ICFO – The Institute of Photonic Sciences
Castelldefels (Barcelona), Spain

PhD thesis

Quantum multipartite entangled states, classical and quantum error correction

Zahra Raissi

July 24, 2020

Thesis supervisor: Prof. Antonio Acín
Thesis cosupervisor: Dr. Christian Gogolin

Acknowledgements

I wish to express my deepest gratitude to Professor Antonio Acín, Toni, for his mentoring, patience, motivation, inspired discussion, and for his trust and supports for both of my PhDs. You encouraged me to be professional and guided me in the right direction.

I would like to recognize the invaluable assistance that Dr. Christian Gogolin provided during my study, visits and research. Without your persistent help and of course your patience, my goal would not have been realized.

I wish to thank Mario for his invaluable help, support and love. We have shared a wonderful time together, I am very grateful and happy. Also, I am indebted and very thankful to my family.

I would like to pay my special regards to the QIT and QOT groups at ICFO. Many thanks to all of my collaborators especially Professor Karol Życzkowski, Dr. Arnau Riera, Professor Dardo Goyeneche and my student Adam Teixidó who helped me to become a better researcher and teacher. I would also thank my friend and collaborator Adam Burchardt.

My sincere thanks goes to Valentin Kasper, Markus Johansson, Jan Kołodyński, Stefan Bäuml, Remigiusz Augusiak, Maciej Demianowicz, Paolo Abiuso, Joseph Bowles, Gabriel Senno, Cristian Boghiu, Bruna De Moraes, Dario de Santis, Matteo Scandi, Vinicius Salem, Jacopo Surace, Flavio Baccari, Senaida Hernández Santana, Osvaldo Jimenez, Michal Oszmaniec, Alejandro Pozas-Kerstjens, Alexia Salavrakos, Paul Skrzypczyk, Ivan Supic, Boris Bourdoncle, Bogna Bylicka, Martí Perarnau, Florian Curchod, Irénée Frérot, Mohammad Mehboudi, Marc-Olivier Renou, Chung-Yun Hsieh, Patrick Huembeli, Korbinian Kottmann, and to the memory of Peter Wittek. I could find very nice friends at ICFO, Lisa Kobayashi Frisk, Oumaima Sliti, Rafael Sibilo, Swapan Rana, Rino, Shahrzad and Zahra.

Resumen

El estudio del entrelazamiento cuántico es esencial para la comprensión de diversas áreas como la óptica cuántica, la materia condensada e incluso la física de altas energías. Además, el entrelazamiento nos permite superar la física y tecnologías clásicas llevando a una mejora en el procesado de la información, la computación y la metrología. Recientemente se ha descubierto que el entrelazamiento desarrolla un papel central en la caracterización y simulación de sistemas cuánticos de muchos cuerpos, de esta manera facilitando nuestra comprensión de la materia cuántica. Mientras que se tiene un buen conocimiento del entrelazamiento en estados puros bipartitos, nuestra comprensión del caso de muchas partes es mucho más limitada, a pesar de que sea un escenario más rico y que presenta un contraste más fuerte con la física clásica. De entre todos los posibles estados entrelazados, una clase especial ha llamado la atención por su amplia gama de aplicaciones. Estos estados se llaman k-uniformes y son los estados multipartitos de n cuerpos con dimensión local q con la propiedad de que todas las reducciones a k cuerpos son máximamente desordenadas. Operacionalmente, en un estado k-uniforme cualquier subconjunto de hasta k cuerpos está máximamente entrelazado con el resto. Los estados $k = \lfloor n/2 \rfloor$-uniformes se llaman estados absolutamente máximamente entrelazados porque son máximamente entrelazados respecto a cualquier partición de los n cuerpos en dos grupos. Estos estados encuentran aplicaciones en varios protocolos y, en particular, forman los elementos de base para la construcción de los códigos de corrección de errores cuánticos con geometría holográfica, los cuales han aportado intuición importante sobre la conexión entre la teoría de la información cuántica y la teoría conforme de campos. Las propiedades y aplicaciones de estos estados son intrigantes porque conocemos poco sobre las mismas: cuándo existen, cómo construirlos, cómo se relacionan con otros estados con entrelazamiento multipartito, cómo los estados grafo, o como se relacionan mediante operaciones locales y comunicación clásica.

Con esta motivación en mente, en esta tesis primero estudiamos las propiedades de los estados k-uniformes y luego presentamos métodos sistemáticos para construir expresiones cerradas de los mismos. La naturaleza de nuestros métodos resulta ser muy útil para entender la estructura de estos estados cuánticos, su representación como estados grafo y su clasificación bajo operaciones locales y comunicación clásica. También construimos varios ejemplos de estados absolutamente máximamente entrelazados, cuya existencia era desconocida. Finalmente,

exploramos una nueva familia de códigos de corrección de errores cuánticos que generalizan y mejoran la conexión entre los códigos de corrección de errores clásicos, los estados entrelazados multipartitos y el formalismo de estabilizadores.

Los resultados de esta tesis pueden desarrollar un papel importante en la caracterización y el estudio de las tres siguientes áreas: entrelazamiento multipartito, códigos de corrección de errores clásicos y códigos de corrección de errores cuánticos. Los estados de entrelazamiento multipartito pueden aportar una conexión para encontrar diferentes recursos para tareas de procesamiento de la información cuántica y cuantificación del entrelazamiento. Al construir dos conjuntos de estados multipartitos altamente entrelazados, es importante saber si son equivalentes entre operaciones locales y comunicación clásica. Entendiendo qué estados pertenecen a la misma clase de recurso cuántico, se puede discutir qué papel desempeñan en ciertas tareas de información cuántica, como la distribución de claves criptográficas cuánticas, la teleportación y la construcción de códigos de corrección de errores cuánticos óptimos. También se pueden usar para explorar la conexión entre la correspondencia holográfica Anti-de Sitter/Conformal Field Theory y códigos de corrección de errores cuánticos, que nos permitiría construir mejores códigos de corrección de errores. A la vez, su papel en la caracterización de redes cuánticas será esencial en el diseño de redes funcionales, robustas ante pérdidas y ruidos locales.

Abstract

Studying entanglement is essential for our understanding of such diverse areas as quantum optics, condensed matter physics and even high energy physics. Moreover, entanglement allows us to surpass classical physics and technologies enabling better information processing, computation, and improved metrology. It was recently discovered that entanglement plays a prominent role in characterizing and simulating quantum many-body states and in this way deepened our understanding of quantum matter. While bipartite pure entangled states are well understood, multipartite entanglement is much richer and leads to stronger contradictions with classical physics. Among all possible entangled states, a special class of states has attracted attention for a wide range of tasks. These states are called k-uniform states and are pure multipartite quantum states of n parties and local dimension q with the property that all of their reductions to k parties are maximally mixed. Operationally, in a k-uniform state any subset of at most k parties is maximally entangled with the rest. The $k = \lfloor n/2 \rfloor$-uniform states are called absolutely maximally entangled because they are maximally entangled along any splitting of the n parties into two groups. These states find applications in several protocols and, in particular, are the building blocks of quantum error correcting codes with a holographic geometry, which has provided valuable insight into the connections between quantum information theory and conformal field theory. Their properties and the applications are, however, intriguing, as we know little about them: when they exist, how to construct them, how they relate to other multipartite entangled states, such as graph states, or how they connect under local operations and classical communication.

With this motivation in mind, in this thesis we first study the properties of k-uniform states and then present systematic methods to construct closed-form expressions of them. The nature of our methods proves to be particularly fruitful in understanding the structure of these quantum states, their graph-state representation and classification under local operations and classical communication. We also construct several examples of absolutely maximally entangled states, whose existence was a subject of an open question. Finally, we explore a new family of quantum error correcting codes that generalize and improve the link between classical error correcting codes, multipartite entangled states, and the stabilizer formalism.

The results of this thesis can have a role in characterizing and studying the following three topics: multipartite entanglement, classical error correcting codes and quantum error correct-

ing codes. The multipartite entangled states can provide a link to find different resources for quantum information processing tasks and quantify entanglement. Constructing two sets of highly entangled multipartite states, it is important to know if they are equivalent under local operations and classical communication. By understanding which states belong to the same class of quantum resource, one may discuss the role they play in some certain quantum information tasks like quantum key distribution, teleportation and constructing optimum quantum error correcting codes. They can also be used to explore the connection between the Anti-de Sitter/Conformal Field Theory holographic correspondence and quantum error correction, which will then allow us to construct better quantum error correcting codes. At the same time their roles in the characterization of quantum networks will be essential to design functional networks, robust against losses and local noise.

List of publications

Publications forming part of the thesis

- Zahra Raissi, Christian Gogolin, Arnau Riera, Antonio Acín, "Constructing optimal quantum error correcting codes from absolute maximally entangled states" Journal of Physics A: Mathematical and Theoretical, **51**, 075301 (2018). arXiv:1701.03359 [quant-ph].

  * This paper has been selected in the Journal of Physics A Highlights of 2018 collection.

- Dardo Goyeneche, Zahra Raissi, Sara Di Martino, Karol Życzkowski, "Entanglement and quantum combinatorial designs", Phys. Rev. A **97**, 062326 (2018). arXiv:1708.05946 [quant-ph].

- Zahra Raissi, Adam Teixidó, Christian Gogolin, Antonio Acín, "New construction for k-uniform and absolutely maximally entangled states", accepted for publication in Phys. Rev. Research arXiv:1910.12789 [quant-ph].

- Zahra Raissi, "Modified-Shortening: Modifying method of constructing quantum codes from highly entangled states", arXiv:2005.01426 [quant-ph].

Other publications

- Adam Burchardt, Zahra Raissi, "Stochastic Local Operations with Classical Communication of Absolutely Maximally Entangled States", accepted for publication in Phys. Rev. A. arXiv:2003.13639 [quant-ph] .

Contents

List of Figures

List of Tables

1. Introduction

Quantum entanglement is certainly one of the most fascinating concepts arising in quantum mechanics. Besides its interest from the foundational point of view, it plays a key role in quantum information science, being a resource for many applications such as quantum communication and quantum computation [RB01, BGM$^+$10, CS96, Ste96a, CGL99, DC00b, Kim08]. This stimulated to the development of entanglement theory, in both bipartite and multipartite cases. The essence of bipartite entanglement is thus that the information about a quantum bipartite system is not only encoded in its parts, but also in the correlations between them. Remarkably, when a bipartite quantum system is maximally entangled, the information appears to be fully encoded in these correlations and no longer in the subsystems which look maximally noisy or mixed. An example of such a situation is the Einstein-Poldolsky-Rosen (EPR) or maximally entangled state of two parties.

A very intriguing question is of course whether similar situations exist if the system is made out of more than two parties. The family of states generalizing this property of the EPR state to an arbitrary number of parties and local dimensions is the family of Absolutely Maximally Entangled (AME) states [HCL$^+$12, AC13, GZ14]. AME states are therefore pure quantum states of n partite systems of local dimension q with the property that all reduced states (marginals) of at most half the system size are maximally mixed. Remarkably, these states are known not to exist for all combinations of number of parties and dimensions [Sco04]. Note that, one way of extending EPR state is based on the purity of reduced density matrices that leads to AME states, the other criteria one can consider focuses on generalization based on Stochastic Local Operations and Classical Communication (SLOCC) classification, for example, GHZ and W classes, see [DVC00]. Moreover, extension based on Mermin formulation of non-locality is another way of generalizing the EPR states, for a good review on this topic see [HHHH09].

Generalizing different properties of the EPR state to an arbitrary number of parties can lead to the discovery of different types of multipartite entangled states. All of these processes and applications depend on the property of the multipartite entangled states that are used as a resource. The applications like measurement-based quantum computation [BBD$^+$09b], quantum error correction schemes [NC00], quantum secret sharing [HBB99], quantum simulations [Llo96], and in principle in any task involving entangled many-body quantum systems

[HHHH09], along with its intriguing properties and applications to condensed matter physics [GTB05]. Although studying relevant sets of multipartite entangled states is very interesting, in this thesis we focus on AME and k-uniform states.

In view of the large number of constraints that an AME state should satisfy, it is obvious that the existence, let alone the systematic construction of these states is a highly nontrivial problem. For instance it has been shown that these states exist only for special values of the number of qubits. It is known that there is no AME state for four qubits [GW10] although there are AME state of five and six-qubits [BPB$^+$07, LMPZ96b]. The existence of an AME states of seven-qubit was an open question until it was shown [HGS17] that there is no such state. It had already been shown that no AME state exists for eight or more qubits [Sco04]. But we should stress that these results are specific to qubits and for any n, it is possible to construct AME states if we choose the dimension of each part q large enough [RGRA18]. Despite all these partial results, it is still largely unknown for which value of n and q AME states exist and how they can be constructed.

AME states are special cases of the class of so-called k-uniform states for $k = \lfloor n/2 \rfloor$. k-uniform states (or for simplicity k-UNI states) are pure states which have the property that all of their reductions up to k parties are maximally mixed. These states have also deep connections with apparently unrelated areas of mathematics such as combinatorial designs. Also, the study of this set of entangled state showed that k-UNI states are a particular type of quantum error correcting codes (QECCs) [Sco04]. These states exhibit highly entangled subspaces that form code spaces of QECCs.

To build a quantum computer which behaves correctly in the presence of errors and many other quantum applications we need the theory of QECCs. It is also known that there is a connection between the Anti-de Sitter/Conformal Field Theory (AdS/CFT) holographic correspondence and QECC [PYHP15, ADH15, LS15]. Code constructions which realize this connection are based on tensor networks in which the fundamental building blocks are AME states. QECC and AdS/CFT holographic correspondence are two very interesting concepts in contemporary physics. QECC are crucial to build and operate in the foreseeable future. The AdS/CFT holographic correspondence is currently our best tool for understanding nonperturbative quantum gravity.

The theory of QECC has some close connection to the theory of classical error correcting codes as well as some striking differences. Using classical codes one can construct a set of k-UNI states and show that they are stabiliser states. Many quantum codes can be described in terms of the stabilizers of the codewords. The stabilizer formalism for k-UNI states and quantum codes illustrates the relationships to classical coding theory.

In this PhD thesis we explore and deepen the relation between k-UNI states and classical

error correcting codes. Building on this, we can construct a large set of k-UNI states. We then construct a basis whose elements are all k-UNI states, generalizing the bipartitie Bell basis, and finally develop a stabilizer formalism for these states. We present two systematic methods to construct k-UNI states and classify them based on SLOCC. We then show how the states derived through our constructions are example of graph states and provide the corresponding graph. Based on the stabilizer formalism we search new encoding and decoding techniques for transmitting quantum information. We show how to construct stabilizer QECCs that encode logical qudits into a subspace spanned by k-UNI states.

1.1. Contributions

In the following, we review the different works that conform this thesis, giving the motivations and explaining the main results.

1.1.1. Constructing absolutely maximally entangled (AME) states from maximum distance separable codes

Entanglement has been identified as a crucial property to investigate and describe in several areas of science. The resource-theory of entanglement considers separated parties sharing a joint quantum state. It is natural to restrict the allowed operations to the set of operations to Local quantum Operations assisted by Classical Communication (LOCC). Then, entanglement arises as a resource allowing to achieve certain tasks that are not possible by LOCC alone.

The study of multipartite entanglement has led to the discovery of different types of entanglement. A set of states which is key in quantum applications is the set of highly entangled states. There are several fundamental roles that multipartite entangled states play in many quantum information processing tasks, like measurement-based quantum computing, quantum error correction, quantum secret sharing, multi-party teleportation, and finally quantum networks. All of these processes and applications depend on the property of the multipartite entangled states that are used as a resource. Recently, a special class of states have attracted the attention for a wide range of tasks, called absolutely maximally entangled states. AME states are of interest for multipartite teleportation and quantum secret sharing and have recently found new applications in the context of high-energy physics in toy models realizing the AdS/CFT-correspondence.

1.1.1.1. Results

In chapter 3, we work out in detail the connection between a certain type of AME states known as of minimal support and classical maximum distance separable (MDS) error cor-

recting codes. The minimal number of terms for which the condition of maximally mixed marginals can still be fulfilled is the dimension of the largest sub-system on which the state is required to still be maximally mixed, namely $q^{\lfloor n/2 \rfloor}$. AME states with this many terms are called minimal support AME states. In this chapter, we provide explicit closed form expressions for AME states of n parties with local dimension q a power of a prime for all $q \geq n-1$. Linear MDS codes are introduced and a systematic construction of AME states of minimal support is presented. Then, we show how to construct an orthonormal basis of AME states from any given AME state. We also develop a stabilizer formalism for AME states of minimal support constructed from MDS codes. These results are also presented in [RGRA18].

1.1.2. New construction for k-uniform and absolutely maximally entangled states

Despite all progress in studying multipartite states, in contrast to the case of bi-partite entanglement, our knowledge about multipartite entanglement is still in its infancy. For example, although there is a well-defined order in the entanglement of bi-partite states, it is now known that for 3-party qubit states such an order is not possible, as there are two LOCC inequivalent classes and for more than three parties these classes are infinite.

As stated in the beginning, maximal mixedness of subsystems is important for many important quantum communication tasks. But, the only known systematic construction of k-UNI quantum states is based on classical error correction codes which leads to those states that contain the minimal number of product terms necessary to obtain a full rank for all of the reductions. Now that it is clear that k-UNI states are useful, we need to find systematic methods to construct them and classify them based on LOCC.

1.1.2.1. Results

To our knowledge, the only known systematic construction of k-UNI quantum states is based on classical error correction codes. In chapter 4, we present a systematic method to construct other set of k-UNI states and show that the states derived through our construction are not equivalent to any k-UNI state constructed from classical MDS error correction codes.

Beside classifying the states based on SLOCC, we use our method to construct k-UNI states with smaller local dimension q compared to the same k-UNI state constructed from MDS codes. We then show how the k-UNI states derived through our construction are example of graph states and provide the corresponding graph for both constructions: using MDS codes and our new systematic method. Furthermore, we use our method to construct several examples of absolutely maximally entangled states whose existence was open so far, these results are also presented in [RTGA19].

1.1.3. Entanglement and quantum combinatorial designs

Classical coding theory and k-UNI states study analogous problems and have a number of parallel results. Codes were originally introduced in order to correct errors in the transmission of data over noisy communication channels. Not only this makes them mathematically interesting, but they also can be considered for more applications. They have been used in a variety of applications, such as increasing the storage capacity of compact disks, and by now coding theory has developed into a major area of quantum information. k-UNI states have deep connections with apparently unrelated areas of mathematics called combinatorial designs. There are several classes of combinatorial designs, namely Latin squares, cubes, hypercubes as well as notion of orthogonality between them.

It is possible to introduce quantum combinatorial designs, like quantum Latin squares, cubes, hypercubes and quantum orthogonal arrays and ask the following questions: Are there more contributions between the states and mathematical aspects? Are quantum combinatorial structures different from their classical counterparts? Are the states constructed from quantum combinatorial designs different from those constructed from classical ones?

1.1.3.1. Results

In chapter 5, we introduce several classes of quantum combinatorial designs, namely quantum Latin squares, cubes, hypercubes and a notion of orthogonality between them. A further introduced notion, quantum orthogonal arrays, generalizes all previous classes of designs. We show that mutually orthogonal quantum Latin arrangements can be entangled in the same way as quantum states. Furthermore, we show that such designs naturally define k-UNI states. We derive infinitely many classes of mutually orthogonal quantum Latin arrangements and quantum orthogonal arrays having an arbitrary large number of columns. These results are also presented in [GRDMZ18].

1.1.4. Optimal quantum error correcting codes from absolutely maximally entangled states

Computers have changed the world in many ways. While computers allow us to solve many problems, there remain problems that require a computational effort too large even for the most powerful computers. Quantum computers which used quantum mechanics might be more powerful than classical computers. Soon after the idea of a quantum computer took hold, the importance of robustness and quantum error correction was in the center of attention.

This was a challenging problem because of three reasons. First of all, in classical error correction we can measure all of the bits of a message in the computer while in a quantum computer, measuring a quantum message can destroy any entanglement between qudits. Second, in clas-

sical theory one can copy information while in quantum mechanics the cloning of arbitrary states is impossible. Last, a classical computer only needs to preserve the bit values of 0 and 1, but a quantum compute needs to keep phase information in superposition states. Therefore, while classical errors are discrete, quantum errors are continuous by nature. In the end, the field of quantum error correction has been able to overcome these challenges.

A class of quantum codes, called quantum stabilizer codes, has a connection with existing classical codes. This provides a great advantage to construct quantum codes using the extra knowledge on code parameters of the classical codes. This also leads us to a better understanding of the connection between quantum codes and highly entangled multipartite states constructed from classical codes. In particular, one application of the AME states is using them to construct quantum error correcting codes. In this construction, one can construct stabilizer quantum codes that the logical qudits are encoded in a subspace spanned by AME states.

1.1.4.1. Results

In chapter 6, we show how to construct stabilizer quantum error correcting codes (QECCs) that encode a logical qudit into a subspace spanned by AME states for every $q \geq n-1$ prime. Under a conjecture for which we provide numerical evidence, this construction produces a family of quantum error correcting codes $[\![n, 1, n/2]\!]_q$ for n even with the highest distance allowed by the quantum Singleton bound. The conjecture we propose discusses the existence of a family of QECC whose code spaces are spanned by AME states. We show that our conjecture is equivalent to the existence of a certain products of generalized Pauli operators that is incompressible in the sense that its weight cannot be decreased by multiplying it with stabilizer products and connect this with a feature of the joint weight enumerators of certain MDS codes. Further we construct such codes for all n up to $n = 8$ by finding several suitable incompressible operators. In these QECCs, a logical qudit is encoded in a q-dimensional subspace spanned by AME states of n parties. Our proposal has a very clear physical motivation and complements other constructions of non-binary QECC. In particular our construction is very explicit and works with a smaller local dimension q given n than previous codes, these results are also presented in [RGRA18].

1.1.5. Quantum codes from highly entangled states

Quantum states are very delicate, therefore, quantum error correction must be used to build reliable quantum computers. The quantum stabilizer codes have proved particularly fruitful in producing codes and also in understanding the structure of them. Moreover, if we want to construct the most general possible stabilizer codes, we should take advantage of connections to classical coding theory. It is shown that the stabilizer formalism for quantum codes also

illustrates the relationships to classical coding theory. This way of constructing quantum codes is very nice in that it allows to use the existing knowledge of the structure of classical codes to construct quantum codes.

The method of constructing new quantum codes from old ones simplifies the task of finding QECCs, which can otherwise be quite a difficult problem. There is a practical method of constructing new codes from old ones that we call the Shortening process. In this method, one starts from a k-UNI state constructed from an MDS code and construct a family of stabilizer QECCs by tracing out $r \geq k$ parties. So far, in previous literature the main focus was on presenting the stabilizers which require finding a special pattern for them. But, to build quantum devices we also need a theory instructing us how to decode and encode using a QECC without losing the protection against errors. We show how to find all the codewords in closed from expressions as well as logical Pauli operators. We then modify the method to produce a new set of stabilizer QECCs with a larger code subspace compared with the existing constructions.

1.1.5.1. Results

In chapter 7, we discuss the connections between classical codes, highly entangled pure states (called k-uniform states), and quantum error correcting codes (QECCs). This leads to a systematic method to construct stabiliser QECCs by starting from a k-UNI state and tracing out one party at each step. We show how to find explicit codespace beside stabiliser formalism. We then modify the method to produce another set of stabiliser QECCs that encode a logical qudit into a subspace spanned by AME states. This construction produces quantum codes starting from an AME state without tracing out any party. Therefore, quantum stabilizer codes with larger codespace can be constructed and that improve the achievable rate compared with the existed construction. These results are also presented in [Rai20].

2. Preliminaries

In this chapter, we give a short introduction to the basic tools of classical and quantum information theory that are used throughout this thesis. It focuses on three main topics: entanglement, classical and quantum error correction. Interested readers can consult Ref. [HHHH09] for more details on entanglement, Ref. [MS77] for classical codes and Refs. [Got97, Got09, Ter15] for quantum codes. These three concepts are also explained in the book by Nielsen and Chuang that is also a very good reference on basic information of quantum theory and quantum information [NC00].

2.1. Entanglement

Besides its interest from the foundational point of view, entanglement plays a key role in quantum information science, being a resource for many applications such as quantum teleportation [BBC$^+$93], quantum dense coding [BW92], measurement-based quantum computing [RB01, BBFM06, BBD$^+$09a], quantum error correction [CRSS98, Ste96b, Sco04], quantum secret sharing [HBB99] and multi-party teleportation [KB98, DC00b], and finally quantum networks [CZKH97, Kim08]. Therefore, the utility of a quantum state in all these applications depends on entanglement. This led to the development of entanglement theory, in both bipartite and multipartite cases.

2.1.1. Bipartite entanglement

The essence of bipartite entanglement is that the information about a quantum bipartite system is encoded in its parts and the correlations between them. There are two extreme cases for quantum states: states that are separable and states that are maximally entangled. The states that contain no entanglement are called product or separable [Wer89]. A pure state $|\psi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$ is product if it can be written in the form

$$|\psi\rangle_{AB} = |\psi\rangle_A \otimes |\psi\rangle_B \ , \tag{2.1}$$

for some $|\psi\rangle_A \in \mathcal{H}_A$ and $|\psi\rangle_B \in \mathcal{H}_B$. A mixed state ρ_{AB} is separable if it can be written in the following form

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

where p_i is a classical probability distribution, $\forall i \; p_i \geq 0$, $\sum_i p_i = 1$, and ρ_A^i are states in system A and ρ_B^i in system B, respectively. These states are not entangled since they can be created by performing Local Operations and Classical Communication (LOCC) between the two systems and thus can be regarded as containing only classical correlations.

Entangled states are those that cannot be written as equation (2.2). Therefore, an entangled state requires a joint quantum operation for its preparation. An example of such a situation is the Einstein-Podolsky-Rosen (EPR) or maximally entangled state of two parties

$$|\phi^+\rangle = |00\rangle + |11\rangle \, , \tag{2.3}$$

also known as Bell state. Here and in the following, we will not always explicitly normalize states for the sake of a more compact notation. For two qudits, q level quantum systems, one can always write a maximally entangled state in the form

$$|\psi\rangle = \sum_{i=0}^{q-1} |i\rangle_A \otimes |i\rangle_B \, , \tag{2.4}$$

where $|i\rangle_A$ and $|i\rangle_B$ form an orthonormal basis in system A and B, respectively.

Also, one should note that two states that are in the same *Local Unitary* (LU) equivalence class have the same entanglement properties. That means performing arbitrary local unitary operators U_1 and U_2 on a given state $|\psi\rangle$, i.e.,

$$|\psi\rangle = U_1 \otimes U_2 |\phi\rangle \, , \tag{2.5}$$

does not change its entanglement properties.

2.1.2. Multipartite entanglement

While the entanglement of bipartite pure states is already well understood [BBPS96, Nie99, HHHH09], we are still far from completely understanding multipartite entanglement [DVC00, VDMV02, SSC$^+$15]. Since entangled states constitute the essential ingredient for many fascinating applications within quantum computation and quantum communication, it is a remarkable area to work on.

The basic definition for entanglement in multipartite states is the same as for bipartite systems. A state is entangled if it cannot be created by local operations and with the help of

classical communication, because this method can only produce classically correlated states. A multipartite state that possesses no entanglement is called fully separable. A given pure multipartite state of n parties is fully separable if it can be written as

$$|\psi\rangle = |\psi\rangle_1 \otimes |\psi\rangle_2 \otimes \cdots \otimes |\psi\rangle_n \ . \tag{2.6}$$

A multipartite pure state of n parties is called entangled if it cannot be written as the tensor product of n single-qudit pure states. Note that, a state is called *genuinely entangled* if all subsystems are correlated and the state is not separable with respect to any possible splitting of n subsystems [HHHH09].

As before, for a mixed state ρ we have

$$\rho = \sum_i p_i \, \rho_1^i \otimes \rho_2^i \otimes \cdots \otimes \rho_n^i \ , \tag{2.7}$$

such that $p_i \geq 0$ is a probability distribution and ρ_j^i for $j \in \{1, \ldots n\}$ represent density matrices for the individual systems. A multipartite state is called entangled if it cannot be written as a convex combination of product states, i.e., equation (2.7).

2.2. Entanglement transformations for pure states

We describe the entanglement properties and LOCC. After that, we show that LOCC provides the framework to quantify how much entanglement a state contains.

2.2.1. Schmidt decomposition of bipartite states

The Schmidt decomposition is an important aspect of bipartite states. For every pure state $|\psi\rangle$ in $\mathcal{H}_A \otimes \mathcal{H}_B$, there exist orthonormal bases $\{|\alpha_i\rangle\} \in \mathcal{H}_A$, and$\{|\beta_i\rangle\} \in \mathcal{H}_B$, such that the state can be expressed as

$$|\psi\rangle = \sum_{i=1}^{l} \lambda_i \, |\alpha_i\rangle \otimes |\beta_i\rangle \ , \tag{2.8}$$

with $l = \min(dim(\mathcal{H}_A), dim(\mathcal{H}_B))$. The *Schmidt coefficients* λ_i are unique, they contain all the information about entanglement in the state and satisfy $\sum_i \lambda_i^2 = 1$. In this notation, the squares of these coefficients are given by the eigenvalues of the reduced states. The number of nonzero Schmidt coefficients is called the *Schmidt rank*. The state $|\psi\rangle$ is entangled if and only if its Schmidt rank is larger than one, i.e., if there exists only one $\lambda_i \neq 0$, the state is separable.

2.2.2. Local operations and classical communication (LOCC)

Considering entanglement as a resource it is reasonable to ask: Given two states, $|\psi\rangle$ and $|\phi\rangle$, with Schmidt coefficients α_i and β_i, respectively, which one is more entangled? To find an answer for this question, we consider the fact that entanglement is usually considered in a scenario where parties are far apart from each other, thus we restrict the quantum operations to be locally implemented. We also allow classical information to be transmitted between the distant parties. Therefore, LOCC is a standard scheme in which we could quantify entangled states. Based on these operational considerations, if the state $|\psi\rangle$ can be transformed into $|\phi\rangle$ by only using LOCC, $|\psi\rangle$ possesses at least as much entanglement as $|\phi\rangle$.

To study this, let us first write two vectors in decreasing order $\vec{v} = (v_1, \ldots, v_q)$ and $\vec{w} = (w_1, \ldots, w_q)$, such that $v_1 \geq v_2 \geq \cdots \geq v_q$ and $w_1 \geq w_2 \geq \cdots \geq w_q$. The q-dimensional vector $\vec{w}$ majorizes $\vec{v}$, written as $w \prec v$, if

$$w \prec v \quad \Longleftrightarrow \quad \sum_{i=0}^{l} w_i \leq \sum_{i=0}^{l} v_i \ , \ \ \forall\, l = 0, \ldots, q-1 \ . \tag{2.9}$$

Transferring two *bipartite states* $|\psi\rangle$ and $|\phi\rangle$ is formulated in [Nie99] by using the concept of vector majorization. It is proven that the state $|\psi\rangle$ with Schmidt coefficients $\vec{\alpha} = (\alpha_1, \ldots, \alpha_q)$ can be transformed into $|\phi\rangle$ with Schmidt coefficients $\vec{\beta} = (\beta_1, \ldots, \beta_q)$ if and only if the vector coefficient α^2 is majorized by the vector coeficients β^2 i.e.,

$$|\psi\rangle \xrightarrow{LOCC} |\phi\rangle \quad \Longleftrightarrow \quad \beta^2 \prec \alpha^2 \tag{2.10}$$

A state such that all the Schmidt coefficients have the same value $1/\sqrt{q}$ is maximally entangled, see Eq. (2.4) as it can be transformed into all other q-dimensional states by LOCC.

One should note that for systems of local dimension larger than two, $q > 2$, it is possible that neither $\beta^2 \prec \alpha^2$, nor $\alpha^2 \prec \beta^2$, and thus neither transformation can be deterministically performed by LOCC.

It is also possible to consider converting the state $|\psi\rangle$ to $|\phi\rangle$ with a non-zero success probability by local operations and classical communication. If such a transformation exists, we say that state $|\psi\rangle$ can be transformed into $|\phi\rangle$ by Stochastic Local Operation and Classical Communications (SLOCC).

The problem of transforming states via SLOCC with the maximal conversion probability was discussed by Vidal [Vid99]. The maximal transformation probability from a given *bipartite*

state $|\psi\rangle$ to $|\phi\rangle$ with Schmidt coefficients α_i and β_i, respectively, is given by

$$p(|\psi\rangle \to |\phi\rangle) = \min \frac{\sum_{l=0}^{q-1} \alpha_i^2}{\sum_{l=0}^{q-1} \beta_i^2} \qquad \forall\, l = 0, \ldots, q-1 \,. \tag{2.11}$$

Note that considering the probability $p = 1$ leads us to majoriation's results $\beta^2 \prec \alpha^2$ by Nielsen [Nie99].

It is also interesting to compare the two sets of LOCC and SLOCC operations mathematically for bipartite and multipratite states In LOCC operation, it is allowed to perform LU operators

$$|\psi\rangle = U_1 \otimes \cdots \otimes U_n |\phi\rangle \,, \tag{2.12}$$

adding ancilla particles, apply unitary operators to system and the ancilla, do measurement, in other words, it contains applying any local operations. Moreover, performing local operations and exchanging classical communication is allowed. On the other side, SLOCC extends this set of operations since it allows the probabilistic conversion between states. Mathematically, SLOCC operations are represented by

$$|\psi\rangle = A_1 \otimes \cdots \otimes A_n |\phi\rangle \,, \tag{2.13}$$

where A_i is a $q \times q$ matrix.

The study of entanglement transformations gave us a good idea about the classification of states based on entanglement. In the context of quantum information, a precise way to define classical correlations is via LOCC operations. Classical correlations can be defined as those that can be generated by LOCC operations. And, entanglement measure can be defined as a function over the state space that cannot increase under LOCC operations [Vid00].

Now that there exists a notion of which states are entangled and are also able, in some cases, to assert that one state is more entangled than another. This naturally raises the question of whether there is a maximally entangled state. For the *two-party systems* consisting of two q-dimensional sub-systems (called qudits), such states exist. Any pure state that is LU equivalent to

$$|\phi^+\rangle = \sum_{i=0}^{q-1} |i, i\rangle = |0,0\rangle + |1,1\rangle + \cdots + |q-1, q-1\rangle \,, \tag{2.14}$$

is maximally entangled. For the case of qubits ($q = 2$) this state can be presented with Eq. (2.4).

This means any pure or mixed state of two qudits can be prepared from such states with certainty using only LOCC operations. However, it is very useful to define a function that quantifies entanglement, the definition for multipartite entanglement is far from solved.

2.3. Entropy of entanglement

Equipped with LOCC processes we may now proceed to discuss the quantification of entanglement of *bipartite systems*. For this, we discuss two measures:

Distillable entanglement. Alice and Bob start from N copies of state ρ and apply an LOCC operation, that ends up with a state σ_N. We now require that for large N the final state approaches the desired Bell state $|\phi^+\rangle^{\otimes m_N}$. If it is impossible, then *entanglement distillation* $E_D = 0$. Otherwise we say that the LOCC operations constitute a *distillation protocol*, P and the rate of distillation is given by $R_P = \lim_N \frac{m_N}{N}$. The distillable entanglement is the supremum of such rates over all possible distillation protocols, or

$$E_D(\rho) = \sup\{r : \lim_{N\to\infty} (\inf_{\Lambda} \|\Lambda(\rho^{\otimes N}) - |\phi^+\rangle\langle\phi^+|_{rN}\|_1) = 0\} \,, \tag{2.15}$$

where $\|.\|_1$ is the trace norm [HHHH09].

Entanglement cost. It is a measure dual to E_D, and it reports how many Bell states are needed to prepare ρ per input copy by LOCC operations. Alice and Bob start from m_N copies of a Bell state and apply an LOCC operation, that ends up with a state σ_N. We now require that for large N the final state approaches the desired N copies of the state ρ. The rate of the protocol is given by $R_P = \lim_N \frac{m_N}{N}$. The entanglement cost is the infimum of such rates over all possible LOCC protocols. The definition is [HHHH09]

$$E_C(\rho) = \inf\{r : \lim_{N\to\infty} (\inf_{\Lambda} \|\rho^{\otimes N} - \Lambda(|\phi^+\rangle\langle\phi^+|_{rN})\|_1) = 0\} \,. \tag{2.16}$$

For pure states, one can start from k Bell states $|\phi^+\rangle_{AB}$ shared between Alice and Bob and prepare N copies of $|\psi\rangle_{AB}$, then distil them to get k' many Bell states, therefore $k' \leq k$. In other words, it is obvious that $k' \leq k$, otherwise, one could employ LOCC operation to create entanglement which is impossible using LOCC operations. Also, it is possible to show that asymptotically in N the entanglement cost and the distillable entanglement coincide in the case of pure states [BBPS96]. It is shown that the two measures $E_C(|\psi\rangle_{AB})$ and $E_D(|\psi\rangle_{AB})$ are given by the reduced single qudit von Neumann entropy

$$E_C(|\psi\rangle_{AB}) = E_D(|\psi\rangle_{AB}) = S(\rho_A) = S(\rho_B) \,, \tag{2.17}$$

where $S(\rho_A)$ is the von Neumann entropy of the reduced density matrix $\rho_A = \mathrm{Tr}_B(|\psi\rangle\langle\psi|)$, and $S(\rho_B)$ is the von Neumann entropy of the other party.

This shows that the process that transforms N copies of state $|\psi\rangle_{AB}$ into some copies of Bell state $|\phi^+\rangle$ is asymptotically reversible [BBPS96]. With this, one can uniquely quantify the

entanglement of a bipartite pure state $|\psi\rangle_{AB}$ as

$$E(|\psi\rangle_{AB}) = S(\rho_A) = S(\rho_B) \tag{2.18}$$
$$= -\sum_i |\lambda_i|^2 \log |\lambda_i|^2 \,, \tag{2.19}$$

that as we discussed before λ_i represents the Schmidt coefficients of the state $|\psi\rangle_{AB}$. In this context the von Neumann entropy $S(\rho_A)$ or $S(\rho_B)$ is known as the *entropy of entanglement*.

