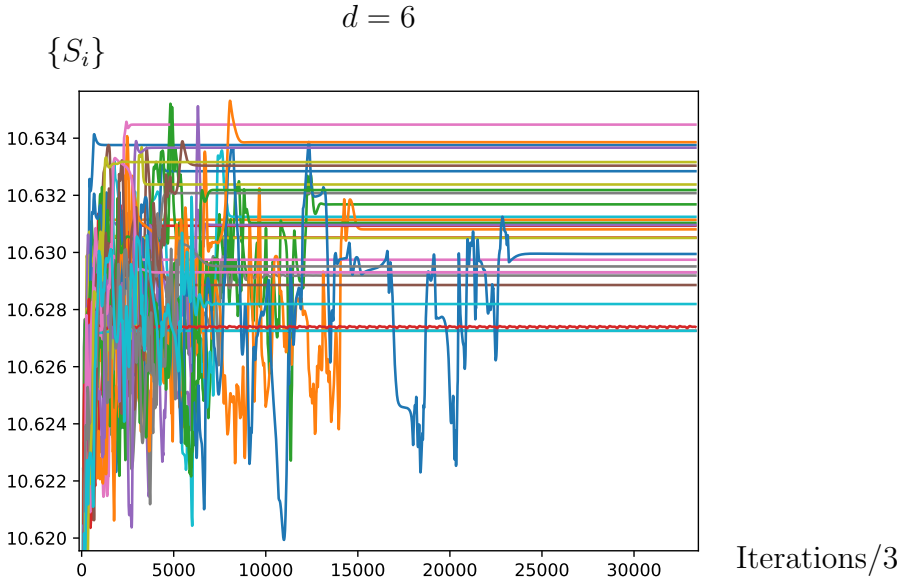


**Figure 6.3.2:** $\{S_i\}$ as a function of the number of iterations corresponding to 50 initial states of local dimension $d = 6$. We show this plot as an example of the fact that for 5 and 6 dimensions, no plateaus are formed. In order to make the plot more clear, we represent the values $\{S_i\}$ only every 3 iterations, taking advantage of the fact that in most of the cases the trajectories are periodic every 3 iterations. That is, all the straight lines represent trajectories which are periodic every three iterations. It is clear that each trajectory reaches its convergence in different values, so that no plateaus are formed. Similarly as in Figure 6.3.1, for several instances we have noticed that the periodicity of the trajectories every three iterations coincides with the fact that the states are periodic every three iterations. However, our analysis is not complete enough to ensure that this coincidence holds as a general rule.

## 6.4 Results by restricting the initial states

As we have seen, the probability of finding AME states for a given sample of instances can be modified depending on how we choose the initial states of the algorithm. Here we will explore this idea. For that aim, first we will design a new algorithm which differs from the previous one because in this case, at each iteration we will apply a different map which also leads to a state which has maximal entropy of entanglement with respect to one particular bipartition. We will see that it converges after few iterations to a very specific state $|\phi\rangle$ up to numerical precision. Using $|\phi\rangle$ as an initial state for algorithm 2, the probability of finding AME states with respect to each local dimension will be change drastically with respect to the probabilities given previously.

Given a quantum state

$$|\psi\rangle = A^{AB} \otimes \mathbb{1} \sum_{i,j=0}^{d-1} \left|\phi_d^+\right\rangle_{AC} \left|\phi_d^+\right\rangle_{BD}, \tag{6.4.1}$$

and denoting the singular value decomposition of $A^{AB} \in \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_B)$ by $A^{AB} = U\Sigma V$ as

we have done above, the operation $\rho_{AB}^{-\frac{1}{2}} \otimes \mathbb{1} |\psi\rangle$ can be written as

$$\begin{array}{rccc} \mathcal{A}: & \mathbb{C}^{d^{\otimes 4}} & \to & \mathbb{C}^{d^{\otimes 4}} \\ |\psi\rangle = U\Sigma V \otimes \mathbb{1} \left|\phi_d^+\right\rangle_{AC} \left|\phi_d^+\right\rangle_{BD} & \mapsto & |\psi^{(1)}\rangle = U\mathbb{1}V \otimes \mathbb{1} \left|\phi_d^+\right\rangle_{AC} \left|\phi_d^+\right\rangle_{BD}. \end{array} \tag{6.4.2}$$

Obviously, the fact that $|\psi^{(1)}\rangle$ has maximal bipartite entanglement with respect to the bipartition $AB|CD$ is because $UV$ is a unitary operator. That is, in general we can create maximal entanglement across the bipartition $AB|CD$ by considering the transformation

$$\begin{array}{rccc} \mathcal{W}: & \mathbb{C}^{d^{\otimes 4}} & \to & \mathbb{C}^{d^{\otimes 4}} \\ |\psi\rangle = A^{AB} \otimes \mathbb{1} \left|\phi_d^+\right\rangle_{AC} \left|\phi_d^+\right\rangle_{BD} & \mapsto & |\psi'\rangle = W \otimes \mathbb{1} \left|\phi_d^+\right\rangle_{AC} \left|\phi_d^+\right\rangle_{BD}, \end{array} \tag{6.4.3}$$

where $W \in \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_B)$ is a unitary operator. Since we are interested in the design of an operation to implement within the iterations $\{r\}$ of a certain algorithm, we are interested in unitary operators $W(A^{AB})$ which depend on the operator $A^{AB}$. One particular transformation which fulfills this condition is as follows,

$$\begin{array}{rcl} \mathcal{W}_{\mathcal{P}}: \mathcal{B}(\mathbb{C}^{d^{\otimes 2}}) & \to & \mathcal{B}(\mathbb{C}^{d^{\otimes 2}}) \\ A^{AB} & \mapsto & A'^{AB} = e^{i(A^{AB} + A^{AB\dagger})}. \end{array} \tag{6.4.4}$$

Consider now the following algorithm defined by the operation $\mathcal{W}_P$.

**Algorithm 3.** *In this algorithm we will use similar notation as in algorithm 2.*

1. *We choose a random 4-partite state* $|\psi\rangle = A^{AB} \otimes \mathbb{1} \left|\phi_d^+\right\rangle_{AC} \left|\phi_d^+\right\rangle_{BD}$.
2. *We apply* $\mathcal{W}_{\mathcal{P}}$ *to the operator* $A^{AB}$. *This leads to the state* $|\psi^{(1)}\rangle = {A^{(1)}}^{AB} \otimes \mathbb{1} \left|\phi_d^+\right\rangle_{AC} \left|\phi_d^+\right\rangle_{BD} = {A^{(1)}}^{BD} \otimes \mathbb{1} \left|\phi_d^+\right\rangle_{AB} \left|\phi_d^+\right\rangle_{DC}$.
3. *We apply* $\mathcal{W}_{\mathcal{P}}$ *to the operator* ${A^{(1)}}^{BD} \in \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_D)$.
4. *Similarly, we apply* $\mathcal{W}_{\mathcal{P}}$ *to the operator* ${A^{(2)}}^{CD} \in \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_C)$. *This leads to the state* $|\psi^{(3)}\rangle = {A^{(3)}}^{AC} \otimes \mathbb{1} \left|\phi_d^+\right\rangle_{AD} \left|\phi_d^+\right\rangle_{CB} = {A^{(3)}}^{BC} \otimes \mathbb{1} \left|\phi_d^+\right\rangle_{AC} \left|\phi_d^+\right\rangle_{BD}$.
5. *We repeat steps 2, 3 and 4 iteratively a certain number of iterations* $f$.

After approximately 50 iterations, algorithm 3 converges to the state

$$|\phi\rangle = \alpha(d) \left|\phi_d^+\right\rangle_{AC} \left|\phi_d^+\right\rangle_{BD} + \beta(d) \left|\phi_d^+\right\rangle_{AD} \left|\phi_d^+\right\rangle_{CB} + \gamma(d) \left|\phi_d^+\right\rangle_{AB} \left|\phi_d^+\right\rangle_{DC} \tag{6.4.5}$$

up to a certain numerical precision $\eta \sim 10^{-14}$ in the coefficients of $|\phi\rangle$. $\alpha$, $\beta$ and $\gamma$ are complex parameters which depend on the dimension. We denote as $\mathcal{H}_\eta \subset \mathcal{H}$ the set of states within the whole Hilbert space $\mathcal{H}$ containing states which are close to the state of equation (6.4.5) up to a precision $\eta$.

Suppose now we use the states in $\mathcal{H}_\eta$ as input states for different instances of algorithm 2. Those states can be generated by running by running algorithm 3 choosing randomly the initial states as described above. Considering this restriction, we obtain the following results for local dimensions $3 \leq d \leq 6$, which are summarized in Table 6.2.

| | $d=3$ | $d=4$ | $d=5$ | $d=6$ |
|---|---|---|---|---|
| Prob(AME) | 0% | 100% | 0.25% | 0% |
| Rand Inst | $10^4$ | $10^4$ | 2000 | $10^5$ |
| Plateaus | Yes | No (AME) | Yes | No |
| Iters needed | 200 | 400 | $10^3$ | $10^4$ |
| Periodicity | 3 | 3 | 3 | 3 |

**Table 6.2:** In this table we show the results of the algorithm by choosing the initial states from the set $\mathcal{H}_\eta$ and according to the samples we have checked. Along the different rows we represent the probability of finding AME states, the number of instances which we have checked starting from randomly chosen states, whether or not plateaus are formed in our plots, the number of iterations needed to reach convergence and the number of iterations every which most of the trajectories are periodic once the convergence is reached. Each of those parameters is represented for the different local dimensions $3 \leq d \leq 6$, each of which corresponds to a column.

- For $d = 3$ no AME state has been found within a statistical ensemble of $10^4$ instances. Once the convergence is reached, the trajectories are periodic every three iterations and form plateaus. The convergence is reached after approximately 200 iterations, similarly as choosing randomly the initial states.

- For $d = 4$ we have found AME states in 100% of the instances, with a statistical ensemble of $10^4$ instances. As a consequence, no plateaus have been found. The convergence is reached after approximately 400 iterations, similarly as choosing randomly the initial states.

- For $d = 5$ we found 5 AME states with a statistical ensemble of 2000 instances. Moreover, we can distinguish plateaus when the convergence is reached and we need a number of iterations of the order of $10^3$ to reach the convergence, in contrast to the number of iterations needed by choosing randomly the initial states. Similarly as choosing randomly the initial states, once the convergence is reached most of the trajectories are periodic every three iterations.

- For $d = 6$ we did not find any AME state with a statistical ensemble of $10^5$ instances and no plateaus have been found as well. However, we empirically observe that we need of the order of $10^4$ iterations to reach convergence, in contrast to the number of iterations needed by choosing randomly the initial states. Similarly as choosing randomly the initial states, once the convergence is reached most of the trajectories are periodic every three iterations.

Those results show that very different results can be obtained by choosing appropriately the initial states. However, it is still unclear how the initial states and the probabilities of finding AME states are related, and hence finding a method to choose the initial states which is specifically focused on trying to find an $AME(4, 6)$ state is left for a further research line.