2.4. Multipartite entangled states

Despite partial progress our knowledge about multipartite entanglement is much more limited. One reason why the problem is difficult is the existence of different types of entanglement. For example, although there is a well-defined order in the entanglement of bipartite states, it is now known that for multipartite states such order is not possible. For 3-party qubit states there are two LOCC inequivalent classes [DVC00] and for $n > 3$ they are infinitely many [MV04, DC02, DC00a, SdVK16].

2.4.1. Multipartite LOCC transformations

In multipartite entanglement there are various types of entanglement that cannot be converted to each other even probabilistically. For 3 qubits the Greenberger-Horne-Zeilinger (GHZ) state and W states are famous in their different physical properties and applications to quantum information processing. The GHZ state $|GHZ\rangle = |000\rangle + |111\rangle$ [GHS90] has the maximal mixed reduced states for each party. It also violates the Mermin Bell's inequality maximally, and enable us to extract one Bell state between any two parties out of three with probability one. On the other hand, the W state $|001\rangle + |010\rangle + |100\rangle$ has the maximal amount of average pairwise entanglement distributed over three parties and can be utilized for optimal quantum cloning.

It is shown that in the case of 4-qubit there exist infinitely many SLOCC classes [SdVK16]. Due to these difficulties LOCC transformation have only been characterized for a few classes of states [TGP10, dVSK13]. As the mathematical study of multipartite LOCC transformation is difficult, other approaches towards the characterization of states have been pursued, such as studying how useful states are for a specific application.

2.4.2. k-uniform and absolutely maximally entangled states

Among multi-partite states, a very special class that has now attracted much attention is the class of k-UNI states [AC13, Hel13, RGRA18, RTGA19]. These are the states which have the property that all of their reductions to k parts are maximally mixed. As an example, the

GHZ state is a 1-UNI state. On the other hand the $|W\rangle$ state is not a 1-UNI state. Obviously a k-UNI state is an l-UNI state for $l < k$.

A given state can be at most a $\lfloor n/2 \rfloor$ -UNI state. Given a real number $r \in \mathbb{R}$ we denote by floor r, $\lfloor r \rfloor$, the largest integer not larger than r and by ceiling r, $\lceil r \rceil$, the smallest integer not smaller than r. Those n-qubit states which are $\lfloor n/2 \rfloor$ -UNI are called Absolutely Maximally entangled states or AME states for short.

In view of the large number of constraints that an AME state should satisfy, it is obvious that the existence, let alone the systematic construction of these states is a highly nontrivial problem. In fact, it has been shown that these states exist only for special values of n [GR15, HESG18]. In the case of qubits, for instance, it has been proven analytically that there are no AME states for $n = 4$ and $n \geq 7$. The non-existence in the cases $n = 4$ and $n \geq 8$ was proven by finding a contradiction in a linear program [Rai99b, Sco04]. Qubit AME states for $n = 2, 3$ were long known, a state for $n = 5$ was found in [LMPZ96a] and more recently such for $n = 5, 6$ were found numerically in [BSSB05, BPB$^+$07, FFPP08, FFM$^+$10]. The existence of such states was previously known in the context of quantum error correction [Rai99a]. Only recently it was shown that there can not be a qubit AME state for the case $n = 7$ [HGS17].

2.5. Graph states

Graph states are entangled pure quantum states that are defined based on a graph. These states are a special class of stabilizer states and are of interest because they can be represented just by a graph that is both succinct and also, captures all the properties of the state. Graph states are useful in quantum error-correcting codes, entanglement measurement and purification, and for the characterization of computational resources in measurement based quantum computing models [SW01, HDE$^+$06, BB06].

2.5.1. Generalised Pauli operators

In this section we define generalised Pauli operators X and Z that are used in many parts of this thesis. Operators X and Z generalize the Pauli operators σ_X and σ_Z to Hilbert spaces of dimension $q \geq 2$. We define these operators through their action on a given basis as follows

$$X|j\rangle = |j + 1 \mod q\rangle \tag{2.20}$$

$$Z|j\rangle = \omega^j |j\rangle , \tag{2.21}$$

with $\omega \coloneqq \mathrm{e}^{\mathrm{i}\,2\pi/q}$ the q-th root of unity. X and Z are unitary, traceless operators, and $X^q = Z^q = \mathbb{1}$. For $a, b \in \{0, \ldots, q-1\}$ it holds that $\mathrm{Tr}(Z^a X^b) = \delta_{a,0}\,\delta_{b,0}$ and $Z\,X = \omega\,X\,Z$.

We call operators that are tensor products of powers of Pauli operators *Pauli strings*. The Pauli strings X_l or Z_l acts on the qudit at position l for example

$$X_l \coloneqq \underbrace{\mathbb{1} \otimes \cdots \otimes \mathbb{1}}_{l-1} \otimes X \otimes \underbrace{\mathbb{1} \otimes \cdots \otimes \mathbb{1}}_{n-l} , \tag{2.22}$$

the same definition holds for Z_l.

Let us also introduce the gate operation known as *discrete Fourier transform* or *Hadamard matrix* H [DM72, Chapter 4][MS77]. The local Fourier transform, F operating on the qudit at position i is given by

$$F = \sum_{l,m \in [q]} \omega^{lm} |l\rangle\langle m| . \tag{2.23}$$

Note that $F^q = \mathbb{1}$ if q is a prime number. For the qubit case, Fourier transform correspond to the well known H matrix

$$H = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} . \tag{2.24}$$

There is connection between Fourier transform and Pauli matrices, $F^{-1}ZF = X$ and $F^{-1}XF = Z^{-1}$.

2.5.2. Stabilizer states

Stabilizer states have first been introduced for qubits [Got97] and later generalized to qudits [AK01, KKKS06]. For a given stabilizer state $|\psi\rangle$ there exists an associated stabilizer group, that consist of a set of pauli strings that leave $|\psi\rangle$ unchanged

$$\forall i \quad S_i|\psi\rangle = |\psi\rangle . \tag{2.25}$$

Any stabilizer state can be defined by a set of stabilizer generators $S_{|\psi\rangle}$, which generates the group under multiplication, i.e., if S_i and S_j are two stabilizers, S_iS_j is a stabilizer. Stabilizer states are further defined as a subset of the n-qudit states that can be efficiently described by a set of n stabilizer generators

$$S_\psi = \{S_i : S_i|\psi\rangle = |\psi\rangle,\ S_i \in P^n,\ i = 1, \ldots, n\} , \tag{2.26}$$

where P^n is the group of n-fold tensor products of Pauli operators $\mathbb{1}$, X and Z.

2.5.3. Definition of graph states

A graph $G = (V, \Gamma)$ is composed of a set V of n vertices and a set of weighted edges specified by the *adjacency matrix* Γ, which is an $n \times n$ symmetric matrix with vanishing diagonal entries and $\Gamma_{ij} = 0$ if vertices i, j are not connected or $\Gamma_{ij} > 0$ otherwise. We are now ready

to define graph states for n qudits of dimension q, wherein this section q is a prime number. The qudits associated to the graph are graphically represented by vertices $V = \{v_i\}$, whose size is $|V| = n$. The graph state associated with a given weighted graph $G = (V, \Gamma)$ of a system of n qudits labelled with $V = \{v_i\}$ and adjacency matrix Γ, reads [BBD$^+$09a]

$$|\Gamma\rangle = \prod_{i>j} CZ_{i,j}^{\Gamma_{ij}} |+\rangle^{\otimes n} \tag{2.27}$$

where $|+\rangle = \sum_{l=0}^{q-1} |l\rangle$ and pairwise controlled-Z gates apply between the systems according to the entries of the adjacency matrix Γ. For two distinct qudits i and j, the controlled-Z gate CZ_{ij} is defined by

$$CZ_{ij} \coloneqq \sum_{l\in[q]} |l\rangle\langle l|_i \otimes Z_j^l = \sum_{l,m\in[q]} \omega^{lm} |l\rangle\langle l|_i \otimes |m\rangle\langle m|_j \,. \tag{2.28}$$

In the case of qubits $|+\rangle = |0\rangle + |1\rangle$, and CZ_{ij} is the controlled Z gate written as

$$CZ_{ij} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} . \tag{2.29}$$

The graph state $|\Gamma\rangle$, Eq. (2.27), is $+1$ eigenstate (up to a global phase factor) of the following n set of stabilizer operators that stabilize $|\Gamma\rangle$

$$S_l^\Gamma = X_l \prod_m (Z_m)^{\Gamma_{lm}} \,, \qquad 1 \le l \le n \,. \tag{2.30}$$

In this formula, the generators of the stabilizer group provide an intuitive framework to consider the graph representation of a pure state. For every $1 \le l \le n$, S_l means that at site l we have considered X, while at all other neighbours connected to l we have Z to the power given by the weight of the connecting edge. This shows that considering the graphical representation, we can uniquely determine the state $|\Gamma\rangle$ and its stabilizers.

2.6. Classical error correcting codes

Error correcting codes are introduced to preserve information transmitted across a noisy channel. These codes provide a way to reduce the influence of noise. The principle of error correcting codes consists of adding redundancy in the message so that the receiver could recover the sent message even if it has been corrupted during the transmission.

2.6.1. Finite fields

In order to discuss coding theory, we first need to introduce a notion of linear independence that is suitable for sequences over a finite set of elements. This brings us to the theory of finite fields [MS77, Chapter 3,4]. Finite fields are used in many known constructions of codes. They are also important in many branches of mathematics, because of its diverse applications in such areas as combinatorics, coding theory, cryptology and the mathematical study of switching circuits. A finite field is also known as Galois Field in honor of Évariste Galois and denoted by GF. It has the following important properties.

A finite field (or Galois field) is a finite set of elements that is closed under addition, subtraction, (commutative) multiplication and division (excluding division by zero). For every prime number p and every natural number m there exists exactly one finite field $GF(p^m)$ (up to isomorphism) of cardinality (also called order) p^m. For every prime p the finite field $GF(p)$ is equal to the integers modulo p. For example $GF(5) = \{0, 1, 2, 3, 4\}$ where summation, addition, multiplication, and division are carried out modulo 5.

The prime-power finite fields $GF(p^m)$ can be explicitly constructed as follows: Let $GF(p)[x]$ be the set of polynomials in x over $GF(p)$, that is, the polynomials whose coefficients, variable x, addition and multiplication are elements from $GF(p)$. Choose a polynomial P over $GF(p)$ of degree m that is irreducible with respect to that field. Irreducible here means that P can not be written as the product of two non-constant polynomials in $GF(p)[x]$. The existence of such a polynomial P is always guaranteed [MS77, chapter 3]. $GF(p^m)$ is then the quotient ring $GF(p^m) = GF(p)[x]/P$, which is actually a field. That is, $GF(p^m)$ is the set of polynomials of degree less than m with the standard addition and subtraction of polynomials over $GF(p)$ and the result of multiplication is the remainder after Euclidean division by P.

In summary, when defining a field of order p^m, one also needs to specify the irreducible polynomial. An important property of the finite field is that all fields of the same order are isomorphic. Therefore, one can choose any irreducible polynomial of degree equal to m for the field $GF(p^m)$.

As an example, let us consider the case $q = 2^2$. The elements of the finite field $GF(2^2)$ can be written in several different ways (see Table 2.1). As the field is a prime-power finite field, it will be convenient to work with the representation in terms of polynomials based on the irreducible polynomial $x^2 + x + 1$. For example we consider multiplication 2.3 or equivalently multiplying 2-tuple 01.11

$$2.3 = 01.11 = (x)(1 + x) = x + x^2 \tag{2.31}$$

Considering the irreducible polynomial $x^2 = x + 1$ one can reduce the answer $x + x^2$ to a

as a 2-tuple	as a polynomial	spin levels
00	0	0
10	1	1
01	x	2
11	x+1	3

Table 2.1.: $GF(2^2)$ generated by $x^2 = x + 1$.

polynomial of degree smaller than 2. In this case we get $x + x^2 = 1$, and hence in spin level language we have $2.3 = 1$. In general, to get the terms in the familiar computational basis representation, after doing all computations in the finite field for each term, one simply has to switch back to the spin level representation.

It is also shown that every finite field contains at least one *primitive element* [MS77, chapter 4]. A primitive element of a finite field $GF(q)$ is an element γ whose multiplicative order equals $q - 1$, which means if γ is a primitive element, then the cyclic group $\{1, \gamma, \gamma^2, \ldots, \gamma^{q-2}\}$ is a set of $q - 1$ distinct nonzero elements of $GF(q)$.

2.6.2. Main problem of coding theory

The first and most classical example of coding theory is the one where two parties are trying to communicate over a noisy channel. All one wants to do is send a single bit 0 or 1 as message words. After going through the channel there is a probability p that the received bit does not match the sent bit. This means, if a 0 is sent through the channel, then the receiver gets a 0 with probability $1 - p$ and a 1 with probability p. One solution would be sending chunks of bits repeated many times. For example, suppose we agree to send message words 000 or 111, and we receive word 001 and we know we are using a channel with at most one error. Therefore we correct it to 000. We can see this by considering the probabilities as well. The probability that we send 000 and receive 001 is $(1 - p)^2 p$, and the probability that we send 111 and receive 001 is $p^2(1 - p)$. If p is small then it is likelier that we sent 000 than that we sent 111, therefore we decode this message as 000.

One needs to *encode* the original message to give them some protection against errors on the channel. After that, we need to *decode* the received message. Given our received word, we determine which of the message words is most likely to have been sent. Thus, we ask for the probability that we make an error in the decoding process. We do this exactly in the case of encoding 0 into 000 and 1 into 111, where there are two or more errors. The probability of this occurring is:

$$\binom{3}{2}(1 - p)p^2 + p^3 \approx 3p^2 \ll p \,, \tag{2.32}$$

when p is small. If we don't use the encoding technique and just send a single bit then the probability that it can be received incorrectly is p. Therefore, we see that when p is small, this

repetition helps us decode correctly.

We can also ask for the expected errors after decoding in a wrong way. In this case, the expected number can be written as

$$3(1-p)p^2 + p^3 \ll p\,, \tag{2.33}$$

where p is the expected error that might cause because of the structure of the channel. The general case is that we encode each bit n times, where for simplicity we assume n is odd. With the same analysis as above, we can check the probability of decoding incorrectly is

$$\binom{n}{\frac{n+1}{n}} p^{\frac{n+1}{2}} (1-p)^{\frac{n-1}{2}} + \cdots + \binom{n}{n} p^n \ll \binom{n}{\frac{n-1}{2}} p^{\frac{n+1}{2}}\,, \tag{2.34}$$

where p is considered to be small. This shows we can decrease the probability of decoding incorrectly at the price of sending longer and longer messages.

The repetition code is providing a useful method to correct errors in transmission, but we would like to find efficient ways. One important measure of the effectiveness of a code is the *rate*. Suppose we consider the length of the messages to be k over finite field $GF(q)$, which means the number of messages will be q^k. And we send the messages in blocks of n symbols of $GF(q)$. The rate R of a code with length n that encodes q^k many messages is defined as

$$R \coloneqq \frac{k}{n}\,. \tag{2.35}$$

The rate of the code of length 3 defined above is $\frac{1}{3}$. And, the rate of the repetition code of length n is $\frac{1}{n}$.

Now we can phrase the main questions in error correction: How can we build redundancy into messages so that the errors caused by the channel can be detected and corrected? What are the most efficient codes, that is those that can correct more errors per sent symbol? For a fixed number of errors what are the largest possible messages?

2.6.3. Classical codes

The purpose of using codes is to correct errors on noisy communication channels [MS77]. Given integers n, K, q, in general, an error correcting code is an injective mapping from a set of K messages to a subset of $[q]^n$. For any $n \in \mathbb{Z}^+$ we denote by $[n] \coloneqq (0, \ldots, n-1)$ the range from 0 to $n-1$. Protection against errors on some of the letters of the codewords can be achieved only if $q^n > K$. In the language of coding theory a $(n, K, d_H)_q$-code is an error correcting code that works with q-level dits and encodes a total of K messages into codewords of length n, all having pairwise Hamming distance at least d_H. A code can correct errors on

any subset of at most $t = \lfloor (d_H - 1)/2 \rfloor$ many dits [MS77, chapter 1].

Liner codes are a special class of codes. These are codes whose set of messages is $[q]^k$ for some integer k and whose injective mapping from this set of messages to the set of codewords is linear. For such codes $K = q^k$ and, as we mentioned before they are denoted as $\mathscr{C} = [n, k, d_H]_q$.

To obtain the largest possible number of codewords with a given minimum distance, sometimes one needs to use nonlinear codes. While the theory of nonlinear codes is rich and subject to many interesting developments, in this thesis we just deal with linear codes.

2.6.4. Linear codes

Classical linear codes represent a very important subset of classical error correcting codes and have many practical advantages [MS77]. They are characterized by three parameters, n, k and d_H over a finite field $GF(q)$. A linear error correcting code is a linear mapping from messages of length k to a subset of *codewords* of length n. Protection against errors on some of the letters of the codewords can be achieved only if $n > k$. The protection depends on the *Hamming distance* between the codewords. The Hamming distance d_H between two codewords is defined as the number of positions in which they differ. The large Hamming distance is essential in guaranteeing to recover the original message if noise causes errors in $t = \lfloor (d_H - 1)/2 \rfloor$ dits of the code.

In summary, in the language of coding theory a linear code denoted as $\mathscr{C} = [n, k, d_H]_q$, is an error correcting code that works with q-level dits and encodes a total of q^k messages into codewords of length n, all having pairwise Hamming distance at least d_H. The repetition code we mentioned as an example is $[3, 1, 3]_2$.

For the encoding procedure of a linear code $\mathscr{C}$, it is possible to define a *generator matrix*, in which the codewords are all possible linear combinations of the rows of such matrix. A generator matrix is a $k \times n$ matrix over a finite field $GF(q)$, and it can always be written in the standard form, up to possible permutations of the n letter of the code [MS77, Chapter 1]

$$G_{k\times n} = [\mathbb{1}_k | A] \, , \tag{2.36}$$

where $\mathbb{1}_k$ is identity matrix with size $k \times k$, and $A \in GF(q)^{k\times(n-k)}$. This standard form will be useful several times in this thesis.

Every linear code $\mathscr{C}$ has a *dual code* $\mathscr{C}^\perp$, that is the code whose codewords are orthogonal to all the codewords of the original code with respect to the standard Euclidean inner product of the finite field. The generator matrix $H_{n-k\times n}$ of the dual code is the so-called parity check matrix of the original code. It satisfies $G_{k\times n} \, (H_{n-k\times n})^T = 0$ and if $G_{k\times n}$ is given in standard

form, then $H_{n-k\times n} = [-A^T|\mathbb{1}_{n-k}]$. The matrix $H_{n-k\times n}$ is called parity check matrix, because for any codeword $\vec{c} \in \mathscr{C}$ of the original code $H_{n-k\times n}\,\vec{c}^{\,T} = 0$, so it can be used to check whether a string is a codeword or not. As an example, a suitable generator matrix of a linear code $[6, 3, 4]_5$ in standard form is

$$G_{3\times 6} = \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 1 & 3 & 4 \end{array}\right]. \tag{2.37}$$

It yields the following closed form expression for the list of the codewords

$$\vec{c} = \vec{v}\,G = i, j, l, i + j + l, i + 2j + 3l, i + 3j + 4l \tag{2.38}$$

where $\vec{v} = (i, j, l)$ and $i, j, l \in GF(5)$.

2.6.5. Dual code

Every linear code $\mathscr{C}$ has a dual code $\mathscr{C}^\perp$, that is the code whose codewords are orthogonal to all the codewords of the original code with respect to the standard Euclidean inner product of the finite field

$$\mathscr{C}^\perp = \{\vec{u} \mid \vec{u}.\vec{v} = 0 \quad \text{for all } \vec{v} \in \mathscr{C}\}\,. \tag{2.39}$$

$\mathscr{C}^\perp$ is the orthogonal subspace to $\mathscr{C}$. This also implies that $\mathscr{C}^\perp$ is exactly the set of all parity checks on $\mathscr{C}$. If $\mathscr{C}$ has generator matrix G and parity check matrix H, then $\mathscr{C}^\perp$ has generator matrix $= H$, and parity check matrix $= G$. Thus, if $\mathscr{C}$ has code parameter $\mathscr{C} = [n, k, d_H]$, $\mathscr{C}^\perp$ is an $[n, n - k, d_H^\perp]$, one should also note that while the code parameters of a code and its dual are related, their Hamming distance are almost independent, as $d_H^\perp$ can be larger or smaller than d_H [MS77, Chapter 5].

2.6.6. Bounds on codes

Our goal is producing a code $\mathscr{C} \subset (\mathbb{C}^q)^{\otimes n}$ with a high rate, and a high relative Hamming distance, that is with message length and Hamming distance as close as possible to n. But, these requirements contradict each other. There are several upper and lower bounds on classical codes for fixed length n over $GF(q)$: upper bounds like the Singleton, Hamming or sphere packing and, Johnson bound, and lower bounds like the Gilbert-Varshamov bound. In this section, we discuss one of the most famous upper bound on the parameters of codes, called Singleton bound. The other bounds on classical codes can be found in textbooks.

The *Singleton bound* is a fundamental result from coding theory that bounds the maximally achievable minimal Hamming distance between any two codewords. It states [Sin64] that for

any code

$$K \leq q^{n-d_H+1}. \tag{2.40}$$

For a linear code $\mathscr{C} = [n, k, d_H]_q$ the Singleton bound reads as

$$k \leq n - d_H + 1. \tag{2.41}$$

This corresponds to the fact that the rank of the parity check matrix H is $r = n - k$ and it is equivalent to the maximum number of linearly independent columns of H.

2.6.7. Maximum distance separable codes

Maximum distance separable (MDS) codes are optimal classical codes. The name comes from the fact that such codes have the maximum possible distance between codewords. We call a code MDS if and only if the Singleton bound Eq. (2.40) is fulfilled with equality. i.e., $K = q^{n-d_H+1}$. This is only possible if $K = q^k$ for some integer k, regardless of whether the code is linear or not (Some authors chose to only call linear codes fulfilling (2.40) with equality MDS codes [MS77, Chapter 11], but others use our broader definition [Sin64]). In this case, the bound simplifies to

$$d_H \leq n - k + 1. \tag{2.42}$$

As the all zero codeword is always a valid codeword in any linear code, this implies that any other codeword of a linear code must have at least $n - k + 1$ non-zero elements because otherwise, it would have a Hamming distance less than $n - k + 1$ to the all zero codeword. One directly verifies that the $[n, k, d_H = n - k + 1]_q$-code saturates the Singleton bound and is an MDS code.

The dual code $\mathscr{C}^\perp$ of any linear MDS code $\mathscr{C}$ is also MDS [MS77, Chapter 11]. If n is even and $k = n/2$, then both codes have the same size, i.e., $|\mathscr{C}| = |\mathscr{C}^\perp|$, but for n odd and $k = \lfloor n/2 \rfloor$ one code has $k = \lfloor n/2 \rfloor$ and the other has $k = \lceil n/2 \rceil$. In general and to avoid ambiguity, for the case $k < \lfloor n/2 \rfloor$ we denote the MDS code as $\mathscr{C} = [n, k]_q$ as the Hamming distance follows from the saturation of the Singleton bound, and the dual code with $\mathscr{C}^\perp = [n, n - k]_q$.

2.6.8. Constructing new codes from old codes

Using old codes to find new ones can simplify the task of finding codes. There is a number of simple modifications that one can make to existing codes to produce new codes with different parameters [HP03].

An operation to get a shorter code from an existing one is called *puncturing*. In this method,

from a linear code $[n, k, d_H]_q$ by deleting one coordinate one obtains a code $[n-1, k, d_H-1]_q$. Another manner to construct a code from another one is called *shortening*. In this construction starting from a linear code $[n, k, d_H]_q$ and by taking an appropriate subcode after deleting one coordinate, one can obtain the code $[n-1, k-1, d_H]$. It is worth noting that both puncturing and shortening operations yield MDS codes when starting with an MDS code.

2.7. Combinatorial designs

Combinatorial designs deal with the existence, construction and properties of finite sets whose arrangements satisfy generalized concepts of balance and symmetry. Some examples are block designs, t-designs, orthogonal Latin squares and orthogonal arrays [HSS99]. Design theory has its roots in recreational mathematics and has important applications in finite geometry, tournament scheduling, lotteries, mathematical chemistry, mathematical biology, algorithm design and analysis, networking, group testing, and cryptography [Sti03]. We will see later that combinatorial designs also provide a tool for constructing k-UNI states [GZ14, GRDMZ18].

2.7.1. Latin squares

Let S be a set of s symbols or levels. We denote the elements by $0, 1, \ldots, s-1$. A Latin square of order s is an $s \times s$ array with entries from the set S such that each element of S appears once in every row and column. It can be shown that a Latin square of order s exists for every positive integer s [HSS99]. For example, one may label the rows and columns by $0, 1, \ldots, s-1$ and take the entry in row i and column j to be $i + j$, modulo s. For instance the Latin square for $s = 4$ is displayed as

$$\begin{array}{cccc} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \\ 2 & 3 & 0 & 1 \\ 3 & 0 & 1 & 2 \end{array} \tag{2.43}$$

Two Latin squares of order s are called orthogonal to each other when one is superimposed to the other and the ordered pairs (i, j) of corresponding entries consist of all possible s^2 pairs. A collection of w orthogonal Latin squares of order s is defined by a set of pairwise orthogonal Latin squares and denoted by $POL(s, w)$. Such a collection is also often called a set of *mutually orthogonal Latin squares*, or $MOLS(s, w)$. As an example, three pairwise

orthogonal Latin squares of order 4 have the form

$$\begin{array}{cccc} 0 & 2 & 3 & 1 \\ 3 & 1 & 0 & 2 \\ 1 & 3 & 2 & 0 \\ 2 & 0 & 1 & 3 \end{array} \qquad \begin{array}{cccc} 0 & 2 & 3 & 1 \\ 1 & 3 & 2 & 0 \\ 2 & 0 & 1 & 3 \\ 3 & 1 & 0 & 2 \end{array} \qquad \begin{array}{cccc} 0 & 2 & 3 & 1 \\ 2 & 0 & 1 & 3 \\ 3 & 1 & 0 & 2 \\ 1 & 3 & 2 & 0 \end{array} \tag{2.44}$$

Finding orthogonal Latin squares is a challenging problem. For example none of the squares in Eq. (2.44) is orthogonal to the square in Eq. (2.43). A given Latin square is called isolated if there is no Latin square orthogonal to it.

2.7.2. Orthogonal arrays

Orthogonal arrays (OAs) are combinatorial arrangements introduced in [Rao46]. The most important applications of OAs are given in statistics and design of experiments. They also have a close connection to error correcting codes, difference schemes, Latin squares and Hadamard matrices [HSS99].

An $r \times n$ array A with entries taken from the set S with q elements is said to be an OAs with r runs, n factors, q levels, strength k and index λ if every $r \times k$ subarray of A contains each k-tuple of symbols from S exactly λ times as a row. Here, r and n denote the number of rows and columns of A, respectively, while q is the cardinality of the set S, that is, the level q is the number of different symbols appearing in A [HSS99]. The notation used to characterize OAs can be written as

$$\mathrm{OA}(r, n, q, k) \; . \tag{2.45}$$

For example we present OAs of strength $k = 1$, $k = 2$ and $k = 3$ respectively, with the sybolic expression $\mathrm{OA}(2, 2, 2, 1)$, $\mathrm{OA}(4, 3, 2, 2)$ and $\mathrm{OA}(8, 4, 2, 3)$

$$\mathrm{OA}(2,2,2,1) = \begin{array}{cc} 0 & 0 \\ 1 & 1 \end{array} \; , \quad \mathrm{OA}(4,3,2,2) = \begin{array}{ccc} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{array} \; , \quad \mathrm{OA}(8,4,2,3) = \begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{array} \; . \tag{2.46}$$

One usually determines an OA by the four independent parameters r, n, q and k, such that the index λ satisfies the relation

$$r = \lambda q^k \; . \tag{2.47}$$

It is shown that given an $OA(r, n, q, k)$ one can easily construct another OA with parameters $OA(r, n', q, k)$ for any $k \leq n' \leq n$ by removing $n - n'$ columns of the OA. Therefore, it is interesting to determine the maximal factor n such that an $OA(r, n, q, k)$ exists for fixed integer numbers r, q and k.

Two OAs are said to be isomorphic if one can be obtained from the other by a sequence of permutations of the columns, the rows, and the levels of each factor. QAs may be regarded as special cases of a more general classes of arrays that are also "orthogonal" in a statistical sense. There are bounds on the existence of OAs discovered in [Rao46]. If q is a prime power then an $OA(q^n, (q^n - 1)/(q - 1), q, 2)$ exists whenever $n \geq 2$.

2.7.3. Construction of orthogonal arrays from codes

Orthogonal arrays and codes are very closely related since we can use the codewords in an error correcting code as the runs of an OA, or conversely, we can regard the runs of an OA as forming a code. We can associate to any orthogonal array $OA(r, n, q, k)$ a code $(n, k, d_H)_q$ formed by its runs. Conversely, to any code $(n, k, d_H)_q$ we can associate the $n \times k$ array whose rows are the codewords. This is an orthogonal array $OA(r, n, q, k)$ for some r. We can now define a parity check matrix for an OA to be any parity check matrix for the associated code, and the dual OA to be the array corresponding to the dual code.

Two codes are said to be isomorphic if one can be obtained one from the other by permuting the coordinates. If $\mathscr{C}$ and $\mathscr{C}'$ are codes with associated orthogonal arrays OA and OA', then it can be shown that $\mathscr{C}$ is isomorphic to $\mathscr{C}'$ if and only if OA is isomorphic to OA' [HSS99].

2.8. Quantum error correcting codes

Quantum error correction plays a crucial role in quantum information processing and communication. With QECCs we can find ways to maintain a pure quantum state against the corrupting effects of decoherence long enough to carry out nontrivial quantum computations or communication protocols. In this section, we discuss QECCs with a focus on stabilizer codes. For this, we first discuss finite fields in quantum codes, then, we review the necessary and sufficient conditions to construct code spaces. Finally, we review some of the existing bounds on the quantum codes and the main differences between classical and quantum codes.

2.8.1. Finite fields in quantum codes

A field is more than just a set of elements. A finite field is a set of elements in which it is possible to do two operations, called addition and multiplication, along with a set of properties governing these operations. The addition and multiplication operations also imply inverse operations called subtraction and division.

Whenever resources are finite we are interested in using finite fields. In coding theory the number of elements, codewords as well as errors is finite. Also, the necessary computation can be managed in finite time, this implies that the results of computations are deterministic and exact.

2.8.2. Basics of quantum error correction

A QECC distinguishes a subspace (code space) of the Hilbert space of a physical system as the space of admissible code states, that is, quantum states of the system that are in a one to one correspondence (via the encoding and decoding maps) with encoded messages. For the code to be useful, the code space must be chosen such that the expected errors never map state from the code space to a state that could also have been produced by a different error from a different code state (this would introduce an unrecoverable error) but always take the state out of the code space in a way such that a subsequent correction can bring the system back into its original state.

We discuss the conditions under which a subspace is a QECC. To do this, we first introduce some notations. Let $\{|\psi_m\rangle\}_{m\in[q^{\tilde{k}}]}$ be a set of orthonormal quantum states of n qudits spanning a subspace $\mathcal{C}$. We denote by $[q^{\tilde{k}}]$ a string of $\tilde{k}$ symbols that range from 0 to $q-1$, e.g., for the case that $\tilde{k}=1$ we have, $[q] \coloneqq (0,\ldots,q-1)$. The code $\mathcal{C}$ with parameters $[\![n,\tilde{k},d]\!]_q$ is a valid QECC if it obeys the Knill-Laflamme conditions [KL97, KKKS06]

$$\forall m,m' \in [q^{\tilde{k}}]\colon\ \langle\psi_m|E^\dagger F|\psi_{m'}\rangle = f(E^\dagger F)\,\delta_{m,m'}\ , \tag{2.48}$$

for all E,F with $\mathrm{wt}(E^\dagger F) < d$. Here, wt is the *weight* of an operator which denotes the number of sites on which it acts non-trivially. The parameter d is the distance of the code, which is the minimal number of local operations that act on single sites to create a non-zero overlap between any two different states $|\psi_m\rangle$ and $|\psi_{m'}\rangle$, i.e.,

$$d \coloneqq \min_{|\phi\rangle,|\phi'\rangle\in\mathcal{C},W}\{\mathrm{wt}(W)\colon \langle\phi|W|\phi'\rangle \neq 0 \wedge \langle\phi|\phi'\rangle = 0\}\,. \tag{2.49}$$

Such a code can correct all errors that act non-trivially on up to $t \coloneqq \lfloor (d-1)/2 \rfloor$ physical qudits.

2.8.3. Quantum stabiliser codes

In the theory of quantum error correcting codes [Got09, Got97] stabilisers are a useful tool to construct and analyse codes. It is natural to consider code spaces that are spanned by computational basis states. The stabiliser (group) of such a code space is the abelian sub-group of the (generalized) Pauli group that leaves every element from the code space invariant. Conversely, every abelian sub-group of the (generalized) Pauli group that does not contain $-\mathbb{1}$

has a non-trivial subspace spanned by computational basis stats that is left invariant [Got09, Got97].

Stabiliser codes are crucial in this thesis. A stabilized subspace $\mathcal{C}$ defines a quantum code space as follows:

$$\mathcal{C} = \{|\psi_m\rangle \in \mathcal{H}(n,q) : \ S_i |\psi_m\rangle = |\psi_m\rangle, \forall S_i \in S\}. \tag{2.50}$$

S is generated by $n - \tilde{k}$ independent stabilizer operators S_i, so that the code space $\mathcal{C}$ encodes $\tilde{k}$ logical qudits into n physical qudits. In the language of coding theory a stabiliser QECC is denoted by $\mathcal{C} = [\![n, \tilde{k}, d]\!]_q$. This code is a $q^{\tilde{k}}$ dimensional subspace $\mathcal{C}$ spanned by a set $\{|\psi_m\rangle\}_{m\in[q^{\tilde{k}}]}$ of orthonormal states that encodes $\tilde{k}$ logical qudits into n physical qudits, if it obeys the Knill-Laflamme conditions Eq. (2.48).

2.8.4. Examples of quantum stabiliser codes

2.8.4.1. The 5-qubit code

As an example we consider the five qubit code $[\![5, 1, 3]\!]_2$, a code with distance 3 with an optimal achievable distance with respect to the quantum Singleton bound. This code encodes one logical qubit in five physical qubits. It is also a stabiliser code with a stabiliser subgroup $S =< S_1, S_2, S_3, S_4 >$ given by the stabiliser generators

$$\begin{aligned} S_1 &= X \otimes Z \otimes Z \otimes X \otimes \mathbb{1} \\ S_2 &= \mathbb{1} \otimes X \otimes Z \otimes Z \otimes X \\ S_3 &= X \otimes \mathbb{1} \otimes X \otimes Z \otimes Z \\ S_4 &= Z \otimes X \otimes \mathbb{1} \otimes X \otimes Z \end{aligned} \tag{2.51}$$

Note that the group is manifestly invariant under cyclic permutations. As is the case in the stabilizer formalism, codes are characterized by an abelian stabilizer subgroup such that $[S_i, S_j] = 0$ and the codespace is the joint +1 eigenspace for this group, satisfying

$$S_i|\psi\rangle = |\psi\rangle \qquad i = 1, \ldots, 4\,. \tag{2.52}$$

Logical operators are unitary operators which preserve the codeword space, but act non-trivially on the codewords. For the 5-qubit code the logical operators are given by

$$\overline{X} = X \otimes X \otimes X \otimes X \otimes X \tag{2.53}$$

$$\overline{Z} = Z \otimes Z \otimes Z \otimes Z \otimes Z \tag{2.54}$$

One can see that $\overline{X}$ and $\overline{Z}$ anti-commute with each other. Yet, they commute with all the stabilizer generators, so they preserve the codeword space. $\overline{X}$ and $\overline{Z}$ behave as logical X and Z Pauli operators for the logical qubit. One can denote two codeword states by $|\tilde{0}\rangle$ and $|\tilde{1}\rangle$ such that

$$\begin{aligned} \overline{Z}|\tilde{0}\rangle &= |\tilde{0}\rangle \\ \overline{Z}|\tilde{1}\rangle &= -|\tilde{1}\rangle \\ \overline{X}|\tilde{0}\rangle &= |\tilde{1}\rangle \\ \overline{X}|\tilde{1}\rangle &= |\tilde{0}\rangle \end{aligned} \tag{2.55}$$

For given logical operators $\overline{X}$ and $\overline{Z}$ there are other Pauli strings $S_i\overline{X}$ and $S_i\overline{Z}$ that perform the same action on the codeword space. Therefore, representations of logical operators are not unique.

2.8.4.2. CSS codes

Calderbank-Shor-Steane (CSS) codes are QECCs formed from two classical error correcting codes. The two classical codes $\mathscr{C}_1$ and $\mathscr{C}_2$ have the property that $\mathscr{C}_2^{\perp} \subseteq \mathscr{C}_1$ ($\mathscr{C}_2^{\perp}$ is the dual code to $\mathscr{C}_2$). If $\mathscr{C}_1$ has code parameters $[n, k_1, d_{H1}]_q$ and $\mathscr{C}_2$ is a code with parameters $[n, k_1, d_{H2}]_q$ (recall single brackets represent classical codes), then the corresponding quantum code is $[\![n, k_1 + k_2 - n, \min(d_{H1}, d_{H2})]\!]_q$.

CSS codes are not as efficient as the most general quantum code, but they are easy to derive from known classical codes. Also, they have a simple form that often makes them ideal for other purposes [Got09]. In general, CSS codes are an interesting class of codes because they are built using classical codes, which have been more studied than quantum codes. Therefore, it is fairly easy to construct useful quantum codes simply by looking at existing classical codes.

2.8.5. Bounds on Quantum error correcting codes

The question of "how efficient is an error correcting code for a given code length n and local dimension q?" can be considered as an interesting and important question in the theories of both classical and quantum error correction. As in classical theory there are upper and lower bounds on the quantum code parameters.