# Chapter 7

# Analytical description of AME states in small system sizes

The main constructions for AME states known so far are based on MDS codes [22, 23, 43], combinatorial designs [23, 66] and qudit graph states [45]. The main necessary conditions for the existence of AME states derived in the current literature are based on bounds for the existence of quantum codes [1, 18]. Inspired by some of those tools, we investigate in this chapter analytically both explicit constructions and the structure of AME states, with the main focus on the 4-partite case. First we will give an explicit construction for minimal support AME states of 4 parties of odd local dimensions and we will generalize our construction to 5 parties in local dimensions which are not a multiple of 2 nor 3, and for 6 parties of odd local dimensions. Then, we will focus on constructing $AME(4,3)$ states having $d^3$ terms in the computational basis. In particular, we will give an explicit construction for 4-partite AME states of odd local dimensions which also involves the construction of two MOLS. This is despite the fact that our construction differs in its methodology from the constructions of AME states of minimal support. This coincidence motivates the exploration of 4-partite AME states in more general scenarios, seeking an understanding of how the connection between $AME(4,d)_{min}$ and two MOLS is generalized to the nonminimal support case. Following this research line, we will give some alternative descriptions of 4-partite AME states through which we attempt to prove that constructing any 4-partite AME state implies constructing two MOLS and we will provide some necessary conditions for the existence of 4-partite AME states.

Throughout the whole section, $\oplus$ and $\ominus$ denote the summation and subtraction $mod(d)$. Similarly, the product will be computed $mod(d)$ and it will be denoted by $\cdot$ if there is the possibility of confusing the notation and by no symbol otherwise.

## 7.1 Explicit constructions for AME states of minimal support

Using the relation between AME states of minimal support and MOLH stated in Theorem 3.2, let us explore an explicit construction of MOLS to give an explicit formula for AME states of minimal support of four parties of odd local dimensions which generalizes the $AME(4,3)$ state given in (1.3.8)[21], as stated in the following proposition.

**Proposition 1.** *The state*

$$|\Psi(4,d)\rangle = \frac{1}{d}\sum_{i,j} |i\rangle\,|j\rangle\,|i\oplus n\cdot j\rangle\,|i\oplus m\cdot j\rangle \text{ with } m,n\in\mathbb{N}\setminus 0 \tag{7.1.1}$$

*is an AME state of* 4 *parties if and only if* $n$, $m$ *and* $n\ominus m$ *are all coprime with* $d$. *Moreover, there exists a suitable choice of* $n$ *and* $m$ *fulfilling this condition if and only if* $d$ *is odd.*

*Proof.* Let us define the two squares $T^{(1)}$ and $T^{(2)}$ as $T^{(1)}_{ij} = i\oplus n\cdot j$ and $T^{(2)}_{ij} = i\oplus m\cdot j$, where $i\in\mathbb{Z}_d$ and $j\in\mathbb{Z}_d$ indicate their rows and columns. Since the state given in equation (7.1.1) is of minimal support, it is necessary and sufficient to show that $T^{(1)}$ and $T^{(2)}$ form two MOLS iff $n$, $m$ and $n\ominus m$ are all coprime with $d$. We will first show that $T^{(1)}$ and $T^{(2)}$ are latin squares iff $n$ and $m$ are coprime with $d$, and then we will see that they are orthogonal iff $n\ominus m$ is coprime with $d$.

Let us first show that if $n$ and $m$ are coprime with $d$, then $T^{(1)}$ and $T^{(2)}$ are latin squares. Suppose $n$ ($m$) is coprime with $d$. Elementary number theory tells us that in such case, all the elements in $n\cdot\{0,...,d-1\}\,mod(d)$ $\big(m\cdot\{0,...,d-1\}\,mod(d)\big)$ are different [75]. As a consequence, the set of numbers $\{n\cdot j\}$ ($\{m\cdot j\}$) contains all the elements in $\mathbb{Z}_d$ with no elements being repeated. Together with the fact that, by construction, each row $i$ of $T^{(1)}$ ($T^{(2)}$) consists of a different cyclic permutation of the elements $\{n\cdot j\}$ ($\{m\cdot j\}$), this implies that no elements are repeated along the rows and along the columns of both $T^{(1)}$ and $T^{(2)}$ (that is, both $T^{(1)}$ and $T^{(2)}$ are latin squares) as long as both $n$ and $m$ are coprime with $d$.

Now let us show that $n$ and $m$ being coprime with $d$ is also a necessary condition for $T^{(1)}$ and $T^{(2)}$ to be latin squares. Suppose that $n$ ($m$) is not coprime with $d$. Then, there exists an integer $a<d$ ($b<d$) such that $a\cdot n = d$ ($b\cdot m = d$), leading to $T^{(1)}_{0,j} = T^{(1)}_{a,j}$ ($T^{(1)}_{i,0} = T^{(1)}_{i,b}$), which is a contradiction to the definition of latin squares. Therefore, it is also necessary that $n$ and $m$ are both coprime with $d$.

Consider the square $S$ constructed by superimposing $T^{(1)}$ and $T^{(2)}$. It remains to show that $n\ominus m$ being coprime with $d$ is necessary and sufficient to have no pairs repeated in $S$. Let us first show that it is sufficient. Suppose that there are two equal pairs in $S$. That is, for $(i,j)\neq(k,l)$, where $i$ and $k$ label the rows of $S$ while $j$ and $l$ label the columns of $S$, we have

$$\begin{aligned} &i\oplus n\cdot j = k\oplus n\cdot l \quad \text{and}\\ &i\oplus m\cdot j = k\oplus m\cdot l. \end{aligned} \tag{7.1.2}$$

Substracting both conditions, we get

$$(n\ominus m)\cdot j = (n\ominus m)\cdot l, \tag{7.1.3}$$

which has two solutions: either $j=l$ (and, since $T^{(1)}$ and $T^{(2)}$ must be latin squares, $i=k$ in equation (7.1.2)), or $n\ominus m$ is not coprime with $d$. This implies that $n\ominus m$ being coprime with $d$ is sufficient for $S$ to have no pairs repeated.

Finally, we want to show that $n\ominus m$ must be coprime with $d$ in order to have no pairs repeated in $S$. To that end, let us rewrite equation (7.1.2), which nontrivial solutions give the coordinates of equal pairs in $S$, as

$$i\ominus k = n(l\ominus j) = m(l\ominus j). \tag{7.1.4}$$

By subtracting $m(l \ominus j)$ at each of the three sides, we are left with

$$\begin{aligned} &(n \ominus m)(l \ominus j) = 0 \quad \text{and} \\ &i \oplus m \cdot j = k \oplus m \cdot l. \end{aligned} \tag{7.1.5}$$

First of all, note that the first equation in (7.1.5) has always no trivial solution if $n \ominus m$ is not coprime with $d$. Therefore, if the second equation also shares this solution, it is proven that $n \ominus m$ being coprime with $d$ is a necessary condition. Second, under the assumption that $T^{(1)}$ and $T^{(2)}$ are both latin squares, each of their rows and each of their columns must contain all the elements in $\mathbb{Z}_d$. Therefore, for any $m \in \mathbb{N} \setminus 0$ coprime with $d$ we have that, given any two columns $j$ and $l$, there exist two respective positions $i$ and $k$ in those columns so that the second equation in (7.1.5) is fulfilled. In particular, we can find such $i$ and $k$ if $j$ and $l$ are arbitrarily chosen to fulfill the first equation in (7.1.5). This implies that it is necessary that the first equation in (7.1.5) is not fulfilled, and this is possible only if $n \ominus m$ is coprmie with $d$. With this argument we conclude the proof that $T^{(1)}$ and $T^{(2)}$ are orthogonal iff $n \ominus m$ is coprime with $d$, which in turns ends the proof of the first claim in proposition 1.

Let us now prove the second claim in our proposition. We will first show that $d$ must be odd. To that end, note that either $n$, $m$ or $n \ominus m$ is necessarily even. Therefore, the three parameters $\{n, m, n \ominus m\}$ can not be simultaneously coprime with any even $d$, and hence to construct the AME state given in equation (7.1.1) it is necessary that $d$ is odd.

To prove that $d$ being odd is also sufficient, it is sufficient to find a particular example. We can choose for instance $n = 1$ and $m = 2$, which obviously fulfills the condition that $n$, $m$ and $n \ominus m$ are coprime with any odd dimension $d$. This can be seen as a generalization of the $AME(4, 3)$ state given in (1.3.8). Another example fulfilling such condition is $n = 1$ and $m = d \ominus 1$, which can also be seen as a generalization of (1.3.8). □

Aside from the examples $(m, n) = (1, 2)$ and $(m, n) = (1, d-1)$ given above, the complete set of all the possible choices for $n$ and $m$ compatible with the fact that $n$, $m$ and $n \ominus m$ are coprime with a given odd dimension $d$ can be found by solving the equations

$$\begin{aligned} a_1 \cdot n &= 1 \\ a_2 \cdot m &= 1 \\ a_3 \cdot (n \ominus m) &= 1, \end{aligned} \tag{7.1.6}$$

which must be simultaneously fulfilled for any possible set $\{a_1, a_2, a_3\}$ of integers in $\mathbb{Z}_d$. Such solutions can be solved by applying a multivariable version of the so-called *Chinese Remainder Theorem* [76].

We are now interested in finding a possible generalization of the construction (7.1.1) for five parties. To that end, we formulate the following proposition.

**Proposition 2.** *Consider the state*

$$|\psi(5, d)\rangle = \frac{1}{d} \sum_{i,j} |i\rangle\, |j\rangle \bigotimes_{s=1}^{3} |i \oplus n_s \cdot j\rangle\,, \tag{7.1.7}$$

*with $n_s \in \mathbb{N} \setminus 0$. $|\psi(5, d)\rangle$ is an AME state if and only if the parameters $\{n_s\}$ are all coprime with $d$ and any subtraction among them mod$(d)$ is also coprime with $d$. Moreover, there*

*exists a suitable choice of* $\{n_s\}$ *fulfilling this condition if and only if* $d$ *is not a multiple of 2 or 3.*

*Proof.* Since the state given in (7.1.7) is of minimal support, it is an AME state iff $T^{(s)} = (i \oplus n_s \cdot j)$ is a MOLS for $s \in \{1,2,3\}$. As explained within the proof of proposition 1, it is straightforward to see that $\{T^{(s)}\}$ are all latin squares if and only if $\{n_s\}$ are all coprime with $d$ and also that they are mutually orthogonal if and only if all the subtractions among any two parameters in $\{n_s\}$ are also coprime with $d$. Therefore, the first claim follows from the proof of proposition 1.

Let us now prove that there exists a suitable choice of $\{n_s\}$ fulfilling this condition if and only if $d$ is not a multiple of 2 or 3. From the previous proof, it also is obvious that the parameters $\{n_s\}$ and all the possible subtractions among them $\{n_s \ominus n_{s'}\}$ cannot be simultaneously coprime with any even dimension $d$, but the fact that now we have three parameters in the set $\{n_s\}$ instead of only two parameters leads to even more restrictions. In particular, let us show that $d$ can not be a multiple of 3 either. To that end, we will suppose a dimension $d$ multiple of 3 and we will reach a contradiction.

Note first that any integer, and in particular any element of the set $\{n_s\}$, is of the form $3x + \lambda$, with $\lambda \in \{0,1,2\}$ and $x \in \mathbb{N}$. Note also that if there exists a parameter in $\{n_s\}$, say $n_1$, which is a multiple of 3, then the corresponding square $T^{(1)}$ is not a latin square for any dimension $d$ which is a multiple of 3 and therefore (7.1.7) is not an AME state for such dimension $d$. This leaves us with only two options for $\{n_s\}$ compatible with dimensions which are multiple of 3, and those options are $3x + 1$ or $3x + 2$. Since we have only two possible values of $\lambda$ and three parameters, there necessary exist at least two elements in $\{n_s\}$, say $n_1 = 3x_1 + \lambda_1$ and $n_2 = 3x_2 + \lambda_2$, so that $\lambda_1 = \lambda_2$, and thus we have

$$n_1 \ominus n_2 = 3(x \ominus y), \tag{7.1.8}$$

which is a multiple of 3. This proves that our construction can not lead to an AME state if $d$ is a multiple of 3.

To show that if $d$ is not a multiple of 2 or 3 our construction can lead to an AME state, it is sufficient to find an example. In particular, the choice $(n_1, n_2, n_3) = (1,2,3)$ fulfills the property all the elements in $\{n_s\} \cup \{n_{s'} \ominus n_{s''}\} \quad \forall s, s', s'' \in \{1,2,3\}$ are coprime with any dimension $d$ which is not a multiple of 2 or 3, and hence this choice leads to an AME state for any arbitrary dimension $d$ which is not a multiple of 2 or 3. This completes the proof. □

In order to generalize our construction to six parties, let us formulate the following proposition.

**Proposition 3.** *The quantum state*

$$|\psi(6,d)\rangle = \frac{1}{\sqrt{d^3}} \sum_{i,j,k} |i\rangle\,|j\rangle\,|k\rangle \bigotimes_{s=1}^{3} |\alpha_s i \oplus \beta_s j \oplus \gamma_s k\rangle\,, \tag{7.1.9}$$

*with* $\alpha_s, \beta_s, \gamma_s \in \mathbb{N}$ *and* $n_s \in \mathbb{N} \setminus 0$*, is an AME state if and only if (1) the elements in* $\{\alpha_s, \beta_s, \gamma_s\}$ *are coprime with* $d$ *and (2) the determinant of the matrix*

$$M = \begin{pmatrix} \alpha_1 & \beta_1 & \gamma_1 \\ \alpha_2 & \beta_2 & \gamma_2 \\ \alpha_3 & \beta_3 & \gamma_3 \end{pmatrix}. \tag{7.1.10}$$

*is both nonzero and coprime with d. Moreover, $|\psi(6,d)\rangle$ is an AME state for any odd local dimension d for the matrix M defined above being*

$$M = \begin{pmatrix} 1 & 1 & 1 \\ 1 & d-1 & 1 \\ 1 & 1 & d-1 \end{pmatrix}. \tag{7.1.11}$$

*Proof.* Let us first define the following three-dimensional arrays,

$$\begin{aligned} T^{(1)} &= (\alpha_1 i \oplus \beta_1 j \oplus \gamma_1 k) \\ T^{(2)} &= (\alpha_2 i \oplus \beta_2 j \oplus \gamma_2 k) \\ T^{(3)} &= (\alpha_3 i \oplus \beta_3 j \oplus \gamma_3 k)\,. \end{aligned} \tag{7.1.12}$$

Similarly as in the two propositions above, $|\psi(6,d)\rangle$ is of minimal support. Together with Theorem 3.2, this means that $|\psi(6,d)\rangle$ will be an AME state if and only if $\{T^{(s)}\}$ are three mutually orthogonal latin cubes.

Let us recall that a latin cube is a three dimensional array so that, fixing any one of the coordinates, we are left with a latin square. This implies that $T^{(1)}$, $T^{(2)}$ and $T^{(3)}$ are latin cubes if and only if the nine integers $\{\alpha_s, \beta_s, \gamma_s\}$ are all coprime with $d$, similarly as before.

Consider the three-dimensional array $S$ resulting from superimposing $T^{(1)}$, $T^{(2)}$ and $T^{(3)}$. The entries of $S$ are thus triplets of three numbers which correspond to $T^{(1)}$, $T^{(2)}$ and $T^{(3)}$ respectively. Let us assume $\{\alpha_s, \beta_s, \gamma_s\}$ to be all coprime with $d$, so that $T^{(1)}$, $T^{(2)}$ and $T^{(3)}$ are latin cubes. As we will prove below, those latin cubes will be mutually orthogonal if and only if the system of equations

$$\begin{aligned} \alpha_1 i \oplus \beta_1 j \oplus \gamma_1 k &= x \\ \alpha_2 i \oplus \beta_2 j \oplus \gamma_2 k &= y \\ \alpha_3 i \oplus \beta_3 j \oplus \gamma_3 k &= z \end{aligned} \tag{7.1.13}$$

has unique solution $mod(d)$. To see that it is necessary that the system of equations (7.1.13) has unique solution for $T^{(1)}$, $T^{(2)}$ and $T^{(3)}$ to be mutually orthogonal, consider the following scenarios.

1. Suppose that any two coordinates are fixed, say $i$ and $j$, so that we are left with a one-dimensional array which entries are labeled by $k$. Since $T^{(1)}$, $T^{(2)}$ and $T^{(3)}$ must be latin cubes, no numbers must be repeated along such array. Equivalently, the solution $\{x, y, z\}$ must be different for each choice $k$.

2. Suppose that any one coordinate is fixed, say $i$, so that we are left with a 2-dimensional array which rows are labeled by $j$ and which columns are labeled by $k$. Since $T^{(1)}$, $T^{(2)}$ and $T^{(3)}$ must be mutually orthogonal, such array must consist of three MOLS. Equivalently, no ordered pairs can be repeated within the triplets $\{x, y, z\}$ of such array. This implies that the solution $\{x, y, z\}$ must be different for each choice of $j$ and $k$.

3. Suppose that no coordinate is fixed. The fact that $T^{(1)}$, $T^{(2)}$ and $T^{(3)}$ are mutually orthogonal latin cubes implies that all the possible combinations $\{x, y, z\}$ must appear exactly once, thus being all different triplets among each other.

This proves that $T^{(1)}$, $T^{(2)}$ and $T^{(3)}$ can be three mutually orthogonal latin cubes only if the system of equations (7.1.13) has unique solution $mod(d)$.

The converse statement can be seen as follows. Let us assume that (7.1.13) has unique solution. Considering this assumption at the first scenario above implies that $T^{(1)}$, $T^{(2)}$ and $T^{(3)}$ are latin cubes. Considering this assumption at the second scenario above implies that they are mutually orthogonal.

At this point of our proof, we conclude that our construction leads to an AME state if and only if (1) $\{\alpha_s, \beta_s, \gamma_s\}$ to be all coprime with $d$ and (2) the system of equations (7.1.13) has unique solution $mod(d)$. In fact, the system of equations (7.1.13) will have unique solution if and only if the determinant of its associated matrix

$$\begin{pmatrix} \alpha_1 & \beta_1 & \gamma_1 \\ \alpha_2 & \beta_2 & \gamma_2 \\ \alpha_3 & \beta_3 & \gamma_3 \end{pmatrix} \tag{7.1.14}$$

is nonzero and coprime with the dimension (see [76] and the references therein). This proves the first claim in 3.

To prove the second claim, consider the construction

$$\begin{aligned} T^{(1)} &= (1i \oplus 1j \oplus 1k) \\ T^{(2)} &= (1i \ominus 1j \oplus 1k) \\ T^{(3)} &= (1i \oplus 1j \ominus 1k)\,. \end{aligned} \tag{7.1.15}$$

First, note that fixing any two of the coordinates in any of the cubes $\{T^{(1)}, T^{(2)}, T^{(3)}\}$, we are always left with one dimensional array with no repeated entries if and only if $d$ is odd. Therefore, those are latin cubes for any $d$ odd. Second, note that the determinant of the matrix associated to (7.1.15) is 4, which is coprime with all odd dimensions. Hence, the set $\{T^{(1)}, T^{(2)}, T^{(3)}\}$ in (7.1.15) defines an AME state for any odd dimension $d$. This ends the proof. □

Let us mention that it would be possible to generalize for few more numbers of parties the constructions above. However, we have not been able to find a general expression for that, e.g., a closed expression which gives a state $AME(N,d)_{min}$ for all $N$ even and $d$ odd. Furthermore, let us comment that the constructions above are based on constructing MOLHs, which have been deeply studied in the literature, and therefore our constructions for MOLHs may be known. In particular, the construction of MOLS which defines one of the examples given in preposition 1 is explained in in [77]. However, the explicit formulas for AME states given above are not written in the literature cited in this thesis. As an example, so far the $AME(4,9)$ state was constructed so far by considering the tensor product of two $AME(4,3)$ states [17].

## 7.2 Additional AME states constructed from two MOLS

The structure and existence of AME states of nonminimal support have been less studied than those of AME states of minimal support. Some similarities among AME states of minimal support and the general case have been considered from the perspectives of structural properties [66, 78], quantum codes [20] and the stabilizer formalism [45]. In fact, all the examples of AME states known so far are stabilizer states [17] and most of the systematic constructions known so far are originated by classical codes, namely from AME states

of minimal support [22, 43, 78]. It is an open question to which extend this connection holds [20].

In what follows we will explore some constructions for $AME(4,d)$ states with support $d^3$ which nonzero coefficients are all phases, namely states of the form

$$|\psi\rangle = \sum_{i,j,k=0}^{d-1} \omega^{a(i,j,k)} \, |i,j,k,b(i,j,k)\rangle \, , \tag{7.2.1}$$

with $\omega = e^{i\frac{2\pi}{d}}$ and where $a(i,j,k)$ and $b(i,j,k)$ are bijective functions of $i$, $j$ and $k$. It will often be useful in the following to write $|\psi\rangle$ as

$$|\psi\rangle = \mathbb{1} \otimes A \sum_{i,j=0}^{d-1} |i,j\rangle \, |i,j\rangle = \sum_{i,j=0}^{d-1} |i,j\rangle \, |\psi_{i,j}\rangle \, , \tag{7.2.2}$$

for a given balanced bipartition.

First of all, let us establish the following observation.

**Observation 1.** *A state of the form*

$$|\varphi\rangle = \sum_{i,j,k=0}^{d-1} \omega^{ka(i,j)} |i,j,k,b(i,j)\rangle, \tag{7.2.3}$$

*where $a(i,j)$ and $b(i,j)$ are bijective functions of $i$ and $j$, is an AME state if and only if $T^{(1)} = \big(a(i,j)\big)$ and $T^{(2)} = \big(b(i,j)\big)$ are mutually orthogonal latin squares with respect to the coordinates $i$ and $j$.*

*Proof.* According to equation (7.2.4),

Let $H$ be the generalized Hadamard gate, $H = \sum_{k,l=0}^{d-1} \omega^{kl} \, |k\rangle \, \langle l|$. The state given in (7.2.3) is of minimal support up to LU operations, since we have

$$\mathbb{1} \otimes \mathbb{1} \otimes H^{-1} \otimes \mathbb{1} \sum_{i,j,k=0}^{d-1} \omega^{ka(i,j)} |i,j,k,b(i,j)\rangle = \sum_{i,j=0}^{d-1} |i,j,a(i,j),b(i,j)\rangle. \tag{7.2.4}$$

Clearly, the right hand side of equation (7.2.4) is an AME state if and only if $T^{(1)} = \big(a(i,j)\big)$ and $T^{(2)} = \big(b(i,j)\big)$ are two MOLS with respect to the coordinates $i$ and $j$, which proves the observation. □

An alternative proof of the fact that any reduction of the state $|\varphi\rangle$ given in (7.2.3) is maximally mixed if and only if $T^{(1)} = \big(a(i,j)\big)$ and $T^{(2)} = \big(b(i,j)\big)$ are two MOLS is given in Appendix A.