There is a quantum analogous of the classical Singleton bound. The quantum Singleton bound [Got97, CC97] states that for any QECC, $\mathcal{C} = [\![n, \tilde{k}, d]\!]_q$

$$d \leq \frac{n - \tilde{k}}{2} + 1. \tag{2.56}$$

Comparing with the classical Singleton bound given in Eq. (2.41), we see that to reach a given code distance in the quantum case, $n - \tilde{k}$ must be twice the necessary value to reach the same Hamming distance in the classical case. The proof of the quantum Singleton bound for $\tilde{k} = 1$ is based on the no-cloning theorem [Got09] and it is known that binary codes, that is codes for qubits $q = 2$, can not achieve it for large n. A QECC is called quantum maximum distance separable (QMDS) if Eq. (2.56) is saturated and in addition n and $\tilde{k}$ have the same parity [Rai99b]. Note that for n and $\tilde{k}$ given, there are codes that, while achieving the highest d allowed by Eq. (2.56), are not called QMDS. However, they are optimal in the sense that they achieve the largest distance for given n and $\tilde{k}$. Therefore, in this thesis we call the codes that saturate the quantum Singleton bound with maximum possible integer distance d *optimal codes*.

2.8.6. Difference between classical codes and quantum codes

The field of QECC is very similar to classical coding theory but there are several issues that need to be considered when transferring classical error correction techniques to the quantum regime.

(i) It is impossible to perfectly copy an unknown quantum state due to the no-cloning theorem of quantum mechanics [WZ82]. This result implies that there exists no transformation resulting in the following mapping,

$$U(|\psi\rangle \otimes |\psi\rangle) = |\psi\rangle \otimes |\phi\rangle \qquad \forall |\phi\rangle \ , \tag{2.57}$$

where U is a unitary operator. This means that coding based on data-copying, which is extensively used in classical error correction, cannot be used in QECC.

(ii) In classical codes, one can perform arbitrary measurements on the codewords. This is tricky in the quantum case because measurements are in general destructive.

(iii) Errors in quantum information are intrinsically continuous while classical errors are discrete.

Because of these fundamental differences between quantum information processing and its classical counterpart, new ideas and different approaches are necessary to construct quantum codes.

3. Constructing AME states from MDS codes

3.1. Introduction

A striking feature of quantum mechanics is entanglement and the fact that having complete knowledge of the state of a system does not imply complete knowledge of its subsystems. A paradigmatic example is an EPR state, in which a pure state of 2-qubits has reduced density matrices on each half of the system that are completely mixed. As mentioned, AME states are family of states generalizing this property of EPR states to an arbitrary number of parties and local dimensions.

Just like EPR states, AME states are known to play an important role in quantum information processing when dealing with many parties like [HCL$^+$12, Pip03]. AME states have also deep connections with apparently unrelated areas of mathematics such as combinatorial designs and structures [GAL$^+$15], classical error correcting codes [Hel13], and quantum error correcting codes (QECC) [Sco04]. Recently, they have gained new relevance as building blocks for holographic theories and in high-energy physics. There they allow for the construction of tensor network states that realize discrete instances of the AdS/CFT correspondence and holography [LS15, PYHP15, ADH15, HNQ$^+$16]. As we discussed before, AME states are special cases of the class of k-uniform (or k-UNI) states for $k = \lfloor n/2 \rfloor$ [AC13, GZ14].

At the same time it is still largely unknown for which values of the number of systems n and local dimension q AME states exist and how they can be constructed. A relevant class of AME states is formed by those states which can be written as superpositions of just $q^{\lfloor n/2 \rfloor}$ product states [Ber17]. These are called *minimal support AME states*, because $q^{\lfloor n/2 \rfloor}$ is the minimal number of product states necessary to obtain a state whose reduced state on $\lfloor n/2 \rfloor$ sites is full rank. There is a direct correspondence between minimal support AME states and classical maximal distance separable (MDS) error correcting codes [GAL$^+$15, Hel13, GZ14].

In this chapter we work out the details of the minimal support AME-MDS correspondence and provide explicit constructions and closed form expressions for AME states for arbitrary n and for all $q \geq n - 1$. Further, from a single AME state, we show how to produce an orthonormal

basis of AME states. Based on our construction of minimal support AME states, we introduce stabilizer operators and conjecture the existence of a family of QECC whose code spaces are spanned by AME states.

3.2. Notation

We begin with introducing some notation: For any $n \in \mathbb{Z}^+$ we denote by $[n] \coloneqq (0, \ldots, n-1)$ the range from 0 to $n-1$. Let $\mathcal{H}(n,q) \coloneqq \mathbb{C}_q^{\otimes n}$ be the Hilbert space of n distinguishable q level quantum systems (also called qudits). For any sequence $j_1, \ldots, j_n \in [q]^n$ we denote the corresponding vector by $\vec{j} \coloneqq (j_1, \ldots, j_n)$, its length by $|\vec{j}| = n$, and write $|\vec{j}\rangle \coloneqq |j_1, \ldots, j_n\rangle \coloneqq |j_1\rangle \otimes \cdots \otimes |j_n\rangle$ for the associated product state in $\mathcal{H}(n,q)$. As is customary we call the set of states $\{|\vec{j}\rangle\}_{\vec{j}}$ the computational basis. For any sequence $j_1, \ldots, j_n$ and subset $S \subset [n]$ of indices, we denote the truncation of $\vec{j}$ to the index set S by $\vec{j}_{|S} \coloneqq (j_l)_{l \in S}$. For instance, given the vector $\vec{j} = (6,4,3,4,5)$ and the subset $S = \{1,2,5\}$ we have $\vec{j}_{|S} = (6,4,5)$.

Any AME state can be written as

$$|\Psi\rangle = \sum_{j_1,\ldots,j_n=0}^{q-1} c_{j_1,\ldots,j_n} |j_1 \ldots, j_n\rangle \,, \tag{3.1}$$

where the coefficients $c_{j_1\ldots,j_n}$ can be regarded as a tensor of n indices with the property of being *multi-unitary* [GAL+15] or *perfect* [PYHP15]. A tensor c is called perfect if for any bipartition of its indices into a set S and complementary set S^c with $|S| \leq |S^c|$, the resulting matrix $C \coloneqq c_{\vec{j}_{|S}, \vec{j}_{|S^c}}$ is proportional to an isometry, i.e., $C^\dagger C \propto \mathbb{1}$. Using this matrix C, Eq. (3.1) can be rewritten as

$$|\Psi\rangle = \sum_{\vec{l} \in [q]^{|S|}} |\vec{l}\rangle \otimes C\,|\vec{l}\rangle \,. \tag{3.2}$$

Note that the states $C|\vec{l}\rangle \in \mathcal{H}(|S^c|, q)$ are in general not product states.

An n-qudit state in $\mathcal{H}(n,q) \coloneqq \mathbb{C}_q^{\otimes n}$ is AME, and denoted concretely by $\mathrm{AME}(n,q)$, whenever

$$\rho_S = \mathrm{Tr}_{S^c} |\psi\rangle\langle\psi| \propto \mathbb{1} \qquad \forall S \subset \{1,\ldots,n\}, |S| \leq \lfloor n/2 \rfloor \,, \tag{3.3}$$

where S^c denotes the complementary set of S. AME states can be classified according to the minimal number of terms they have, when expanded in any product basis [GAL+15]. The minimal number of terms for which the condition of maximally mixed marginals can still be fulfilled is the dimension of the largest sub-system on which the state is required to still be maximally mixed, namely $q^{\lfloor n/2 \rfloor}$. AME states with these many terms are minimal support AME states. In this section, we focus on AME states of minimal support.

Being an AME state of minimal support puts strong constraints on the coefficients $c_{j_1,\ldots,j_n}$ in the expansion in Eq. (3.1). Let the Hamming distance between two sequences $j_1,\ldots,j_n$ and $k_1,\ldots,k_n$ be the number of sub-indices l for which $j_l \neq k_l$. Then, $|\Psi\rangle$ can only be a minimal support AME state if $|c_{j_1\ldots,j_n}| \in \{0, 1/\sqrt{q^{\lfloor n/2 \rfloor}}\}$ and if all sequences $j_1\ldots,j_n$ for which $|c_{j_1\ldots,j_n}| \neq 0$ have pairwise Hamming distance at least $\lceil n/2 \rceil + 1$ [GAL+15]. To see this, let us consider a bipartiton $S \cup S^c = \{1,\ldots,n\}$ and look at $C = c_{\vec{j}_{\restriction S},\vec{j}_{\restriction S^c}}$ as a linear map from the space $\mathcal{H}(|S|,q)$ to $\mathcal{H}(|S^c|,q)$. As $|\psi\rangle$ is of minimal support, the states $C|\vec{j}_{\restriction S}\rangle$ are product states and hence every column of the matrix C contains only a single non-zero element. Now consider the case $|S| = \lfloor n/2 \rfloor$. Then, C associates to any sequence $\vec{l}$ of length $\lfloor n/2 \rfloor$ a sequence $\vec{m}$ of length $\lceil n/2 \rceil$, namely the one for which $C_{\vec{l},\vec{m}} \neq 0$. As the AME state is minimal support, there are precisely $q^{\lfloor n/2 \rfloor}$ such sequences of length $\lceil n/2 \rceil$. Consider now the set of sequences that is obtained by concatenating any sequence of length $\lfloor n/2 \rfloor$ with the associated sequence of length $\lceil n/2 \rceil$, i.e., the set $\{\vec{l} \circ \vec{m} : \vec{l} \in [q]^{\lfloor n/2 \rfloor} \wedge C_{\vec{l},\vec{m}} \neq 0\}$.

3.3. Correspondence between minimal support AME states and maximum distance separable codes

There is a direct correspondence between minimal support AME states and classical MDS codes [Hel13]. We first describe how an MDS code can be obtained from any minimal support AME state, then explain more generally how to obtain MDS codes. Finally, we show how any MDS code that encodes $\lfloor n/2 \rfloor$ dits (q level classical systems) into n dits allows for the construction of minimal support AME states in $\mathrm{AME}(n,q)$.

As we discussed in Preliminaries (2), in the language of coding theory a $(n, K, d_H)_q$-code is an error correcting code that encodes a total of K messages into codewords of length n, all having pairwise Hamming distance at least d_H. The Singleton bound is a fundamental result from coding theory that bounds the maximally achievable minimal Hamming distance between any two codewords. Recall that for any code the Singleton bound Eq. (2.40) reads

$$K \leq q^{n-d_H+1}. \tag{3.4}$$

We call a code maximum distance separable (MDS) if and only if the above bound is fulfilled with equality. This is only possible if $K = q^k$ for some integer k, regardless of whether the code is linear or not. Some authors chose to call MDS only those linear codes fulfilling (2.40) with equality [MS77, Chapter 11], but others use our broader definition [Sin64, KKO15]. For linear codes, the bound simplifies to Eq. (2.42), recall

$$d_H \leq n - k + 1. \tag{3.5}$$

As the all-zero code word is always a valid code word in any linear code, this implies that any other code word of a linear code must have at least $n-k+1$ non-zero elements because otherwise it would have a Hamming distance less than $n-k+1$ to the all zero codeword. One directly verifies that the $(n, q^{\lfloor n/2 \rfloor}, \lceil n/2 \rceil + 1)_q$-code constructed above saturates this bound with equality for all n. Thus from any minimal support AME state a classical MDS code can be constructed.

Conversely from any MDS code with $k = \lfloor n/2 \rfloor$ an AME state can be constructed by simply taking the equally weighted superposition of the computational basis states corresponding to all the code words [GAL+15]. For linear MDS codes particularly nice and explicit constructions can be achieved. The encoding map of a linear code is a linear map from the space of messages to the space of codewords, that is the generator matrix $G_{k\times n}$. The encoded version of an arbitrary message can be obtained by splitting the message up into blocks of length k and multiplying the corresponding row vectors from the right with the $k \times n$ generator matrix, thereby yielding the corresponding codeword. Multiplication and addition are thereby to be performed in a finite field whose cardinality is at least as large as that of the message alphabet.

We already know that the generator matrix $G_{k\times n}$ of any $[n, k, d_H]$-code over a finite field $GF(p^m)$ can always be written in the standard form, $G_{k\times n} = [\mathbb{1}_k|A]$ Eq. (2.36) [MS77, chapter 1]. Given the generator matrix $G_{\lfloor n/2 \rfloor \times n}$, or alternatively the matrix A, of a suitable linear MDS code $\mathscr{C}$ with $k = \lfloor n/2 \rfloor$ over a finite field of cardinality q (equal to a power of a prime), it is straightforward to construct an $\mathrm{AME}(n, q)$ state. As the Hamming distance of the MDS code is $d_H = \lceil n/2 \rceil + 1$, for any two different $\vec{v}, \vec{w} \in [q]^{\lfloor n/2 \rfloor}$ the states $|\vec{v}\, G_{\lfloor n/2 \rfloor \times n}\rangle$ and $|\vec{w}\, G_{\lfloor n/2 \rfloor \times n}\rangle$ are orthogonal on all subsystems of size at least $\lceil n/2 \rceil$. The state

$$|\Psi\rangle = \sum_{\vec{v}\in[q]^{\lfloor n/2 \rfloor}} |\vec{v}\, G_{k\times n}\rangle = \sum_{\vec{v}\in[q]^{\lfloor n/2 \rfloor}} |\vec{v}, \vec{v}\, A\rangle. \tag{3.6}$$

is hence a minimal support AME state in $\mathrm{AME}(n, q)$.

AME states can hence be constructed whenever a suitable matrix $G_{k\times n}$ or A is known. The first examples of matrices A with the desired properties were presented by Singleton [Sin64] for the cases $q = 5$ and $q = 7$ and later a general construction was found in [RS85, SR86].

We come back to explaining how suitable matrices A and $G_{k\times n}$ can be constructed in the next section. First, as an example, we go through the construction of a minimal support state $\mathrm{AME}(6, 5)$. In this example the local dimension $q = 5$ is prime so that the finite field $GF(5)$ is simply the set $\{0, 1, 2, 3, 4\}$ with the standard arithmetic modulo 5. The number of free indices in the closed form expression of the AME state with minimal support is $k = \lfloor n/2 \rfloor = 3$, so we can write $\vec{v} = (i, j, l)$. A suitable generator matrix of a $[6, 3, 4]_5$ MDS code in standard

form is

$$G_{3\times 6} = \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 1 & 3 & 4 \end{array}\right]. \tag{3.7}$$

It yields the following closed form expression for a minimal support state $\mathrm{AME}(6,5)$:

$$\begin{aligned} |\Psi\rangle &= \sum_{\vec{v}\in GF(5)^3} |\vec{v}\,G\rangle \\ &= \sum_{i,j,l=0}^{4} |i,j,l,i+j+l,i+2j+3l,i+3j+4l\rangle \end{aligned} \tag{3.8}$$

We present an example with a prime-power finite field in the next section.

3.4. Explicit construction of generator matrices for MDS codes and AME states

We now show explicitly how generator matrices of linear MDS codes and hence minimal support AME states can be constructed and how closed formulas, reminiscent of the example in the end of the last Section, can be obtained for all n. To do this, we first discuss the properties of the generator matrices of MDS codes in more detail.

Coming back to the standard form of the generator matrices of linear codes $G_{k\times n} = [\mathbb{1}_k|A]$, we can readily see that a linear code can only be an MDS code if all entries of the matrix A are non-zero and that $d_H = n-k+1$ is the optimal achievable Hamming distance between all codewords. If A had a zero somewhere, there would be a codeword with less than $n-k+1$ non-zero symbols and which hence would have Hamming distance less than $n-k+1$ to the all zero codeword (which is a valid codeword in any linear code).

In fact, a linear code with a given matrix A is an MDS code if and only if every square submatrix of A is nonsingular [MS77, Chapter 11], [Sin64]. To show this we first need to prove the following: Every square submatrix of A is nonsingular if and only if any subset of up to k of the column vectors of $G_{k\times n} = [\mathbb{1}_k|A]$ is linearly independent. First note that it is enough to show this for subsets of size exactly k. Let now K be the square matrix of any given set of k column vectors of $G_{k\times n}$. These vectors are linearly independent if and only if the determinant $\det(K)$ is non-zero. By shuffling all the columns that came from the $\mathbb{1}_k$ part of $G_{n\times k}$ to the left and then using Laplace's expansion of $\det(K)$ in terms of the determinants of minors, one realizes that $\det(K)$ is (up to possibly a sign) equal to the determinant of a square sub-matrix of A, and hence non-zero. This is true for all sub-sets of at most k columns only if all sub-matrices of A are non-singular.

As we are looking at linear codes, and hence any linear combination of codewords is again a valid codeword, to find the minimal distance between any two codewords it is sufficient to find the codeword with the minimal Hamming distance from the all zero codeword. This however is exactly n minus the maximal number of zeros that can occur in any linear combination of rows of $G_{k\times n}$. Due to the linear independence of any subset of k columns the maximum number of such zeros is $k-1$. This implies that the achieved Hamming distance is exactly $d_H = n-k+1$, saturating the Singleton bound.

To construct suitable matrices A, we now introduce concept of the so-called *Singleton arrays*. As we discussed in the Preliminaries, any finite field $GF(q)$, with q a power of a prime, contains at least one primitive element [MS77, chapter 4]. Given any primitive element γ, the Singleton array of size q is defined to be

$$S_q \coloneqq \begin{array}{ccccccc} 1 & 1 & 1 & \dots & 1 & 1 & 1 \\ 1 & a_1 & a_2 & \dots & a_{q-3} & a_{q-2} & \\ 1 & a_2 & a_3 & \dots & a_{q-2} & & \\ \vdots & \vdots & \vdots & & & & \\ 1 & a_{q-3} & a_{q-2} & & & & \\ 1 & a_{q-2} & & & & & \\ 1 & & & & & & \end{array} , \tag{3.9}$$

with

$$a_i \coloneqq \frac{1}{1-\gamma^i}. \tag{3.10}$$

The Singleton array is a special case of a more general construction known as a Cauchy matrix [MS77, chapter 11]. Every submatrix of a Cauchy matrix is again a Cauchy matrix and an explicit formula for the determinant of any Cauchy matrix is known, which in particular shows that it is non-zero. The Singleton array S_q thus has the sought after property that all its square sub matrices are non-singular [RS85, Mar90]. By taking rectangular sub-matrices of S_q, it is hence possible to construct generator matrices $G_{k\times n} = [\mathbb{1}_k | A_{k,n-k}]$ of MDS codes and thereby minimal support AME states. All one has to do is to take a power of a prime q sufficiently large such that S_q contains a sub-matrix of size at least $\lfloor (q+1)/2 \rfloor \times \lceil (q+1)/2 \rceil$, and then take this as the matrix A in Eq. (3.6). We provide a Mathematica notebook for the explicit construction of Singleton arrays, see [ame] (also Table. 3.1).

One straightforwardly verifies that S_q contains such a sufficiently large sub-matrix whenever $q \geq n-1$. Further, if q is even, the element a_1 can be appended to the third and the $(q-1)$-st rows of S_q, without creating singular submatrices [MS77, chapter 11],[RS85]. For $q = 2^2$ this increases the size of the largest square sub-matrix, as the extended Singleton array S_4' has the

form

$$S_4' = \begin{matrix} 1 & 1 & 1 & 1 \\ 1 & a_1 & a_2 & \\ 1 & a_2 & a_1 & \\ 1 & & & \end{matrix} . \tag{3.11}$$

This yields a matrix A of size 3×3 for $q = 4$, giving a closed form formula for a minimal support $AME(6, 4)$. For this, let us list the elements of the singleton arrays S_4'. The elements of the finite field $GF(2^2)$ can be written in several different ways (see Table. 2.1). As the field is a prime-power finite field, it is convenient to work with the representation in terms of polynomials based on the irreducible polynomial $x^2 = x + 1$. We chose $\gamma = x$ as a primitive element and, using the polynomial representation of $GF(2^2)$, the appearing elements can be calculated to be

$$a_1 = \frac{1}{1-x} = x \tag{3.12}$$

$$a_2 = \frac{1}{1-x^2} = \frac{1}{x} = x + 1. \tag{3.13}$$

Let us now take the the largest submatrix of size 3×3 as the matrix A

$$A = \begin{bmatrix} 1 & 1 & 1 \\ 1 & x & x+1 \\ 1 & x+1 & x \end{bmatrix} \tag{3.14}$$

and construct an $\mathrm{AME}(6, 4)$. The number of free indices in the closed form expression of the state $\mathrm{AME}(6, 4)$ with minimal support is $k = 3$, so $\vec{v} = (i, j, l)$, and it can be written as,

$$|\Psi\rangle = \sum_{\substack{i,j,l \in \\ \{0,1,x,x+1\}}} |i, j, l, i + j + l, i + x\, j + (1 + x)\, l, i + (x + 1)\, j + x\, l\rangle . \tag{3.15}$$

To get the terms of $|\Psi\rangle$ in the familiar computational basis representation, after doing all computations in the finite field for each term, one simply has to switch back to the spin level representation, i.e., make the replacement $\{0, 1, x, x + 1\} \mapsto \{0, 1, 2, 3\}$ according to Table. 2.1.

As another example, let us consider the case $q = 5$. Taking $\gamma = 3$, which is a primitive

element in $GF(5) = \{0, 1, 2, 3, 4\} \mod (5)$, we find

$$a_1 = \frac{1}{1-3} = \frac{1}{3} = 2 \qquad \text{because } 1 = 6 \bmod 5 \tag{3.16}$$

$$a_2 = \frac{1}{1-9} = \frac{1}{2} = 3 \qquad \text{because } 1 = 6 \bmod 5 \tag{3.17}$$

$$a_3 = \frac{1}{1-27} = \frac{1}{4} = 4 \qquad \text{because } 1 = 16 \bmod 5 \tag{3.18}$$

and obtain

$$S_5 = \begin{matrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & \\ 1 & 3 & 4 & & \\ 1 & 4 & & & \\ 1 & & & & \end{matrix} . \tag{3.19}$$

The biggest submatrix has size 3×3. Hence, taking

$$A_{3\times 3} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \\ 1 & 3 & 4 \end{bmatrix} \tag{3.20}$$

we can construct a $[6, 3, 4]_5$-code, which is an MDS code, and the resulting AME state is precisely the one given in Eq. (3.8).

Finally, we present a number of Singleton arrays that can be used to construct closed form expression of AME states with minimal support in Table. 3.1. A Mathematica notebook to create these and various larger tables is made available under [ame].

3.5. Basis of AME states

The Bell basis of the Hilbert space of 2 qubits is an orthonormal basis of maximally entangled states. In what follows, we show how, starting from a single AME state $|\Psi\rangle \in \mathcal{H}(n, q)$, a complete orthonormal basis of AME states for $\mathcal{H}(n, q)$, an *AME basis*, can be constructed. Given an AME state $|\Psi\rangle$ written in the form of (3.2) with respect to some fixed product basis, we first recall the definition of the operators X, Eq. (2.20) and Z, Eq. (2.21) that generalize the Pauli operators σ_X and σ_Z to Hilbert spaces of dimension $q \geq 2$. X and Z are defined through their action on this local elements of the product basis states $|j\rangle$ via

$$X|j\rangle = |j + 1 \mod q\rangle \tag{3.21}$$

$$Z|j\rangle = \omega^j |j\rangle . \tag{3.22}$$

As a side remark, note that only for q prime are the integers modulo q equal to the finite field $GF(q)$. In all other cases, the algebraic structure of X and Z as defined above does not correspond to that of the respective finite field (if it even exists). This however is irrelevant for this section. The following works for arbitrary q not necessarily prime or a power of a prime. Only the properties of X and Z discussed above are used.

For every $\vec{a}$ we define the operator

$$M(\vec{a}) \coloneqq (\underbrace{\mathbb{1} \otimes \cdots \otimes \mathbb{1}}_{\lfloor n/2 \rfloor} \otimes X^{a_1} \otimes \ldots \otimes X^{a_{\lceil n/2 \rceil}}) (\underbrace{\mathbb{1} \otimes \cdots \otimes \mathbb{1}}_{\lceil n/2 \rceil} \otimes Z^{a_{\lceil n/2 \rceil + 1}} \otimes \cdots \otimes Z^{a_n}) \,. \quad (3.23)$$

Note that, for n even, the maximal number of X's and that of Z's are equal, namely $n/2$. In contrast, if n is odd, the maximal number of X's is one larger than the maximal number of Z's. We now use this family of operators to construct complete orthonormal bases of AME states:

Lemma 3.1. *Consider a Hilbert space $\mathcal{H}(n, q)$ of n parties with local dimension q with at least one AME state $|\Psi\rangle \in \mathcal{H}(n, q)$. If n is even or $|\Psi\rangle$ is minimal support, then the q^n states*

$$|\Psi_{\vec{a}}\rangle \coloneqq M(\vec{a}) \, |\Psi\rangle \quad (3.24)$$

with $\vec{a} \in [q]^n$ form a complete orthonormal basis of AME states of $\mathcal{H}(n, q)$.

Proof. First, all the $|\Psi_{\vec{a}}\rangle$ are AME states, as acting with local unitaries on $|\Psi\rangle$ does not change the entanglement properties. It remains to show orthonormality, i.e., that

$$\langle \Psi | M(\vec{a})^\dagger \, M(\vec{b}) | \Psi \rangle = \prod_i \delta_{a_i, b_i} \,. \quad (3.25)$$

To show this we use that according to Eq. (3.2) any AME state $|\Psi\rangle$ can be written as

$$|\Psi\rangle = \sum_{\vec{l} \in [q]^{|S|}} |\vec{l}\rangle \otimes C \, |\vec{l}\rangle \,, \quad (3.26)$$

with $|S| = \lfloor n/2 \rfloor$ and C an isometry. It thus follows from the cyclicity of the trace that

$$\begin{aligned} \langle \Psi | M(\vec{a})^\dagger \, M(\vec{b}) | \Psi \rangle &= \sum_{\vec{l}, \vec{m} \in [q]^{|S|}} \langle \vec{l} | \vec{m} \rangle \, \langle \vec{l} | \, C^\dagger \, M(\vec{a})^\dagger \, M(\vec{b}) \, C \, | \vec{m} \rangle & (3.27) \\ &= \sum_{\vec{l} \in [q]^{|S|}} \langle \vec{l} | \, C^\dagger \, M(\vec{a})^\dagger \, M(\vec{b}) \, C \, | \vec{l} \rangle & (3.28) \\ &= \mathrm{Tr}(M(\vec{a})^\dagger \, M(\vec{b}) \, C \, C^\dagger) \,. & (3.29) \end{aligned}$$

Now, if n is even, then C is proportional to a unitary, i.e., $C^\dagger C = C C^\dagger \propto \mathbb{1}$, and thus

$$\langle\Psi|M(\vec{a})^\dagger M(\vec{b})|\Psi\rangle = \frac{1}{q^n}\operatorname{Tr}(M(\vec{a})^\dagger M(\vec{b})) = \prod_{i=1}^{n}\delta_{a_i,b_i}\,, \tag{3.30}$$

where we have used that $\operatorname{Tr}(Z^a X^b) = \delta_{a,0}\,\delta_{b,0}$. For n odd $C C^\dagger \not\propto \mathbb{1}$ but if $|\Psi\rangle$ is a minimal support AME state, then there exists a local product basis $|\vec{l}\rangle$ such that C maps product states to product states. This implies that if $\vec{a}_{\restriction\lceil n/2\rceil\rfloor} \neq \vec{b}_{\restriction\lceil n/2\rceil\rfloor}$ then $M(\vec{a})^\dagger M(\vec{b})$ contains at least one X and then each term in Eq. (3.28) vanishes individually. But now, whenever $\vec{a}_{\restriction\lceil n/2\rceil\rfloor} = \vec{b}_{\restriction\lceil n/2\rceil\rfloor}$, then $M(\vec{a})^\dagger M(\vec{b}) = \mathbb{1}\otimes\cdots\otimes\mathbb{1}\otimes Z^{b_{\lceil n/2\rceil+1}-a_{\lceil n/2\rceil+1}}\otimes\cdots\otimes Z^{b_n-a_n}$, i.e., it has weight at most $\lfloor n/2\rfloor$ and thus, because $|\psi\rangle$ is AME we have

$$\begin{aligned}&\langle\Psi|M(\vec{a})^\dagger M(\vec{b})|\Psi\rangle\\ &= \frac{1}{q^n}\operatorname{Tr}(\underbrace{\mathbb{1}\otimes\cdots\otimes\mathbb{1}}_{\lceil n/2\rceil}\otimes Z^{b_{\lceil n/2\rceil+1}-a_{\lceil n/2\rceil+1}}\otimes\cdots\otimes Z^{b_n-a_n})\prod_{i=1}^{\lceil n/2\rceil}\delta_{a_i,b_i} = \prod_{i=1}^{n}\delta_{a_i,b_i}\,.\end{aligned} \tag{3.31}$$

□

The general case of constructing an AME basis is always possible if the states are stabilizers.

3.6. Stabilizer operators for AME states of minimal support

Stabilisers are a useful tool to construct and analyse codes [Got09, Got97] . In an analogous fashion, we can construct a set of Pauli strings that generate a stabilizer group that stabilizes a given individual AME state. In the next section we use this generating set to construct a stabilizer group for a subspace spanned by q orthonormal AME states. The construction we present only works for AME states constructed from a linear MDS code as described in Section 3.3 and can hence only work for q being a power of a prime. For the sake of simplicity we further restrict from now on to the case q prime, for which the algebraic structure of the X and Z operators defined in (2.20) and (2.21) coincides with that of the finite field $GF(q)$. For q a power of a prime, a much more elaborate construction based on the (discrete) Heisenberg-Weyl group [Wey50, WF89, BBRV02, Gra04, Dur05] would have to be employed.

Remember that, given a generator matrix $G_{k\times n}$, the corresponding AME state takes the form (recall Eq. (3.6))

$$|\Psi\rangle = \sum_{\vec{v}\in[q]^{\lfloor n/2\rfloor}}|\vec{v}\,G_{\lfloor n/2\rfloor\times n}\rangle. \tag{3.32}$$

Denote the matrix elements of $G_{\lfloor n/2\rfloor\times n}$ by $g_{l,m}$ and that of the code's parity check matrix

$H_{\lceil n/2 \rceil \times n}$ by $h_{l,m}$. For q prime, the state $|\Psi\rangle$ is then the plus one eigenstate of the following n stabilizer operators:

$$s_l^{\Psi} \coloneqq \begin{cases} \bigotimes_{m=1}^{n} X^{g_{l,m}} & 1 \leq l \leq \lfloor n/2 \rfloor \\ \bigotimes_{m=1}^{n} Z^{h_{l,m}} & \lfloor n/2 \rfloor < l \leq n \end{cases}. \tag{3.33}$$

The first $\lfloor n/2 \rfloor$ stabilizers, involving the X operators, permute the computational basis states in the decomposition of $|\Psi\rangle$ and hence leave it invariant. The second set of $\lceil n/2 \rceil$ stabilizers, that involve the Z operators, also leave $|\Psi\rangle$ invariant as

$$s_l^{\Psi} |\Psi\rangle = \sum_{\vec{v} \in [q]^{\lfloor n/2 \rfloor}} \omega^{H_{\lceil n/2 \rceil \times n} (G_{\lfloor n/2 \rfloor \times n})^T \vec{v}} |\vec{v} G_{\lfloor n/2 \rfloor \times n}\rangle = |\Psi\rangle, \tag{3.34}$$

because $H_{\lceil n/2 \rceil \times n} (G_{\lfloor n/2 \rfloor \times n})^T = 0$.

One should note that any stabilizer state is equivalent to a graph state under the action of local Clifford group, see [NC00, BB06]. It is also shown that one can start from an associated graph states and find a graph basis which is a collection of orthonormal states of the form of graph states. With this, as soon as one can show a state is a stabilizer state, it guarantees of the existence the graph state corresponding to it and a complete orthonormal basis.

3.7. Conclusions

In this chapter we have shown in detail how to explicitly construct AME states of n parties with local dimension $q \geq n - 1$ of minimal support by means of linear MDS codes. For an AME state of minimal support constructed via such a linear MDS code and q prime, we have derived a set of stabilizer operators that stabilize the AME state. Along the way, we have also shown how, starting from any single AME state, a complete basis of the Hilbert space consisting of AME states can be constructed.

$GF(2) = \{0, 1\}$ modulo (2)	$\gamma = 1,$ $S_2 = \begin{array}{cc} 1 & 1 \\ 1 & \end{array}$
$GF(3) = \{0, 1, 2\}$ modulo (3)	$\gamma = 2,$ $S_3 = \begin{array}{ccc} 1 & 1 & 1 \\ 1 & 2 & \\ 1 & & \end{array}$
$GF(2^2) = \{0, 1, a_1, a_2\}$ modulo $(1 + x + x^2)$ $a_1 = x, a_2 = 1 + x.$	$\gamma = x,$ $S_4' = \begin{array}{cccc} 1 & 1 & 1 & 1 \\ 1 & a_1 & a_2 & \\ 1 & a_2 & a_1 & \\ 1 & & & \end{array}$
$GF(5) = \{0, 1, 2, 3, 4\}$ modulo (5)	$\gamma = 3,$ $S_5 = \begin{array}{ccccc} 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & \\ 1 & 3 & 4 & & \\ 1 & 4 & & & \\ 1 & & & & \end{array}$
$GF(7) = \{0, 1, 2, 3, 4, 5, 6\}$ modulo (7)	$\gamma = 3,$ $S_7 = \begin{array}{ccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 3 & 6 & 4 & 2 & 5 & \\ 1 & 6 & 4 & 2 & 5 & & \\ 1 & 4 & 2 & 5 & & & \\ 1 & 2 & 5 & & & & \\ 1 & 5 & & & & & \\ 1 & & & & & & \end{array}$
$GF(2^3) = \{0, 1, a_1, a_2, a_3, a_4, a_5, a_6\}$ modulo $(1 + x^2 + x^3)$ $a_1 = x^2,\ a_2 = 1 + x + x^2,\ a_3 = 1 + x,$ $a_4 = x,\ a_5 = x + x^2$ and $a_6 = 1 + x^2.$	$\gamma = x,$ $S_8 = \begin{array}{cccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & \\ 1 & a_2 & a_3 & a_4 & a_5 & a_6 & & \\ 1 & a_3 & a_4 & a_5 & a_6 & & & \\ 1 & a_4 & a_5 & a_6 & & & & \\ 1 & a_5 & a_6 & & & & & \\ 1 & a_6 & & & & & & \\ 1 & & & & & & & \end{array}$
$GF(3^2) = \{0, 1, a_1, a_2, a_3, a_4, a_5, a_6, a_7\}$ modulo $(2 + x + x^2)$ $a_1 = 2 + x,\ a_2 = 1 + x,\ a_3 = 1 + 2x,$ $a_4 = 2,\ a_5 = x,\ a_6 = 2x$ and $a_7 = 2 + 2x.$	$\gamma = x,\ S_9 = \begin{array}{ccccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & \\ 1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & & \\ 1 & a_3 & a_4 & a_5 & a_6 & a_7 & & & \\ 1 & a_4 & a_5 & a_6 & a_7 & & & & \\ 1 & a_5 & a_6 & a_7 & & & & & \\ 1 & a_6 & a_7 & & & & & & \\ 1 & a_7 & & & & & & & \\ 1 & & & & & & & & \end{array}$
$GF(11) = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ modulo (11)	$\gamma = 2,\ S_{11} = \begin{array}{ccccccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 10 & 7 & 3 & 8 & 6 & 4 & 9 & 5 & 2 & \\ 1 & 7 & 3 & 8 & 6 & 4 & 9 & 5 & 2 & & \\ 1 & 3 & 8 & 6 & 4 & 9 & 5 & 2 & & & \\ 1 & 8 & 6 & 4 & 9 & 5 & 2 & & & & \\ 1 & 6 & 4 & 9 & 5 & 2 & & & & & \\ 1 & 4 & 9 & 5 & 2 & & & & & & \\ 1 & 9 & 5 & 2 & & & & & & & \\ 1 & 5 & 2 & & & & & & & & \\ 1 & 2 & & & & & & & & & \\ 1 & & & & & & & & & & \end{array}$

Table 3.1.: Singleton array for various finite fields.

4. New construction for k-uniform and absolutely maximally entangled states

4.1. Introduction

Multipartite entangled states play an important role in many quantum information processing tasks. Providing a general framework for multipartite entanglement represents a highly complex problem, probably out of reach. Therefore, many efforts have focused on the study of relevant sets of states such as, for instance, graph states [HEB04, HDE$^+$06] or tensor network states [Or𝟙4]. Operationally, k-UNI states are a set of multipartite entangled states that are interested in this point of view. It is relevant question to find general constructions for them and classifying them based on SLOCC.

In the previous chapter (3), we focused on constructing AME states from MDS codes. Until now, using MDS codes is the only systematic method to construct AME and k-UNI states [Hel13, RGRA18]. With this method, one can construct minimal support k-UNI states as they can be expressed with the minimum number of product terms needed to guarantee that the reduced states are maximally mixed. In this chapter, we go beyond that and introduce a new systematic method of constructing k-UNI states. We prove that this method constructs different states as the derived states are not of minimal support.

We call this method Cl+Q because it combines a given classical MDS code with a basis made of k-UNI quantum states. With this method we construct k-UNI states with smaller local dimension q that cannot be obtained from MDS codes. Also, we prove that the Cl+Q method constructs different states as the derived states are not minimal support states anymore.

We show that our states cannot be obtained from any state of minimal support by SLOCC. We then show how the k-UNI states derived through our construction are example of graph states and provide the corresponding graph, which is different from the graphs associated to states of minimal support. Finally, we present generalizations of the Cl+Q method and use them to construct two examples of AME states whose existence was open so far, namely $\mathrm{AME}(19, 17)$

and $\mathrm{AME}(21, 19)$.

4.2. MDS codes and k-UNI states

As we discussed, in the language of coding theory, linear error correcting codes are specified by the tuple of integer numbers $[n, k, d_H]_q$ and defined over a finite field $GF(q)$. Such codes encode q^k many messages specified by vectors $\vec{v}_i \in [q]^k$, with $i = 1, \ldots, q^k$, into a subset of codewords $\vec{c}_i \in [q]^n$, all having Hamming distance d_H [MS77, Chapter 1]. Given an $[n_{\text{cl}}, \ell, n_{\text{cl}} - \ell]_q$ MDS code, it is possible to define its dual, which is an $[n_{\text{cl}}, n_{\text{cl}} - \ell, \ell + 1]_q$ MDS code. In what follows, we take initial MDS codes with $\ell \leq n_{\text{cl}}/2$ so that the number of codewords in the dual is $n_{\text{cl}} - \ell > n/2$.