### 2 MOLS to construct $AME(4,d)$ in odd dimension $d$

Observation 1 implies that if $a(i,j,k)$ and $b(i,j,k)$ in (7.2.1) are functions which depend only on $i$ and $j$, then the resulting state is AME if and only if it is LU-equivalent to a state of support $d^2$. Let us recall that the unitary matrix which maps any orthonormal basis of bipartite separable states to any other orthonormal basis of bipartite separable

states is always a local unitary. This implies that the fact that the state given in (7.2.1) is of minimal support (up to LU operations) if $a(i,j,k)$ and $b(i,j,k)$ depend only on $i$ and $j$ can be alternatively seen by noting that, writing the state given in equation (7.2.3) in the form (7.2.1), the states $\{|\psi_{i,j}\rangle\}$ are separable. Since we are interested in constructing nonminimal support AME states, it is necessary to consider constructions of AME states for which (1) either $a(i,j,k)$, $b(i,j,k)$ or both depend on $i$, $j$ and $k$ and not only on $i$ and $j$, and (2) $\{|\psi_{i,j}\rangle\}$ are entangled states. To that end, we construct a set of AME states for which $\{|\psi_{i,j}\rangle\}$ are maximally entangled states.

**Proposition 4.** *Let $|\psi\rangle$ be the 4-partite state*

$$|\psi\rangle = \frac{1}{\sqrt{d^3}} \sum_{i,j=0}^{d-1} |i,j\rangle \, |\phi_{T_{i,j}^{(1)},T_{i,j}^{(2)}}\rangle \tag{7.2.5}$$

*with local dimension $d$, $|\phi_{T_{i,j}^{(1)},T_{i,j}^{(2)}}\rangle = \sum_{r=0}^{d-1} \omega^{rT_{i,j}^{(1)}} |r \oplus T_{i,j}^{(2)}, r\rangle$, $T_{i,j}^{(1)} = i \ominus j$ and $T_{i,j}^{(2)} = i \oplus j$. $|\psi\rangle$ is an AME state if and only if $d$ is odd.*

*Proof.* We will denote the four parties of $|\psi\rangle$ as $A$, $B$, $C$ and $D$ and we will show that the reductions $\rho_{AB}$, $\rho_{AC}$ and $\rho_{BC}$ corresponding to each bipartition are all proportional to the identity.

As we have seen in section 3.1, it is necessary and sufficient that the set $\{|\phi_{T_{i,j}^{(1)},T_{i,j}^{(2)}}\rangle\}$ is an orthonormal basis to have $\rho_{AB} \propto \mathbb{1}$. Clearly, this will happen if and only if no pairs $(T_{i,j}^{(1)}, T_{i,j}^{(2)})$ are repeated. Due to the construction of $T_{i,j}^{(1)}$ and $T_{i,j}^{(2)}$, this will happen if and only if the dimension $d$ is odd, as we have seen in the last example of the proof of proposition 1. As a remark, note the coincidence that in this case $T_{i,j}^{(1)}$ and $T_{i,j}^{(1)}$ are two MOLS. For the rest of the proof, we will restrict ourselves to odd local dimensions $d$.

For the bipartition $AC|BD$, we have

$$\rho_{AC} = \frac{1}{d^3} \sum_{i,i',j,r=0}^{d-1} |i\rangle \langle i'| \otimes |r \oplus T_{i,j}^{(2)}\rangle\langle r \oplus T_{i',j}^{(2)}| \omega^{r(T_{i,j}^{(1)} \ominus T_{i',j}^{(1)})}. \tag{7.2.6}$$

This will give the identity if and only if the following conditions are fulfilled.

*First condition.* When $i = i'$, we need to have

$$\sum_{j,r=0}^{d-1} |r \oplus T_{i,j}^{(2)}\rangle\langle r \oplus T_{i',j}^{(2)}| \omega^{r(T_{i,j}^{(1)} \ominus T_{i',j}^{(1)})} = d\mathbb{1}. \tag{7.2.7}$$

Let us recall that we are restricting ourselves to $d$ odd. Since in this case $T_{i,j}^{(1)}$ and $T_{i,j}^{(2)}$ are uniquely determined by $i$ and $j$, the fact that $i = i'$ and $j = j'$ implies that $T_{i,j}^{(1)} = T_{i',j}^{(1)}$ and $T_{i,j}^{(2)} = T_{i',j}^{(2)}$. By construction $T_{i,j}^{(2)}$ is a latin square, and therefore all the the terms appear $d$ times in equation (7.2.7), which means that it is fulfilled.

*Second condition.* When $i \neq i'$, we need

$$\sum_{j,r} |r \oplus T_{i,j}^{(2)}\rangle\langle r \oplus T_{i',j}^{(2)}| \omega^{r(T_{i,j}^{(1)} \ominus T_{i',j}^{(1)})} = 0. \tag{7.2.8}$$

To see the result of the calculation of the left hand site of equation (7.2.8), it is useful to rewrite the expression above as follows,

$$\begin{aligned}\sum_{j,r} |i \oplus r \oplus j\rangle \langle i' \oplus r \oplus j| \, \omega^{r(i \ominus i')} &= \sum_{p=0}^{d-1} \sum_{j,r:j\oplus r=p} |i \oplus r \oplus j\rangle \langle i' \oplus r \oplus j| \, \omega^{r(i \ominus i')} \\ &= \sum_{s,t=0}^{d-1} |i \oplus s\rangle \langle i' \oplus s| \, \omega^{t(i \ominus i')} = 0.\end{aligned} \tag{7.2.9}$$

To see that the bipartition $AD|CB$ is maximally entangled, it is sufficient to see that $\rho_{BC} \propto \mathbb{1}$. In this case the *first condition* and *second condition* above must be fulfilled up to some differences regarding the indices $i$ and $j$. For the *first condition*, we have equation (7.2.7) summing over $i$ instead of $j$, and clearly the same result holds in this case. For the *second condition*, we need

$$\sum_{i,r} |i \oplus r \oplus j\rangle \langle i \oplus r \oplus j'| \, \omega^{-r(j \ominus j')} = 0, \tag{7.2.10}$$

which can be seen by rewriting the corresponding expression in a similar way as we do in equation (7.2.9). □

Note that proposition 4 can be generalized to $T^{(1)}_{i,j} = i \oplus n \cdot j$ and $T^{(2)}_{i,j} = i \oplus m \cdot j$ iff $n$, $m$ and $n \ominus m$ are coprime with $d$. This is because in such case, (1) we have $\rho_{AB} \propto \mathbb{1}$ because the states $\{|\phi_{T^{(1)}_{i,j},T^{(2)}_{i,j}}\rangle\}$ form an orthonormal basis, and (2) we have $\rho_{AC} = \rho_{AD} \propto \mathbb{1}$ because we are left with corresponding expressions in which the diagonal elements are all equal and the off-diagonal elements vanish in a similar way as (7.2.9) does.

Although our construction given in proposition 4 might be LU-equivalent to an AME state of minimal support or to a graph state, note that the way we have constructed the state $|\psi\rangle$ in (7.2.5) is different from the constructions given in the literature which is cited in this thesis.

### Can we also use 2 MOLS to construct $AME(4, d)$ states in even dimension $d$?

For odd dimensions, the construction given in proposition 4 leads to an AME state by means of constructing two objects, namely $T^{(1)} = \left(T^{(1)}_{i,j}\right)$ and $T^{(2)} = \left(T^{(2)}_{i,j}\right)$, which are two MOLS for the indices of the generalized Bell states (1.2.14). It is natural to ask whether or not a similar construction as (7.2.5) in which $T^{(1)}$ and $T^{(2)}$ are constructed from two MOLS in even dimension $d$, the resulting state is an AME state. However, this is in general not true. In particular, for $d = 4$ there exists the following counterexample. Consider the choice

$$(T^{(1)}T^{(2)}) = \begin{pmatrix} 00 & 11 & 22 & 33 \\ 12 & 03 & 30 & 21 \\ 23 & 32 & 01 & 10 \\ 31 & 20 & 13 & 02 \end{pmatrix}, \tag{7.2.11}$$

where the rows are denoted by the index $i$ and the columns are denoted by the index $j$. This construction consists of two MOLS in dimension 4. Consider now a similar construction

as (7.2.5) which reads

$$|\psi\rangle = \frac{1}{\sqrt{4^3}} \sum_{i,j=0}^{d-1} |i,j\rangle \, |\phi_{T^{(1)}_{i,j},T^{(2)}_{i,j}}\rangle, \tag{7.2.12}$$

where $T^{(1)}_{i,j}$ and $T^{(2)}_{i,j}$ are the entries of the two MOLS defined in (7.2.11). Using the same notation as in the proof of proposition 4, the reduction $\rho_{AD}$ of the state given in equation (7.2.12) reads

$$\rho_{AD} = \frac{1}{4^3} \sum_{i,i'} |i\rangle \langle i'| \otimes \sum_{j,r=0}^{d-1} |r \oplus T^{(2)}_{i,j}\rangle\langle r \oplus T^{(2)}_{i',j}| \omega^{r(T^{(1)}_{i,j} \ominus T^{(1)}_{i',j})}. \tag{7.2.13}$$

To have an AME state, it is necessary that the off-diagonal elements of $\rho_{AD}$, namely the elements with $i \neq i'$, vanish. However, we see that the element corresponding to $i = 0$ and $i' = 2$ reads

$$\begin{aligned} &\frac{1}{4^3} |0\rangle \langle 2| \otimes \sum_{j,r=0}^{d-1} |r \oplus T^{(2)}_{0,j}\rangle\langle r \oplus T^{(2)}_{2,j}| \omega^{r(T^{(1)}_{0,j} \ominus T^{(1)}_{2,j})} = \\ &\qquad \frac{2}{4^3} \omega^0 |0\rangle \langle 2| \otimes \Big( |0\rangle \langle 3| + |1\rangle \langle 2| + |2\rangle \langle 1| + |3\rangle \langle 0| \Big) + \\ &\qquad \frac{2}{4^3} \omega^2 |0\rangle \langle 2| \otimes \Big( |1\rangle \langle 0| + |2\rangle \langle 3| + |3\rangle \langle 2| + |0\rangle \langle 1| \Big) \neq 0 \end{aligned} \tag{7.2.14}$$

and therefore we have $\rho_{AD} \not\propto \mathbb{1}$, which implies that (7.2.12) is not an AME state.

**Partial projections in 4-partite AME states**

We will finish this section with an observation regarding the states constructed in proposition 4. Let us introduce some notation. Given a quantum state $|\theta\rangle \in \mathcal{H}_C \otimes \mathcal{H}_D$, we call the *partial projection* $D$ $\left|\theta^D\right\rangle := \left(\sum_{s=0}^{d-1} \langle s| \otimes \mathbb{1}\right) |\theta\rangle$, and the *partial projection* $C$ the expression $\left|\theta^C\right\rangle := \left(\mathbb{1} \otimes \sum_{s=0}^{d-1} \langle s| \right) |\theta\rangle$. Furthermore, let us introduce the following definitions.

- We say that two states $|\phi\rangle, |\varphi\rangle \in \mathcal{H}_C \otimes \mathcal{H}_D$ are *orthogonal in only one partial projection* if either $\left\langle \phi^C \middle| \varphi^C \right\rangle = 0$ or $\left\langle \phi^D \middle| \varphi^D \right\rangle = 0$.
- We say that two states $|\phi\rangle, |\varphi\rangle \in \mathcal{H}_C \otimes \mathcal{H}_D$ are *orthogonal in two partial projections* if $\left\langle \phi^C \middle| \varphi^C \right\rangle = 0$ and $\left\langle \phi^D \middle| \varphi^D \right\rangle = 0$.

**Observation 2.** *Consider any two states of the basis $\{|\phi_{T^{(1)}_{i,j},T^{(2)}_{i,j}}\rangle\}$ defined in proposition 4, namely $|\phi_{T^{(1)}_{i,j},T^{(2)}_{i,j}}\rangle$ and $|\phi_{T^{(1)}_{i',j'},T^{(2)}_{i',j'}}\rangle$. Suppose $i \neq i'$ and $j = j'$, or $i = i'$ and $j \neq j'$. Then, those two states are orthogonal in two partial projections.*

*Proof.* This observation follows trivially from the definition of the states in $\{|\phi_{T^{(1)}_{i,j},T^{(2)}_{i,j}}\rangle\}$ given in proposition 4 and from the two definitions given above. □

## 7.3 Analytical description of 4-partite AME states

To our knowledge, most of the systematic constructions of $AME(N,d)$ states which are currently known are of minimal support (up to LU operations) [51, 79, 72, 23, 21, 22, 45, 17], or their constructions involves AME states of minimal support of smaller system sizes [78].

More precisely, most of the constructions for $AME(4,d)$ states within the literature cited in this thesis are of minimal support (up to LU operations). The construction given in proposition 4, which is inspired by the the constructions given in [66], is different in its methodology from the constructions for AME states of minimal support, but still it requires the construction of two MOLS. Therefore, it is natural to attempt to understand how the relation between $AME(4,d)_{min}$ states and two MOLS can be generalized to the nonminimal support AME states. In particular, we can ask ourselves whether or not it is true that constructing an $AME(4,d)$ state implies constructing two MOLS in dimension $d$. A positive answer to this question would imply that an $AME(4,6)$ state does not exist, as it has been proven that two MOLS in dimension 6 [63].

Attempting to shed some light upon the existence of AME states, we will analyze the structure of 4-partite AME states from an analytical perspective. For that, the only tool we have in the most general case is the definition of AME states, namely that all the bipartitions are maximally entangled. In particular, the bipartite entanglement present across a bipartition between parties the parties $\{X,Y\}$ and the rest of the system can easily be described, for instance by means of the Schmidt decomposition corresponding to that specific bipartition. However, and although there exist multipartite generalizations of the Schmidt decomposition and similar methods [80], we have to face the problem that when we write down a quantum state in such a way that the entanglement across one of the bipartitions can be easily computed, in general the entanglement across other bipartitions is less easy compute. One attempt to solve this problem and to find a unified description which captures whether or not a given state is an AME state is proposed in [66]. Inspired by this work, in this section we will analyze the structure of 4-partite AME states. In our approach we will attempt to show that in order to construct an $AME(4,d)$ state, it is necessary to construct two MOLS in dimension $d$. We will give a particular example of our argumentation by considering AME states in which observation 2 holds.

**Exploring the necessary and sufficient conditions for the existence of AME states**

We are specially interested in deriving necessary and sufficient conditions for the existence of AME states shared among four parties, $\{A,B,C,D\}$. This means reformulating the condition that all reductions to any two parties $X,Y \subset \{A,B,C,D\}$ of an AME state are maximally mixed, in terms of alternative statements which are easier to deal with. In particular, here we will first reformulate the fact that the reductions $\rho_{AC}$ and $\rho_{AD}$ are maximally mixed in terms of two conditions, which we call *diag* and *off-diag*.

Consider a 4-partite state written in the bipartition $AB|CD$,

$$|\psi\rangle = \mathbb{1}\otimes A \sum_{i,j=0}^{d-1} |i,j\rangle\,|i,j\rangle = \sum_{i,j=0}^{d-1} |i,j\rangle\,|\psi_{i,j}\rangle\,. \tag{7.3.1}$$

Inspired by the relation between AME states and MOLS, $\{i,j\}$ can be interpreted as the coordinates of a square with entries $\{|\psi_{i,j}\rangle\}$ [66]. Following this idea, we construct the object

$$\mathcal{A} = \begin{pmatrix} |\psi_{0,0}\rangle & \cdots & |\psi_{0,d-1}\rangle \\ \vdots & \ddots & \\ |\psi_{d-1,0}\rangle & & |\psi_{d-1,d-1}\rangle \end{pmatrix}. \tag{7.3.2}$$

If $|\psi\rangle$ is an AME state of minimal support, the elements of $\mathcal{A}$ are separable states of the form $|k\rangle \otimes |l\rangle$, where $|k\rangle$ and $|l\rangle$ are elements of the computational basis, and the set $\{k, l\}$ defines two MOLS with respect to the coordinates $\{i, j\}$ (and viceversa). If $|\psi\rangle$ is not of minimal support, the states $\{|\psi_{i,j}\rangle\}$ are in general entangled and this property does not hold. Instead, $\mathcal{A}$ must have a more general property. Seeking this property, we are interested in reformulating the necessary and sufficient conditions for the state $|\psi\rangle$ in (7.3.1) to be an AME state in terms of properties of $\mathcal{A}$. Let us introduce those conditions and see how they are linked to some properties of $\mathcal{A}$.

Considering $|\psi\rangle$ written as in (7.3.1), it is clear that we will have $\rho_{AB} \propto \mathbb{1}$ if and only if both $\{|i, j\rangle\}$ and $\{|\psi_{i,j}\rangle\}$ form an orthonormal basis, up to a normalization factor $d^{-1}$. Keeping that in mind and computing the reductions $\rho_{AC}$ and $\rho_{AD}$, we see that a necessary and sufficient condition for $|\psi\rangle$ to be an AME state is that the following conditions are fulfilled simultaneously,

$$\{|i, j\rangle\} \ \& \ \{|\psi_{i,j}\rangle\} \text{ are orthonormal bases,} \tag{7.3.3}$$

$$tr_C \sum_{i,j,j'=0}^{d-1} |j\rangle \langle j'| \otimes |\psi_{i,j}\rangle \langle \psi_{i,j'}| = \frac{1}{d^2} \mathbb{1} \otimes \mathbb{1}, \tag{7.3.4}$$

$$tr_D \sum_{i,j,j'=0}^{d-1} |j\rangle \langle j'| \otimes |\psi_{i,j}\rangle \langle \psi_{i,j'}| = \frac{1}{d^2} \mathbb{1} \otimes \mathbb{1}. \tag{7.3.5}$$

Equation (7.3.4) can be reformulated with the following conditions, which se call *diag* and *off-diag* respectively,

$$\begin{aligned} &\text{diag}: \quad tr_C \sum_i |\psi_{i,j}\rangle \langle \psi_{i,j}| = \frac{1}{d^2} \mathbb{1} \quad \forall j \\ &\text{off-diag}: \quad tr_C \sum_i |\psi_{i,j}\rangle \langle \psi_{i,j' \neq j}| = 0 \quad \forall j \neq j' \,. \end{aligned} \tag{7.3.6}$$

Similarly, equation (7.3.5) can be reformulated as

$$\begin{aligned} &\text{diag}: \quad tr_D \sum_i |\psi_{i,j}\rangle \langle \psi_{i,j}| = \frac{1}{d^2} \mathbb{1} \quad \forall j \\ &\text{off-diag}: \quad tr_D \sum_i |\psi_{i,j}\rangle \langle \psi_{i,j' \neq j}| = 0 \quad \forall j \neq j' \,. \end{aligned} \tag{7.3.7}$$

That is, conditions (7.3.3), (7.3.6) and (7.3.7) are together a set of necessary and sufficient conditions for $|\psi\rangle$ to be an AME state. In the following observation we use this fact to identify a property that the rows and columns of $\mathcal{A}$ must fulfill in order for $\mathcal{A}$ to define an AME state.

**Observation 3.** *Assuming that* $\{|\psi_{i,j}\rangle\}$ *are orthonormal states, the* diag *conditions in* (7.3.6) *and* (7.3.7) *are equivalent to the condition that*

$$\Big\{ \sum_{i=0}^{d-1} |i\rangle \, |\psi_{i,j}\rangle \Big\}_j \tag{7.3.8}$$

*is a set of 3-partite 1-uniform states for all $j$.*

*Proof.* If the states within the set in (7.3.8) are 1-uniform, then the *diag* conditions in (7.3.6) and (7.3.7) are fulfilled by definition of 1-uniformity. The converse statement requires in addition the assumption that $\{|\psi_{i,j}\rangle\}$ are orthonormal states, since otherwise the reduction to the first party of the states given in (7.3.8) would not necessarily be maximally mixed. □

Arguing similarly as above, we see that the condition $\rho_{AB} = \rho_{BC} = \rho_{BD} \propto \mathbb{1}$ can be reformulated as

$$\begin{aligned} &\text{diag}: \quad tr_C \sum_j |\psi_{i,j}\rangle \langle\psi_{i,j}| = \frac{1}{d^2}\mathbb{1} \quad \forall i \\ &\text{off-diag}: \quad tr_C \sum_j |\psi_{i,j}\rangle \langle\psi_{i\neq i',j}| = 0 \quad \forall i \neq i' \end{aligned} \tag{7.3.9}$$

and

$$\begin{aligned} &\text{diag}: \quad tr_D \sum_j |\psi_{i,j}\rangle \langle\psi_{i,j}| = \frac{1}{d^2}\mathbb{1} \quad \forall i \\ &\text{off-diag}: \quad tr_D \sum_j |\psi_{i,j}\rangle \langle\psi_{i\neq i',j}| = 0 \quad \forall i \neq i' \,, \end{aligned} \tag{7.3.10}$$

together with (7.3.3). Although those conditions are equivalent to the conditions we have obtained by imposing $\rho_{AB} = \rho_{AC} = \rho_{AD} \propto \mathbb{1}$, it is useful to explicitly write them down because at several points of this thesis it will be convenient to refer to them.

Considering conditions (7.3.3), (7.3.9) and (7.3.10) and arguing similarly as in observtion 3, we see that if the state $|\psi\rangle$ given in equation (7.3.1) is an AME state, then the states

$$\Big\{ \sum_{j=0}^{d-1} |j\rangle |\psi_{i,j}\rangle \Big\}_i \tag{7.3.11}$$

must be 1-uniform for all $i$, and this condition is not equivalent to equation (7.3.8). A counterexample that shows this inequivalence can be found by considering $|\psi\rangle$ to be of minimal support. In this case, we can apply any arbitrary permutation to the elements of any arbitrary column of $\mathcal{A}$ and the property that the states $\{\sum_{i=0}^{d-1} |i\rangle |\psi_{i,j}\rangle\}_j$ are all 1-uniform will obviously not be affected, while we will affect the property that the states $\{\sum_{j=0}^{d-1} |j\rangle |\psi_{i,j}\rangle\}_i$ are 1-uniform. In particular, one trivial counterexample to see this fact can be found by constructing the square $\mathcal{A}$ corresponding to the $AME(4,3)$ state given in equation (1.3.8) and permuting the elements of any arbitrary column.

The description of 4-partite AME states in terms of the square $\mathcal{A}$ may be a useful tool for their analysis. Let us give the following example of why this approach can be useful. In the literature cited in this thesis [23, 53], the equivalence between $AME(4,d)_{min}$ and two MOLS is proven by (1) recalling the equivalence between $AME(4,d)_{min}$ and MDS codes of 4 digits, which is proven in [22, 23] and then (2) recalling that MDS codes of 4 digits and 2 MOLS are equivalent, which is proven in [52]. The formalism discussed above leads to an alternative proof of the equivalence between $AME(4,d)_{min}$ and two MOLS by noting that observation 2 is always fulfilled for $AME(4,d)_{min}$ states. That is, consider the following alternative proof of the equivalence between $AME(4,d)$ states of minimal support and two MOLS, which is part of the Theorem 3.2 formulated in [53].