MDS codes $[n_{\text{cl}}, \ell, n_{\text{cl}} - \ell]_q$ have been used to derive AME states of minimal supports when $\ell = \lfloor n/2 \rfloor$, or alternatively from the dual codes $[n_{\text{cl}}, n_{\text{cl}} - \ell, \ell + 1]_q$ when $\ell = \lceil n/2 \rceil$ [Hel13, RGRA18] . It is also possible to construct k-UNI states from a given MDS code. Consider the pure quantum state corresponding to the equally weighted superposition of all the codewords $\vec{c}_i$ of the code, i.e.,

$$|\psi\rangle = \sum_{i=1,\ldots,q^k} |\vec{c}_i\rangle \,, \tag{4.1}$$

It is instructive for what follows to recall why (4.1) is a k-UNI state, that it, to show why all reductions up to k parties are maximally mixed. For that we use two properties of MDS codes. First, since all codewords have a distance at least equal to the Singleton bound (2.41), all the off-diagonal elements of the reduced density matrices of at most k parties are zero. What remains to be proven is that all the diagonal elements of the reduced state of k parties are equal. But this follows from the fact that any MDS code has a systematic encoder in which any set of symbols of length k of the codewords can be taken as message symbols [MS77, Chapter 11], that is, all the q^k possible combinations of messages appear.

Using the construction of MDS codes, this superposition of all codewords of MDS codes reads

$$|\psi\rangle = \sum_i |\vec{c}_i\rangle = \sum_i |\vec{v}_i \, G_{k\times n}\rangle = \sum_i |\vec{v}_i,\ \vec{v}_i A\rangle \,. \tag{4.2}$$

The dual code $\mathscr{C}^\perp$ of any linear MDS code $\mathscr{C}$ is also MDS. As above, one can construct the two states $|\psi\rangle$ and $|\psi^\perp\rangle$ by taking the equally weighted superposition of the codewords of $\mathscr{C}$ and its dual $\mathscr{C}^\perp$, respectively. However, considering the connection between the codewords of the original code and its dual, one can check that the states $|\psi\rangle$ and $|\psi^\perp\rangle$ can be transformed one into the other by local unitary operations, more precisely by applying Fourier gates that map the Z-eigenbasis into the X-eigenbasis to each party. Therefore, not only $|\psi\rangle$, but also $|\psi^\perp\rangle$ is a k-UNI state of minimal support.

Finally, let us recall that MDS codes over finite fields $GF(q)$ have been found for the following intervals

$$\begin{cases} n \geq 2 & k = 1 \text{ or } n-1 \\ n \leq q+2 & q \text{ is even and } k = 3 \text{ or } q-1 \\ n \leq q+1 & \text{all other cases} \end{cases} , \tag{4.3}$$

which in turn defines an existence interval of k-UNI$_{\min}$ states, i.e., $k \leq \lfloor n/2 \rfloor$ (see [MS77, Chapter 11], [RS85]).

4.3. Orthonormal basis

In what follows we show how to construct an orthonormal basis starting from a k-UNI$_{\min}$ state built from an $[n, k, n-k]_q$ MDS code. In particular, we focus on the operators $M(\vec{v})$ labelled by $\vec{v} \in [q^n]$, that have the form

$$M(\vec{v}) \coloneqq \underbrace{Z^{v_1} \otimes \cdots \otimes Z^{v_k}}_{k} \otimes \underbrace{X^{v_{k+1}} \otimes \cdots \otimes X^{v_n}}_{n-k} . \tag{4.4}$$

This family of Pauli string can be used to derive a complete orthonormal basis of k-UNI states. As we see next, these q^n unitary operators define a basis when acting on a k-UNI$_{\min}$ state.

Lemma 4.1. *Consider a k-UNI$_{\min}$ state $|\psi\rangle \in \mathcal{H}(n,q)$ and all possible vectors $\vec{v}_i \in [q^n]$, with $i = 1, \ldots, q^n$. Then, the states $|\psi_i\rangle \coloneqq M(\vec{v}_i)\,|\psi\rangle$ form a complete orthonormal basis of k-UNI$_{\min}$ states.*

Proof. First, note that all the $|\psi_i\rangle$ are k-UNI states, since local unitary operations do not change the entanglement properties of the state $|\psi\rangle$. Then we should just check the orthonormality of the states, i.e., check that

$$\langle\psi|M(\vec{v}_i)^\dagger\, M(\vec{v}_{i'})|\psi\rangle = \prod_i \delta_{i,i'} . \tag{4.5}$$

To show this we use the fact that, for any k-UNI state $|\psi\rangle$ constructed from an MDS code $\mathscr{C} = [n, k, d_H = n-k+1]_q$, the Hamming distance between all the terms is at least $d_H = n-k+1$. The large Hamming distance between the terms in the superposition of state $|\psi\rangle$ implies

$$\langle\psi|M(\vec{v}_i)^\dagger\, M(\vec{v}_{i'})|\psi\rangle = \langle\psi|M(\vec{v}_Z^{(i)})^\dagger\, M(\vec{v}_Z^{(i')})|\psi\rangle \prod_{i=k+1}^{n} \delta_{i,i'} , \tag{4.6}$$

where $M(\vec{v}_Z^{(i)})$ has the Z operators of $M(\vec{v}_i)$ and no X operators. Now, by considering the

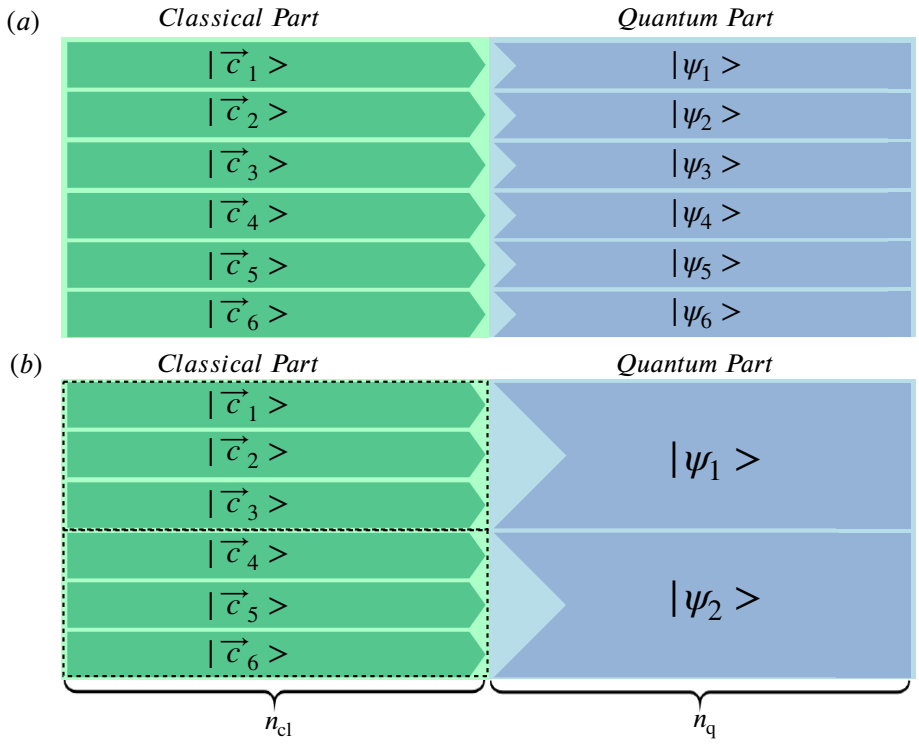


Figure 4.1.: Methods of constructing k-UNI states. (a) *Cl+Q method.* Constructing k-UNI states by concatenating each codeword of an MDS code with a given ℓ'-UNI state of an orthonormal basis. (b) *Cl+Q with repetition.* Constructing AME states by repeating states in the quantum part.

property of having k-UNI state, we yield

$$\langle\psi|M(\vec{v}_i)^\dagger M(\vec{v}_{i'})|\psi\rangle = \mathrm{Tr}(M(\vec{v}_Z^{(i)})^\dagger M(\vec{v}_Z^{(i')})) \prod_{i=k+1}^{n} \delta_{i,i'} = \prod_{i=1}^{n} \delta_{i,i'} \,. \tag{4.7}$$

Here we also used the fact that the operator $M(\vec{v}_Z^{(i)})^\dagger M(\vec{v}_Z^{(i')})$ has weight at least k. □

In the previous chapter this result was proven for the particular case of AME states of minimal support, leading to an AME basis. The above lemma generalizes the result to any k-UNI$_{\mathrm{min}}$ states.

4.4. Constructing k-UNI states of non-minimal support

We now present the new construction of k-UNI states, which combines the codeword of a given MDS code with an orthonormal basis where all elements are ℓ'-UNI states, see figure 4.1(a).

Lemma 4.2 (Cl+Q method)**.** *Consider an* $[n_{\mathrm{cl}}, \ell, n_{\mathrm{cl}} - \ell]_q$ *MDS code of codewords* $\vec{c}_i$ *and a complete* ℓ'-UNI(n_{q}, q) *orthonormal basis with states* $|\psi_i\rangle$ *such that* $n_{\mathrm{q}} = \ell$*. Construct the*

state

$$|\phi\rangle = \sum_{i=1,\ldots,q^\ell} \underbrace{|\vec{c}_i\rangle}_{n_{\rm cl}} \underbrace{|\psi_i\rangle}_{n_{\rm q}} \ . \tag{4.8}$$

This state is a $(\ell'+1)$-UNI *state of* $n = n_{\rm cl} + n_{\rm q}$ *parties. One can use the dual of an MDS code for the classical part. In this case, one then demands that* $n_{\rm q} = n_{\rm cl} - \ell$ *and obtains* $k = \min\{\ell+1, \ell'+1\}$-UNI *state.*

The condition $n_{\rm q} = \ell$ is needed to ensure that the number of codewords in the code match the number of elements in the basis, as required by the construction. Note that the number of states in the ℓ'-UNI$(n_{\rm q}, q)$ basis is $q^{n_{\rm q}}$, while the number of codewords in the MDS code is q^ℓ. This requirement implies that $\ell' < \ell$. But, the conditions for the lemma are more general, as one can use the dual of an MDS code for the classical part. One then demands that $n_{\rm q} = n_{\rm cl} - \ell$ and obtains a $k = \min\{\ell+1, \ell'+1\}$-UNI state.

Proof. For the classical part in our construction, it is possible to use an MDS code $\mathscr{C} = [n_{\rm cl}, \ell]_q$ or its dual $\mathscr{C}^\perp = [n_{\rm cl}, n_{\rm cl} - \ell]_q$. The resulting states can be written as

$$|\phi\rangle = \sum_i \underbrace{|\vec{c}_i\rangle}_{n_{\rm cl}} \underbrace{|\psi_i\rangle}_{n_{\rm q}} = \sum_i |\vec{v}_i\, G_{k\times n}\rangle\, |\psi_i\rangle = \sum_i |\vec{v}_i,\, \vec{v}_i A\rangle\, |\psi_i\rangle \ , \tag{4.9}$$

where as above we denote by $|\phi\rangle$ ($|\phi^\perp\rangle$) the state associated to code $\mathscr{C}$ ($\mathscr{C}^\perp$). The above equation is the generalized form of Eq. (4.8). The difference between $|\phi\rangle$ and $|\phi^\perp\rangle$ is in the generator matrix, or alternatively the A matrix. For the state $|\phi^\perp\rangle$ we have $\vec{v}_i \in [q]^{n_{\rm cl}-\ell}$.

The pure states $|\phi\rangle$ or $|\phi^\perp\rangle$ are k-UNI states iff the reduced density matrix σ_S of any subset of k parties, $S \subseteq \{1,\ldots,n\}$ with $|S| = k$, is maximally mixed. This subset may be (i) entirely contained in the support of the classical part $\mathrm{Cl} = \{1,\ldots,n_{\rm cl}\}$; (ii) entirely contained in the support of the quantum part $\mathrm{Q} = \{1,\ldots,n_{\rm q}\}$, (iii) split between the two parts $\mathrm{Cl} \cup \mathrm{Q} = \{1,\ldots,n\}$. We consider these three different cases separately.

Case (i): If the S qudits of the reduced density matrix σ_S are contained in the classical part, $S \subseteq \mathrm{Cl}$, the reduced density matrix resulting from tracing out all the quantum part and the complement of S in Cl, $S^c_{\rm Cl} = S^c \cap \mathrm{Cl}$, of the state $|\phi\rangle$, Eq. (4.9), is

$$\begin{aligned} \sigma_S &= \mathrm{Tr}_{S^c_{\rm Cl}}\, \mathrm{Tr}_{\rm Q}\, |\phi\rangle\langle\phi| \\ &= \sum_{i,i'} (\mathrm{Tr}_{S^c_{\rm Cl}}\, |\vec{v}_i,\, \vec{v}_i A\rangle\langle \vec{v}_{i'},\, \vec{v}_{i'}\, A|)\, \langle\psi_i|\psi_{i'}\rangle \\ &= \sum_i \mathrm{Tr}_{S^c_{\rm Cl}}\, |\vec{v}_i,\, \vec{v}_i A\rangle\langle \vec{v}_i,\, \vec{v}_i A| \ , \end{aligned} \tag{4.10}$$

which is a direct consequence of having a complete basis in the quantum part, i.e., $\langle\psi_i|\psi_{i'}\rangle = \delta_{i,i'}$. In case of considering the state $|\phi^\perp\rangle$, the same procedure holds when

we calculate the reduced density matrix σ_S with the same condition for the set $S \subseteq \mathrm{Cl}$. We should just replace $\vec{v}_i \in [q]^\ell$ with $\vec{v}_i \in [q]^{n_{\mathrm{cl}}-\ell}$. As argued for state (4.1), σ_S is proportional to the identity matrix whenever its size is equal to the number of free indices in the code used in the classical part, equal to ℓ for the state $|\phi\rangle$ and $n_{\mathrm{cl}} - \ell$ for $|\phi^\perp\rangle$.

Case (ii): If the qudits are all contained the quantum part, $S \subseteq \mathrm{Q}$, the reduced density matrix σ_S resulting from tracing out all of the qudits of the classical part and the complement of S in Q, $S^c_{\mathrm{Q}} = S^c \cap \mathrm{Q}$, is

$$\begin{aligned}\sigma_S &= \mathrm{Tr}_{\mathrm{Cl}} \mathrm{Tr}_{S^c_{\mathrm{Q}}} |\phi\rangle\langle\phi| \\ &= \sum_{i,i'} \langle \vec{v}_i | \vec{v}_{i'} \rangle \langle \vec{v}_i A | \vec{v}_{i'} A \rangle \left(\mathrm{Tr}_{S^c_{\mathrm{Q}}} |\psi_i\rangle\langle\psi_{i'}| \right) \\ &= \mathrm{Tr}_{S^c_{\mathrm{Q}}} \sum_i |\psi_i\rangle\langle\psi_i| \,,\end{aligned} \tag{4.11}$$

where we have used that $\langle \vec{v}_i | \vec{v}_{i'} \rangle = \delta_{i,i'}$. The quantum part is a complete orthogonal basis, then the reduced density matrix in this case is maximally mixed for any subset S fully contained in the quantum part, which may be of size at most $n_{\mathrm{q}} = \ell$ or $n_{\mathrm{q}} = n_{\mathrm{cl}} - \ell$ depending on the MDS code used for the classical part.

Case (iii): Finally, we consider the case where $S \cap \mathrm{Cl} = S_{\mathrm{Cl}} \neq S$ and $S \cap \mathrm{Q} = S_{\mathrm{Q}} \neq S$. We then have the general formula

$$\sigma_S = \mathrm{Tr}_{S^c} |\phi\rangle\langle\phi| = \sum_{i,i'} \mathrm{Tr}_{S^c_{\mathrm{Cl}}} (|\vec{v}_i,\, \vec{v}_i A\rangle\langle \vec{v}_{i'},\, \vec{v}_{i'} A|) \otimes \mathrm{Tr}_{S^c_{\mathrm{Q}}} (|\psi_i\rangle\langle\psi_{i'}|). \tag{4.12}$$

We start by the state $|\phi\rangle$ in which the MDS code used for the classical part has $\ell \leq n_{\mathrm{Cl}}/2$ and consider the case in which $|S| = \ell' + 1$. We first show that

$$\mathrm{Tr}_{S^c_{\mathrm{Cl}}} (|\vec{v}_i, \vec{v}_i A\rangle\langle \vec{v}_{i'}, \vec{v}_{i'} A|) \propto \delta_{i,i'}, \tag{4.13}$$

for all S with $|S_{\mathrm{Cl}}| \leq \ell'$. As the terms $|\vec{v}_i, \vec{v}_i A\rangle$ that make up the classical part of the state $|\phi\rangle$ are coming from an MDS code, they are all product states in, say, the computational basis. Fix any S, with $|S_{\mathrm{Cl}}| \leq \ell'$, and let $\{|s\rangle\}$ be the computational basis for S_{Cl} and $\{|t\rangle\}$ be that of S^c_{Cl}. We can then write

$$\mathrm{Tr}_{S^c_{\mathrm{Cl}}} (|\vec{v}_i, \vec{v}_i A\rangle\langle \vec{v}_{i'}, \vec{v}_{i'} A|) = \sum_{s,s',t} |s\rangle\langle s'| \langle s, t | \vec{v}_i, \vec{v}_i A\rangle \langle \vec{v}_{i'}, \vec{v}_{i'} A | s', t\rangle \tag{4.14}$$

For $\vec{v}_i \neq \vec{v}_{i'}$, the two inner products in the right hand side of the last equation can be simultaneously non-zero only if $|\vec{v}_i, \vec{v}_i A\rangle$ and $|\vec{v}_{i'}, \vec{v}_{i'} A\rangle$ are identical in at least $|S^c_{\mathrm{Cl}}|$ many locations, because otherwise they cannot both be non-orthogonal to $|t\rangle$. But this

means that their Hamming distance could not be larger than $d_H \leq n_{\text{cl}} - |S^{\text{c}}_{\text{Cl}}| = |S_{\text{Cl}}| \leq \ell' \leq n_q/2 = \ell/2$. But, at the same time, we know that the Hamming distance between any two $|\vec{v}_i, \vec{v}_i A\rangle$ and $|\vec{v}_{i'}, \vec{v}_{i'} A\rangle$ for $\vec{v}_i \neq \vec{v}_{i'}$ is at least $d_H = n_{\text{cl}} - \ell + 1 \geq \ell + 1$, where the inequality follows from $n_{\text{cl}} \geq 2\ell$. These were only compatible if $\ell + 1 \leq \ell/2$, which is never fulfilled. We now use (4.13) into (4.12) to get

$$\sigma_S = \sum_i \text{Tr}_{S^{\text{c}}_{\text{Cl}}}(|\vec{v}_i,\, \vec{v}_i A\rangle\langle \vec{v}_i,\, \vec{v}_i A|) \otimes \text{Tr}_{S^{\text{c}}_{\text{Q}}}(|\psi_i\rangle\langle\psi_i|). \tag{4.15}$$

Any set S of size $\ell' + 1$ with non-zero intersection with the classical and quantum part is such that $|S_{\text{Q}}| \leq \ell'$. Therefore, as all the states in the quantum part $|\psi_i\rangle$ are ℓ'-UNI states, one has $\text{Tr}_{S^{\text{c}}_{\text{Q}}}(|\psi_i\rangle\langle\psi_i|) \propto \mathbb{1}, \forall i$. We are therefore left with

$$\sigma_S \propto \sum_i \text{Tr}_{S^{\text{c}}_{\text{Cl}}}(|\vec{v}_i,\, \vec{v}_i A\rangle\langle \vec{v}_i,\, \vec{v}_i A|) \otimes \mathbb{1}, \tag{4.16}$$

which is maximally mixed because $|S_{\text{Cl}}| \leq \ell' < \ell$.

Let us finally consider the state $|\phi^{\perp}\rangle$ in which the classical part is constructed from the dual code $\mathscr{C}^{\perp}$ and the condition $n_{\text{cl}} - \ell = n_{\text{q}}$ is necessary. We can now repeat the same analysis as above. To conclude that the terms in the classical part are proportional to $\delta_{i,i'}$ we need that $d_H^{\perp} = \ell + 1 > |S_{\text{Cl}}|$, while for the traces in the quantum part to be maximally mixed it is required that $|S_{\text{Q}}| \leq \ell'$. These two conditions can be fulfilled if $|S| = \min\{\ell + 1, \ell' + 1\}$.

Now, considering all the three cases, we see that Case (iii) is the most restrictive and implies that our construction leads in general to $\min\{\ell + 1, \ell' + 1\}$-UNI states, this minimum being equal to $(\ell' + 1)$-UNI for the state $|\phi\rangle$. □

Note that the the previous proof also implies that some reduced states σ_S in our construction are maximally mixed even for sizes $|S| > \ell'$.

It just remains to present instances in which the construction applies. Recall that the Cl+Q method, requires an $[n_{\text{cl}}, \ell]_q$ MDS code and a complete ℓ'-UNI(n_{q}, q) orthonormal basis, with $n_{\text{q}} = \ell$ or $n_{\text{q}} = n - \ell$ depending on the MDS code. For the quantum basis, we can employ the direct correspondence between minimal support states and classical MDS codes. Then, in order to find instances of the Cl+Q method, one can simply check the known conditions for the existence of MDS codes. To show this we use that according to Eq. (4.3), we should find $\max\{n_{\text{cl}}, n_{\text{q}}\}$ for given local dimension q. Considering this, one simply can verify that $\max\{n_{\text{cl}}, n_{\text{q}}\} = n_{\text{cl}}$. Thus the existence of MDS code with n_{cl} parties and local dimension q is enough to guarantee that such a non-minimal support k-UNI state can be constructed by our method. In Table 4.1 we provide examples of k-UNI states for systems of smaller dimension than those obtained using the existing MDS codes.

uniformity	n	Cl part	Basis for Q part	Cl+Q method	MDS code
$k=2$	$n=5$	$[3,2,2]_q$	Bell basis	$q \geq 2$	$q \geq 4$
	$n=6$	$[4,2,3]_q$	Bell basis	$q \geq 3$	$q \geq 4$
	$n=7$	$[5,2,4]_q$	Bell basis	$q \geq 4$	$q \geq 7$
	$n=8$	$[5,3,3]_q$	GHZ basis	$q \geq 4$	$q \geq 7$
	$n=9$	$[6,3,4]_q$	GHZ basis	$q \geq 4$	$q \geq 8$
	$n=10$	$[7,3,5]_q$	GHZ basis	$q \geq 7$	$q \geq 9$
$k=3$	$n=11$	$[7,4,4]_q$	$AME(4,q)$ basis	$q \geq 7$	$q \geq 11$
	$n=12$	$[8,4,5]_q$	$AME(4,q)$ basis	$q \geq 7$	$q \geq 11$
	$n=13$	$[9,4,6]_q$	$AME(4,q)$ basis	$q \geq 8$	$q \geq 13$
	$n=14$	$[9,5,5]_q$	$AME(5,q)$ basis	$q \geq 8$	$q \geq 13$
	$n=15$	$[10,5,6]_q$	$AME(5,q)$ basis	$q \geq 9$	$q \geq 16$
	$n=16$	$[11,5,7]_q$	$AME(5,q)$ basis	$q \geq 11$	$q \geq 16$

Table 4.1.: Comparison between local dimension q of the two methods.

As a concrete example, we can consider the state $\mathrm{AME}(5,q)$ with the following closed form expression [GRDMZ18]

$$|\phi^{\perp}\rangle = \sum_{l,m=0}^{q-1} |l, m, l+m\rangle |\psi_{(l,m)}\rangle \ , \tag{4.17}$$

where the states $\psi_{(l,m)}$ define a Bell basis

$$|\psi_{(l,m)}\rangle = X^l \otimes Z^m \sum_r |r, r\rangle \ . \tag{4.18}$$

For the qubit case we have

$$\begin{aligned} |\phi^{\perp}\rangle = &|000\rangle|\phi^+\rangle + |011\rangle|\psi^+\rangle \\ &+ |101\rangle|\phi^-\rangle + |110\rangle|\psi-\rangle \ , \end{aligned} \tag{4.19}$$

where $|\phi^{\pm}\rangle$ and $|\psi^{\pm}\rangle$ are the Bell basis of the Hilbert space of 2 qubits. One can easily check that all the reduced density matrices σ_S up to 2 parties are maximally mixed.

4.5. Inequivalence under stochastic LOCC (SLOCC)

After presenting our construction, we now show that it provides states that could not be obtained using the previously known method based on MDS codes. In order to do so, we show that states obtained using our construction cannot be obtained by SLOCC from k-$\mathrm{UNI}_{\mathrm{min}}$, that is, they belong to different SLOCC classes.

It is a well-known result that the number of product states needed to specify a pure state is an upper bound to the rank of all possible reduced states. For a k-$\mathrm{UNI}_{\mathrm{min}}$ state, this implies that,

for any subset $S \subset \{1, \ldots, n\}$, one has

$$\mathrm{rank}(\rho_S) \leq q^k \,, \tag{4.20}$$

where $\rho_S = \mathrm{Tr}_{S^c} |\psi\rangle\langle\psi|$. It is also well known that this number cannot be increased by SLOCC [EB01].

Now consider k-UNI state $|\phi\rangle$ in $\mathcal{H}(n, q)$ constructed from Cl+Q method. All the reductions up to k parties of the state $|\phi\rangle$ are maximally mixed. However, it is possible to show that there exists at least one subset of size $|S| = k + 1$ parties such that the reduced density matrix $\sigma_S = \mathrm{Tr}_{S^c} |\phi\rangle\langle\phi| \propto \mathbb{1}$. This specific set contains k parties of the classical part and one party from the quantum part. This implies that the state $|\phi\rangle$ is not minimal support and hence the two states $|\psi\rangle$ and $|\phi\rangle$ cannot be mapped into the other probabilistically via LOCC. Therefore, they belong to different SLOCC classes.

4.6. Graph states

All the codewords of the code space that construct the minimal support k-UNI state are linear combinations of the rows of a generator matrix $G_{k\times n}$, or the parity check matrix $H_{n-k\times n}$ in case of considering the dual MDS code. For a k-$\mathrm{UNI}_{\mathrm{min}}$ state constructed via the generator matrix of a linear MDS code Eq. (4.2), the stabilizer generators can be constructed as follows,

$$s_l^{\psi} := \begin{cases} \bigotimes_{m=1}^{n} X^{g_{l,m}} & 1 \leq l \leq k \\ \bigotimes_{m=1}^{n} Z^{h_{l-k,m}} & k < l \leq n \end{cases} . \tag{4.21}$$

We use $g_{l,m}$ to denote the matrix elements of the generator matrix $G_{k\times n}$ and that of the code's parity check matrix $H_{n-k\times n}$ by $h_{l,m}$. In particular, the above equation contains n simultaneous linear equation that can be listed as follows

$$\begin{array}{cc} & \overbrace{\qquad\qquad\qquad\qquad}^{k} \qquad\qquad\qquad\qquad \overbrace{\qquad\qquad\qquad\qquad}^{n-k} \\ \begin{array}{c} s_1 \\ s_2 \\ \vdots \\ s_k \end{array} & \begin{array}{cccccccccc} = & X & \mathbb{1} & \ldots & \mathbb{1} & X^{a_{11}} & X^{a_{12}} & \ldots & X^{a_{1(n-k)}} \\ = & \mathbb{1} & X & \ldots & \mathbb{1} & X^{a_{21}} & X^{a_{22}} & \ldots & X^{a_{2(n-k)}} \\ & & & & & & & & \\ = & \mathbb{1} & \mathbb{1} & \ldots & X & X^{a_{k1}} & X^{a_{k2}} & \ldots & X^{a_{k(n-k)}} \end{array} \\ \begin{array}{c} s_{k+1} \\ s_{k+2} \\ \vdots \\ s_n \end{array} & \begin{array}{cccccccccc} = & Z^{-a_{11}} & Z^{-a_{21}} & \ldots & Z^{-a_{k1}} & Z & \mathbb{1} & \ldots & \mathbb{1} \\ = & Z^{-a_{12}} & Z^{-a_{22}} & \ldots & Z^{-a_{k2}} & \mathbb{1} & Z & \ldots & \mathbb{1} \\ & & & & & & & & \\ = & Z^{-a_{1(n-k)}} & Z^{-a_{2(n-k)}} & \ldots & Z^{-a_{k(n-k)}} & \mathbb{1} & \mathbb{1} & \ldots & Z \,, \end{array} \end{array} \tag{4.22}$$

where we denote the matrix elements of A by $a_{l,m}$. For the sake of simplicity we did not write the tensor product between each element.

The state $|\psi\rangle$, Eq. (4.2), is the plus one eigenstate of the set of Pauli strings constructed by the stabilizer generators. To show this, we use that in the decomposition of $|\psi\rangle$ the first k stabilizers which involve X operators, permute the computational basis and hence leave it invariant. And if we perform the second part of the $n-k$ stabilizers, involving Z operators, on the state $|\psi\rangle$

$$s_l^{\psi}\,|\psi\rangle = \sum_{\vec{v}\in[q]^k} \omega^{H_{n-k\times n}\,(G_{k\times n})^T\,\vec{v}}\,|\vec{v}\,G_{k\times n}\rangle = |\psi\rangle\;, \tag{4.23}$$

where $k < l \leq n$, and we used the condition $H_{n-k\times n}\,(G_{k\times n})^T = 0$. The same construction holds if we consider the dual code $\mathscr{C}^{\perp}$ to construct the minimal support state $|\psi^{\perp}\rangle$. Taking the parity check matrix $H_{n-k\times n}$ as the generator matrix and $G_{k\times n}$ as the parity check matrix we can construct $|\psi^{\perp}\rangle$. In this case, it is obvious that the Pauli strings that generate the stabilizer group can be constructed from Eq. (4.21) if the local unitary transformation acts on all of the qudits and transform the computational basis to the X-basis. This implies that the k-uniform state constructed from the MDS code $\mathscr{C}$ is local unitary equivalent to the k-UNI state constructed from the dual code $\mathscr{C}^{\perp}$, i.e., the state $|\psi^{\perp}\rangle$.

If one performs local Fourier transforms $F_i = \sum_{i,j}\omega^{ij}|i\rangle\langle j|$ on all the last $n-k$ parties of the state $|\psi\rangle$ in (4.1), the stabiliser formalism Eq. (4.22) can be written as

$$s_l^{\psi} = \begin{cases} X_l \bigotimes_{m=1}^{n-k} Z^{-a_{l,m}} & 1 \leq l \leq k \\ X_l \bigotimes_{m=1}^{k} Z^{-a_{m,l-k}} & k < l \leq n \end{cases}. \tag{4.24}$$

This directly leads us to get the stabiliser formalism of graph states

$$s_l^{\psi} = X_l \prod_{m=0}^{n} (Z_m)^{\Gamma^{\psi}_{l,m}} \qquad 1 \leq l \leq n\;, \tag{4.25}$$

where for k-$\mathrm{UNI}_{\mathrm{min}}$ states the adjacency matrix is

$$\Gamma^{\psi} = -\left[\begin{array}{c|c} 0 & A \\ \hline A^T & 0 \end{array}\right]_{n\times n}. \tag{4.26}$$

For the k-$\mathrm{UNI}_{\mathrm{min}}$ constructed from the dual MDS code $\mathscr{C}^{\perp}$, one has to replace $-a$ for each term and also take the transposition as well, i.e., make the replacement $a_{l,m} \mapsto -a_{m,l}$.

Therefore k-$\mathrm{UNI}_{\mathrm{min}}$ states derived from MDS codes $[n, k, n-k]_q$ are examples of graph states as it is possible to connect the adjacency matrix Γ and the code parameters [Hel13, RGRA18].

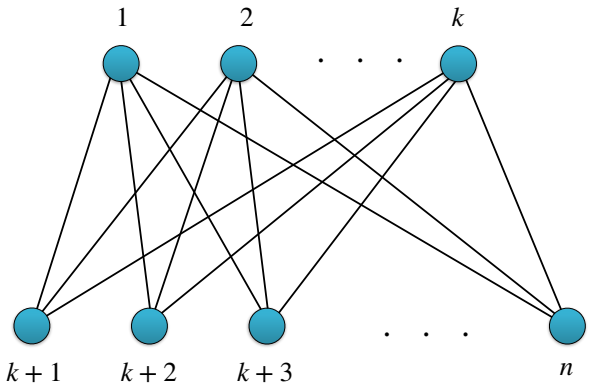


Figure 4.2.: *A complete bipartite graph.* Graph state which is local unitary equivalent to the k-$\mathrm{UNI}_{\min}$ states constructed from MDS codes.

After performing the local Fourier transforms the resulting state is a graph state corresponding to a *complete bipartite graph*, see Figure 4.2. This graph is partitioned into two subsets, one containing k vertices and the other one $n-k$ vertices. The weights of the edges connecting the vertices in the two subsets depend on the details of the construction of the MDS code but the structure is the same for all the states $|\psi\rangle$ (4.1). Note that, when q is a power of a prime, discrete Heisenberg-Weyl groups should be considered for the stabiliser formalism [Fad95, AR95].

The states $|\phi\rangle$ constructed from the Cl+Q method are formed by concatenating the two parts,

$$|\psi\rangle = \sum_{i=1,\ldots,q^\ell} |\vec{c}_i\rangle \tag{4.27}$$

$$|\psi_i\rangle = M(\vec{v}_i)\,|\psi\rangle\ . \tag{4.28}$$

For the operator $M(\vec{v})$ after performing local Fourier transforms on the last $n_{\mathrm{q}} - \ell'$ parties we get

$$M_F(\vec{v}) = F^{-1} M(\vec{v}) F = \underbrace{Z^{v_1} \otimes \cdots \otimes Z^{v_{\ell'}}}_{\ell'} \otimes \underbrace{Z^{-v_{\ell'+1}} \otimes \cdots \otimes Z^{-v_{n_{\mathrm{q}}=\ell}}}_{n_{\mathrm{q}}-\ell'}\ , \tag{4.29}$$

which contains only Z matrices, that in the graph state representation represent edges that connect vertices, as shown in Figure 4.3.

Further, we should note that the dual code $\mathscr{C}^\perp = [n_{\mathrm{cl}}, n_{\mathrm{cl}} - \ell, \ell + 1]_q$, can be used to construct the classical part of the state $|\phi^\perp\rangle$. In this case the condition $n_{\mathrm{cl}} - \ell = n_{\mathrm{q}}$ is necessary. The graphical representation is shown in Figure (4.4).

The graph state representation of the states $|\phi\rangle$ constructed from the Cl+Q method, Eq. (4.8), when the states in the basis are k-$\mathrm{UNI}_{\min}$ derived from an MDS code, is rather intuitive and

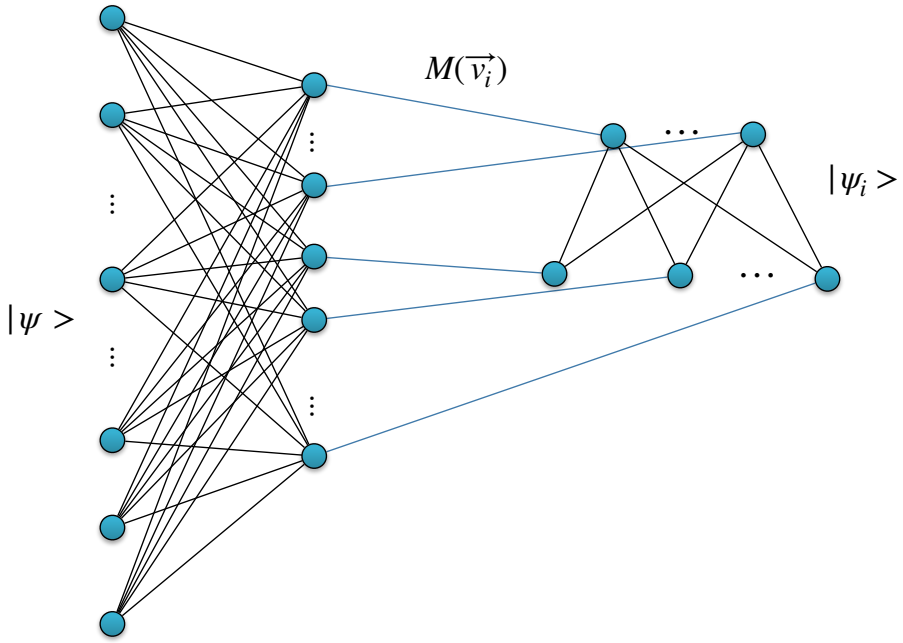


Figure 4.3.: *Graph state representing the k-UNI states constructed from the Cl+Q method.* The graph can be considered as two parts connected as the method. The left-hand side is the graph state representing the state constructed from $|\psi\rangle = \sum_i |\vec{c_i}\rangle$, i.e., the Cl part. The right-hand side is the graph state representing the Q part, states $|\psi_i\rangle$. The operators $M(\vec{v}_i)$ describe how the two parts connect.

shows the structure of the method: it is formed by concatenating the two complete bipartite graphs associated to each MDS code or, equivalently, the corresponding k-$\mathrm{UNI}_{\mathrm{min}}$ state.

4.7. Constructions of previously unknown AME states

We now show how using our method one can construct AME states whose existence was unknown so far. For that we need to introduce a generalization of the method, which we call *Cl+Q with repetition*, where states in the quantum part are repeated, that is, several codewords of the classical part concatenate to the same quantum state of the quantum part. For this to be possible, one should employ MDS codes with the property that the codewords can be distributed into subsets each forming MDS codes with smaller parameters. In particular, we need MDS codes $\mathscr{C} = [n_{\mathrm{cl}}, \left\lceil \frac{n_{\mathrm{cl}}}{2} \right\rceil, \left\lfloor \frac{n_{\mathrm{cl}}}{2} \right\rfloor + 1]_q$ such that its codewords can be partitioned into q^2 subsets each forming an MDS code, with parameters $\mathscr{C}_i = [n_{\mathrm{cl}}, \left\lceil \frac{n_{\mathrm{cl}}}{2} \right\rceil - 2, \left\lfloor \frac{n_{\mathrm{cl}}}{2} \right\rfloor + 3]_q$. Comparing the code parameters of the MDS code $\mathscr{C}$ with each subclass $\mathscr{C}_i$, we see that they require the same number of physical qudits but the number of logical qudits decreases by 2 (while obviously the Hamming distance increases by the same amount). The idea is now to associate all the elements of each subclass to the same state in a Bell basis, see Figure4.1(b).