**Proposition 5** ([53]). *Let $|\psi\rangle$ be a 4-partite quantum state with local dimension $d$ and support $d^2$ of the form*

$$|\psi\rangle = \sum_{i,j=0}^{d-1} |i\rangle\,|j\rangle\,|a(i,j)\rangle\,|b(i,j)\rangle\,, \tag{7.3.12}$$

*where $a(i,j) \in \mathbb{Z}_d$ and $b(i,j) \in \mathbb{Z}_d$ are bijective functions of $i$ and $j$. Let $T^{(1)} = \big(a(i,j)\big)$ and $T^{(2)} = \big(b(i,j)\big)$ be two squares with entries $\{a(i,j)\}$ and $\{b(i,j)\}$ respectively. $|\psi\rangle$ is an $AME(4,d)$ state if and only if $T^{(1)}$ and $T^{(2)}$ are two MOLS with respect to the coordinates $\{i,j\}$.*

*Proof.* First of all, note that $\rho_{AB}$ will be maximally mixed, namely $\{|\psi_{i,j}\rangle\}$ will form an orthonormal basis, if and only if no pairs are repeated in the set $\{a(i,j), b(i,j)\}$.

Second, note that the *diag* condition in equation (7.3.6) will be fulfilled if and only if fixing $i$, the elements $\{|a(i,j)\rangle\}_i$ form an orthonormal basis and the elements $\{|b(i,j)\rangle\}_i$ also form an orthonormal basis. By considering the *diag* condition in equation (7.3.9), similar results hold for the sets $\{|a(i,j)\rangle\}_j$ and $\{|b(i,j)\rangle\}_j$ resulting from fixing $j$.

Third, note that the condition that both $\{|a(i,j)\rangle\}_i$ and $\{|b(i,j)\rangle\}_i$ form an orthonormal basis is sufficient for the *off-diag* conditions in equation (7.3.6) and equation (7.3.9) to be fulfilled.

By the construction of the state $|\psi\rangle$, in this case the object $\mathcal{A}$ is constructed as follows,

$$\mathcal{A} = \begin{pmatrix} |a(0,0)\rangle\,|b(0,0)\rangle & \dots & |a(0,d-1)\rangle\,|b(0,d-1)\rangle \\ \vdots & \ddots & \\ |a(d-1,0)\rangle\,|b(d-1,0)\rangle & & |a(d-1,d-1)\rangle\,|b(d-1,d-1)\rangle \end{pmatrix}. \tag{7.3.13}$$

It is trivial that the conditions given above are equivalent to the condition that superimposing $T^{(1)}$ and $T^{(2)}$, we have that (1) no pairs $\{a(i,j), b(i,j)\}$ are repeated and (2) fixing any of the coordinates, no entries are repeated in $T^{(1)}$ nor in $T^{(2)}$. That is, $|\psi\rangle$ is an AME state if and only if $T^{(1)}$ and $T^{(2)}$ form two MOLS.

□

**Exploring necessary and sufficient conditions in terms of different products of matrices**

In observation 3 we identify a necessary condition for the construction of 4-partite AME states in terms of the properties of $\mathcal{A}$. In addition, we would be interested in finding an equivalent reformulation of the *off-diag* conditions in (7.3.6) and (7.3.7) in terms of properties of $\mathcal{A}$, in order to capture the necessary and sufficient conditions for the construction of AME states in the formalism of $\mathcal{A}$. We will tackle this problem as follows. Writing

$$|\psi_{i,j}\rangle = A_{i,j} \otimes \mathbb{1}\,\big|\phi_d^+\big\rangle \tag{7.3.14}$$

and using that $A_{i,j} \otimes \mathbb{1}\,\big|\phi_d^+\big\rangle = \mathbb{1} \otimes A_{i,j}^T\,\big|\phi_d^+\big\rangle$, where $A_{i,j}^T$ is the transposed of $A_{i,j}$, we have that

$$\begin{aligned} tr_D\,|\psi_{i,j}\rangle\,\langle\psi_{i,j}| &= A_{i,j}A_{i,j}^\dagger \quad \text{and} \\ tr_C\,|\psi_{i,j}\rangle\,\langle\psi_{i,j}| &= A_{i,j}^T A_{i,j}^*\,, \end{aligned} \tag{7.3.15}$$

where $A_{i,j}^*$ denotes the complex conjugated of $A_{i,j}$ in the computational basis.

As we have previously seen, the condition $\rho_{AB} \propto \mathbb{1}$ is equivalent to the condition that $|\psi_{i,j}\rangle$ is an orthonormal basis. Equivalently, we have $\rho_{AB} \propto \mathbb{1}$ if and only if the elements $\{A_{i,j}\}$ are orthonormal under the Hilbert-Schmidt product,

$$tr(A_{i,j}A_{i',j'}^{\dagger}) = \delta_{i,i'}\delta_{j,j'}\,, \tag{7.3.16}$$

which means that they form a basis of mutually orthogonal $d \times d$ matrices.

The condition $\rho_{AC} \propto \mathbb{1}$ can be reformulated as

$$\begin{aligned} \text{diag}: &\quad \sum_{i=0}^{d-1} A_{i,j}A_{i,j}^{\dagger} = \mathbb{1}, \quad \forall j \\ \text{off-diag}: &\quad \sum_{i=0}^{d-1} A_{i,j}A_{i,j'}^{\dagger} = 0, \quad \forall j \neq j'\,, \end{aligned} \tag{7.3.17}$$

analogously to the condition (7.3.6), and similar results summing over $j$ hold for the condition $\rho_{BC} \propto \mathbb{1}$.

Using this notation for the entries of $\mathcal{A}$, we can interpret equation (7.3.16), equation (7.3.17) and its counterpart for the condition $\rho_{BC} \propto \mathbb{1}$ and reformulate the necessary and sufficient conditions for the existence of any 4-partite AME state as the conditions that (1) the entries of $\mathcal{A}$ are mutually orthogonal under the Hilbert-Schmidt product and (2) both the rows and columns of $\mathcal{A}$ are orthonormal vectors. However, conditions (7.3.16) and (7.3.17) provided above are related to different notions of orthogonality defined by different scalar products. It would be interesting to find a unique description for both conditions which we can interpret in terms of properties which must be fulfilled within the rows and columns of $\mathcal{A}$.

Finally, let us provide the following necessary condition for the existence of any 4-partite AME state.

**Proposition 6.** *Let $\tilde{\mathcal{A}}$ be an object with indices $\{i,j\}$ which entries are $\tilde{\mathcal{A}}_{i,j} = A_{i,j}A_{i,j}^{\dagger}$, where $A_{i,j}$ are defined as in* (7.3.14)*. An $AME(4,d)$ state can exist only if each row of $\tilde{\mathcal{A}}$ defines a positive operator-valued measure (POVM) and each column of $\tilde{\mathcal{A}}$ also defines a POVM.*

*Proof.* This proposition is simply an interpretation of the *diag* condition in (7.3.17) and the similar equation which arises from considering $\rho_{BC} \propto \mathbb{1}$. They are better illustrated by constructing the following object,

$$\tilde{\mathcal{A}} = \begin{pmatrix} A_{0,0}A_{0,0}^{\dagger} & \dots & A_{0,d-1}A_{0,d-1}^{\dagger} \\ \vdots & \ddots & \\ A_{d-1,0}A_{d-1,0}^{\dagger} & & A_{d-1,d-1}A_{d-1,d-1}^{\dagger} \end{pmatrix}, \tag{7.3.18}$$

where the elements within any row of $\tilde{\mathcal{A}}$ must sum up to the identity, and similarly for the elements within any column. The elements $\{A_{i,j}A_{i,j}^{\dagger}\}$ are by definition positive semidefinite, and therefore each row and each column in (7.3.18) defines a POVM. This proves the first claim. The second claim is exactly the description of equation (7.3.16). □

Note that if we choose for $\{A_{i,j}\}$ an orthonormal basis spanned by unitary matrices, the condition defined by proposition 6 is fulfilled for any choice of the position of the entries with respect to the coordinates $\{i,j\}$. In particular, recalling the generalization of the Pauli

matrices $X$ and $Z$ given in (1.1.11), the choice $\{A_{i,j} = X^{a(i,j)}Z^{b(i,j)}\}$ with $a(i,j) = i \ominus j$ and $b(i,j) = i \oplus j$ is equivalent to the construction (7.2.5).

**An attempt to prove that any 4-partite AME states is related to 2 MOLS**

We are interested in the generalization of the equivalence between $AME(4,d)_{min}$ and 2 MOLS for the nonminimal support case, and the reformulation of the conditions for the existence of AME states in terms of $\mathcal{A}$ given in equation (7.3.13) may be a suitable framework for that. One possible generalization of this equivalence could be that the the existence of any $AME(4,d)$ state always requires the existence of two MOLS. In what follows we will attempt to prove that this necessary condition holds. We are interested in proving this claim because, given that two MOLS of dimension 6 do not exist [63], such proof would imply that an $AME(4,6)$ state does not exist.

Let $\mathcal{A}$ be a square defined as in (7.3.13) which describes an $AME(4,d)$ state $|\psi\rangle$. Let $P$ be a symmetric relation between some of the elements of $\mathcal{A}$ which holds pairwise. This means that if one element $|\psi_{i,j}\rangle \in \mathcal{A}$ is related to another element $|\psi_{i',j'}\rangle \in \mathcal{A}$ by the relation $P$, then $|\psi_{i',j'}\rangle$ is related to $|\psi_{i,j}\rangle$ by the relation $P$. We denote as $\mathcal{A}_P$ a square $\mathcal{A}$ so that any two elements within the same row of $\mathcal{A}$ are related by $P$, and any two elements within the same column of $\mathcal{A}$ are also related by $P$. Furthermore, Let $\mathcal{B}_P$ be a $d \times d$ square which has the same elements as $\mathcal{A}$ reordered in such a way that any two elements within the same row of $\mathcal{B}_P$ are *not* related by $P$, and any two elements within the same column of $\mathcal{B}_P$ are also *not* related by $P$. Let us define the following two claims.

**Claim 1.** *There exists a symmetric relation $P$ so that any $AME(4,d)$ state of any local dimension $d$ must be defined by a corresponding square of the type $\mathcal{A}_P$.*

**Claim 2.** *Given a symmetric relation $P$, for any bipartite basis $\{|\psi_{i,j}\rangle\}$ of any local dimension $d$, $\mathcal{B}_P$ exists.*

Although there is no proof that the two claims above are true nor false, they will be central for our discussion.

Let $\Gamma$ be the set of reorderings $\{\gamma\}$ of the elements $\{|\psi_{i,j}\rangle\}$ so that

$$\gamma : \mathcal{B}_P \to \mathcal{A}_P \,, \tag{7.3.19}$$

and let $\Gamma_{MOLS}$ be the set of reorderings $\{\gamma_{MOLS}\}$ which generate two MOLS,

$$\gamma_{MOLS} : \begin{pmatrix} 0,0 & \dots & 0,d-1 \\ \vdots & \ddots & \\ d-1,0 & & d-1,d-1 \end{pmatrix} \to 2\,MOLS(d)\,. \tag{7.3.20}$$

Note that any permutation $\gamma \in \Gamma$ has the property that any two elements in the same row *or* the same column of $\mathcal{B}_P$ must be mapped to a different row *and* a different column of $\mathcal{A}$. Therefore, by definition of 2 MOLS we have

$$\Gamma \subseteq \Gamma_{MOLS}\,. \tag{7.3.21}$$

This implies that if there exists a relation $P$ so that the claims 1 and 2 described above are fulfilled, then two MOLS in dimension $d$ must exist if an $AME(4,d)$ state exists. We would

be interested in finding a relation $P$ so that the claims 1 and 2 are fulfilled because this would prove that in general the existence of any $AME(4,d)$ state requires the existence of two MOLS. In particular, since two MOLS of dimension 6 do not exist [63], this would prove that an $AME(4,6)$ state can not exist.

As an example, let us restrict ourselves to the set of AME states fulfilling observation 2, that is, AME states which have the property that any two elements in the same row or in the same column of $\mathcal{A}$ must be orthogonal in two partial projections. We call this property $P = \perp$. Let us call this set of AME states $AME(4,d)_\perp$. In this case, the claim 2 means that for any bipartite basis $\{|\psi_{i,j}\rangle\}$ in any local dimension $d$ there exists a square $\mathcal{B}_\perp$ containing the elements $\{|\psi_{i,j}\rangle\}$ so that any two elements in the same row or in the same column are *not* orthogonal in two partial projections. If the claim 2 was true for $P = \perp$, then equation (7.3.21) would imply that the existence of an $AME(4,d)_\perp$ state implies the existence of two MOLS in dimension $d$. Given that two MOLS in dimension $d = 6$ do not exist, this would imply that an $AME(4,6)_\perp$ state can not exist.

The equivalence between AME states and pure quantum codes, and in particular the fact that a 4-partite state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C \otimes \mathcal{H}_D$ is an AME state if and only if we have

$$\langle\psi| M |\psi\rangle = \frac{1}{d^4} tr(M) \tag{7.3.22}$$

for any local operator $M \in \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C \otimes \mathcal{H}_D)$ of weight 2 or less, might be a suitable tool to either prove or disprove that claims 1 and 2 hold for $P = \perp$. For instance, writing $|\psi\rangle = \sum_{i,j=0}^{d-1} |i,j\rangle |\psi_{i,j}\rangle$ and choosing appropriately the operator $M$, it is easy to see that if $|\psi\rangle$ is an AME state, then the partial projections $\{|\psi^C_{i,j}\rangle\}$ must fulfill equations

$$\begin{aligned} \sum_{i=0}^{d-1} \left\langle \psi^C_{i,r} \right| \left. \psi^C_{i,s} \right\rangle &= d \cdot \delta_{r,s} \\ \sum_{j=0}^{d-1} \left\langle \psi^C_{r,j} \right| \left. \psi^C_{s,j} \right\rangle &= d \cdot \delta_{r,s} \end{aligned} \tag{7.3.23}$$

and equation

$$\sum_{i,j} \left\langle \psi^C_{i,j} \right| M^{(C)} \left| \psi^C_{i,j} \right\rangle = d \cdot tr(M^{(C)}) \tag{7.3.24}$$

for any arbitrary operator $M^{(C)} \in \mathcal{B}(\mathcal{H}_C)$. Analogous conditions must hold for the partial projections $\{|\psi^D_{i,j}\rangle\}$ and an arbitrary operator $M^{(D)} \in \mathcal{B}(\mathcal{H}_D)$. Although this result does not help to prove nor disprove claims 1 or 2, attempting to find suitable local errors that lead to similar conditions which do prove or disprove claims 1 or 2 is left as a further research line.

# Conclusions

In the first part of this thesis we have reviewed the main results concerning the existence and applications of absolutely maximally entangled (AME) states. First of all, we have introduced the notion of absolute maximal entanglement in the context of multipartite entanglement theory and we have presented the main applications of AME states in different areas of quantum information theory and related fields. Then, we have reviewed the basics of quantum error correction, which are deeply linked to the constructions, the existence and the applications of AME states. Next, we have discussed how AME states can be constructed from graph states. Furthermore, we have explained the equivalence between AME states and pure quantum codes and how this connection leads to the main tools which have been used to bound the system sizes for which there exists an AME state. Finally, we have reviewed how it has been proven that an AME state shared among seven qubits can not exist by means of a completely different approach than those mentioned above.

In the second part of this thesis, we have tackled the open problem in quantum information theory which represents the existence of AME states. We have particularly focused on (1) trying to find an AME state shared among four parties in local dimension six ($AME(4,6)$), which existence is currently unknown, and (2) trying to disprove its existence by means of investigating the general properties of 4-partite AME states. Those two research lines and their results can be summarized as follows.

First, we have focused on designing a numerical algorithm which is inspired by the research performed in [73] and by means of which we attempt to convert an initial randomly chosen 4-partite quantum state into an $AME(4,6)$ state, thus proving its existence. Although we have not reached this goal, we have analyzed some particular properties of the algorithm we propose and we have shown that particular results can be attained by means of restricting the initial states.

Then, we have moved to the analytical approach of describing the structure of AME states of small system sizes. First, we have given specific constructions for 4-partite, 5-partite and 6-partite AME states of minimal support with some restrictions for the local dimensions. Then, we have presented a new construction for 4-partite AME states of odd local dimensions. Even though we have used a different methodology than the tools which are used in the literature cited in this thesis, our construction requires the existence of two mutually orthogonal latin squares (MOLS). Motivated by this fact, we have analyzed the structure of 4-partite AME states and the necessary and sufficient conditions for their existence, attempting to generalize the relation between 4-partite AME states of minimal support and MOLS to the case of nonminimal support. In this direction, we have introduced a possible research line attempting to prove that any 4-partite AME state exists only if two MOLS exist, thus seeking a disproof for the existence of an $AME(4,6)$ state.

# Appendix A

# Alternative proof of observation 1

Equation (7.2.3) gives a construction for 4-AME states of support $d^3$ which are LU-equivalent to AME states of minimal support. Although in section 7.2 we give a simple proof that two MOLS are necessary and sufficient for the state given in (7.2.3) to be an AME state, in what follows we will give an alternative proof of it. That is, consider the following proposition.

**Proposition 7.** *Consider the 4-partite state*

$$|\psi\rangle = \frac{1}{\sqrt{d^3}} \sum_{i,j,k=0}^{d-1} \omega^{jb(i,k)} |i\rangle |j\rangle |k\rangle |a(i,k)\rangle , \tag{A.0.1}$$

*where* $\omega = e^{\frac{i2\pi}{d}}$ *and we have* $a(i,k), b(i,k) \in \mathbb{Z}_d$. $|\psi\rangle$ *is a state* $AME(4,d)$ *iff* $a(i,k)$ *and* $b(i,k)$ *are two MOLS with respect to the coordinates* $\{i,k\}$.

*Proof.* Using the same notation used in proposition 4, let us first compute the reduction $\rho_{AD}$,

$$\rho_{AD} = \frac{1}{d^3} \sum_{i,i',j,k=0}^{d-1} |i\rangle \langle i'| \otimes |a(i,k)\rangle \langle a(i',k)| \, \omega^{j\left(b(i,k)\ominus b(i',k)\right)}. \tag{A.0.2}$$

- The diagonal terms are all equal to 1 and span the whole space of $d^2$ dimensions of $\mathbb{1}_{d^2\times d^2}$ iff the condition

$$\sum_{k=0}^{d-1} |a(i,k)\rangle \langle a(i,k)| = \mathbb{1} \tag{A.0.3}$$

  is fulfilled. That is, iff, fixing $i$, $a(i,k)$ takes a different value for each $k$. Similarly, the diagonal terms in $\rho_{CD}$ will be all equal to 1 iff, fixing $k$, $a(i,k)$ takes a different value for each $i$. That is to say, the diagonal terms of $\rho_{AD}$ and $\rho_{CD}$ are 1 and span the whole space of $\mathbb{1}_{d^2\times d^2}$ simultaneously iff $a(i,k)$ defines a latin square with respect to the coordinates $\{i,k\}$.

- The off-diagonal terms will vanish iff the condition

$$\sum_{j,k=0}^{d-1} |a(i,k)\rangle \langle a(i',k)| \, \omega^{j\left(b(i,k)\ominus b(i',k)\right)} = 0 \quad \forall i \neq i' \tag{A.0.4}$$

  is fulfilled. Fixing $k$ and given that $i \neq i'$, we need $b(i,k) \neq b(i',k)$. Considering similar conditions for the reduction $\rho_{CD}$, we see that fixing $i$ and given $k \neq k'$, we need also

$b(i,k) \neq b(i,k')$. Therefore, $b(i,k)$ must define a latin square. Note that this condition is both necessary and sufficient. Recalling the results for the diagonal terms of both $\rho_{AD}$ and $\rho_{CD}$ derived above, we see that $\rho_{AD} = \rho_{CD} \propto \mathbb{1}$ *iff* $a(i,k)$ *and* $b(i,k)$ *are both latin squares with respect to the coordinates* $\{i,k\}$.

Let us now consider the reduction to parties $\rho_{BD}$,

$$\rho_{BD} = \frac{1}{d^3} \sum_{i,j,j',k=0}^{d-1} |j\rangle \langle j'| \otimes |a(i,k)\rangle \langle a(i,k)| \, \omega^{b(i,k)(j\ominus j')}. \tag{A.0.5}$$

The condition that the diagonal elements are $\frac{1}{d^2}$ and span the whole space follows from the fact that $a(i,k)$ defines a latin square.

The off-diagonal terms will vanish iff the condition

$$\sum_{i,k=0}^{d-1} |a(i,k)\rangle \langle a(i',k)| \, \omega^{b(i,k)(j\ominus j')} = 0 \quad \forall j \neq j' \tag{A.0.6}$$

is fulfilled. By definition, each of the values $a(i,k) \in \mathbb{Z}_d$ appears $d$ times along all the coordinates $\{i,k\}$. Let us denote as $S_c$ one of the $d$ sets of $d$ combinations $(i,k)$ corresponding to the same value $a(i,j) := c$. Equation (A.0.6) will be fulfilled for any $j \ominus j'$ coprime with $d$ iff one of the following conditions is fulfilled.

1. $b(i,j)$ is never repeated in $\{S_c\}$. In such case, if we superimpose the squares $a$ and $b$ using $\{i,k\}$ as coordinates, no pairs can be repeated. That is, $a$ and $b$ are orthogonal latin squares.

2. $b(i,j)$ is repeated a number of times $d_1$ taking values $\{rd_1\}$ with $r \in \mathbb{Z}_{d_2}$, where $d_1 d_2 = d$. Note that this is possible only if $d$ is not prime. Hence, if $d$ is prime, the condition that $a$ and $b$ are two MOLS is necessary and sufficient.

In the second case and assuming that $d$ is not prime, consider a combination$(j,j')$ so that $j \ominus j' = d_2$. Then, all the exponents in (A.0.6) will vanish and hence the sum (A.0.6) will not, which is a contradiction. As a consequence, *the state* $|\psi\rangle$ *in* (A.0.1) *is AME state iff* $a$ *and* $b$ *are two MOLS with respect to the coordinates* $\{i,k\}$. □

# Bibliography


[1] A. J. Scott, "Multipartite entanglement, quantum-error-correcting codes, and entangling power of quantum evolutions," *Physical Review A*, vol. 69, p. 052330, 2004.

[2] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels," *Physical Review Letters*, vol. 70, pp. 1895–1899, 1993.

[3] A. Peres, "Separability criterion for density matrices," *Physical Review Letters*, vol. 77, pp. 1413–1415, 1996.

[4] G. Vidal and R. F. Werner, "Computable measure of entanglement," *Physical Review A*, vol. 65, p. 032314, 2002.

[5] S. Hill and W. K. Wootters, "Entanglement of a pair of quantum bits," *Physical Review Letters*, vol. 78, p. 5022–5025.

[6] M. Huber and J. I. de Vicente, "Structure of multidimensional entanglement in multipartite systems," *Physical Review Letters*, vol. 110, p. 030501, 2013.

[7] T. J. Osborne and F. Verstraete, "General monogamy inequality for bipartite qubit entanglement," *Physical Review Letters*, vol. 96, p. 220503, 2006.

[8] W. Dür, G. Vidal, and J. I. Cirac, "Three qubits can be entangled in two inequivalent ways," *Physical Review A*, vol. 62, 2000.