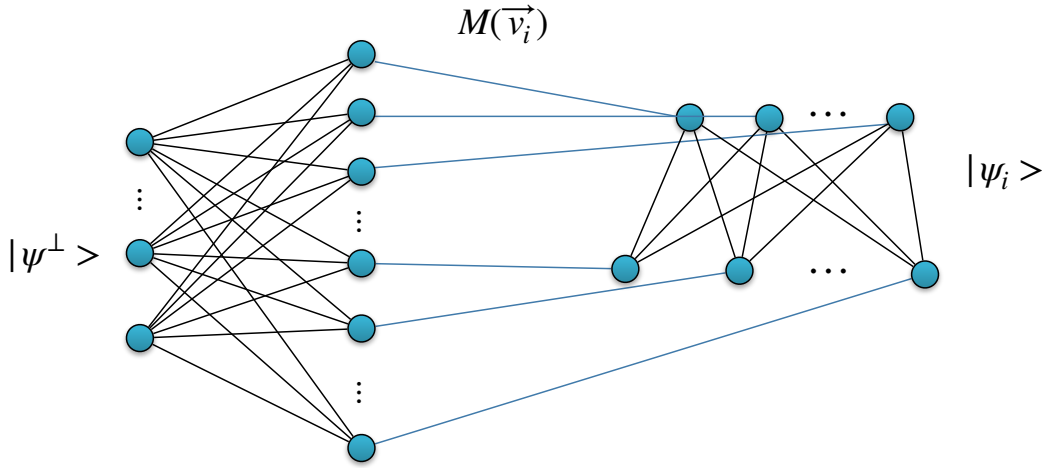


Figure 4.4.: *Graph state representing the k-UNI states constructed from the Cl+Q method.* The graph represent k-UNI state of non-minimal support that is constructed using the dual code $\mathscr{C}^{\perp} = [n_{\text{cl}}, n_{\text{cl}} - \ell, \ell + 1]_q$ as the classical part. The necessary condition is $n_{\text{cl}} - \ell = n_{\text{q}}$.

Lemma 4.3 (Cl+Q with repetition)**.** *Consider an $\mathscr{C} = [n_{\text{cl}}, \left\lceil \frac{n_{\text{cl}}}{2} \right\rceil, \left\lfloor \frac{n_{\text{cl}}}{2} \right\rfloor + 1]_q$ MDS code such that its codewords can be partitioned into q^2 subsets each forming MDS code with parameters $\mathscr{C}_i = [n_{\text{cl}}, \left\lceil \frac{n_{\text{cl}}}{2} \right\rceil - 2, \left\lfloor \frac{n_{\text{cl}}}{2} \right\rfloor + 3]_q$. An $AME(n, q)$ state $|\phi\rangle$ for n odd, with $n = n_{\text{cl}} + 2$, can be constructed by concatenating all the terms of each subclass with one of the Bell states of the quantum part, see also Figure 4.1(b).*

In general, this configuration leads to AME states for n odd when $n \leq q + 3$. To show that the state $|\phi\rangle$ is an AME state we need to check all the reduced states $\sigma_S = \text{Tr}_{S^c} |\phi\rangle\langle\phi|$ on up to half of the systems. For the purpose of the proof, we proceed as above and check three different cases, depending on how the k parties are distributed between the classical and quantum part. We then use two properties of the construction:, (i) the fact that subsets $\mathscr{C}_i$ of the MDS code are also MDS codes and (ii) the large Hamming distance between codewords of two different subsets $\mathscr{C}_i$ and $\mathscr{C}_j$.

Proof. In the proof of the theorem, we assume the existence of MDS codes $\mathscr{C} = [n_{\text{cl}}, \left\lceil \frac{n_{\text{cl}}}{2} \right\rceil, \left\lfloor \frac{n_{\text{cl}}}{2} \right\rfloor + 1]_q$ that can be divided into q^2 MDS codes with smaller parameters $\mathscr{C}_i = [n_{\text{cl}}, \left\lceil \frac{n_{\text{cl}}}{2} \right\rceil - 2, \left\lfloor \frac{n_{\text{cl}}}{2} \right\rfloor + 3]_q$, where $i = 1, \ldots, q^2$. For each code $\mathscr{C}_i$, codewords are presented by $\vec{c}_{i,j}$ with $j = 1, \ldots, q^{\left\lceil \frac{n_{\text{cl}}}{2} \right\rceil - 2}$. The state

$$|\phi\rangle = \sum_i \sum_j \underbrace{|\vec{c}_{i,j}\rangle}_{n_{\text{cl}}} \underbrace{|\psi_i\rangle}_{n_{\text{q}}} \tag{4.30}$$

is a modification of Eq. (4.9), and it is an AME state if all the reduced density matrices $\sigma_S = \mathrm{Tr}_{S^c} |\phi\rangle\langle\phi|$ are proportional to identity for $|S| \leq \left\lfloor \frac{n}{2} \right\rfloor = \left\lceil \frac{n_{\mathrm{cl}}}{2} \right\rceil$. As in lemma 4.2, we check three different cases depending on how the subset S distributes between the classical and quantum part: it may be entirely contained in the support of the classical part $\mathrm{Cl} = \{1, \ldots, n_{\mathrm{cl}}\}$, or it can be split between the classical and quantum parts, S_{Q} and S_{Cl}. For the last case we have two possibilities, depending on whether the support in the the quantum part is partial, $|S_{\mathrm{Q}}| = 1$, and then $|S_{\mathrm{Cl}}| = \left\lfloor \frac{n}{2} \right\rfloor - 1$, or or complete, having $|S_{\mathrm{Q}}| = 2$ and $|S_{\mathrm{Cl}}| = \left\lfloor \frac{n}{2} \right\rfloor - 2$.

Case (i): If the set S is contained entirely in the support of the classical part, the reduced density matrix can be written as

$$\sigma_S = \mathrm{Tr}_{S^c_{\mathrm{Cl}}} \mathrm{Tr}_{\mathrm{Q}} |\phi\rangle\langle\phi| = \sum_i \sum_{j,j'} \mathrm{Tr}_{S^c_{\mathrm{Cl}}} |\vec{c}_{i,j}\rangle\langle\vec{c}_{i,j'}| \,, \tag{4.31}$$

where we used the orthogonality of the states $|\psi_i\rangle$. Since the codewords with the same value of i have Hamming distance $d_H \geq \left\lceil \frac{n_{\mathrm{cl}}}{2} \right\rceil + 2$, which is larger than the size of the subset S, the partial trace is non-zero only when $j = j'$, having

$$\sigma_S = \sum_{i,j} (\mathrm{Tr}_{S^c_{\mathrm{Cl}}} |\vec{c}_{i,j}\rangle\langle\vec{c}_{i,j}|) \propto \mathbb{1}_{\lfloor n/2 \rfloor} \,. \tag{4.32}$$

where we used the fact that the number of free indices of the classical part is equal to $\left\lceil \frac{n_{\mathrm{cl}}}{2} \right\rceil = \left\lfloor \frac{n}{2} \right\rfloor$.

Case (ii): The subset S splits in two parts such that $|S_{\mathrm{Q}}| = 1$ and $|S_{\mathrm{Cl}}| = \left\lceil \frac{n_{\mathrm{cl}}}{2} \right\rceil - 1 = \left\lfloor \frac{n_{\mathrm{cl}}}{2} \right\rfloor$. Then the reduced density matrix σ_S simplifies to

$$\sigma_S = \mathrm{Tr}_{S^c} |\phi\rangle\langle\phi| = \sum_{i,i'} \sum_{j,j'} \mathrm{Tr}_{S^c_{\mathrm{Cl}}} (|\vec{c}_{i,j}\rangle\langle\vec{c}_{i',j'}|) \otimes \mathrm{Tr}_{S^c_{\mathrm{Q}}} (|\psi_i\rangle\langle\psi_{i'}|). \tag{4.33}$$

For the classical part, since $|S_{\mathrm{Cl}}| = \left\lfloor \frac{n_{\mathrm{cl}}}{2} \right\rfloor$ is smaller than the Hamming distance of the code $\mathscr{C}$, $d_H = \left\lfloor \frac{n_{\mathrm{cl}}}{2} \right\rfloor + 1$, only the diagonal terms give a non-zero contribution, getting

$$\sigma_S = \sum_{i,j} \mathrm{Tr}_{S^c_{\mathrm{Cl}}} (|\vec{c}_{i,j}\rangle\langle\vec{c}_{i,j}|) \otimes \mathrm{Tr}_{S^c_{\mathrm{Q}}} (|\psi_i\rangle\langle\psi_i|). \tag{4.34}$$

The trace over the quantum part gives the identity, as $|\psi_i\rangle$ are all Bell states, getting

$$\sigma_S \propto \sum_{i,j} \mathrm{Tr}_{S^c_{\mathrm{Cl}}} (|\vec{c}_{i,j}\rangle\langle\vec{c}_{i,j}|) \otimes \mathbb{1}_q \tag{4.35}$$

The remaining sum in the classical part is the same as the reduced state obtained from the superposition of the all codewords of the MDS code $\mathscr{C}$, i.e., $\sum_{i,j} |\vec{c}_{i,j}\rangle$, which is an

AME states of n_{cl} parties and all its reduced density matrices up to $\left\lfloor \frac{n_{\text{cl}}}{2} \right\rfloor$ are maximally mixed. Putting all this together, we conclude that the reduced density matrix σ_S is also maximally mixed.

Case (iii): We consider a subset S that $|S_{\text{Q}}| = |\text{Q}| = 2$ and $|S_{\text{Cl}}| = \left\lceil \frac{n_{\text{cl}}}{2} \right\rceil - 2 = \left\lfloor \frac{n_{\text{cl}}}{2} \right\rfloor - 1$. We then have the following formula

$$\sigma_S = \text{Tr}_{S^c} |\phi\rangle\langle\phi| = \sum_{i,i'} \sum_{j,j'} \text{Tr}_{S^c_{\text{Cl}}}(|\vec{c}_{i,j}\rangle\langle\vec{c}_{i'j'}|) \otimes (|\psi_i\rangle\langle\psi_{i'}|). \tag{4.36}$$

As for case (ii), the Hamming distance between the terms of the classical part, $d_H = \left\lfloor \frac{n_{\text{cl}}}{2} \right\rfloor + 1$, is larger than the size of the subset $|S_{\text{Cl}}| = \left\lfloor \frac{n_{\text{cl}}}{2} \right\rfloor - 1$, therefore $\text{Tr}_{S^c_{\text{Cl}}}(|\vec{c}_{i,j}\rangle\langle\vec{c}_{i'j'}|) = 0$ whenever $i \neq i'$ and $j \neq j'$ and Eq. (4.36) simplifies to

$$\sigma_S = \sum_{i} \sum_{j} \text{Tr}_{S^c_{\text{Cl}}}(|\vec{c}_{i,j}\rangle\langle\vec{c}_{i,j}|) \otimes (|\psi_i\rangle\langle\psi_i|). \tag{4.37}$$

As explained, all the codewords with the same value of i define MDS codes with parameters $[n_{\text{cl}}, \left\lceil \frac{n_{\text{cl}}}{2} \right\rceil - 2, d_H = \left\lceil \frac{n_{\text{cl}}}{2} \right\rceil + 2]_q$. They all give raise to $\left(\left\lfloor \frac{n_{\text{cl}}}{2} \right\rfloor - 1 \right)$-UNI states, that is, all the reduced density matrices up to $\left\lfloor \frac{n_{\text{cl}}}{2} \right\rfloor - 1$ are proportional to the identity. But the sum over index j in (4.37) is precisely equal to one of these reduced states for the set of parties S_{Cl}, that is

$$\sum_{j} \text{Tr}_{S^c_{\text{Cl}}}(|\vec{c}_{i,j}\rangle\langle\vec{c}_{i,j}|) \propto \mathbb{1}_{\lfloor \frac{n_{\text{cl}}}{2} \rfloor - 1} \,. \tag{4.38}$$

Then, we get

$$\sigma_S = \sum_{i=1}^{q^2} \mathbb{1}_{\lfloor \frac{n_{\text{cl}}}{2} \rfloor - 1} \otimes (|\psi_i\rangle\langle\psi_i|) \,. \tag{4.39}$$

The quantum part is a complete orthonormal basis, therefore $\sum_i |\psi_i\rangle\langle\psi_i| \propto \mathbb{1}_2$. Then, the reduced density matrix in this case $\sigma_S \propto \mathbb{1}_{\lfloor \frac{n_{\text{cl}}}{2} \rfloor + 1} = \mathbb{1}_{\lfloor \frac{n}{2} \rfloor}$.

□

What remains to be shown is that the construction can find an application, that is, that there exist MDS codes that can be partitioned into q^2 subsets forming MDS codes. We proved this for MDS codes with parameters $\mathscr{C} = [n_{\text{cl}}, \lceil n_{\text{cl}}/2 \rceil, \lfloor n_{\text{cl}}/2 \rfloor + 1]_q$ where $n_{\text{cl}} \leq q$, whose codewords can be partitioned into q^2 MDS codes $\mathscr{C}_i = [n_{\text{cl}}, \lceil n_{\text{cl}}/2 \rceil - 2, \lfloor n_{\text{cl}}/2 \rfloor + 3]_q$. This result then allows us to construct $\text{AME}(n \leq q + 2, q)$ states, while q is an odd prime power.

Lemma 4.4 (Subcode of MDS codes)**.** *For $n_{\text{cl}} \leq q$ it is possible to find MDS codes $\mathscr{C} = [n_{\text{cl}}, \lceil n_{\text{cl}}/2 \rceil, \lfloor n_{\text{cl}}/2 \rfloor + 1]_q$ whose codewords can be partitioned into q^2 subsets each forming MDS codes $\mathscr{C}_i = [n_{\text{cl}}, \lceil n_{\text{cl}}/2 \rceil - 2, \lfloor n_{\text{cl}}/2 \rfloor + 3]_q$.*

Proof. We restrict our analysis to the biggest size $\mathscr{C} = [q, \lceil q/2 \rceil, \lfloor q/2 \rfloor + 1]_q$, as the other codes can be constructed in the same way. As we discussed in Preliminaries 2, in general, to find an MDS code $[n, k, n-k]_q$ we need to provide a suitable generator matrix $G_{k\times n} = [\mathbb{1}_k|A]$. To do that, we first recall the Singleton arrays (3.9)

$$S_q \coloneqq \begin{array}{ccccccc} 1 & 1 & 1 & \dots & 1 & 1 & 1 \\ 1 & a_1 & a_2 & \dots & a_{q-3} & a_{q-2} & \\ 1 & a_2 & a_3 & \dots & a_{q-2} & & \\ \vdots & \vdots & \vdots & & & & \\ 1 & a_{q-3} & a_{q-2} & & & & \\ 1 & a_{q-2} & & & & & \\ 1 & & & & & & \end{array}, \tag{4.40}$$

with

$$a_i \coloneqq \frac{1}{1-\gamma^i}. \tag{4.41}$$

It is also known that by taking a rectangular sub-matrix A of size $k \times (n-k)$ of S_q one can construct a suitable generator of an MDS code [MS77, Chapter 11] [RGRA18].

Theorem 4.5. *Let $G_{k\times n} = [\mathbb{1}_k|A_{k\times(n-k)}]$ be the generator matrix of a code $\mathscr{C}$ with parameters $[n, k, d_H]_q$. The following statements are equivalent:*

(i) $\mathscr{C}$ is MDS.

(ii) every square submatrix of A is nonsingular.

(iii) any k column vectors of $G_{k\times n} = [\mathbb{1}|A]$ are linearly independent.

(iv) any $n-k$ column vectors of $H_{(n-k)\times n} = [-A^T|\mathbb{1}]$ are linearly independent.

For q being an odd prime power dimension, the biggest submatrix A has size $\lceil q/2 \rceil \times \lceil q/2 \rceil$. Using this construction, the biggest generator matrix $G_{\lceil q/2 \rceil \times (q+1)} = [\mathbb{1}_{\lceil q/2 \rceil}|A]$ has size $\lceil q/2 \rceil \times (q+1)$, and equivalently the MDS code has parameters $\mathscr{C} = [q+1, \lceil q/2 \rceil, \lfloor q/2 \rfloor]_q$.

We start from an MDS code $\mathscr{C} = [q+1, \lceil q/2 \rceil, \lfloor q/2 \rfloor]_q$ and generator matrix $G_{\lceil q/2 \rceil \times (q+1)} = [\mathbb{1}_{\lceil q/2 \rceil}|A]$, by puncturing we get (the basic definition of puncturing method is presented in Preliminaries section 2.6.8)

$$G_{\lceil q/2 \rceil \times q} = \left[\begin{array}{ccc|c} & \mathbb{1}_{\lceil q/2 \rceil - 1} & & \\ & & & A_{\lceil q/2 \rceil \times \lceil q/2 \rceil} \\ 0 & \dots & 0 & \end{array}\right], \tag{4.42}$$

where column $\lceil q/2 \rceil$ has been removed. This generator matrix is not in the standard form but it constructs an MDS code.

The second step is showing that codewords of the constructed MDS code $\mathscr{C}$ distribute into subsets forming MDS codes $\mathscr{C}_i = [q, \lceil q \rceil - 2, \lfloor q \rfloor + 3]_q$. In order to do this, we use the shortening procedure (for details of the method see Preliminaries section 2.6.8). We take an appropriate subcode by choosing the codewords which have all the same value in the deleted coordinate, for instance 0. Thanks to this, all the differences between codewords must be in the coordinates that we did not delete, and thus the Hamming distance cannot decrease, $d'_H \geq d_H$.

We first show the existence of a subset $\mathscr{C}_0$ and then we will discuss the rest of subsets. We define the matrix Q

$$Q_{\lceil q/2 \rceil \times 2} \coloneqq \begin{bmatrix} 1 & 0 \\ a_{\lceil q/2 \rceil} & 0 \\ \vdots & \vdots \\ a_{q-2} & 0 \\ 0 & 1 \end{bmatrix}, \tag{4.43}$$

that contains two columns, called Q_1 and Q_2. The $\lceil q/2 \rceil - 1$ elements of Q_1 are exactly the same as for the $\big(\lceil q/2 \rceil + 1\big)$-th column of the Singleton array S_q. The biggest rectangular submatrix of the singleton array S_q is used to construct the generator matrix $G_{\lceil q/2 \rceil \times q}$, Eq. (4.42), and the $\big(\lceil q/2 \rceil + 1\big)$-th column contains $\lceil q/2 \rceil - 1$ many elements that we used as Q_1 (we added a zero for the last element). The column Q_2 is the only column of the matrix $\mathbb{1}_{\lceil q/2 \rceil}$ that is missing in $G_{\lceil q/2 \rceil \times q}$. Now, let's consider the following matrix

$$[G|Q]_{\lceil q/2 \rceil \times (q+2)} = \left[\begin{array}{ccc|c|cc} & & & & 1 & 0 \\ & \mathbb{1}_{\lceil q/2 \rceil - 1} & & & a_{\lceil q/2 \rceil} & 0 \\ & & & A_{\lceil q/2 \rceil \times \lceil q/2 \rceil} & \vdots & \vdots \\ & & & & a_{q-2} & 0 \\ 0 & \dots & 0 & & 0 & 1 \end{array}\right]. \tag{4.44}$$

G is the generator matrix of the MDS code $\mathscr{C} = [q, \lceil q/2 \rceil, \lfloor q/2 \rfloor + 1]_q$. The matrix $[G|Q]$ does not define an MDS code, Theorem 4.5 can show that its parameters are $\mathscr{C} = [q + 2, \lceil q/2 \rceil, \lfloor q/2 \rfloor + 2]_q$. Now, we repeat the shortening process two times to get the subset $\mathscr{C}_0$. Every time we remove one of the last two columns of the $[G|Q]$ matrix because G is the generator matrix of the code $\mathscr{C}$ and we are looking for a right set of its codewords to form the code $\mathscr{C}_0$. After one step of shortening, removing the last row and the last column of the $[G|Q]$

matrix, we get

$$\tilde{G}_{(\lceil q/2\rceil-1)\times(q+1)} = \left[\begin{array}{c|cccc} & 1 & 1 & \dots & 1 \\ & 1 & a_1 & \dots & a_{\lceil q/2\rceil} \\ \mathbb{1}_{\lceil q/2\rceil-1} & \vdots & \vdots & \ddots & \vdots \\ & 1 & a_{\lceil q/2\rceil-2} & \dots & a_{q-2} \end{array}\right]. \tag{4.45}$$

Theorem 4.5 tells us that the above matrix is the generator matrix of an MDS code with parameters $[q+1, \lceil q/2\rceil - 1, \lfloor q/2\rfloor + 3]_q$. To perform the shortening process for the second time we need to find the right combination of rows of the generator matrix. To that end we define the following matrix

$$C_{(\lceil q/2\rceil-1)\times(\lceil q/2\rceil-1)} \coloneqq \left[\begin{array}{ccc|c} & & & 1 \\ & \mathbb{1}_{\lceil q/2\rceil-2} & & a_{\lceil q/2\rceil} \\ & & & \vdots \\ \hline 0 & \dots & 0 & a_{q-2} \end{array}\right] \tag{4.46}$$

We perform the C^{-1} matrix on the generator matrix $\tilde{G}$ to get the right combination of the rows of the generator matrix to do the shortening process. We get

$$C^{-1}\tilde{G} = \left[\begin{array}{ccc|c|c} & & & & 0 \\ & \mathbb{1}_{\lceil q/2\rceil-2} & & C^{-1}B & \vdots \\ & & & & 0 \\ \hline 0 & \dots & 0 & & 1 \end{array}\right], \tag{4.47}$$

where B is a submatrix of $\tilde{G}$

$$B_{(\lceil q/2\rceil-1)\times(\lceil q/2\rceil+1)} \coloneqq \begin{bmatrix} 0 & 1 & 1 & \dots & 1 \\ 0 & 1 & a_1 & \dots & a_{\lceil q/2\rceil-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 1 & a_{\lceil q/2\rceil-3} & \dots & a_{q-4} \\ 1 & 1 & a_{\lceil q/2\rceil-2} & \dots & a_{q-3} \end{bmatrix}. \tag{4.48}$$

Now, the matrix $C^{-1}\tilde{G}$ is presented in a form in which the rows are in the right combination to easily perform the shortening process. By removing the last row and the last column we

get the following matrix of size$(\lceil q/2\rceil - 2) \times q$

$$G_0 = \left[\begin{array}{c|c} \mathbb{1}_{\lceil q/2\rceil - 2} & \mathbf{D} \end{array}\right], \tag{4.49}$$

where $D_{(\lceil q/2\rceil-2)\times(\lceil q/2\rceil+1)} = C^{-1}B$ removing the bottom row, and G_0 is the generator matrix of the shortened code, $\mathscr{C}_0$. We performed a shortening that keeps or grows the Hamming distance. Since we started with a MDS code $[q+1, \lceil q/2\rceil - 1, \lfloor q/2\rfloor + 3]_q$, thus the shortened code is an MDS code $\mathscr{C}_0 = [q, \lceil q/2\rceil - 2, \lfloor q/2\rfloor + 3]_q$. It is in fact easy to check that the Singleton bound continues to saturate. Moreover, one verifies that the generator matrix G_0 is a linear combination of the rows of the generator matrix $G_{\lceil q/2\rceil\times q}$, Eq. (4.42). This implies that the codewords of MDS code $\mathscr{C}_0$ are a subset of the codewords of the original MDS code $\mathscr{C} = [q, \lceil q/2\rceil, \lfloor q/2\rfloor + 1]_q$.

It remains to show that all of the codewords of the MDS code $\mathscr{C}$ can be partitioned into subsets each forming $\mathscr{C}_i = [q, \lceil q/2\rceil - 2, \lfloor q/2\rfloor + 3]_q$. So far we were able to show that $q^{\lceil q/2\rceil-2}$ of its codewords distribute into an MDS code with parameters $\mathscr{C}_0 = [q, \lceil q/2\rceil - 2, \lfloor q/2\rfloor + 3]_q$. The fact that both MDS codes $\mathscr{C}$ and $\mathscr{C}_0$ are linear codes implies the existence of the other subsets. Each of these subsets $\mathscr{C}_i$ can be achieved by adding a different codeword $\vec{c}_i$ of code $\mathscr{C}$ that is not inside the code $\mathscr{C}_0$ to all the codewords of code $\mathscr{C}_0$. □

In the following, we present the AME states $\mathrm{AME}(7,4)$, $\mathrm{AME}(19,17)$, and $\mathrm{AME}(21,19)$. To our knowledge, the states $\mathrm{AME}(19,17)$ and $\mathrm{AME}(21,19)$ were not known. For the simplest case $q = 4$ we also provide a closed form of states $\mathrm{AME}(7,4)$. Table of known $\mathrm{AME}(n,q)$ states for different local dimension q can be found in [GR15, HW19, HESG18]

The state $\mathrm{AME}(7,4)$ can be constructed by using an MDS code with parameters $[5,3,3]_4$ and showing that all the terms can be divided into 4^2 subgroups each forming an MDS code $[5,1,5]_4$. Thus, the following closed form expression is an $\mathrm{AME}(7,4)$

$$|\phi\rangle = \sum_{i,j,l\in GF(4)} |i,j,l,i+j+l,i+xj+(1+x)l\rangle \otimes |\varphi_{\alpha\beta}\rangle\,, \tag{4.50}$$

where $\varphi_{\alpha\beta}$ represents one of the Bell states such that $\alpha = i+j$, $\beta = i+xl$ over finite field $GF(4) = \{0,1,x,1+x\}$ generated by $x^2 = x+1$. The detailed description of the subcodes $[5,1,5]_4$ connected to the Bell states $\varphi_{\alpha\beta}$ are presented in Table 4.2. Note that, in order to achieve the AME state, it is important to have different Bell states for different subclasses but the pattern of the states is not important.

For the other two states, $\mathrm{AME}(19,17)$ and $\mathrm{AME}(21,19)$ we can only provide the closed form

expressions of the AME states $|\phi\rangle$ with the G and Q matrices

$$|\phi\rangle = \sum_{\vec{v}\in GF(q)^{\lceil q/2\rceil}} |\vec{v}G\rangle\,|\psi_{\vec{v}Q}\rangle\ , \tag{4.51}$$

with

$$|\psi_{\vec{v}Q}\rangle = X^{\vec{v}Q_1}\otimes Z^{\vec{v}Q_2}\sum_{l=0}^{q-1}|l,l\rangle\ . \tag{4.52}$$

The G and Q matrices to construct $\mathrm{AME}(19,17)$ are as follows

$$G = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1\\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 8 & 2 & 15 & 7 & 4 & 6 & 5 & 9\\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 15 & 7 & 4 & 6 & 5 & 9 & 13\\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 15 & 7 & 4 & 6 & 5 & 9 & 13 & 12\\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 7 & 4 & 6 & 5 & 9 & 13 & 12 & 14\\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 4 & 6 & 5 & 9 & 13 & 12 & 14 & 11\\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 6 & 5 & 9 & 13 & 12 & 14 & 11 & 3\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 5 & 9 & 13 & 12 & 14 & 11 & 3 & 16\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 9 & 13 & 12 & 14 & 11 & 3 & 16 & 10
\end{bmatrix}, \tag{4.53}$$

and,

$$Q = \begin{bmatrix}
1 & 0\\
13 & 0\\
12 & 0\\
14 & 0\\
11 & 0\\
3 & 0\\
16 & 0\\
10 & 0\\
0 & 1
\end{bmatrix}. \tag{4.54}$$

To produce the state $\mathrm{AME}(21, 19)$ the G and Q matrices are

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 18 & 6 & 8 & 5 & 11 & 3 & 16 & 7 & 10 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 6 & 8 & 5 & 11 & 3 & 16 & 7 & 10 & 13 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 8 & 5 & 11 & 3 & 16 & 7 & 10 & 13 & 4 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 5 & 11 & 3 & 16 & 7 & 10 & 13 & 4 & 17 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 11 & 3 & 16 & 7 & 10 & 13 & 4 & 17 & 9 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 3 & 16 & 7 & 10 & 13 & 4 & 17 & 9 & 15 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 16 & 7 & 10 & 13 & 4 & 17 & 9 & 15 & 12 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 7 & 10 & 13 & 4 & 17 & 9 & 15 & 12 & 14 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 10 & 13 & 4 & 17 & 9 & 15 & 12 & 14 & 2 \end{bmatrix}, \quad (4.55)$$

and,

$$Q = \begin{bmatrix} 1 & 0 \\ 13 & 0 \\ 4 & 0 \\ 17 & 0 \\ 9 & 0 \\ 15 & 0 \\ 12 & 0 \\ 14 & 0 \\ 2 & 0 \\ 0 & 1 \end{bmatrix}. \quad (4.56)$$

Both AME states are constructed using G matrices that generate MDS codes $[q, \lceil q/2 \rceil, \lfloor q/2 \rfloor + 1]_q$, for $q = 17$ or 19 respectively, whose codewords are partitioned into subsets each forming MDS codes $[q, \lceil q/2 \rceil - 2, \lfloor q/2 \rfloor + 3]_q$. We found the right combination of the MDS codes, or alternatively the G and Q matrices, using a Python code.

Before concluding this part, we would like to mention that the Cl+Q method can be generalized in a different way where the same quantum part is concatenated several times with the classical part. With this method, if r is the number of times that each state of the quantum part concatenates to the terms of the classical part, the k-UNI state contains $n = n_{\mathrm{cl}} + r\, n_{\mathrm{q}}$ many parties.

4.8. Conclusion

We have presented a method that combines a classical error correcting code with a basis of k-UNI states to generate other k-UNI states. We have shown that our construction is different

from the other systematic construction previously known based on MDS codes: they belong to different SLOCC classes and have a different graph-state representations. Then, we have used our method to construct k-UNI states of n parties with smaller local dimensions q compared to MDS codes, and examples of AME states with its closed expression, such as $\mathrm{AME}(19, 17)$, $\mathrm{AME}(21, 19)$ and $\mathrm{AME}(7, 4)$, that were unknown so far. Due to the importance that k-UNI and AME states have, it is an interesting avenue to explore how to use the method presented here for quantum information tasks and, in particular, in the context of quantum error correction.

0	0	0	0	0		0	0	3	3	2	
1	1	3	3	1		1	1	0	0	3	
2	2	1	1	2		2	2	2	2	0	
3	3	2	2	3	φ_{00}	3	3	1	1	1	φ_{01}
0	0	1	1	3		0	0	2	2	1	
1	1	2	2	2		1	1	1	1	0	
2	2	0	0	1		2	2	3	3	3	
3	3	3	3	0	φ_{02}	3	3	0	0	2	φ_{03}
1	0	3	2	3		1	0	0	1	1	
0	1	0	1	2		0	1	3	2	0	
3	2	2	3	1		3	2	1	0	3	
2	3	1	0	0	φ_{10}	2	3	2	3	2	φ_{11}
1	0	2	3	0		1	0	1	0	2	
0	1	1	0	1		0	1	2	3	3	
3	2	3	2	2		3	2	0	1	0	
2	3	0	1	3	φ_{12}	2	3	3	2	1	φ_{13}
2	0	1	3	1		2	0	2	0	3	
3	1	2	0	0		3	1	1	3	2	
0	2	0	2	3		0	2	3	1	1	
1	3	3	1	2	φ_{20}	1	3	0	2	0	φ_{21}
2	0	0	2	2		2	0	3	1	0	
3	1	3	1	3		3	1	0	2	1	
0	2	1	3	0		0	2	2	0	2	
1	3	2	0	1	φ_{22}	1	3	1	3	3	φ_{23}
3	0	2	1	2		3	0	1	2	0	
2	1	1	2	3		2	1	2	1	1	
1	2	3	0	0		1	2	0	3	2	
0	3	0	3	1	φ_{03}	0	3	3	0	3	φ_{31}
3	0	3	0	1		3	0	0	3	3	
2	1	0	3	0		2	1	3	0	2	
1	2	2	1	3		1	2	1	2	1	
0	3	1	2	2	φ_{32}	0	3	2	1	0	φ_{33}

Table 4.2.: Codewords of MDS code $[5, 3, 3]_4$ are partitioned into $q^2 = 16$ subsets $[5, 1, 5]_4$. $\mathrm{AME}(7, 4)$, Eq. (4.50), formed by concatenating codewords of one subset to one of the Bell states.

5. Entanglement and quantum combinatorial designs

5.1. Introduction

Quantum information theory offers interesting connections with other scientific disciplines. In previous chapters, we discussed the connection between k-UNI states and error correction. Here, we focus on combinatorics and see how combinatorial designs extend to the quantum domain.

In this chapter, we introduce novel classes of combinatorial designs by extending classical symbols to pure quantum states. Our starting point is the notion of *quantum Latin squares* (QLS), which we generalize to quantum Latin cubes (QLC) and hypercubes (QLH). We also introduce a notion of orthogonality between them and identify a crucial ingredient missing in previous approaches: two orthogonal QLS could be entangled, in such a way that they cannot be expressed as two separated arrangements.

These entangled designs are intrinsically associated to a larger class of quantum designs that include all previous quantum Latin arrangements: *quantum orthogonal arrays*. After setting up the quantum combinatorial tools we apply our method again to the problem of constructing k-UNI and AME states for multipartite systems having an arbitrary large number of parties.

5.2. Latin arrangements and orthogonal arrays

We first recall some basic combinatorial concepts that will be used later. As we discussed in Preliminaries 2 a Latin square $\mathrm{LS}(q)$ is a square arrangement of size q such that every entry, taken from the set $\{0,\ldots,q-1\}$, occurs once in each row and each column. For instance, arrangements

$$\begin{array}{cc} 0 & 1 \\ 1 & 0 \end{array}, \quad \begin{array}{ccc} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{array}, \quad \begin{array}{cccc} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{array}, \tag{5.1}$$

are Latin squares of size q equal to two, three and four, respectively.

An *orthogonal array*, denoted as $\mathrm{OA}(r, n, q, k)$, is an arrangement composed by r rows, n columns and entries taken from the set $\{0, \ldots, q-1\}$, such that every subset of k columns contains all possible combinations of symbols, occurring the same number λ of times along the rows. Here, parameters k and λ are called *strength* and *index* of the OA, respectively [HSS99]. Two OA are called equivalent if one array can be transformed into the other by applying permutations or relabelling of symbols in rows or columns.

An OA is called *irredundant orthogonal array* denoted as IrOA if every subset of $n-k$ columns contains no repeated rows [GZ14]. In particular, an $\mathrm{OA}(r, n, q, k)$ is irredundant if by removing any k columns from the array all remaining r rows, containing $n-k$ different symbols. For examples we can consider

$$\mathrm{OA}(4,3,2,2) = \begin{matrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{matrix} . \tag{5.2}$$

5.2.1. Orthogonal Latin squares from orthogonal arrays

It is simple to show that any $\mathrm{LS}(q)$ is equivalent to an $\mathrm{OA}(q^2, 3, q, 2)$ [HSS99, Chapter 8]. For example, the array $\mathrm{OA}(4,3,2,2)$ produces a $\mathrm{LS}(2)$, as shown below:

$$\mathrm{OA} = \begin{matrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ -- & -- & -- \\ i & j & LS \end{matrix} \quad \Rightarrow \quad \mathrm{LS} = \begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix} . \tag{5.3}$$

Here, the first two columns of the OA identify coordinates (i, j) of symbols for the LS, whose values are determined by the third column LS of the OA.

Two Latin squares LS^A and LS^B of size q are *orthogonal* if the set of pairs $[(\mathrm{LS}^A)_{ij}, (\mathrm{LS}^B)_{ij}]$ is composed by all possible q^2 combinations symbols, where $i, j \in \{0, \ldots, q-1\}$.

A collection of m LS of order q is called mutually orthogonal (MOLS) if they are pairwise orthogonal. For instance, any $\mathrm{OA}(q^2, 2+m, q, 2)$ defines a set of m MOLS of size q [HSS99]. In particular, an $\mathrm{OA}(9, 4, 3, 2)$ implies two classical OLS of size 3. As before, first two columns (i, j) of the OA address entries of OLS, while the two latter yield the values of the squares A

and B,

$$OA(9,4,3,2) = \begin{array}{cccc} 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 1 \\ 1 & 0 & 2 & 2 \\ 1 & 1 & 1 & 0 \\ 1 & 2 & 0 & 1 \\ 2 & 1 & 0 & 2 \\ 2 & 2 & 2 & 0 \\ 2 & 0 & 1 & 1 \\ 0 & 2 & 1 & 2 \\ - & - & - & - \\ i & j & A & B \end{array} \tag{5.4}$$

$$\Rightarrow \quad \mathrm{LS}^A = \begin{array}{ccc} 0 & 2 & 1 \\ 2 & 1 & 0 \\ 1 & 0 & 2 \end{array} \qquad \mathrm{LS}^B = \begin{array}{ccc} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{array} .$$

Entries of two OLS are typically denoted as ordered pairs in a single array. For instance, the two OLS of Eq.(5.4) are denoted as

$$\mathrm{OLS} = \begin{array}{ccc} 00 & 21 & 12 \\ 22 & 10 & 01 \\ 11 & 02 & 20 \end{array} . \tag{5.5}$$

The elements consist all possible $q^2 = 9$ pairs. Also, a Latin square is called orthogonally isolated (or simply isolated) if there is no Latin square orthogonal to it [HSS99].

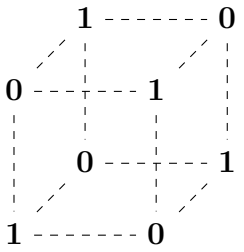
5.2.2. Orthogonal Latin cubes from orthogonal arrays

Orthogonal arrays can be associated to Latin cubes. An $\mathrm{OA}(q^3, 4, q, 3)$ defines a Latin cube $\mathrm{LC}(q)$, which consists on a cubic arrangement composed by q rows, q columns and q files, such that every entry taken from the set $\{0, \ldots, q-1\}$ occurs once in each row, each column and each file.

For instance, $\mathrm{OA}(8, 4, 2, 3)$ defines a LC of size 2, where now the first three bits (i, j, k) determine the position of a given element of the cube LC, while the last bit determines its

value,

$$\mathrm{OA}(8,4,2,3) = \begin{array}{cccc} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ - & - & - & - \\ i & j & k & LC \end{array}, \ \mathrm{LC} = \quad (5.6)$$



In general, an $\mathrm{OA}(q^k, k+m, q, k)$ defines m mutually orthogonal Latin hypercube (LH) of size q in dimension k, denoted MOLH (q). Figure 5.1 summarizes the existing relations between OA and Latin arrangements.

To emphasize the differences between the above described standard combinatorial designs and their quantum generalizations discussed in subsequent sections we will refer to OA, LS and MOLS and MOLC as the *classical* arrangements. An OA having r rows, n columns and q symbols can be associated with a pure quantum state of n qudit system having r terms [GZ14]. Each row of the array corresponds to a single term of the state, so the left hand side of the arrangement (5.4) yields the unnormalized state of $\mathrm{AME}(4,3)$

$$\begin{aligned} |\phi\rangle \;=\; & |0000\rangle + |0121\rangle + |1022\rangle + \\ & |1110\rangle + |1201\rangle + |2102\rangle + \\ & |2220\rangle + |2011\rangle + |0212\rangle. \end{aligned} \quad (5.7)$$

This state is maximally entangled with respect to the $\binom{4}{2} = 6$ possible balanced bipartitions and it is an $\mathrm{AME}(4,3)$ state.

5.3. Quantum Latin arrangements

These concepts are used to define unitary error bases [MV16] and mutually unbiased bases [Mus17]. In this section, we extend those results by introducing some classes of quantum Latin arrangements.

5.3.1. Quantum Latin squares

Recently, quantum Latin squares (QLS) [MV16, Mus17] have been introduced, where classical symbols appearing in entries of arrangements were extended to quantum states. The

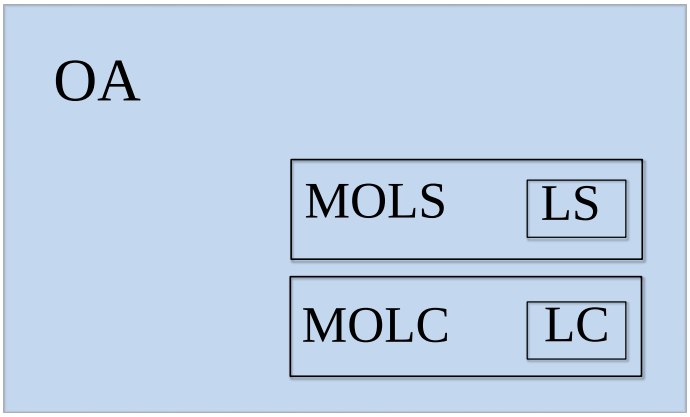


Figure 5.1.: Orthogonal arrays generalize some classes of combinatorial arrangements: Latin squares (LS), Latin cubes (LC), and mutually orthogonal LS and LC (MOLS and MOLC, respectively). These arrangements can be generalized to Latin hypercubes (LH) and mutually orthogonal LH (MOLS), respectively. Along this work, we develop a theory of quantum combinatorial designs and show that quantum Latin arrangements arise from QOA in the same way as classical Latin arrangements arise from OA.

following notion of quantum Latin squares was introduced by Musto and Vicary [MV16].

Definition 5.1. *A quantum Latin square of size q is a square arrangement,*

$$\mathrm{QLS}(q) = \begin{array}{ccc} |\psi_{0,0}\rangle & \cdots & |\psi_{0,q-1}\rangle \\ \vdots & & \vdots \\ |\psi_{q-1,0}\rangle & \cdots & |\psi_{q-1,q-1}\rangle \end{array} \tag{5.8}$$

composed of q^2 single particle quantum states $|\psi_{ij}\rangle \in \mathcal{H}_q$, $i,j \in \{0,\ldots,q-1\}$, such that each row and each column determines an orthonormal basis for a qudit system.

For instance, the following example of a quantum Latin square was given in Ref. [MV16],

$$\begin{array}{cccc} |0\rangle & |1\rangle & |2\rangle & |3\rangle \\ |3\rangle & |2\rangle & |1\rangle & |0\rangle \\ |\chi_-\rangle & |\xi_-\rangle & |\xi_+\rangle & |\chi_+\rangle \\ |\chi_+\rangle & |\xi_+\rangle & |\xi_-\rangle & |\chi_-\rangle \end{array}, \tag{5.9}$$

where two lower rows contain entangled states, $|\chi_\pm\rangle = \frac{1}{\sqrt{2}}(|1\rangle \pm |0\rangle)$, $|\xi_+\rangle = \frac{1}{\sqrt{5}}(i|0\rangle + 2|3\rangle)$ and $|\xi_-\rangle = \frac{1}{\sqrt{5}}(2|0\rangle + i|3\rangle)$. As a first observation, we realize that any QLS is naturally related to a tripartite pure state having maximally mixed single particle reductions.

Proposition 5.1. *A set of q^2 vectors $|\psi_{ij}\rangle \in \mathcal{H}_q$ forms a $\mathrm{QLS}(q)$ if and only if every single*

particle reduction of the three qudit state

$$|\Phi\rangle = \sum_{i,j=0}^{q-1} |i\rangle_A |j\rangle_B |\psi_{ij}\rangle_C \ , \tag{5.10}$$

is maximally mixed.

Proof. Let $|\psi_{ij}\rangle \in \mathcal{H}_q$ be the q^2 entries of a $\mathrm{QLS}(q)$ and let us define the state $|\Phi\rangle = \sum_{i,j=0}^{q-1} |i\rangle|j\rangle|\psi_{ij}\rangle$. Therefore

$$\begin{aligned} \rho_A &= \mathrm{Tr}_{BC} |\Phi\rangle\langle\Phi| \\ &= \mathrm{Tr}_{BC} \left(\sum_{i,j,i',j'=0}^{q-1} |ij\rangle_{AB}\langle i'j'| \otimes |\psi_{ij}\rangle_C \langle\psi_{i'j'}| \right) \\ &= \sum_{i,j,i'=0}^{q-1} \langle\psi_{ij}|\psi_{i'j}\rangle_{BC} |i\rangle_A\langle i'| = \sum_{i,j,i'=0}^{q-1} |i\rangle_A\langle i| = \mathbb{1}_q, \end{aligned}$$

where we used the fact that $|\psi_{ij}\rangle \in \mathcal{H}_q$ defines a $\mathrm{QLS}(q)$ and denoted A, B, C for first, second and third party, respectively. Analogously, one can check that $\rho_B = \mathbb{1}_q$. Furthermore, we have

$$\begin{aligned} \rho_C &= \mathrm{Tr}_{AB} \left(\sum_{i,j,i',j'=0}^{q-1} |ij\rangle\langle i'j'| \otimes |\psi_{ij}\rangle\langle\psi_{i'j'}| \right) \\ &= \sum_{i,j=0}^{q-1} |\psi_{ij}\rangle\langle\psi_{ij}| = \mathbb{1}_q \ , \end{aligned} \tag{5.11}$$

and, therefore, state (5.10) has every single particle reduction maximally mixed. □

Let us exemplify Proposition. 5.1 by considering the 1-UNI state of a three qudit system,

$$|\phi\rangle = F_q \otimes F_q \otimes \mathbb{1}_q \, |GHZ_q\rangle = \sum_{l,m=0}^{q-1} |lm\rangle \, |\psi_{l,m}\rangle \ . \tag{5.12}$$

Here $|GHZ_q\rangle = \sum_{n=0}^{q-1} |nnn\rangle$ denotes a generalized GHZ state of three subsystems with q levels each, $F_q = \sum_{i,j=0}^{q-1} \omega^{ij} |i\rangle\langle j|$ is the discrete Fourier transform of size q containing an unimodular number $\omega = e^{2\pi i/q}$ and the state reads

$$|\psi_{l,m}\rangle = \sum_{n=0}^{q-1} \omega^{n(l+m)} |n\rangle. \tag{5.13}$$

This construction works for any $q \geq 2$. The q^2 states from Eq. (5.13) determine a QLS of size q, which is equivalent to the classical $[\mathrm{LS}(q)]_{lm} = l + m$ modulo q with $l, m \in \{0, \ldots, q-1\}$, as the classical arrangement can be obtained by applying suitable local unitary operation to all elements of columns of the QLS. The state (5.12) is 1-UNI and it is equivalent to the

three-qudit GHZ state, in agreement with Proposition 5.1. Let us generalize this fact in the following observation.

Observation 5.1. *A* $\mathrm{QLS}(q)$ *is equivalent to a classical* $\mathrm{LS}(q)$ *if and only if one arrangement can be transformed into the other by applying the same local unitary operation to all elements of every column.*

Furthermore, note that a unitary operation U applied to a single column of a LS implies a controlled U operation acting on the third party of the corresponding three-partite 1-UNI state (see Proposition. 5.1). As a consequence, the entanglement of the state is changed and the Latin arrangement is changed by a single column unitary operation.

Let us now introduce the notion of orthogonality for QLS, which is not equivalent to orthogonality for two separated quantum arrangements.

Definition 5.2. *A set of* q^2 *pure quantum states of two parties* $|\psi_{i,j}\rangle \in \mathcal{H}_q^{\otimes 2}$ *arranged as*

$$\begin{array}{ccc} |\psi_{0,0}\rangle & \cdots & |\psi_{0,q-1}\rangle \\ \vdots & & \vdots \\ |\psi_{q-1,0}\rangle & \cdots & |\psi_{q-1,q-1}\rangle \end{array} \tag{5.14}$$

forms orthogonal quantum Latin squares (OQLS) if the following properties hold:

1. *The set of* q^2 *states* $\{|\psi_{i,j}\rangle\}$ *are orthogonal and form a basis in* $\mathcal{H}_q \otimes \mathcal{H}_q$.
2. *The sum of every row in the array (5.14), i.e.* $\sum_{j=0}^{q-1} |\psi_{i,j}\rangle$, *is a* 1-UNI *state.*
3. *The sum of every column in the array (5.14), i.e.* $\sum_{i=0}^{q-1} |\psi_{i,j}\rangle$, *is a* 1-UNI *state.*

Observation 5.2. *Two* OQLS *composed of separable states,* $|\psi_{i,j}^{AB}\rangle = |\eta_{ij}^{A}\rangle \otimes |\eta_{ij}^{B}\rangle$ *for every* $i, j \in \{0, \ldots, q-1\}$, *imply than both arrangements* $\{|\eta_{ij}^{A}\rangle\}$ *and* $\{|\eta_{ij}^{B}\rangle\}$ *determine* QLS, *according to Definition 5.1.*

Indeed, single party reductions to A and B of the states defined in items 2 and 3 above are proportional to the maximally mixed state, so that every row and every column of arrangements $\{|\eta_{ij}^{A}\rangle\}$ and $\{|\eta_{ij}^{B}\rangle\}$ form an orthonormal basis. Moreover, if entries of each QLS are given by elements of the computational basis then Definitions 5.1 and 5.2 reduces to the classical definition of LS and OLS, respectively.

5.3.2. Quantum Latin cubes

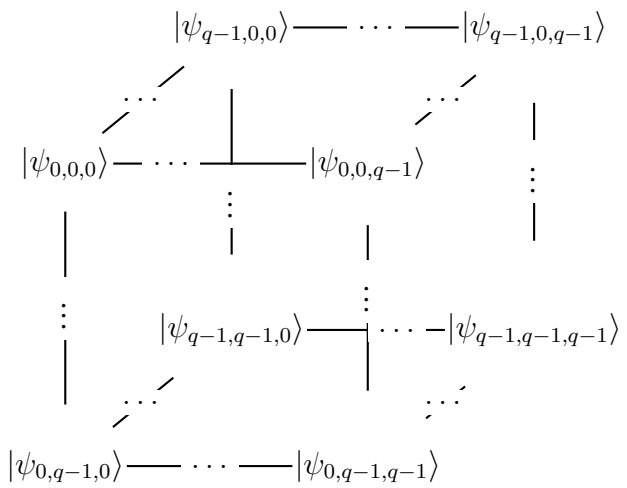
Let us go a step forward and introduce quantum Latin cubes.

Definition 5.3. *A quantum Latin cube (QLC) of size* q *is a cubic arrangement composed of* q^3 *single particle quantum pure states* $|\psi_{ijk}\rangle \in \mathcal{H}_q$, $i, j, k \in \{0, \ldots, q-1\}$, *such that every row,*

every column and every file form a set of orthogonal states.

For instance, in the case of a cubic arrangement composed by qubit quantum states, i.e. $q = 2$, we have the cube (5.6). Let us introduce a notion of orthogonality between cubic arrangements.

Definition 5.4. *A set of q^3 tri-partite pure states $|\psi_{x,y,z}\rangle$ belonging to a composed Hilbert space $\mathcal{H}_q^3$, arranged as*



forms a triple of mutually orthogonal quantum Latin cubes (MOQLC) if the following properties hold:

1. *The set of q^3 states $\{|\psi_{x,y,z}\rangle\}$ are orthogonal.*
2. *The sum of every row in the array (5.4), i.e. $\sum_{i=0}^{q-1} |\psi_{x,y,z}\rangle$, is a* 1-UNI *state.*
3. *The sum of every column in the array (5.4), i.e. $\sum_{j=0}^{q-1} |\psi_{x,y,z}\rangle$, is a* 1-UNI *state.*
4. *The sum of every file in the array (5.4), i.e. $\sum_{k=0}^{q-1} |\psi_{x,y,z}\rangle$, is a* 1-UNI *state.*

Analogously to Definition 5.2, if the q^3 states forming a set of MOQLC are fully separable, i.e. $|\psi_{x,y,z}^{ABC}\rangle = |\eta_{x,y,z}^{A}\rangle \otimes |\eta_{x,y,z}^{B}\rangle \otimes |\eta_{x,y,z}^{C}\rangle$, then each set of states $\{\eta_{x,y,z}^{A}\rangle\}$, $\{\eta_{x,y,z}^{B}\rangle\}$ and $\{|\eta_{x,y,z}^{C}\rangle\}$ forms a QLS according to Definition 5.1.

Furthermore, in such case a fully separable MOQLC is equivalent to a classical MOLC, in the sense that one can be connected to the other by applying local unitary operations acting in columns of the arrangements. This is so because any single-party orthonormal basis can be transformed into the computational basis by applying a suitable local unitary transformation. Also, if the states forming the cube (5.4) are biseparable with respect to a given partition, e.g. $|\psi_{x,y,z}^{ABC}\rangle = |\eta_{x,y,z}^{A}\rangle \otimes |\eta_{x,y,z}^{BC}\rangle$ for every $x, y, z \in \{0, \ldots, q-1\}$, then the single-party

arrangement $\{|\eta^A_{x,y,z}\rangle\}$ defines a QLC according to Definition 5.4. It is important here to note that the bipartite arrangement $\{|\eta^{BC}_{x,y,z}\rangle\}$ not necessarily forms a pair of OQLC. This surprising fact is closely related to the lack of some classes of multipartite absolutely maximal entanglement, e.g. $\mathrm{AME}(n,2)$ states exist only if the number of qubits is given by $n = 2,3,5,6$ [Sco04, HGS17].

5.3.3. Quantum Latin hypercubes

As the concepts of OQLS and OQLC are settled, let us define an arbitrary dimensional kind of quantum combinatorial arrangements, called *quantum Latin hypercubes*. These quantum arrangements can be connected to k-UNI states for n qudit systems having q levels each for any k, n and q, as we will show later.

Definition 5.5. *A quantum Latin hypercube (QLH) of size q and dimension k, denoted $\mathrm{QLH}(q,k)$, is an arrangement composed of q^k single particle quantum states $|\psi_{i_1,\ldots,i_k}\rangle \in \mathcal{H}_q^{\otimes k}$, $i_1,\ldots,i_k \in \{0,\ldots,q-1\}$, such that all states belonging to an edge of the hypercube are orthogonal.*

In particular, for $k=2$ quantum hypercube $QLH(q,2)$ reduces to the square $QLS(q)$, while for $k=3$ they form a cube, $QLH(q,3) = QLC(q)$.

We can extend the sets of OQLS and OQLC to sets of m mutually orthogonal quantum Latin hypercubes (MOQLH) of size q and dimension $k \leq m$. The following definition contains all previously defined combinatorial designs.

Definition 5.6. *A set of m mutually orthogonal quantum Latin hypercubes of size q in dimension k, denoted m $MOQLH(q)$, is a k-dimensional arrangement composed of m-qudit states $|\psi_{i_1,\ldots,i_k}\rangle \in \mathcal{H}_q^{\otimes m}$, $i_1,\ldots,i_m \in \{0,\ldots,q-1\}$ such that the following properties hold:*

1. *The set of q^k states $\{|\psi_{i_1,\ldots,i_k}\rangle\}$ are orthogonal.*

2. *The sum of q states belonging to the same edge of the hypercube, i.e. $\sum_{i_s=0}^{q-1} |\psi_{i_1,\ldots,i_s,\ldots,i_m}\rangle$ for every $1 \leq s \leq m$, forms a 1-UNI state.*

In particular, a set of m MOLS are also MOQLS, e.g. the classical arrangements (5.4) agree Definition 5.6. In Section 5.4, we introduce a suitable tool to generate quantum Latin arrangements, called *quantum orthogonal arrays*, and also establish its connection with quantum Latin arrangements.

5.3.4. Bounds for mutually orthogonal quantum Latin hypercubes

Let us now study upper bounds for the maximal number of classical and quantum Latin arrangements. The theory of orthogonal arrays provides a bound [Bus52] for the maximal number of columns of an $\mathrm{OA}(q^k, 2 + m_C, q, k)$, that has index unity. Therefore, it is easy to derive an upper bound for the maximal allowed number m_C of classical MOLH of size q and dimension k:

$$m_C \leq \begin{cases} k-1 & \text{if } q \leq k \\ q+k-4 & \text{if } 3 \leq k < q \\ q+k-3 & \text{in all other cases.} \end{cases} \tag{5.15}$$

For example, in dimension $k = 2$ we have that m MOLS of size q can only exist for $m_C \leq q - 1$, for any $q \geq 2$. The upper bound $m = q - 1$ can be saturated for q being a prime power number. These results, well-known in standard combinatorics, motivate us to derive similar results for quantum Latin arrangements. However, derivation of such a generalized bound requires solving a complicated optimization problem formalized (see Eqs. (39)–(41) in Ref. [Sco04]). Given the set of parameters n, q, k (or triple n, D, d in the original notation) these equations can be solved by considering linear programming techniques. The particular case $k = \lfloor n/2 \rfloor$, for which the arrangements are associated to AME states, can be analytically solved. Therefore, we are able to provide an analytic bound for the maximal number m_Q of MOQLH in the case of maximal possible dimension $k = \lfloor n/2 \rfloor$ as follows:

$$m_Q \leq \begin{cases} 2(q^2-1) & \text{if } n \text{ is even} \\ 2q(q+1)-1 & \text{if } n \text{ is odd.} \end{cases} \tag{5.16}$$

For instance, for $n = 4$ and $k = 2$ we have that $m_Q \leq 2(q^2 - 1)$ MOQLS exist for any size q, which is $2(q + 1)$ times larger than the classical bound $m_C \leq q - 1$. It is important to note that bounds (5.16) are not tight, as the bounds provided by Scott [Sco04] are not tight (see also [HESG18]).

Inequalities (5.15) and (5.16) can be useful to detect genuine quantumness in MOQLH. In general, given a set of m MOQLH it is hard to detect inequivalence to a classical set of MOLS. Typically, such kind of comparison would require to consider a full set of entanglement invariants. However, for those cases where $m > m_C$ it is ensured that a MOQLH is essentially quantum. For instance, a single LS of size two exists and there are no two QOLS of size two.

5.4. Quantum orthogonal arrays

In this section, we introduce quantum orthogonal arrays. This concept allows us to derive a simple rule to generate infinitely many classes of k-UNI states and AME states, in particular.

Definition 5.7. *A quantum orthogonal array* $\mathrm{QOA}(r,n,q,k)$ *is an arrangement consisting of* r *rows composed by* n*-partite normalized pure quantum states* $|\varphi_j\rangle \in \mathcal{H}_q^{\otimes n}$*, having* q *internal levels each, such that*

$$k\sum_{j=0}^{r-1}\mathrm{Tr}_{i_1,\ldots,i_{n-k}}\Big(|\varphi_j\rangle\langle\varphi_j|\Big)=r\,\mathbb{1}_k, \tag{5.17}$$

for every subset of $n-k$ *parties* $\{i_1,\ldots,i_{n-k}\}$.

In words, a QOA is an arrangement having n columns, possibly entangled, such that every reduction to k columns defines a *Positive Operator Valued Measure* (POVM). We recall that a POVM is a set of positive semidefinite operators such that they sum up to identity, determining a generalized quantum measurement [NC00].

We can also provide a view to error correction codes that suggest us to consider generalized measurements instead of projective measurements in QOA. We know that any AME state (or k-UNI state) are related to a certain quantum error correction code [Sco04]. An AME state of n parties with local dimension q, corresponds to a quantum code. This code can be considered as an injective mapping from the space of $K=1$ messages to a subset $\mathcal{C}$ of the set of codewords with length n, denoted by $(\!(n,K=1,d=\lfloor n/2\rfloor+1)\!)_q$. Knill-Laflamme theorem Eq. (2.48) implies that a subspace $\mathcal{C}$ of the Hilbert space $\mathcal{H}=\mathbb{C}_q^{\otimes n}$ generates an error correcting quantum code, if there exist recovery operators $R_1,R_2,\ldots$ such that for any state ρ with support in $\mathcal{C}$ and any collection of error operators with $\sum_e E_e^\dagger E_e=\mathbb{1}$, we have $\sum_{r,e}R_rE_e\rho E_e^\dagger R_r^\dagger=\rho\otimes\mathbb{1}$. In this case $R_1,R_2,\ldots$ are a finite sequence of operators in $\mathcal{H}$ satisfying the relation $\sum_r R_r^\dagger R_r=\mathbb{1}$. This theorem combined with the fact that an AME state yields an error correction code allows us to define quantum orthogonal arrays in a way that every reduction produces a POVM.

Definition 5.7 forms a natural extension of the classical concept of orthogonal arrays to quantum theory: the classical digits from $(0,\ldots,q-1)$ are generalized to quantum states from $\mathcal{H}_q$, while the classical concept of subsets of columns are replaced by partial trace.

From now on, we assume that columns of quantum arrangements are connected by the Kronecker product. Also, QOA having the minimal possible number of rows, i.e. $r=q^k$, are called *index unity*, as occurs in the classical case.

Let us introduce equivalent classes of QOA as a natural generalization of its classical counterpart, defined in Section 5.2. Two QOA are *equivalent* if one can transform one arrangement into the other one by applying suitable local unitary operations to columns and permutation

of rows or columns. Note that permutation of columns in quantum states produce states inequivalent under LOCC, in general. Nevertheless, as interchange of particles does not change the amount of entanglement in quantum states, from now on we will restrict our attention to QOA inequivalent under swap operations.

Note that the only allowed local unitary operations in classical OA are permutation matrices, equivalent to relabelling of symbols. In contrast to quantum Latin arrangements, in QOA we are allowed to apply any local unitary operation to any column without spoiling the orthogonal array. To illustrate these ideas let us consider the following example:

$$(\mathbb{1} \otimes \sigma_x) \begin{array}{cc} |0\rangle & |0\rangle \\ |1\rangle & |1\rangle \end{array} = \begin{array}{cc} |0\rangle & |1\rangle \\ |1\rangle & |0\rangle \end{array},$$

where σ_x is the Pauli X operator. In this way, we obtain two equivalent classical OA. Instead, by applying the Hadamard gate $H = \{\{1,1\},\{1,-1\}\}$ to the second column, i.e.,

$$(\mathbb{1} \otimes H) \begin{array}{cc} |0\rangle & |0\rangle \\ |1\rangle & |1\rangle \end{array} = \begin{array}{cc} |0\rangle & |+\rangle \\ |1\rangle & |-\rangle \end{array}, \tag{5.18}$$

with $|\pm\rangle = |0\rangle \pm |1\rangle$, we obtain a QOA which is equivalent under local unitary operations to a classical OA.

One example of QOA is

$$\mathrm{QOA}(4,5,2,2) = \begin{array}{cccc} |0\rangle & |0\rangle & |0\rangle & |\phi^+\rangle \\ |0\rangle & |1\rangle & |1\rangle & |\psi^+\rangle \\ |1\rangle & |0\rangle & |1\rangle & |\psi^-\rangle \\ |1\rangle & |1\rangle & |0\rangle & |\phi^-\rangle \end{array}, \tag{5.19}$$

where, $|\phi^\pm\rangle = |00\rangle \pm |11\rangle$ and $|\psi^\pm\rangle = |01\rangle \pm |10\rangle$ denote the Bell basis. To emphasize that some of these columns are separable (classical) and some of them are entangled (quantum), we shall also write $\mathrm{QOA}(4, 3_{cl} + 2_q, 2, 2)$, as the second argument denotes three classical and two quantum columns. Note that the number of classical and quantum columns, i.e. n_{cl} and n_{q} such that $n = n_{\mathrm{cl}} + n_{\mathrm{q}}$, are invariant under local unitary operations acting on columns of the QOA.

A QOA is equivalent to a classical OA if and only if $n_{\mathrm{q}} = 0$, thus also implying a classical set of MOLS and a classical error correction code [HSS99]. Roughly speaking, the parameter n_{q} quantifies the difference between QOAs and OAs. As a further comment, note that every reduction to two columns of the arrangement (5.19) form a POVM, where partial trace should be considered for entangled columns. The fact that QOA (5.19) is not equivalent to a classical OA is in correspondence with the fact that $\mathrm{AME}(5,2)$ state cannot be written as a linear

combination of q^2 elements of the 5-qubit computational basis.

5.4.1. Orthogonal quantum Latin squares from quantum orthogonal arrays

We have seen in Section 5.2, OLS arise from OA. First the two columns of the OA specify the entries of the first and second LS, whose values are determined by the third and fourth column of the OA, see Eq. (5.4). In the same way, as an example one can derive three MOQLS of size 2 from $\mathrm{QOA}(4,5,2,2)$ of Eq.(5.19). A triple of mutually orthogonal quantum Latin squares reads,

$$\mathrm{MOQLS}(2) = \begin{array}{cc} |0\rangle|\phi^+\rangle & |1\rangle|\psi^+\rangle \\ |1\rangle|\psi^-\rangle & |0\rangle|\phi^-\rangle \end{array} . \tag{5.20}$$

The first two columns of QOA (5.19) specify the entries of the three MOQLS (5.20). Note that these three MOQLS are entangled, which is a direct consequence of the fact that QOA (5.19) is not equivalent to a classical one. Indeed, QOA (5.19) contains entangled columns.

According to the results shown in Section 5.3, a single party arrangement belonging to a set of MOQLS determines a QLS, what can be seen from Eq.(5.20) after tracing out the second and third party. However, the bipartite arrangement obtained from taking partial trace over the first subsystem of the QOA (5.20), i.e.

$$\begin{array}{cc} |\phi^+\rangle & |\psi^+\rangle \\ |\psi^-\rangle & |\phi^-\rangle \end{array} , \tag{5.21}$$

is not a pair of orthogonal QLS. This is simple to observe if we take into account Definition 5.2. Indeed, the sum of every column of the arrangement (5.21) determines a 1-UNI state but the sum of every row gives a separable state. It is possible to prove that such $\mathrm{QOA}(r,4,2,2)$ does not exist for any $r \in \mathbb{N}$, which is related to the fact that an $\mathrm{AME}(4,2)$ state does not exist [HS00].

5.4.2. Orthogonal quantum Latin cubes from quantum orthogonal arrays

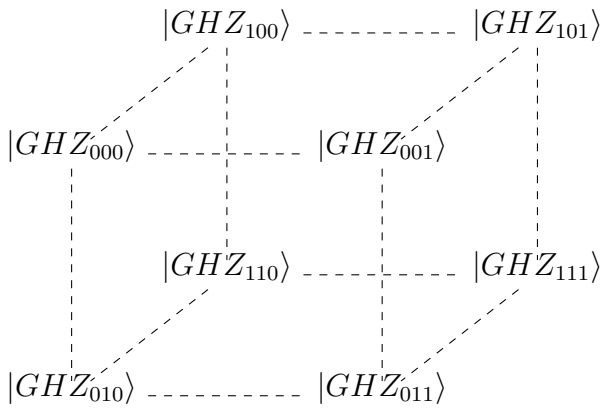
We will discuss later that OQLS are closely related to 2-UNI states. In order to achieve higher classes of multipartite entanglement, i.e. k-uniformity for $k > 2$, one has to generalize quantum combinatorial arrangements to higher dimensions. Now, let us introduce orthogonal quantum Latin cubes (OQLC). To study this, we consider the following array consisting of

three classical and three quantum columns,

$$\mathrm{QOA}(8, 3_{cl}+3_q, 2, 3) = \begin{array}{cccc} |0\rangle & |0\rangle & |0\rangle & |GHZ_{000}\rangle \\ |0\rangle & |0\rangle & |1\rangle & |GHZ_{001}\rangle \\ |0\rangle & |1\rangle & |0\rangle & |GHZ_{010}\rangle \\ |0\rangle & |1\rangle & |1\rangle & |GHZ_{011}\rangle \\ |1\rangle & |0\rangle & |0\rangle & |GHZ_{100}\rangle \\ |1\rangle & |0\rangle & |1\rangle & |GHZ_{101}\rangle \\ |1\rangle & |1\rangle & |0\rangle & |GHZ_{110}\rangle \\ |1\rangle & |1\rangle & |1\rangle & |GHZ_{111}\rangle \end{array}. \tag{5.22}$$

This QOA produces three MOQLC of size 2:

$\mathrm{MOQLC}(2) =$



(5.23)

Here, the tri-partite orthonormal basis is composed by eight states locally equivalent to the 3-qubit GHZ state. These states form an orthonormal basis in $\mathcal{H}_8 = \mathcal{H}_2 \otimes \mathcal{H}_2 \otimes \mathcal{H}_2$,

$$|GHZ_{ijk}\rangle = (-1)^{\alpha_{ijk}} \sigma_i \otimes \sigma_j \otimes \sigma_k |GHZ\rangle, \tag{5.24}$$

where $i, j, k = \{0, 1\}$ and σ_0 and σ_1 represent the Pauli matrices σ_x and σ_z, respectively. Global phases given by $\alpha_{ijk} = 1$ if $i = j = k$ and $\alpha_{ijk} = 0$ otherwise are added to states (5.24) forming the GHZ basis, in such a way that the construction (5.23) forms a quantum Latin cube.

5.4.3. Orthogonal quantum Latin hypercubes from quantum orthogonal arrays

Any set of m mutually orthogonal Latin hypercubes, in particular any set of m MOQLS, is linked to a QOA (see Figure. 5.2). As a natural generalization of this result, we have the following proposition.

Proposition 5.2. *A* $\mathrm{QOA}(q^k, k+m, q, k)$ *generates* m *MOQLH of size* q *in dimension* k*.*

We generate MOQLH from QOA in the same way as MOLH arise from classical OA. That is, first k classical columns of a QOA address the location of entries and the remaining m columns determine the values of every entry of the quantum Latin arrangement.

Now we are in position to establish the following result.

Proposition 5.3. *A set of* m $\mathrm{MOQLH}\{|\varphi_{i_1,\ldots,i_m}\rangle\}$ *of size* q *defined in dimension* k*, composed by* q^k *states of* m *qudit systems having* q *levels each, defines a* k-UNI *state for* $n = k+m$ *qudit systems, given by*

$$|\phi\rangle = \sum_{i_1,\ldots,i_k=0}^{q-1} |i_1,\ldots,i_k\rangle|\varphi_{i_1,\ldots,i_m}\rangle. \tag{5.25}$$

Even more, if $k' \leq k$ *subsystems belonging to the first* k *qudits are measured then the remaining entangled state is* $(k-k')$-UNI*.*

Proof. The state $|\phi\rangle$ defined for $n = k+m$ subsystems with q levels each is k-UNI, since the following two facts hold:

(i) the set of m MOQLH defined in dimension k define a QOA(q^k, n, q, k) and *(ii)* Proposition. 5.4 applies. □

For instance, the state AME(5,2) defined in (5.26), constructed through MOQLS (5.20), satisfies $\mathcal{C} = 1$, and defines a 1-dimensional subspace protected under decoherence [LMPZ96b].

5.4.4. Comparing orthogonal arrays with quantum orthogonal arrays

We can show that a $\mathrm{QOA}(r, n, q, k)$ determines a k-UNI state of n qudits, in the same way as an irredundant $\mathrm{OA}(r, n, q, k)$ implies a k-UNI state of n subsystems with q levels each [GZ14].

Proposition 5.4. *The sum of rows of a* $\mathrm{QOA}(r, n, q, k)$ *produces a* k-UNI *state of a quantum system composed of* n *parties with* q *levels each.*

Proof. Every reduction to k columns of a $\mathrm{QOA}(r, n, q, k)$ defines a POVM, and thus the sum of its elements produces the identity operator. □

For instance, $\mathrm{QOA}(4, 5, 2, 2)$ of Eq.(5.19), related to the squares (5.20), produces the 2-UNI

five-qubit state [LMPZ96b]

$$\begin{aligned} |\psi\rangle &= |000\rangle|\phi^+\rangle + |011\rangle|\psi^+\rangle + \\ &\quad |101\rangle|\psi^-\rangle + |110\rangle|\phi^-\rangle. \end{aligned} \tag{5.26}$$

Furthermore, the array $\mathrm{QOA}(8,6,2,3)$ presented in Eq.(5.22), and related to the cube (5.23), produces the $\mathrm{AME}(6,2)$ state [BPB$^+$07],

$$|\phi\rangle = \sum_{x,y,z=0}^{1} |x,y,z\rangle|GHZ_{xyz}\rangle. \tag{5.27}$$

Proposition 5.4 reveals that QOA generalizes the notion of irredundant OA and *not* the entire set of OA. For instance, the non-irredundant classical array,

$$\mathrm{OA}(4,3,2,1) = \begin{matrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{matrix}, \tag{5.28}$$

is not equivalent to a $\mathrm{QOA}(r,3,2,1)$ for any r. This is so because OA (5.28) does not produce a 1-UNI state and, by definition, any QOA produces at least a 1-UNI state. The key difference existing between classical and quantum OA relies on the fact that the action of removing columns in classical OA is not equivalent to taking the partial trace in the quantum case. Precisely, these operations are equivalent only if the orthogonal array considered is irredundant.

Furthermore, the juxtaposition of two OA is still an OA, whereas the same statement does not hold for QOA. This is connected to the fact that the sum of two k-UNI states is not necessarily a k-UNI (see in Section 5.5). Nonetheless, all classical $\mathrm{OA}(q^k, 2+m, q, 2)$, associated to m mutually orthogonal hypercubes of size q are irredundant [GZ14].

Let us summarize some important connections existing between classical and quantum arrangements and k-UNI states derived along this section. First, we start considering previously known connections. The following standard ('classical') notions are equivalent:

1. QOA with fully separable columns ($\equiv$ OA)

   [e.g. QOA$(9, 4_{normalfontcl} + 0_q, 3, 2)$ $\equiv$OA(9,4,3,2) in Eq.(5.4)]

2. Sets of m separable MOQLH(q) in dimension k
   ($\equiv$ MOLH) [e.g. classical LS_A and LS_B in Eq.(5.4)]

3. n qudit k-UNI states with minimal support

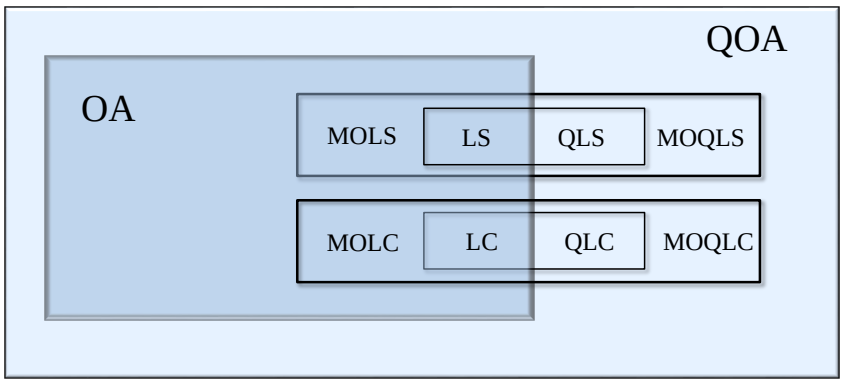


Figure 5.2.: Generalization of orthogonal arrays (OA) to quantum orthogonal arrays (QOA). This extension allows us to naturally generalize some classical arrangements to quantum mechanics: Quantum Latin squares (QLS), Quantum Latin cubes (QLC) and Mutually orthogonal quantum arrangements (MOQLS and MOQLC).

[e.g. AME(4,3) state in Eq.(5.7)]

Here, the symbol $\equiv$ denotes equivalence under local unitary operations applied to columns of an array. Connection *1-2* is well known in mathematics since the early times of orthogonal arrays theory (see Chapter 8 in Ref. [HSS99]). Connections *1-3* and *2-3* have been recently established, see Refs. [GZ14] and [GAL$^+$15], respectively. Furthermore, in the case of $n = 2k$ there exists a link between AME states and multi-unitary permutation matrices [GAL$^+$15].

In a similar manner, the following generalized ('quantum') notions are equivalent,

a. QOA with entangled columns ($\not\equiv$ OA)

[e.g. Eqs.(5.19) and (5.22)]

b. Entangled MOQLH ($\not\equiv$ fully separable MOQLH)

[e.g. Eqs. (5.20)]

c. n qudit k-UNI states with non-minimal support. ($\not\equiv$ to minimal support states)

[e.g. Eqs.(5.26) and (5.27)]

Note that a QOA having at least one pair of entangled columns necessarily implies the existence of entangled OQLS that cannot be separated, in the same way as entangled states cannot be represented as the tensor product of two single party pure states.

5.5. k-UNI states from quantum orthogonal arrays

As we have seen in Proposition 5.4, quantum arrays $\mathrm{QOA}(r, n, q, k)$ imply the existence of k-UNI states for n qudit systems having q levels each. In this section, we derive k-UNI states

with the maximal possible value $k = \lfloor n/2 \rfloor$ for $n = 5$ and arbitrary $q \geq 2$ from QOA. Those states determine AME states for 5-qudit systems.