[9] J. S. Kim, G. Gour, and B. C. Sanders, "Limitations to sharing entanglement," *Contemporary Physics*, vol. 53, p. 417–432, 2012.

[10] V. Coffman, J. Kundu, and W. K. Wootters, "Distributed entanglement," *Physical Review A*, vol. 61, 2000.

[11] I. Bengtsson and K. Życzkowski, "A brief introduction to multipartite entanglement," *arXiv*, quant-ph, eprint 1612.07747, 2016.

[12] M. Koashi and A. Winter, "Monogamy of quantum entanglement and other correlations," *Physical Review A*, vol. 69, p. 022309, 2004.

[13] T. R. de Oliveira, M. F. Cornelio, and F. F. Fanchini, "Monogamy of entanglement of formation," *Physical Review A*, vol. 89, p. 034303, 2014.

[14] M. Koashi and A. Winter, "Monogamy of quantum entanglement and other correlations," *Physical Review A*, vol. 69, 2004.

[15] J. S. Kim, A. Das, and B. C. Sanders, "Entanglement monogamy of multipartite higher-dimensional quantum systems using convex-roof extended negativity," *Physical Review A*, vol. 79, p. 012329, 2009.

[16] D. A. Meyer and N. R. Wallach, "Global entanglement in multiparticle systems," *Journal of Mathematical Physics*, vol. 43, pp. 4273–4278, 2002.

[17] F. Huber and N. Wyderka, "Table of AME states," `http://www.tp.nt.uni-siegen.de/+fhuber/ame.html`, 2020.

[18] F. Huber, C. Eltschka, J. Siewert, and O. Gühne, "Bounds on absolutely maximally entangled states from Shadow inequalities, and the quantum macwilliams identity," *Journal of Physics A: Mathematical and Theoretical*, vol. 51, p. 175301, 2018.

[19] A. Higuchi and A. Sudbery, "How entangled can two couples get?," *Physics Letters A*, vol. 273, p. 213–217, 2000.

[20] F. Huber and M. Grassl, "Quantum codes of maximal distance and highly entangled subspaces," *arXiv*, quant-ph, eprint 1907.07733, 2019.

[21] W. Helwig, W. Cui, J. I. Latorre, A. Riera, and H.-K. Lo, "Absolute maximal entanglement and quantum secret sharing," *Physical Review A*, vol. 86, p. 052335, 2012.

[22] W. Helwig and W. Cui, "Absolutely maximally entangled states: Existence and applications," quant-ph, eprint 1306.2536, 2013.

[23] D. Goyeneche, D. Alsina, J. I. Latorre, A. Riera, and K. Życzkowski, "Absolutely maximally entangled states, combinatorial designs, and multiunitary matrices," *Physical Review A*, vol. 92, p. 032316, 2015.

[24] M. Żukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, "Event-ready-detectors Bell experiment via entanglement swapping," *Physical Review Letters*, vol. 71, pp. 4287–4290, 1993.

[25] R. Cleve, D. Gottesman, and H.-K. Lo, "How to share a quantum secret," *Physical Review Letters*, vol. 83, p. 648–651, 1999.

[26] F. Pastawski, B. Yoshida, D. Harlow, and J. Preskill, "Holographic quantum error-correcting codes: Toy models for the bulk/boundary correspondence," *Journal of High Energy Physics*, vol. 2015, p. 149, 2015.

[27] A. Almheiri, X. Dong, and D. Harlow, "Bulk locality and quantum error correction in AdS/CFT," *Journal of High Energy Physics*, vol. 163, 2015.

[28] J. Maldacena, "The large-N limit of superconformal field theories and supergravity," *International Journal of Theoretical Physics*, vol. 38, 1999.

[29] A. Neumann, *The Cosets Code.* 2010.

[30] E. Knill, "Group representations, error bases and quantum codes," *arXiv*, quant-ph, 9608049, 1996.

[31] E. Knill and R. Laflamme, "Theory of quantum error-correcting codes," *Physical Review A*, vol. 55, p. 900, 1997.

[32] M. Hayashi and T. Morimae, "Verifiable measurement-only blind quantum computing with stabilizer testing," *Physical Review Letters*, vol. 115, p. 220502, 2015.

[33] S. Aaronson and D. Gottesman, "Improved simulation of stabilizer circuits," *Physical Review A*, vol. 70, p. 052328, 2004.

[34] V. Veitch, S. H. Mousavian, D. Gottesman, and J. Emerson, "The resource theory of stabilizer quantum computation," *New Journal of Physics*, vol. 16, p. 013009, 2014.

[35] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. 10th ed., 2011.

[36] D. Gottesman, "Stabilizer codes and quantum error correction," *arXiv*, quant-ph, eprint 9705052, 1997.

[37] A. Steane, "Multiple-particle interference and quantum error correction," *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, vol. 452, pp. 2551–2577, 1996.

[38] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Physical Review A*, vol. 54, p. 1098–1105, 1996.

[39] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. V. den Nest, and H. J. Briegel, "Entanglement in graph states and its applications," quant-ph, eprint 0602096, 2006.

[40] R. Raussendorf and H. J. Briegel, "A one-way quantum computer," *Physical Review Letters*, vol. 86, pp. 5188–5191, 2001.

[41] M. Van den Nest, J. Dehaene, and B. De Moor, "Graphical description of the action of local clifford transformations on graph states," *Physical Review A*, vol. 69, p. 022316, 2004.

[42] M. Hein, J. Eisert, and H. J. Briegel, "Multiparty entanglement in graph states," *Physical Review A*, vol. 69, 2004.

[43] Z. Raissi, C. Gogolin, A. Riera, and A. Acín, "Optimal quantum error correcting codes from absolutely maximally entangled states," *Journal of Physics A: Mathematical and Theoretical*, vol. 51, p. 075301, 2018.

[44] M. Grassl, T. Beth, and M. Rötteler, "On optimal quantum codes," *International Journal of Quantum Information*, vol. 2, p. 55–64, 2004.

[45] W. Helwig, "Absolutely maximally entangled qudit graph states," *arXiv*, quant-ph, eprint 1306.2879, 2013.

[46] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli, "Nonbinary stabilizer codes over finite fields," *IEEE Transactions on Information Theory*, vol. 52, no. 11, pp. 4892–4914, 2006.

[47] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction via codes over gf(4)," in *Proceedings of IEEE International Symposium on Information Theory*, vol. 44, p. 1369–1387, 1997.

[48] D. Forney, "Channel coding: Techniques, analysis and design principles," vol. 2, Lecture notes, 2007.

[49] L. E. Danielsen, "On the classification of hermitian self-dual additive codes over gf(9)," *IEEE Transactions on Information Theory*, vol. 58, p. 5500–5511, 2012.

[50] M. Grassl and M. Rotteler, "Quantum MDS codes over small fields," *2015 IEEE International Symposium on Information Theory (ISIT)*, 2015.

[51] D. Alsina, "Multipartite entanglement and quantum algorithms," PhD thesis, 2017.

[52] S. T. Dougherty and T. A. Szczepanski, "Latin k-hypercubes," *Australasian Journal of Combinatorics*, vol. 40, p. 145, 2008.

[53] A. Bernal, "On the existence of absolutely maximally entangled states of minimal support II," quant-ph, eprint 1807.00218, 2018.

[54] D. Stinson, *Combinatorial designs: constructions and analysis*. 2007.

[55] B. Tang, "Orthogonal array-based latin hypercubes," *Journal of the American Statistical Association*, vol. 88, pp. 1392–1397, 1993.

[56] A. S. Hernandez, "Breaking barriers to design dimensions in nearly orthogonal latin hypercubes," tech. rep., Naval Postgraduate School Monterey CA, 2008.

[57] C. D. Lin and B. Tang, "Latin hypercubes and space-filling designs," *Handbook of design and analysis of experiments*, 2015.

[58] F. Sun, M.-Q. Liu, and D. K. Lin, "Construction of orthogonal latin hypercube designs with flexible run sizes," *Journal of Statistical Planning and Inference*, vol. 140, pp. 3236–3242, 2010.

[59] C. J. Colbourn and J. H. Dinitz, "Mutually orthogonal latin squares: a brief survey of constructions," *Journal of Statistical Planning and Inference*, vol. 95, pp. 9 – 48, 2001. Design Combinatorics.

[60] C. J. Colbourn and J. H. Dinitz, *Handbook of combinatorial designs*. 2006.

[61] V. N. Potapov, "On the number of SQSs, latin hypercubes and MDS codes," *Journal of Combinatorial Designs*, vol. 26, no. 5, p. 237–248, 2018.

[62] G. L. Mullen and W. C. Schmid, "An equivalence between (t, m, s)-nets and strongly orthogonal hypercubes," *journal of combinatorial theory, Series A*, vol. 76, pp. 164–174, 1996.

[63] G. Terry, "Le probléme des 36 officiers," *Compte Rendu de l'Association Française pour l'Avancement des Sciences*, vol. 2, pp. 170–203, 1901.

[64] M. Bahramgiri and S. Beigi, "Graph states under the action of local clifford group in non-binary case," *arXiv*, quant-ph, eprint 0610267, 2006.

[65] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, "Perfect quantum error correcting code," *Physical Review Letters*, vol. 77, pp. 198–201, 1996.

[66] D. Goyeneche, Z. Raissi, S. Di Martino, and K. Życzkowski, "Entanglement and quantum combinatorial designs," *Physical Review A*, vol. 97, p. 062326, 2018.

[67] J. Preskill, "Lecture notes for physics 229: Quantum information and computation," *California Institute of Technology*, vol. 16, 1998.

[68] G. Gour and N. R. Wallach, "Entanglement of subspaces and error-correcting codes," *Physical Review A*, vol. 76, p. 042309, 2007.

[69] E. M. Rains, "Quantum weight enumerators," *IEEE Transactions on Information Theory*, vol. 44, pp. 1388–1394, 1998.

[70] P. Shor and R. Laflamme, "Quantum analog of the macwilliams identities for classical coding theory," *Physical Review Letters*, vol. 78, p. 1600, 1997.

[71] F. Huber, O. Gühne, and J. Siewert, "Absolutely maximally entangled states of seven qubits do not exist," *Physical Review Letters*, vol. 118, p. 200502, 2017.

[72] M. Gaeta, A. Klimov, and J. Lawrence, "Maximally entangled states of four nonbinary particles," *Physical Review A*, vol. 91, 2015.

[73] F. Verstraete, J. Dehaene, and B. De Moor, "Normal forms and entanglement measures for multipartite quantum states," *Physical Review A*, vol. 68, 2003.

[74] D. Bruss and G. Leuchs, *Quantum Information: From Foundations to Quantum Technology Applications*. 2019.

[75] M. Erickson and A. Vazzana, *Introduction to number Theory*. 2007.

[76] O. Knill, "A multivariable chinese remainder theorem," *arXiv preprint arXiv:1206.5114*, 2012.

[77] "Orthogonal latin squares," *Cut The Knot,* *https://www.cut-the-knot.org/arithmetic/latin3.shtml*.

[78] Z. Raissi, A. Teixido, C. Gogolin, and A. Acin, "New construction for k-uniform and absolutely maximally entangled states," *arXiv*, quant-ph, eprint 1910.12789, 2019.

[79] A. Cervera-Lierta, J. I. Latorre, and D. Goyeneche, "Quantum circuits for maximally entangled states," *Phys. Rev. A*, vol. 100, p. 022342, Aug 2019.

[80] H. A. Carteret, A. Higuchi, and A. Sudbery, "Multipartite generalization of the schmidt decomposition," *Journal of Mathematical Physics*, vol. 41, p. 7932–7939, 2000.