Let us present a simple construction for $\mathrm{AME}(5, q)$ states for every $q \geq 2$ derived from QOA. These states are known to exist [Rai99a] but its explicit closed form has not been presented before, as far as we know. We first define the state $\mathrm{AME}(3, q)$

$$|\psi\rangle = \sum_{i=0}^{q-1} |i, j, i + j\rangle, \tag{5.29}$$

which has associated a classical array $\mathrm{IrOA}(q^2, 3, q, 1)$. As usual in the Thesis, sums inside kets are understood to be modulo q. By considering this state and the generalized Bell basis for 2-qudit systems, we are going to construct a QOA composed of 5 columns and q^2 rows that defines an $\mathrm{AME}(5, q)$ state for every integer q.

The first three classical columns of the quantum arrangement are induced by the state (5.29), whereas the remaining two quantum columns are given by the elements of the Bell basis

$$|\phi_{i,j}\rangle = \sum_{l=0}^{q-1} \omega^{il} |l + j, l\rangle, \tag{5.30}$$

where $\omega = \mathrm{e}^{2\pi \mathrm{i}/q}$. We are now in position to establish the following result.

Proposition 5.5. *The following three existing quantum objects, determined by a collection of q^2 states $|\phi_{i,j}\rangle \in \mathcal{H}_q^{\otimes 2}$ are equivalent:*

(A) $\mathrm{QOA}(q^2, 3_{cl} + 2_q, q, 2)$

$$\begin{array}{cccc} |0\rangle & |0\rangle & |0\rangle & |\phi_{0,0}\rangle \\ |0\rangle & |1\rangle & |1\rangle & |\phi_{0,1}\rangle \\ \vdots & \vdots & \vdots & \vdots \\ |q-1\rangle & |q-1\rangle & |q-2\rangle & |\phi_{q-1,q-1}\rangle \end{array} . \tag{5.31}$$

(B) Triple of MOQLS of size q

$$\begin{array}{ccc} |0\rangle|\phi_{0,0}\rangle & \dots & |q-1\rangle|\phi_{0,q-1}\rangle \\ \vdots & \ddots & \vdots \\ |q-1\rangle|\phi_{q-1,0}\rangle & \dots & |q-2\rangle|\phi_{q-1,q-1}\rangle \end{array} . \tag{5.32}$$

(C) Quantum state $\mathrm{AME}(5,q)$

$$|\psi\rangle = \sum_{i,j=0}^{q-1} |i,\ j,\ i+j\rangle|\phi_{i,j}\rangle, \tag{5.33}$$

for any integer $q \geq 2$.

Proof. Proof of *(A)* follows from two facts: *(i)* every subset of two columns produces an orthonormal basis *(ii)* every reduction to three columns contains orthogonal rows. These conditions ensure that every reduction to two columns produces a POVM. These two properties are an extension of the so-called *uniformity* and *irredundancy*, considered to construct k-UNI states from classical OA (see Section IV in Ref. [GZ14]).

Equivalence between *(A)* and *(C)* follows directly from Propostion 5.4, while the last relation between *(A)* and *(B)* can be obtained by Propostion 5.2. □

In the case of $q = 2$, this construction reduces to QOA (5.19), MOQLS (5.20) and AME(5,2) state (5.26). Note that the QOA (5.31) has its last two columns entangled, implying that MOQLS (5.32) are necessarily entangled and AME state (5.33) does not have minimal support. This is consistent with the summary of results presented at the end of Section 5.4.

Observation 5.3. *QOA allow us to add a classical column to the arrangement (5.31) in order to define the following* 2-UNI *states of 6 qudits, i.e.,*

$$|\psi\rangle = \sum_{i,j=0}^{q-1} |i,j,i+j,i+2j\rangle|\phi_{i,j}\rangle, \tag{5.34}$$

where q *is an odd prime number and both sums in kets are taken modulo* q*. When* q *is a prime power number, it is convenient using polynomial representation based on irreducible polynomials. In such cases, the* 2-UNI *states of* 6 *qubits is written as*

$$\sum_{i,j=0}^{q-1} |i,j,i+j,i+a_1 j\rangle|\phi_{i,j}\rangle,$$

where a_1 *is the first element of the finite set using the polynomial representation for which* $a_1 \neq 0, 1$.

Here, note that the classical and quantum parts are composed of four and two columns, respectively. It is simple to check that the underlying arrangement is a $\mathrm{QOA}(q^2, 4_{cl} + 2_q, q, 2)$.

In the constructions presented above, the key point was to produce a QOA from combining a classical OA and an orthonormal basis composed of generalized Bell states. It is simple to realize that the multiplication of quantum columns produce another QOA having a larger

number of columns. For example, the QOA (5.19) can be extended by considering m copies of the quantum part in the following way:

$$\begin{array}{cccc} 1 & 1 & 1 & |\phi^+\rangle \ \ldots \ |\phi^+\rangle \\ 0 & 0 & 1 & |\phi^-\rangle \ \ldots \ |\phi^-\rangle \\ 0 & 1 & 0 & |\psi^+\rangle \ \ldots \ |\psi^+\rangle \\ 1 & 0 & 0 & \underbrace{|\psi^-\rangle \ \ldots \ |\psi^-\rangle}_{m} \end{array}, \tag{5.35}$$

which produces a 2-UNI state of $3 + 2m$ qubit systems. Furthermore, constructions (5.33) and (5.34) can be generalized in the same way. That is, we construct 2-UNI states for an odd number of $n = 5 + 2m$ qudits

$$\sum_{i,j=0}^{q-1} |i,\ j,\ i+j\rangle \underbrace{|\phi_{i,j}\rangle \cdots |\phi_{i,j}\rangle}_{m},$$

and also 2-UNI states for an even number of $n = 6 + 2m$ qudits

$$\sum_{i,j=0}^{q-1} |i, j, i+j, i+2j\rangle \underbrace{|\phi_{i,j}\rangle \cdots |\phi_{i,j}\rangle}_{m},$$

where q is a prime number. As we described in (5.34), when q is a prime power we should consider the set of polynomial representation of the finite sets. For these constructions it is straightforward to check that every reduction to two parties forms a POVM.

5.6. Conclusions

A generalization of classical combinatorial arrangements to quantum mechanics has been established. We studied the notion of quantum Latin squares (QLS), quantum Latin cubes (QLC), quantum Latin hypercubes (QLH) and introduced a suitable notion of orthogonality between them. We also introduced the notion of quantum orthogonal arrays (QOA), that generalizes all the classical and quantum arrangements. Moreover, we derived quantum Latin arrangements from QOA in the same way as classical Latin arrangements can be obtained from classical OA.

Our findings allowed us to realize that a pair of orthogonal quantum Latin arrangements not necessarily implies existence of two separated arrangements satisfying an orthogonality cirterion. Indeed, orthogonal Latin arrangements can be entangled in the same way as quantum states are entangled. This astonishing property is one-to-one related to the fact that columns of QOA can be entangled. This turned out to be a crucial property in order to reproduce some classes of highly entangled multipartite states, the so-called AME states with non-minimal

support, for instance the states AME(5,2) and AME(6,2) consisting of five and six qubits, see Eqs. (5.26) and (5.27), respectively.

Furthermore, QOA define k-UNI states. We demonstrated that k-UNI states constructed from quantum Latin arrangements have high persistency of entanglement, which makes them ideal candidates for quantum information protocols.

We constructed three genuinely entangled MOQLS of size q, QOA composed of five columns and an arbitrary number q of internal levels and AME states for five parties with q levels each, for every $q \geq 2$. This result evidences the usefulness of the quantum combinatorial designs introduced along the work.

6. Optimal quantum error correcting codes from absolutely maximally entangled states

6.1. Introduction

Quantum error correction provides promising techniques to solve the inherent fragility of quantum systems interacting with the environment. AME states are linked to quantum codes as well. In particular, AME states are formally shown to be equivalent to a special QECC that has only one codeword , i.e., $[\![n, 0, \lfloor n/2 \rfloor + 1]\!]_q$ [Sco04]. However, having just one codeword in the code space may not be useful for communication purposes as we need to encode a number of qudits into different codewords.

In chapter 3 we discussed the direct correspondence between minimal support AME states and classical MDS codes. In this chapter we conjecture the existence of a family of QECC whose code spaces are spanned by AME states. We show that our conjecture is equivalent to the existence of a Pauli string satisfying a compressibility condition. A Pauli string is incompressible in the sense that its weight cannot be decreased by multiplying it with stabilizer products of the code.

Further we construct such codes for all n up to $n = 8$ by finding several suitable incompressible operators. In the corresponding QECCs, a logical qudit is encoded in a q-dimensional subspace spanned by AME states of n parties. Our proposal has a very clear physical motivation and complements other constructions of non-binary QECC. In particular our construction is very explicit and works with a smaller local dimension q given n than previous codes with similar code parameters.

6.2. Properties of stabilizer quantum error-correcting codes

A given stabilizer QECC, $\mathcal{C} = [\![n, \tilde{k}, d]\!]_q$ appends physical qudits to logical qudits that we want to protect (details discussed in Preliminary section (2.8)). For the code to be useful, the code space must be chosen such that the expected errors never map a state from the code space to a state that could also have been produced by a different error from a different code state. This would introduce an unrecoverable error. One should always take the state out of the code space in a away such that a subsequent correction can bring the system back into its original state.

An error $E \in \mathcal{E}$ that affects a given encoded quantum state either commutes or anticommutes with any particular element of stabilisers S_i. One can say the error E is detectable by computing an *error syndrome*, for this, we need to check if E commutes or anticommutes with each element S_i. The syndrome $\mathbf{r}$ is a vector with length $n-\tilde{k}$ whose elements identify whether the error E commutes or anticommutes with each S_i. The error E is correctable if (i) it anticommutes with an element S_i or (ii) it is one of the stabilisers. It corrupts the encoded message if the weight of $|E| \leq t$ and it commutes with all S_i but does not lie in the stabiliser group.

In the following we present one examples of stabilizer QECC.

6.2.1. $\mathrm{AME}(4,3)$ state and QECC with 1-UNI codewords

Here, we discuss an example of constructing a QECC with parameters $[\![n-1, 1, \lfloor n/2 \rfloor]\!]_q$ from a given $\mathrm{AME}(n,q)$ state. For this, we consider the $\mathrm{AME}(4,3)$ state constructed from the classical MDS code $[4,2,3]_3$

$$\begin{aligned} |\psi\rangle &= \sum_{i,j=0}^{2} |i, j, i+j, i+2j\rangle \\ &= |000\rangle + |0112\rangle + |0221\rangle + |1011\rangle + |1120\rangle + |1202\rangle + |2022\rangle + |2101\rangle + |2210\rangle \end{aligned} \tag{6.1}$$

In this example the local dimension $q = 3$ is prime so that the finite field $GF(3)$ is simply the set $\{0,1,2\}$ with the standard arithmetic modulo 3. The state $|\psi\rangle$ is a QECC with parameters $[\![4,0,3]\!]_3$ and our purpose is constructing a quantum code $[\![3,1,2]\!]_3$.

We take the first party of the state $|\psi\rangle$ as the logical qudit, and encode it with the projection onto the remaining particles. The resulting codewords are

$$|\psi_i\rangle = \sum_{j=0}^{2} |j, i+j, i+2j\rangle \qquad i = 0,1,2\,, \tag{6.2}$$

or, equivalently,

$$|\psi_0\rangle = \sum_{j=0}^{2} |j, j, 2j\rangle = |000\rangle + |112\rangle + |221\rangle \tag{6.3}$$

$$|\psi_1\rangle = \sum_{j=0}^{2} |j, j+1, 2j+1\rangle = |011\rangle + |120\rangle + |202\rangle \tag{6.4}$$

$$|\psi_2\rangle = \sum_{j=0}^{2} |j, j+2, 2j+2\rangle = |022\rangle + |101\rangle + |210\rangle \ . \tag{6.5}$$

One can simply check that the above states are orthogonal 1-UNI states and the minimal number of single-qudit operations that are needed to create a non-zero overlap between any two states is equal to 2.

6.3. Quantum error correcting codes from AME states

In this section we show that the $\mathrm{AME}(n, q)$ states of minimal support constructed from linear MDS codes allow to construct QECC with parameters $[\![n, 1, \lfloor n/2 \rfloor]\!]_q$. As we show below, we need to find suitable incompressible operators that when applied to a given $\mathrm{AME}(n, q)$ construct the code space of the QECC. In this QECC, a logical qudit is encoded in a q dimensional subspace spanned by $\mathrm{AME}(n, q)$ states.

Our construction provides codes that are different from the example presented in the previous section. In this example, one starts from an $\mathrm{AME}(4, 3)$ and by eliminating one of the parties derived a QECC with codewords containing $n = 3$ parties and consequently code parameters $[\![3, 1, 2]\!]_3$. In our construction one want to start from an $\mathrm{AME}(n, q)$ and by using the incompressible operators and without eliminating any parties construct stabilizer QECCs. Our construction is comparably simply, very explicit, physically motivated, and works with a smaller local dimension q given n than previous codes with similar code parameters (we provide a detailed comparison at the end of this section).

First we recall that a subspace $\mathcal{C}$ spanned by a set $\{|\psi_m\rangle\}_{m\in[q^{\tilde{k}}]}$ of orthonormal states is a $[\![n, \tilde{k}, d]\!]_q$ QECC, i.e., a code that encodes $\tilde{k}$ logical qudits into n physical qudits, if it obeys the Knill-Laflamme conditions, Eq. (2.48) [KL97, Got97]

$$\forall m, m' \in [q^{\tilde{k}}]\colon \ \langle\psi_m|E^\dagger F|\psi_{m'}\rangle = f(E^\dagger F)\, \delta_{m,m'} \tag{6.6}$$

for all E, F with $\mathrm{wt}(E^\dagger F) < d$. Thereby wt is the *weight* of an operator, defined to be the number of sites on which it acts non-trivially. The parameter d is the distance of the code, which is the minimal number of single-qudit operations that are needed to create a non-zero

overlap between any two orthogonal states from the code state space $\mathcal{C}$, i.e.,

$$d \coloneqq \min_{|\phi\rangle,|\phi'\rangle\in\mathcal{C},W} \{\mathrm{wt}(W)\colon \langle\phi|W|\phi'\rangle \neq 0 \wedge \langle\phi|\phi'\rangle = 0\}\,. \tag{6.7}$$

Such a code can correct all errors that act non-trivially on up to $t \coloneqq \lfloor (d-1)/2 \rfloor$ physical qudits (for more details see Preliminaries section (2.8).

The code space of the QECC that we are going to construct will be spanned by AME states generated by acting with a Pauli string M onto a given minimal support AME state $|\Psi\rangle$ constructed from an MDS code. Let us first introduce the notion of different *realizations* of such a Pauli string M. Recall first that AME states generated by Eq. (3.6) are stabilized by a set of q^n Pauli strings, the elements of the stabilizer group, denoted by

$$S(\alpha_1,\ldots,\alpha_n) \coloneqq \prod_{l=1}^{n} \left(S_l^{\Psi}\right)^{\alpha_l}, \tag{6.8}$$

where S_l^{Ψ} are the stabilizers defined in Eq. (A.7) and the $\alpha_i \in [q]$. This implies that, for a given Pauli string M acting on $|\Psi\rangle$, there are $q^n - 1$ other Pauli strings that perform exactly the same action on $|\Psi\rangle$, namely, since

$$M|\Psi\rangle = M\,S(\alpha_1,\ldots,\alpha_n)|\Psi\rangle, \tag{6.9}$$

all $\tilde{M}(\alpha_1,\ldots,\alpha_n) \coloneqq MS(\alpha_1,\ldots,\alpha_n)$ act identically on $|\Psi\rangle$. All such *realizations* $\tilde{M}(\alpha_1,\ldots,\alpha_n)$ of a Pauli string form an equivalence class.

The elements of such an equivalence class act on different subsets of the sites. For example, the operator $X\otimes\mathbb{1}\otimes\cdots\otimes\mathbb{1}$, when acting on an AME state generated from a generator matrix in standard form, can be *pushed* to the second half of the system by inserting the operator $(S_1^{\Psi})^{\dagger}$ as then

$$X\otimes\mathbb{1}\ldots\mathbb{1}|\Psi\rangle = (X\otimes\mathbb{1}\ldots\mathbb{1})(S_1^{\Psi})^{\dagger}|\Psi\rangle \tag{6.10}$$

$$= \mathbb{1}\ldots\mathbb{1}\otimes\overbrace{X^{-g_{1,\lfloor n/2\rfloor+1}}\otimes\ldots\otimes X^{-g_{1,n}}}^{\lceil\frac{n}{2}\rceil}|\Psi\rangle. \tag{6.11}$$

For the EPR state $\Phi^+ \coloneqq \sum_j |j\rangle|j\rangle$ this property is well known. For every unitary U acting on site 1 there is another unitary that transforms this state in the same way but acts only on site 2, i.e., $(U\otimes\mathbb{1})|\Phi^+\rangle = (\mathbb{1}\otimes U^T)|\Phi^+\rangle$. In the case of AME states, any Pauli string can always be pushed to act non-trivially only on sites inside any subset of size $\lceil n/2\rceil$:

Lemma 6.1. *Consider a minimal support AME state $|\Psi\rangle$ constructed from a linear MDS code according to Eq.* (3.6) *and a Pauli string M acting on n q-level systems. For every set S of at least $\lceil n/2\rceil$ of the systems there is a realization $\tilde{M}(\alpha_1,\ldots,\alpha_n)$ that transforms $|\Psi\rangle$ in the*

same way, i.e., $M|\Psi\rangle = \tilde{M}(\alpha_1, \ldots, \alpha_n)|\Psi\rangle$ *and acts non-trivially only on the systems in* S*.*

Proof. This is a direct consequence of the fact that the tensor of coefficients of a minimal support AME state is a perfect tensor. More explicitly, constructing a realization $\tilde{M}(\alpha_1, \ldots, \alpha_n)$ that acts trivially on $\lfloor n/2 \rfloor$ sites is equivalent to solving two systems of each $\lfloor n/2 \rfloor$ linear equations, one for the powers of the X operators and one for the powers of the Z operators, because

$$\begin{aligned} &\tilde{M}(\alpha_1, \ldots, \alpha_n) \\ &= M \left(\bigotimes_{m=1}^{n} X^{\sum_{l=1}^{\lfloor n/2 \rfloor} \alpha_l \, g_{l,m}} \right) \left(\bigotimes_{m=1}^{n} Z^{\sum_{l=\lfloor n/2 \rfloor + 1}^{n} \alpha_l \, h_{l,m}} \right). \end{aligned} \tag{6.12}$$

As any subset of up to $\lfloor n/2 \rfloor$ columns of the generator and any subset of up to $\lceil n/2 \rceil$ columns of the parity check are linearly independent, this can always be done. □

When pushing Pauli strings around, as the example above demonstrates, their weight can change. In particular, it can happen that after pushing a Pauli string into a certain set of sites, it doesn't actually act non-trivially on all sites in this set. We define the minimal weight of an equivalence class of operators as the weight of the "lightest" element within the class. When a given M belongs to a class of minimal weight w, this means that it cannot be pushed into any subset of less than w sites, i.e., it can not be compressed to have weight less than w.

For the sake of simplicity we now restrict our considerations to the case n even. In the following theorem we show how a Pauli string M, belonging to a class of minimal weight w, defines an AME state based QECC.

Theorem 6.2. *Let* $|\Psi\rangle$ *be an* $\mathrm{AME}(n, q)$ *state constructed from a linear MDS code via Eq.* (3.6) *with* n *even and* $q \geq n - 1$ *prime and* M *a Pauli string. The subspace* $\mathcal{C} \coloneqq \mathrm{span}(\{|\Psi_m\rangle_{m=0}^{q-1}\}) \subset (\mathbb{C}^q)^{\otimes n}$*, with*

$$|\Psi_m\rangle \coloneqq M^m |\Psi\rangle \tag{6.13}$$

is a QECC code parameters $[\![n, 1, w]\!]_q$ *if and only if* M *belongs to an equivalence class of Pauli strings of minimal weight* $0 < w \leq n/2$*. Moreover, generators for the stabilizers group of the code state space can be constructed explicitly.*

Proof. The subspace is manifestly spanned by orthogonal AME states, as the $|\Psi_m\rangle$ are part of an orthonormal basis of AME states. This is a direct consequence of the fact that, because of Lemma 6.1, for n even, a Pauli string acting on an AME state either stabilizes it or produces an orthogonal state, i.e., $\langle\Psi|(M|\Psi\rangle) \in \{0, 1\}$. Further, $\mathcal{C}$ is a QECC that can correct all errors from a set $\mathcal{E}$ if and only if there exists some function f such that for all $E, F \in \mathcal{E}$ and all

$m, m' \in [q]$ [Got09]

$$\langle \Psi_{m'} | E^\dagger F | \Psi_{m'+m \mod q} \rangle = \delta_{m,0}\, f(E^\dagger F). \tag{6.14}$$

In our case, $\mathcal{E}$ is the set of all operators with weight at most $\lfloor (w-1)/2 \rfloor \leq \lfloor (n-2)/4 \rfloor$. We first prove the "only if" part. Assume that M could be compressed into some subsystem of size less than or equal to $w-1$. As the compressed M would still be a Pauli string and therefore product, there would be some error operators E, F such that $E^\dagger F = M$ and hence the above condition would be violated. This proves necessity. We now turn to the "if" part. If $m = 0$, then because $|\Psi_{m'}\rangle$ is an AME state

$$\langle \Psi_{m'} | E^\dagger F | \Psi_{m'+m \mod q} \rangle = q^{n/2}\, \mathrm{Tr}(E^\dagger F). \tag{6.15}$$

Consider now the case $m \neq 0$. As n is even, we know that we can push any Pauli string into any subset of size $n/2$. Denote the result of pushing M^m with the product of stabilizers S into some subset of size $n/2$ that completely contains the sites on which $E^\dagger F$ acts non-trivially by $\widetilde{M^m} \coloneqq M^m S$. As $|\Psi_{m'}\rangle$ is AME

$$\begin{aligned} \langle \Psi_{m'} | E^\dagger F | \Psi_{m'+m \mod q} \rangle &= \langle \Psi_{m'} | E^\dagger F\, \widetilde{M}^m | \Psi_{m'} \rangle & (6.16) \\ &= \mathrm{Tr}(E^\dagger F\, \widetilde{M^m})\, q^{n/2}. & (6.17) \end{aligned}$$

Notice that $\widetilde{M^m}$ is not the m-th power of M pushed into the same subset, but $|\widetilde{M^m}| = |M^m S| = |(M S^{1/m})^m| = |M S^{1/m}|$ (as the Pauli matrices commute up to a phase, which does not change the weight) and so M^m can be compressed into a certain number of sites if and only if M can be compressed into the same number of sites. Thus $\widetilde{M^m}$ is, up to possibly a phase, a product of traceless Pauli operators that act non-trivially on at least one site on which $E^\dagger F$ does not act, and therefore $\mathrm{Tr}(E^\dagger F\, \widetilde{M^m}) = 0$. This proves Eq. (6.14) with $f(\cdot) = q^{n/2}\, \mathrm{Tr}(\cdot)$.

It remains to show how to construct the generators $S_r^{\mathcal{C}}$ of the stabilizers group of $\mathcal{C} = \mathrm{span}(\{|\Psi_m\rangle\}_{m=0}^{q-1})$. The generators have to satisfy

$$\forall r, m: \quad S_r^{\mathcal{C}}\, M^m\, |\Psi\rangle = M^m\, |\Psi\rangle. \tag{6.18}$$

The special case $m = 0$ of this condition implies that they must be products of the stabilizers of $|\Psi\rangle$, i.e., that there exist vectors $\vec{\alpha}_r \in [q]^n$ such that $S_r^{\mathcal{C}} = \prod_{l=1}^n (S_l^\Psi)^{(\vec{\alpha}_r)_l}$, hence they are in particular also Pauli strings. Further, the above condition implies that the $s_r^{\mathcal{C}}$ must commute with M (and hence M^m) when acting on $|\Psi\rangle$, i.e,

$$S_r^{\mathcal{C}}\, M^m |\Psi\rangle = M^m\, S_r^{\mathcal{C}} |\Psi\rangle. \tag{6.19}$$

The commutator of two Pauli strings, however is, up to a phase again a Pauli string. More precisely, any Pauli string A can be brought into the standard form

$$A = \mathrm{e}^{\mathrm{i}\,\varphi(A)}\; A_X^{\vec{a}^X}\, A_Z^{\vec{a}^Z}\,, \tag{6.20}$$

where $\varphi(A)$ is a phase, and $A_X^{\vec{a}^X} = \bigotimes_{j=1}^n X^{(\vec{a}^X)_j}$ and equivalently for $A_Z^{\vec{a}^Z}$. As can be verified by direct computation, for any two Pauli strings A, B it holds that

$$A\,B = \omega^{\vec{a}\odot\vec{b}}\,B\,A \tag{6.21}$$

where $\vec{a} = (\vec{a}^X, \vec{a}^Z)$ and $\vec{b}$ is defined in the same way in terms of the standard form of B and $\odot$ is the bilinear symplectic inner product

$$\vec{a}\odot\vec{b} \coloneqq \vec{a}^Z\cdot\vec{b}^X - \vec{a}^X\cdot\vec{b}^Z. \tag{6.22}$$

This implies that Eq. (6.19) is satisfied if for all m it holds that $\vec{s_r}\odot(m\,\vec{m}) \mod q = 0$, which is equivalent to just $\vec{s_r}\odot\vec{m} \mod q = 0$, where $\vec{s}_r$ is the vector coming from the standard representation of $s_r^{\mathcal{C}}$ and $\vec{m}$ that of M. More specifically

$$\vec{s}_r \coloneqq \begin{pmatrix} G^T & 0 \\ 0 & H^T \end{pmatrix} \vec{\alpha}_r \tag{6.23}$$

and as M has weight less than $n/2+1$ the condition $\vec{s_r}\odot\vec{m} = 0$ imposes a non-trivial constraint, so that there are $n-1$ linearly independent $\vec{\alpha}_r$ that satisfy it and are of the form given above. A Mathematica code to find all these $\vec{\alpha}_r$ is given under [ame]. □

In order for the code resulting from the above construction with a given Pauli string M to yield the maximum distance allowed by the Singleton bound the minimal weight w of the Pauli strings equivalence class has to satisfy

$$w = \left\lfloor \frac{n-1}{2} + 1 \right\rfloor = \left\lceil \frac{n}{2} \right\rceil, \tag{6.24}$$

which precisely matches the lower bound set by Lemma 6.1. We conjecture that for any n, and any AME states constructed in the above way from a linear MDS code, an equivalence class of Pauli strings exists that saturate this bound (for n even):

Conjecture 6.1. *Given an AME state $|\Psi\rangle$ produced by a linear MDS code of n sites and $q \geq n-1$ prime, there exists at least one equivalence class of Pauli strings with minimal weight $\lfloor n/2 \rfloor$.*

As a side remark, note that our proof of Theorem 6.2 in any case only works for n even.

QECC	q	M (first primitive element and smallest q)
$[\![3,1,1]\!]_q$	$2,3,4,5$	$\mathbb{1}\otimes\mathbb{1}\otimes Z$
$[\![4,1,2]\!]_q$	$3,4,5,7$	$\mathbb{1}\otimes\mathbb{1}\otimes X\otimes Z$
$[\![5,1,2]\!]_q$	$4,5,7,8$	$\mathbb{1}\otimes\mathbb{1}\otimes\mathbb{1}\otimes X\otimes Z$
$[\![6,1,3]\!]_q$	$5,7,8,9,11,13$	$\mathbb{1}\otimes\mathbb{1}\otimes X\otimes Z\otimes\mathbb{1}\otimes Z$
$[\![7,1,3]\!]_q$	$7,8$	$Z\otimes\mathbb{1}\otimes Z\otimes\mathbb{1}\otimes\mathbb{1}\otimes\mathbb{1}\otimes Z$
$[\![8,1,4]\!]_q$	$7,8$	$\mathbb{1}\otimes\mathbb{1}\otimes\mathbb{1}\otimes Z\otimes\mathbb{1}\otimes Z\otimes Z\otimes X$

Table 6.1.: List of QECCs whose existence we have verified by symbolic computation and exemplary M matrices that generate a code form the respective family. All codes for n even have the highest distance allowed by the quantum Singleton bound for the given n and k, moreover the code $[\![7,1,3]\!]_q$ is able to correct errors on the same amount of subsystems as the QMDS code $[\![7,1,4]\!]_q$. We do not obtain the codes $[\![5,1,3]\!]_{4,5,7,8}$ from our construction, but we have found M operators not compressible to less than $d=3$ sites.

We have not been able to prove the above conjecture for all even n, but using the computer algebra system Mathematica we were able to construct all incompressible M operators with the conjectured properties for all $n\in\{2,4,6,7,8\}$, where $n=8$ is the largest n for which we can exhaustively check all ways of pushing [ame].

In all cases we were able to find such M operators for q down to $q=n-1$, except in the case $n=7$, where we had to chose $q=7$, because $n-1=6$ is not a power of a prime, and the case $n=2$, where our conjecture is known to be true for $q\geq 2$ and the case $q=1$ does not make sense. For $n=6$, the existence of the extended Singleton array S_4' (see Eq. (3.11)) for $q=4$ might give one hope that in this case an incompressible M might exist for $q=n-2$, but our calculations show that no such M exists. We summarize our results in Table 6.1.

Further we can prove that Pauli strings containing only X or only Z operators and that have weight $\sim n/4$ can not be compressed to have weight less than $\sim n/4$:

Lemma 6.3. *Any Pauli string M of weight $\mathrm{wt}(M)=\left\lfloor(\lfloor n/2\rfloor+1)/2\right\rfloor$ and consisting of only X or only Z operators is incompressible.*

Proof. Any product S of stabilizers is again a stabilizer. Any such product S, apart from the trivial stabilizer, the identity, hence necessarily has weight at least $\mathrm{wt}(S)\geq\lfloor n/2\rfloor+1$ (if it contains at least one Z stabilizer, it actually has weight at least $\lceil n/2\rceil+1$). If the weight of M is $\mathrm{wt}(M)=\left\lfloor(\lfloor n/2\rfloor+1)/2\right\rfloor$, then for any S we have $\mathrm{wt}(M\,S)\geq\min(\mathrm{wt}(M),(\lfloor n/2\rfloor+1)-\mathrm{wt}(M))=\mathrm{wt}(M)$. □

The above lemma shows that both the X part M_X and the Z part M_Z each consisting of $\left\lfloor(\lfloor n/2\rfloor+1)/2\right\rfloor$ many X and Z operators of an operator $M=M_X\,M_Z$ are individually incompressible. If M_X and M_Z act on two disjoint sets of sites, and n is even, then $\mathrm{wt}(M)\geq n/2$. Unfortunately, the above lemma is not enough to guarantee that such an M is also

incompressible as a whole. When pushing it into some subset of sites, its X and Z part can in principle start to overlap and thereby its weight can shrink. Our numerical calculations show that M operators exist for which this does not happen up to the largest n that we can check.

In this chapter we were able to find all possible incompressible operators M for all codes with $n =\in \{2, 3, 4, 5, 6, 7, 8\}$ parties. In the next chapter, we present a general construction of an incompressible M operator for a given AME state constructed from MDS code. This provide a systematic method that prove the conjecture (6.1). We call this method modified-Shortening in an analogous way as the Shortening method which constructs new codes from existing ones in the classical case.

6.4. Joint weight enumerator

There is an interesting connection between incompressibility of M matrices that contain both X and Z operators and a concept known as the *joint weight enumerator* of two non-linear codes that are derived from the code generated by the $G_{\lfloor n/2 \rfloor \times n}$ matrix and its dual code with generator matrix $H_{\lceil n/2 \rceil \times n}$. The joint weight enumerator $\mathscr{J}_{\mathscr{A},\mathscr{B}}$ of two classical codes $\mathscr{A}$ and $\mathscr{B}$ is a function of four real variables that encodes information about the overlap of zeros in the codewords of the two codes [MMS72] (see also [MS77, Chapter 5]. To relate this to the situation at hand, let $\mathscr{C}$ be the code generated by the $G_{\lfloor n/2 \rfloor \times n}$ matrix and $\mathscr{C}^\perp$ its dual code with generator matrix $H_{\lceil n/2 \rceil \times n}$. Now let $\mathscr{A}$ be the non-linear MDS code constructed from $\mathscr{C}$ by adding to each codeword the vector of exponents of the X operators in M and $\mathscr{B}$ the non-linear MDS code constructed by adding to each codeword of $\mathscr{C}^\perp$ the vector of exponents of the Z operators. Then the maximum number $i_{\max}$ of positions in which both a codeword from $\mathscr{A}$ and a codeword from $\mathscr{B}$ have zeros is given by

$$i_{\max} = \lim_{a \to \infty} \log \mathscr{J}_{\mathscr{A},\mathscr{B}}(a, 1, 1, 1). \tag{6.25}$$

The minimal weight of the class of operators equivalent to M is given by $n - i_{\max}$.

6.5. Comparison with existing QECCs

Let us return to the QECC we construct and compare its properties to known QECCs. Many other QECC for various combinations of parameters are known (see for example [KKKS06, GR15] for an overview and [Gra] for tables of known codes with $q = 2$). In some cases the achievable distances are limited by $d \leq q$ or some fraction of q [SK05, Theorem 5] or scale only like $\sqrt{n}$ [KKKS06, Theorem 40 and 41]. In general, it is difficult to construct QECC that saturate the quantum Singleton bound and have a large code distances [JX14]. For example in [KKKS06, Corollary 32] a QMDS code with a code distance of the order of $n/2$ was shown

to exist, the proof however requires that q grows faster than exponentially with n. Families of QMDS codes with a code distance up to $d = q + 1$ have been constructed in [JX14, GR15] (for an earlier construction with $d = q$ see [GBR04b]), but all of these (as well as the code from [SK05, Theorem 5] when d is chosen to scale linear with q) have code lengths n that scale quadratically with q.

Our construction only requires $n \leq q + 1$ to achieve a code distance that scales like $n/2$ (or equivalently like $q/2$). We can show the existence of these codes with $n = q + 1$ explicitly for $n = \{4, 6, 8\}$, and in the next chapter when we show that the above conjecture holds true, an infinite family of such codes for arbitrarily large and even n exists. A priory, for physical implementations with independent local noise it appears to be important to achieve a large ratio d/n. In this respect our codes perform well compared with the constructions discussed above. However, in practice, of course, one might rather want to use code especially tailored to the predominant type of noise in a system.

There are two construction that are similar to ours in terms of code parameters. The first was presented in [ABO97] and later used in [CGL99]. It yields QECCs for all prime q with $q > n = 2\,d - 1$. The second is based on [KKKS06, Lemma 70], which shows that the existence of a pure stabilizer QECC $[\![n, k, d]\!]_q$ with $n, d \geq 2$ implies the existence of a code $[\![n - 1, k + 1, d - 1]\!]_q$. The possibility to construct stabilizers for AME states with q prime and the fact that such AME states are QECCs of the form $[\![q + 1, 0, \lfloor (q + 1)/2 \rfloor + 1]\!]_q$ [Sco04, Proposition 3] implies the existence of QECCs of the form $[\![q, 1, \lfloor (q + 1)/2 \rfloor]\!]_q$ for all q prime. The first construction requires $q \geq n+1$ and the second works in the case $q = n$, but neither of the two can straightforwardly be expanded to the case $q = n - 1$. To sum up, as a function of q, there are constructions that achieve larger code distances d and larger k than our proposal, but all such constructions we are aware of require (asymptotically) larger code lengths n.

6.6. Conclusions

For every $n \leq q + 1$ we show how to construct QECCs that encode a logical qudit into a q-dimensional subspace spanned by AME states of n parties with local dimension q prime. Under a conjecture for which we provide numerical evidence and later a proof, this construction produces an infinite family of quantum error correcting codes for $k = 1$ and arbitrary large n that achieve the maximum distance allowed by the quantum Singleton bound, i.e., the no-cloning theorem. For $n \mod 4 = 3$ these codes can correct arbitrary errors on the same number t of subsystems as a QMDS code with the same n and k. We construct such codes for all n up to $n = 8$ by finding suitable incompressible operators. Our proposal has a very clear physical motivation and complements other constructions of non-binary QECC. In particular our construction is very explicit and works with a smaller local dimension q given n than previous codes with similar code parameters.

7. Quantum codes from highly entangled states

7.1. Introduction

Quantum error correction is one of the main challenges in the field of quantum computation and one of our attempts to use multipartite entangled states in applications [Ste96a, Rai99a]. Investigation of the connection between stabilizer quantum codes and existing classical error correcting codes led us to understand the structure of quantum codes [Ste96b, Got09, CRSS98, Sco04]. In particular, there are two well-known methods for constructing stabilizer QECCs. First, a general framework is constructing QECCs from known classical codes and the associated entangled states [RGRA18]. The second method is constructing new codes from existing ones [Got97, CRSS98].

It is now well understood that a given k-UNI state represents a stabilizer QECC [Sco04]. As we discussed before one method of constructing these states is based on the connection between them and MDS codes [RTGA19, Hel13]. This represents a method of constructing QECCs from classical codes (CSS construction Preliminaries section 2.8.4.2). Moreover, the extra knowledge on code parameters of classical codes provides a great advantage to construct quantum codes [Got97].

The second method that simplifies the task of finding quantum codes is to use existing codes to construct new ones. Implementing some modification techniques on a given code can produce new code with different parameters [Got97, CRSS98]. A non trivial manipulation is to remove the last party of a given stabilizer code and convert it into a new code with one fewer party. In this method, the derived code from a stabilizer code is a stabilizer code [Rai99a].

Combining the two methods leads to a family of QECCs. With this technique, one starts from a k-UNI state of n parties and constructs the QECC by taking partial trace over one particle, i.e., generates a code with $n-1$ parties. Repeating this technique produces a family of QECCs with a different set of code parameters [HG20, AR95]. This method can be called *Shortening* which refers to the connection it has with the classical codes and the subspace of constructed quantum codes which are spanned by the highly entangled states [CRSS98, KKKS06, GR15,

SK05].

So far, in the previous literatures, the description of the stabilizer formalism of the codes constructed from the Shortening process was in the center of attention [Got97, AR95]. There, in order to construct the quantum codes one needs to find the generators of stabilizer of the state in the way that one of them ends to X, one other ends to Z and the rest of the stabilizers end $\mathbb{1}$, for details see [Got97]. This could be done more easier for the binary codes but for higher local dimension q finding this specific pattern needs effort. Also, we aim at using quantum codes in quantum communication and computation applications, therefore, we need to know the form of the codewords and logical operators. In this chapter, we work on constructing a set of QECCs starting from a k-UNI states. Unlike previous construction, we present the list of the codewords and logical operators as well as presenting the stabilizer formalism. We also discuss the structure of the highly entangled subspaces of the quantum stabilizer codes.

Moreover, we introduce a new systematic way of constructing quantum codes from existing ones. This method that we call *modified-Shortening*, produce QECCs without removing any party (without taking the partial trace). Therefore, quantum stabilizer codes with larger codespace can be constructed that improve the achievable rate compared with the existing construction. For this, we start from an AME state and without removing any party we construct a QECC whose codewords are all AME states. More precisely, starting from an AME state or alternatively the quantum code $[\![n, 0, \lfloor n/2 \rfloor + 1]\!]_q$, we show how to produce a family of quantum error correcting codes $[\![n, 1, \lfloor n/2 \rfloor]\!]q$. We present the codewords and stabilizer formalism.

7.2. Classical codes, k-uniform states and optimal quantum codes

The Stabilizer QECCs are attractive as they have a close connection with classical linear codes, so that, the knowledge on the code parameters of the classical codes provides a great advantage that one can use to construct quantum codes. We know that k-UNI states of minimal support can be constructed from MDS codes and are a set of stabilizer QECCs [CRSS98, KKKS06, Got97, Got09, Sco04]. Stabilizer quantum codes have also the property that they can be shortened, which means that the existence of a quantum pure stabilizer code (in this case a k-UNI state), implies the existence of a stabilizer QECC with larger code dimension whose spanning vectors are $(k-1)$-UNI states, see [CRSS98, Theorem 6][KKKS06, Lemma 70] and [GR15, SK05]. Shortening process of the quantum stabilizer code $\mathcal{C} = [\![n, 0, k+1]\!]_q$, yields the following code

Proposition 7.1 (Shortening)**.** *The existence of a pure stabilizer code* $[\![n, \tilde{k} = 0, d = k+1]\!]_q$ *associated to a* k-UNI(n, q) *state guarantees the existence of a pure stabilizer QECC,* $[\![n -$

$1, 1, d-1=k]\!]_q$ *with a non-trivial subspace spanned by a set of* $(k-1)$-UNI *states.*

The Shortening process guarantees the construction of a new quantum code from an existing code $\mathcal{C} = [\![n, 0, k+1]\!]_q$ (or k-UNI state) with larger code dimension. Repeating the Shortening process yields codes with $\tilde{k} > 0$ and hence $q^{\tilde{k}} > 1$ dimensional subspace.

7.3. Explicit construction of the Shortening process

After recalling the theory of the Shortening process, in this section we show explicitly how to find the codewords of the quantum codes. For this, unlike the previous works where one needs to find specific patterns for the stabilizers to compute the partial trace, we start from the generator matrix of a given k-UNI state and describe what the partial trace does on the corresponding generator matrix. This leads us to an explicit closed form expression of the codewords and the logical Pauli $\overline{X}$ and $\overline{Z}$ operators of the code. More specifically, we construct the code space of a quantum code $[\![n-r, r, d-r]\!]_q$, with $r > 0$, from a given k-UNI(n, q) state, such that the subspace are spanned by $(k-r)$-UNI states of $n-r$ parties. This construction requires $n - r \leq q + 1$ [GBR04a], which refers to the existence condition of the classical MDS codes.

7.3.1. First step:

As the first step, the Shortening procedure can convert the code $[\![n, 0, k+1]\!]_q$, into a code with parameters $[\![n-1, 1, k]\!]_q$ such that a logical qudit of dimension q is encoded in a q-dimensional subspace spanned by $(k-1)$-UNI states. In the following we show how to find the code space $\mathcal{C} = \text{span}(\{|\psi_m\rangle\}_{m\in[q]})$. We start with the generator matrix $G_{k\times n} = [\mathbb{1}_k | A_{k\times(n-k)}]$ and remove the last row. Because the generator matrix has the standard form, the k-th column of the resulting matrix contains only 0s, so we remove this column too. With these changes the generator matrix now transforms into a matrix of size $(k-1)\times(n-1)$

$$G_{k\times n} = [\mathbb{1}_k | A_{k\times(n-k)}] \;\longrightarrow\; G_{\widehat{k}} = [\mathbb{1}_{k-1} | A_{(k-1)\times(n-k)}]\,, \tag{7.1}$$

where we denote by $G_{\widehat{i}}$ the result of removing the i-th row and column from the original matrix G. $G_{\widehat{k}}$ contains $k-1$ linearly independent columns, therefore $G_{\widehat{k}}$ is a valid generator matrix to construct an MDS code $\mathscr{C} = [n-1, k-1, n-k+1]_q$ (while obviously every square submatrix of $A_{(k-1)\times(n-k)}$ is non-singular). Hence, the state

$$|\psi_0\rangle = \sum_{\vec{v}\in GF(q)^{k-1}} |\vec{v}\, G_{\widehat{k}}\rangle\,, \tag{7.2}$$

is a $(k-1)$-UNI state. Now, we define the operator M which is a string of powers of X where the exponents correspond to the removed last row of matrix G, concretely

$$M \coloneqq \underbrace{\mathbb{1} \otimes \cdots \otimes \mathbb{1}}_{k-1} \otimes \underbrace{X^{a_{k,1}} \otimes X^{a_{k,2}} \otimes \cdots \otimes X^{a_{k,(n-k)}}}_{n-k} \ . \tag{7.3}$$

where we denoted elements of matrix $A_{k\times(n-k)}$ by $a_{i,j}$. In the following lemma, we show how the Pauli string M, defines a QECC made of $(k-1)$-UNI states.

Lemma 7.1. *Consider the* $(k-1)$-UNI *state* $|\psi_0\rangle$*, Eq.* (7.2)*, constructed from the generator matrix* $G_{\widehat{k}}$ *and the* M *operator constructed from the elements of the last row of the* $G_{k\times n}$ *matrix, Eq.* (7.3)*. The subspace* $\mathcal{C} = \mathrm{span}(\{|\psi_m\rangle_{m\in[q]}\}) \subset \mathbb{C}_q^{\otimes n-1}$ *with*

$$|\psi_m\rangle = M^m|\psi_0\rangle \qquad 0 \leq m \leq q-1, \tag{7.4}$$

is a QECC with parameters $[\![n-1, 1, k]\!]_q$*.*

Proof. First of all we need to show that any two codewords from the code space are orthogonal. To do this, we recall that all rows of the $G_{k\times n}$ matrix and every linear combination of them form codewords with specific Hamming distance, $d_H = n-k+1$ [MS77, Chapter 11]. The state $|\psi_0\rangle$ and operator M are formed by combination of the rows of the G matrix after removing the k-th column. Performing the operator M^m for a given $m \in [q]$ on the state $|\psi_0\rangle$ is the same as adding a specific codeword (linear combination of the last row of $G_{k\times n}$) to the set of codewords that form the state $|\psi_0\rangle$. Hence, performing two different M^m and $M^{m'}$ operators for all $m, m' \in [q]$ on the state $|\psi_0\rangle$ produce two states such that

$$\langle\psi_m|\psi_{m'}\rangle = \delta_{m,m'} \tag{7.5}$$

$$\langle\psi_m|W|\psi_{m'}\rangle = 0 \ , \tag{7.6}$$

where $\mathrm{wt}(W) < d_H - 1 = n-k$. Note that all the states $|\psi_m\rangle$ are $(k-1)$-UNI, as acting with local unitaries does not change the entanglement properties.

The code space $\mathcal{C} = \mathrm{span}\{|\psi_m\rangle\}$ is a QECC if and only if it satisfies two conditions. (i) In the presence of errors one should be able to distinguish two different codewords [Got09, Got97]. Considering this, Eq. (7.6) implies that the minimum number of single-qudit operations that are needed to create a non-zero overlap between any two orthogonal states is $n-k$. Therefore, for all errors E and F with weight such that $1 < \mathrm{wt}(E^\dagger F) < n-k$ and all $m, m' \in [q]$ with $m \neq m'$ we have

$$\langle\psi_m|E^\dagger F|\psi_{m'}\rangle = 0 \ . \tag{7.7}$$

The above condition is a direct consequence of the fact that the minimum distance between

two different codewords $|\psi_m\rangle$ and $|\psi_{m'}\rangle$ is $d_H - 1 = n - k$. (ii) In addition, one should also be able to distinguish different errors when they act non-trivially on a given codeword $|\psi_m\rangle$ (see Eq. (28) of [Got09]). As the states $|\psi_m\rangle$ for every $m \in [q]$, are $(k-1)$-UNI state, then one gets

$$\langle\psi_m|E^\dagger F|\psi_m\rangle = \mathrm{Tr}(E^\dagger F) = 0 \ , \qquad \forall m \in [q] \ . \tag{7.8}$$

for errors $E^\dagger F$ that act non-trivially on any subset of less than $k-1$ sites, i.e., $\mathrm{wt}(E^\dagger F) < k-1$. As we always have $n-k \geq k-1$, then, considering the conditions (i) and (ii) the code distance is $d = \min(n-k+1, k) = k$. By the definition Eq. (2.48), one can conclude that the subspace $\mathcal{C}$ is a $[\![n, 1, d = k]\!]_q$ QECC. □

As a side remark, note that if the M operator, (7.3), contains only k of the X operators with the vector of exponents described above, the distance of the code is still $d = k$. The stabilizer formalism is presented in Appendix A.1.

Now that the codewords and the code distance are determined, we can find logical $\overline{X}$ and $\overline{Z}$ operators. Logical Pauli operators are unitary operators which act non-trivially on the codeword space or logical states $|\psi_m\rangle$, but preserve it. The logical Pauli operators $\overline{X}$ and $\overline{Z}$ preserve the codeword space since they commute with all the stabilizer generators. The logical operators anti-commute with each other. It can always be useful if one expresses $\overline{X}$ and $\overline{Z}$ in terms of their action as Pauli operators X and Z on the physical qudits used in codespace.

In the Shortening construction, the logical qudits are the set of the states $\{|\psi_m\rangle\}_{m\in[q^k]}$, Eq. (7.4), which are constructed by performing the powers of M operator on the state $|\psi_0\rangle$. This shows that the M operator is the logical $\overline{X}$ pauli operator that by starting from the logical qudit $|\psi_0\rangle$, Eq. (7.2), it can construct entire codespace

$$\overline{X}^m|\psi_0\rangle \equiv M^m|\psi_0\rangle = |\psi_m\rangle \ , \tag{7.9}$$

for all $m \in [q^m]$. In this construction, we started from a k-UNI state constructed from MDS code that has stabilizers involving X or Z operators, namely X stabilizers or Z stabilizers respectively. The X stabilizers are powers of X where the exponents corresponding to every row of the generator matrix $G_{k\times n} = [\mathbb{1}_k|A]$, and the Z stabilizers are Z Pauli string that the exponents correspond to the rows of parity check matrix $H = [A^T|\mathbb{1}_{n-k}]$ (for more details see Chapter 4.6). After eliminating one row and column of the G matrix to construct the M (or logical $\overline{X}$) operator, the stabilizer that corresponds to the last row of matrix H does not commute with M any more while it communicates with the rest of the stabilizers. Therefore, $\overline{Z}$ is a string of powers of Z where the exponents correspond to the last row of the parity check

matrix $H_{(n-k)\times k} = [A^T|\mathbb{1}_{n-k}]$ when the k-th column is removed, i.e.,

$$\overline{Z} \coloneqq \underbrace{Z^{-a_{1,(n-k)}} \otimes Z^{-a_{2,(n-k)}} \otimes \cdots \otimes Z^{-a_{(k-1),(n-k)}}}_{k-1} \otimes \underbrace{\mathbb{1} \otimes \cdots \otimes \mathbb{1} \otimes Z}_{n-k} \ . \tag{7.10}$$

7.3.2. Second step:

The second step of the Shortening procedure converts the code $[\![n-1, 1, k]\!]_q$, into a code with parameters $[\![n-2, 2, k-1]\!]_q$ with a q^2-dimensional subspace spanned by $(k-2)$-UNI states. For that we proceed in a similar way and remove the $k-1$ and the k-th columns and rows of the original generator matrix

$$G_{k\times n} = [\mathbb{1}_k|A_{k\times(n-k)}] \ \longrightarrow \ G_{\widehat{k-1},\widehat{k}} = [\mathbb{1}_{k-2}|A_{(k-2)\times(n-k)}] \ . \tag{7.11}$$

The structure is the same as the first step, and hence, it is obvious that $G_{\widehat{k-1},\widehat{k}}$ is the generator matrix of an MDS code $[n-2, k-2, n-k+1]_q$. Therefore, a $(k-2)$-UNI state $|\psi_{00}\rangle$ can be constructed via

$$|\psi_{00}\rangle = \sum_{\vec{v}\in GF(q)^{k-2}} |\vec{v}\, G_{\widehat{k-1},\widehat{k}}\rangle \ . \tag{7.12}$$

Two Pauli strings M_1 and M_2 that involve X operators can be defined such that the vector of exponents are the $k-1$ and the k-th rows of matrix $G_{k\times n}$ while both the $k-1$ and k-th columns are removed:

$$M_1 \coloneqq \underbrace{\mathbb{1} \otimes \cdots \otimes \mathbb{1}}_{k-2} \otimes \underbrace{X^{g_{k-1,1}} \otimes X^{g_{k-1,2}} \otimes \cdots \otimes X^{g_{k-1,(n-k)}}}_{n-k} \tag{7.13}$$

$$M_2 \coloneqq \underbrace{\mathbb{1} \otimes \cdots \otimes \mathbb{1}}_{k-2} \otimes \underbrace{X^{g_{k,1}} \otimes X^{g_{k,2}} \otimes \cdots \otimes X^{g_{k,(n-k)}}}_{n-k} \ . \tag{7.14}$$

Finally, the code space $\mathcal{C}$ is spanned by the $(k-2)$-UNI states

$$|\psi_{m_1,m_2}\rangle = M_1^{m_1} M_2^{m_2} |\psi_{00}\rangle \qquad 0 \le m_1, m_2 \le q-1 \ . \tag{7.15}$$

By the same argument as above, the fact that the state $|\psi_{00}\rangle$ and operators M_1 and M_2 are linear combination of the rows of the matrix $G_{k\times n}$ (or codewrods of the MDS code $[n, k, n-k+1]_q$), where two parties are removed, leads us to the first Knill-Laflamme condition (i):

$$\langle\psi_{m_1,m_2}|\psi_{m_1',m_2'}\rangle = \delta_{m_1,m_1'}\delta_{m_2,m_2'} \tag{7.16}$$

$$\langle\psi_{m_1,m_2}|E^\dagger F|\psi_{m_1',m_2'}\rangle = 0 \ , \tag{7.17}$$

with $\mathrm{wt}(E^\dagger F) < d_H - 2 = n - k - 1$. The second condition can be satisfied because: (ii) the subspace $\mathcal{C}$ is manifestly spanned by orthogonal $(k-2)$-UNI states $|\psi_{m_1,m_2}\rangle$ so that,

$$\langle\psi_{m_1,m_2}|E^\dagger F|\psi_{m_1,m_2}\rangle = \mathrm{Tr}(E^\dagger F) = 0\,, \tag{7.18}$$

for $\mathrm{wt}(E^\dagger F) < k-2$. This implies that the code distance of the QECC with code space $\mathcal{C} = \mathrm{span}\{|\psi_{m_1,m_2}\rangle\}$ is $d = \min(n-k, k-1) = k-1$.

The two operators M_1 and M_2, Eqs. (7.13) and (7.14), are the logical $\overline{X}$ operators for the two qudits of the code. And the logical $\overline{Z}$ operators are Pauli strings of powers Z where the exponents correspond to rows $n-k$- and $n-k-1$-th of matrix H. More specifically the two operators

$$\overline{Z}_1 \coloneqq \underbrace{Z^{-a_{1,(n-k-1)}} \otimes Z^{-a_{2,(n-k-1)}} \otimes \cdots \otimes Z^{-a_{(k-1),(n-k-1)}}}_{k-1} \otimes \underbrace{\mathbb{1} \otimes \cdots \otimes Z \otimes \mathbb{1}}_{n-k} \tag{7.19}$$

$$\overline{Z}_2 \coloneqq \underbrace{Z^{-a_{1,(n-k)}} \otimes Z^{-a_{2,(n-k)}} \otimes \cdots \otimes Z^{-a_{(k-1),(n-k)}}}_{k-1} \otimes \underbrace{\mathbb{1} \otimes \cdots \otimes \mathbb{1} \otimes Z}_{n-k}\,, \tag{7.20}$$

commute with all the stabilizers, yet anti-commute with M_1 and M_2.

As an example of our construction, we start with $\mathrm{AME}(6,5)$ which is constructed from an MDS code $[6,3,4]_5$, over $GF(5)$ [RGRA18]. The generator matrix $G_{3\times 6}$ of the MDS code, and the reduced generator matrix $\overline{G}_{2\times 5}$ are

$$G_{3\times 6} = \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 1 & 3 & 4 \end{array}\right] \longrightarrow G_{\widehat{3}} = \left[\begin{array}{cc|ccc} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 2 & 3 \end{array}\right]\,. \tag{7.21}$$

Matrix $G_{\widehat{3}}$ is the generator matrix of an MDS code $[5,2,4]_5$. After the second step we get

$$G_{3\times 6} = \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 1 & 3 & 4 \end{array}\right] \longrightarrow G_{\widehat{3,2}} = \left[\begin{array}{c|ccc} 1 & 1 & 1 & 1 \end{array}\right]\,, \tag{7.22}$$

which is the generator matrix of the code $[4,1,4]_5$. By taking the coherent superposition of its codeworks one has the 1-UNI state of 4 parties

$$|\psi_{00}\rangle = \sum_{\vec{v}\in GF(5)} |\vec{v}\,G_{\widehat{3,2}}\rangle = \sum_{i=0}^{4} |i,i,i,i\rangle\,. \tag{7.23}$$

Starting point:		Step 1:		Step 2:
k-UNI state $\equiv [\![n, 0, k+1]\!]_q$	$\longrightarrow$	$[\![n-1, 1, k]\!]_q$	$\longrightarrow$	$[\![n-2, 2, k-1]\!]_q$
1-dimensional subspace		q-dimensional subspace		q^2-dimensional subspace
		$(k-1)$-UNI states		$(k-2)$-UNI states

		Step r:				Step $k-1$:
$\longrightarrow$	$\ldots$	$[\![n-r, r, k-r+1]\!]_q$	$\longrightarrow$	$\ldots$	$\longrightarrow$	$[\![n-k+1, k-1, 2]\!]_q$
		q^r-dimensional subspace				q^{k-1}-dimensional subspace
		$(k-r)$-UNI states				1-UNI states

Table 7.1.: Shortening process: List of the stabilizer QECCs one can construct from a given k-UNI state.

As it is discussed above in this case there are two operators

$$M_1 = \mathbb{1} \otimes X \otimes X^2 \otimes X^3 \tag{7.24}$$

$$M_2 = \mathbb{1} \otimes X \otimes X^3 \otimes X^4 \,. \tag{7.25}$$

States $|\psi_{m_1,m_2}\rangle = M_1^{m_1} M_2^{m_2} |\psi_{00}\rangle$, where $0 \leq m_1, m_2 \leq q-1$ form the subspace $\mathcal{C} = \mathrm{span}(|\psi_{m_1,m_2}\rangle)$, which is a QECC with parameters $[\![4, 2, 2]\!]_5$. And the logical $\overline{Z}$ operators are

$$\overline{Z}_1 = Z^4 \otimes \mathbb{1} \otimes Z \otimes \mathbb{1} \tag{7.26}$$

$$\overline{Z}_2 = Z^4 \otimes \mathbb{1} \otimes \mathbb{1} \otimes Z \,. \tag{7.27}$$

which are the last two rows of the parity check matrix $H_{3\times 6} = G_{3\times 6}^T$ when the second and third columns are removed.

In general, the Shortening procedure can be repeated $k-1$ times and codes with fewer particles and higher code dimension $\tilde{k}$ can be obtained (see Table 7.1). Note that these codes can be optimal, saturating the quantum Singleton bound, only if $k = \lfloor n/2 \rfloor$. For that the starting point should be an AME state.

7.4. Optimal quantum codes from AME states without tracing out particles

Shortening is an example of a method of finding new QECCs from existing ones. The structure of the Shortening process is based on removing one particle (taking partial trace) from a given stabilizer QECC at each step. In the previous section, we introduced a different view of constructing new QECCs from a k-UNI state, that allows us to produce codewords and study the structure of the code space. In this section, we discuss a method of constructing new codes from previous ones without tracing out any parties starting from an AME state. We name this

method modified-Shortening. To introduce the method, we first review a systematic way of constructing generator matrices to construct classical MDS codes which provide explicit constructions and closed form expressions for AME states, i.e., $k = \lfloor n/2 \rfloor$ -UNI, or code $[\![n, 0, \lfloor n/2 \rfloor + 1]\!]_q$. Then we present the modified-Shortening which is a systematic method to construct QECC with parameters $[\![n, 1, \lfloor n/2 \rfloor]\!]_q$ from an AME state defined by an MDS.

In chapter 3 we defined the Singleton array for any finite field $GF(q)$

$$
S_q \coloneqq \begin{array}{cccccc|ccc}
1 & 1 & 1 & \dots & 1 & 1 & \dots & 1 & 1 \\
1 & a_1 & a_2 & \dots & a_{\lfloor q/2 \rfloor - 1} & a_{\lfloor q/2 \rfloor} & \dots & a_{q-2} & \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & & & \\
1 & a_{\lceil q/2 \rceil - 1} & a_{\lceil q/2 \rceil} & \dots & a_{q-3} & a_{q-2} & \longrightarrow & A & \\
\hline
1 & a_{\lceil q/2 \rceil} & a_{\lceil q/2 \rceil + 1} & \dots & a_{q-2} & & \longrightarrow & \text{use for} & \mathcal{M} \\
\vdots & \vdots & & & & & & & \\
1 & a_{q-2} & & & & & & & \\
1 & & & & & &
\end{array} ,
$$

with

$$
a_i \coloneqq \frac{1}{1 - \gamma^i} , \tag{7.28}
$$

We discussed that by taking rectangular sub-matrix A, a suitable generator matrix $G = [\mathbb{1}|A]$ for an MDS code can be constructed. The largest A matrix this method constructs over $GF(q)$ has size $\left\lfloor \frac{q+1}{2} \right\rfloor \times \left\lceil \frac{q+1}{2} \right\rceil$. By taking $n = q + 1$, one can construct the generator matrix $G_{\lfloor n/2 \rfloor \times n} = [\mathbb{1}|A]$ and hence an MDS code with parameters $[n, \lfloor n/2 \rfloor, \lceil n/2 \rceil + 1]_q$. The corresponding AME state $|\phi_0\rangle$ has the closed form expression (chapter 3)

$$
|\phi_0\rangle = \sum_{\vec{v} \in GF(q)^{\lfloor n/2 \rfloor}} |\vec{v} G_{\lfloor n/2 \rfloor \times n}\rangle . \tag{7.29}
$$

Now, we consider the $\lfloor (q+1)/2 \rfloor + 1$-th row of the Singleton array S_q containing $\lceil (q+1)/2 \rceil - 1$ elements $(1, a_{\lceil q/2 \rceil}, a_{\lceil q/2 \rceil + 1}, \dots, a_{q-2})$. Using this, we define the Pauli string $\mathcal{M}$ of length n, such that, the first $\lfloor n/2 \rfloor$ elements are identity matrices (as we have in each row of the generator matrix $G_{\lfloor n/2 \rfloor \times n}$), the vector of exponents of the X operators is the $\lfloor (q+1)/2 \rfloor + 1$-th row of S_q, and it contains one Z operator as the n-th element, i.e.,

$$
\mathcal{M} \coloneqq \underbrace{\mathbb{1} \otimes \cdots \otimes \mathbb{1}}_{\lfloor \frac{n}{2} \rfloor} \otimes \underbrace{X \otimes X^{a_{\lceil q/2 \rceil}} \otimes X^{a_{\lceil q/2 \rceil + 1}} \otimes \cdots \otimes X^{a_{q-2}}}_{\lceil \frac{n}{2} \rceil - 1} \otimes Z , \tag{7.30}
$$

where $n = q + 1$. In the following lemma we show that the AME states generated by acting with the Pauli string $\mathcal{M}$ onto the state $|\phi_0\rangle$, Eq. (7.29) from a QECC with parameters

$[\![n, 1, \lfloor n/2 \rfloor]\!]_q$.

Lemma 7.2. *From the AME state $|\phi_0\rangle$, or equivalently quantum code $[\![n, 0, \lfloor n/2 \rfloor + 1]\!]_q$, Eq.* (7.29)*, a QECC with parameters $[\![n, 1, \lfloor n/2 \rfloor]\!]_q$ can be constructed defined by the subspace $\mathcal{C} = \operatorname{span}(\{|\phi_m\rangle_{m \in [q]}\}) \subset \mathbb{C}_q^{\otimes n}$ with*

$$|\phi_m\rangle \coloneqq \mathcal{M}^m |\phi_0\rangle \qquad 0 \leq m \leq q-1\,. \tag{7.31}$$

All $|\phi_m\rangle$ are AME states of n parties with $n = q+1$.

Proof. The Codewords are produced by applying the $\mathcal{M}^m$ operators for $m \in [q]$ on the AME state $|\phi_0\rangle$. $\mathcal{M}$ contains X operators with the vector of exponents $\lfloor (q+1)/2 \rfloor + 1$-th row of S_q and one Z operator. More explicitly, $\mathcal{M} = M_X\, M_Z$ where,

$$M_X \coloneqq \underbrace{\mathbb{1} \otimes \cdots \otimes \mathbb{1}}_{\lfloor \frac{n}{2} \rfloor} \otimes \underbrace{X \otimes X^{a_{\lceil q/2 \rceil}} \otimes \cdots \otimes X^{a_{q-2}}}_{\lceil \frac{n}{2} \rceil - 1} \otimes \mathbb{1} \tag{7.32}$$

$$M_Z \coloneqq \underbrace{\mathbb{1} \otimes \mathbb{1} \otimes \mathbb{1} \cdots \otimes \mathbb{1} \otimes \mathbb{1} \otimes \mathbb{1} \otimes \cdots \otimes \mathbb{1} \otimes \mathbb{1}}_{n-1} \otimes Z\,. \tag{7.33}$$

For the purpose of the proof we discuss how M_X and M_Z act on the state $|\phi_0\rangle$ separately.

First, we show that the application of M_X^m for $m \in [q]$ provides states with distance $\lceil n/2 \rceil - 1$. To do this, we take sub-matrix $A'_{(\lfloor \frac{q+1}{2} \rfloor + 1) \times (\lceil \frac{q+1}{2} \rceil - 1)}$

$$S_q = \begin{array}{cccccccccc}
1 & 1 & 1 & \ldots & 1 & 1 & \ldots & 1 & 1 \\
1 & a_1 & a_2 & \ldots & a_{\lfloor q/2 \rfloor - 1} & a_{\lfloor q/2 \rfloor} & \ldots & a_{q-2} & \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & & & \\
1 & a_{\lceil q/2 \rceil - 1} & a_{\lceil q/2 \rceil} & \ldots & a_{q-3} & a_{q-2} & & & \\
1 & a_{\lceil q/2 \rceil} & a_{\lceil q/2 \rceil + 1} & \ldots & a_{q-2} & & \searrow & & \\
\vdots & \vdots & & & \downarrow & & & A & \\
1 & a_{q-2} & & & A' & & & & \\
1 & & & & & & & &
\end{array},$$

of S_q. Comparing it with the largest submatrix A of size $\left\lfloor \frac{q+1}{2} \right\rfloor \times \left\lceil \frac{q+1}{2} \right\rceil$, the matrix A' contains one more row and one less column. Using A', one can construct the generator matrix $G'_{(\lfloor n/2 \rfloor + 1) \times n} = [\mathbb{1}_{\lfloor n/2 \rfloor + 1} | A']$ and MDS code $\mathscr{C}' = [n, \lfloor n/2 \rfloor + 1, \lceil n/2 \rceil]_q$. After one step of

Shortening we get

$$G'_{(\lfloor n/2\rfloor+1)\times n} = [\mathbb{1}_{\lfloor n/2\rfloor+1} \mid A'_{(\lfloor \frac{q+1}{2}\rfloor+1)\times(\lceil \frac{q+1}{2}\rceil-1)}] \longrightarrow G'_{\widehat{\lfloor \frac{n}{2}\rfloor+1}} = [\mathbb{1}_{\lfloor n/2\rfloor} \mid A'_{\lfloor \frac{q+1}{2}\rfloor\times(\lceil \frac{q+1}{2}\rceil-1)}] , \tag{7.34}$$

which is the generator matrix of an MDS code $[n-1, \lfloor n/2\rfloor, \lceil n/2\rceil]_q$. Hence, an AME state $|\psi'_0\rangle$ of $n-1$ parties can be written as

$$|\psi'_0\rangle = \sum_{\vec{v}} |\vec{v}\, G'_{\widehat{\lfloor \frac{n}{2}\rfloor+1}}\rangle . \tag{7.35}$$

$G'_{\widehat{\lfloor \frac{n}{2}\rfloor+1}}$ is the same generator matrix as $G_{\lfloor n/2\rfloor\times n} = [\mathbb{1}|A]$ if one deletes the last column, as well as the state $|\psi'_0\rangle$ is the same as state $|\phi_0\rangle$, Eq. (7.29), without considering the last party. As we discussed in the Shortening procedure, the M operator that produces a subspace with specific distance d is a string of only powers of the X operators with the vector of exponents defined by the last row of the generator matrix. In this case, M is the Pauli string of X operators with the exponent vector $(\lfloor (q+1)/2\rfloor+1)$-th row of S_q. Therefore, M contains the first $n-1$ Pauli operators in M_X, Eq. (7.32). We can get the set of states

$$|\psi'_m\rangle = M^m |\psi'_0\rangle \qquad 0 \le m \le q-1 . \tag{7.36}$$

The same proof as that of Lemma 7.1 establishes that the distance between every two different states of the above set of states is $d_H - 1 = \lceil n/2\rceil - 1$. This shows that because $|\psi_m\rangle$ is the same as $|\phi_m\rangle$ if one removes the last party, the distance between any two states $|\phi_m\rangle$ and $|\phi_{m'}\rangle$ is at least $d = \lceil n/2\rceil - 1$.

Let us now consider the operator M_Z, Eq. (7.33). For two different powers m and m', performing M_Z^m and $M_Z^{m'}$ on the state $|\phi_0\rangle$ increases the distance by one, because it adds different phases for different powers m and m'. Therefore, for two different codewords, we have

$$\langle\phi_m|E^\dagger F|\phi_{m'}\rangle = 0 \qquad \text{if} \;\; \mathrm{wt}\,(E^\dagger F) < \lceil n/2\rceil \;\; . \tag{7.37}$$

This is one of the Knill-Laflamme conditions Eq. (2.48), in which two different codewords should be distinguishable in the presence of errors that act non-trivially on $\mathrm{wt}\,(E^\dagger F) < d$ sites.

Moreover, errors E and F should not be able to change an encoded state for the weight $\mathrm{wt}\,(E^\dagger F) < d$, i.e., for two given codewords it is necessary to have $\langle\phi_m|E^\dagger F|\phi_m\rangle = \langle\phi_{m'}|E^\dagger F|\phi_{m'}\rangle$. As the unitary operator $\mathcal{M}$ is local, its application does not change the entanglement properties of a state, therefore all the states $|\phi_m\rangle$ are AME states, then

$$\langle\phi_m|E^\dagger F|\phi_m\rangle = \mathrm{Tr}\,(E^\dagger F) = 0 \qquad \forall m \in [q] , \tag{7.38}$$

Shortening

$\mathrm{AME}(n,q)$	$\longrightarrow$	$[\![n-1,1,\lfloor n/2\rfloor]\!]_q$	q-dimensional Subspace
$[\![4,0,3]\!]_{q\geq 3}$	$\longrightarrow$	$[\![3,1,2]\!]_{q\geq 3}$	$\mathrm{AME}(3,q)$
$[\![5,0,3]\!]_{q\geq 4}$	$\longrightarrow$	$[\![4,1,2]\!]_{q\geq 4}$	1-$\mathrm{UNI}(4,q)$
$[\![6,0,4]\!]_{q\geq 4}$	$\longrightarrow$	$[\![5,1,3]\!]_{q\geq 4}$	$\mathrm{AME}(5,q)$
$[\![7,0,4]\!]_{q\geq 7}$	$\longrightarrow$	$[\![6,1,3]\!]_{q\geq 7}$	2-$\mathrm{UNI}(6,q)$
$[\![8,0,5]\!]_{q\geq 7}$	$\longrightarrow$	$[\![7,1,4]\!]_{q\geq 7}$	$\mathrm{AME}(7,q)$
$[\![9,0,5]\!]_{q\geq 8}$	$\longrightarrow$	$[\![8,1,4]\!]_{q\geq 8}$	3-$\mathrm{UNI}(8,q)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$[\![n,0,\left\lfloor\frac{n}{2}\right\rfloor+1]\!]_{q\geq n-1}$	$\longrightarrow$	$[\![n-1,1,\left\lfloor\frac{n}{2}\right\rfloor]\!]_{q\geq n-1}$	$\left\lfloor\frac{n-2}{2}\right\rfloor$-$\mathrm{UNI}(n-1,q)$

Modified-Shortening

$\mathrm{AME}(n,q)$	$\longrightarrow$	$[\![n,1,\lfloor n/2\rfloor]\!]_q$	q-dimensional Subspace
$[\![4,0,3]\!]_{q\geq 3}$	$\longrightarrow$	$[\![4,1,2]\!]_{q\geq 3}$	$\mathrm{AME}(4,q)$
$[\![5,0,3]\!]_{q\geq 4}$	$\longrightarrow$	$[\![5,1,2]\!]_{q\geq 4}$	$\mathrm{AME}(5,q)$
$[\![6,0,4]\!]_{q\geq 4}$	$\longrightarrow$	$[\![6,1,3]\!]_{q\geq 4}$	$\mathrm{AME}(6,q)$
$[\![7,0,4]\!]_{q\geq 7}$	$\longrightarrow$	$[\![7,1,3]\!]_{q\geq 7}$	$\mathrm{AME}(7,q)$
$[\![8,0,5]\!]_{q\geq 7}$	$\longrightarrow$	$[\![8,1,4]\!]_{q\geq 7}$	$\mathrm{AME}(8,q)$
$[\![9,0,5]\!]_{q\geq 8}$	$\longrightarrow$	$[\![9,1,4]\!]_{q\geq 8}$	$\mathrm{AME}(9,q)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$[\![n,0,\left\lfloor\frac{n}{2}\right\rfloor+1]\!]_{q\geq n-1}$	$\longrightarrow$	$[\![n,1,\left\lfloor\frac{n}{2}\right\rfloor]\!]_{q\geq n-1}$	$\mathrm{AME}(n,q)$

Table 7.2.: Comparison between code parameters and subspaces one can construct starting from $\mathrm{AME}(n,q)$ state over $GF(q)$, Eq. (7.29), using Shortening and modified-Shortening processes.

for $\mathrm{wt}\,(E^\dagger F) < \lfloor n/2\rfloor$. In general, based on the knill-Laflamme condition the subspace $\mathcal{C} = \mathrm{span}(\{|\phi_m\rangle_{m\in[q]}\})$ is a QECC $[\![n,1,\lfloor n/2\rfloor]\!]_q$. □

In Table 7.2 we compare the QECCs one can construct from AME state $|\phi_0\rangle$ Eq.(7.29), using the Shortening and modified-Shortening processes. We can see that the modified-Shortening provides quantum codes with smaller local dimension q given n than previous codes. With this method we also provide explicit codewords besides stabilizer formalism.

7.5. Conclusions

In this chapter we have studied the relation between classical optimal codes, maximally multipartite entangled states, and quantum error correcting codes. This study, in general, can lead to the construction of optimal quantum error correcting codes from highly entangled subspaces. We discussed a method that starts from a k-UNI state and by removing one party constructs a set of stabilizer QECCs. Our construction provided the list of codewords besides presenting the stabilizer formalism. Along the way, we have also shown that this method

can be iterated and how to find the codewords in each step. Then, we extended the connection between classical codes, k-UNI states and quantum codes to provide codes with larger code subspace compared with the existing constructions. We have shown how to modify the method to produce QECCs starting from an AME state without removing any party. Our method, called the Modified-Shortening construction, is explicit, physically motivated and works with a smaller local dimension than previous codes. This has led to a proof for the conjecture of the previous chapter, Conjecture (6.1), therefore to a method of constructing stabilizer QECCs $[\![n, 1, \lfloor n/2 \rfloor]\!]_q$ starting from AME state or quantum code $[\![n, 0, \lfloor n/2 \rfloor + 1]\!]_q$.

8. Conclusions and outlook

Quantum information science is the research field that has become an active research area in the last two decades. There, entanglement is recognized to be one of the key resources for quantum information tasks. The theory of multipartite entangled states plays important roles in many fields of physics which deal with many-body systems like quantum optics, high energy physics, and condensed matter physics. In quantum information science itself multipartite entanglement plays an essential role in quantum communication and computation,for instance in measurement-based quantum computation, metrology, quantum error correction, secret sharing, multi-party teleportation, and quantum networks.

This thesis deals with three main topics. The first is the connection between classical error correcting codes and highly entangled k-uniform (or for short k-UNI) states which leads us to construct complete orthonormal basis made of these states and providing their stabiliser formalism. This also provides necessary ingredients to present a systematic method to construct other examples of k-UNI states and show that the states derived through our construction are not equivalent to any k-UNI state constructed from classical error correction codes. Furthermore, we use this method to construct several examples of absolutely maximally entangled states whose existence was open so far. The second main topic is studying combinatorial designs and introducing a class of quantum combinatorial designs called quantum orthogonal arrays (QOA). Finally, the third topic is quantum error correcting codes, whose code spaces are spanned by highly entangled quantum states.

Our results provide new methods to study and insights into quantum many body physics. In the following we briefly review the main conclusions of this thesis.

8.1. Constructing AME states from MDS codes

Presenting the closed form expression, stabiliser formalism, graph state representation and complete orthonormal basis of maximally multipartite entangled states gives a better understanding of the non-local properties of quantum states and also a better view for quantum applications. In chapter 3, we explored the relation between AME states, which have the property that all reduced states of at most half the system size are maximally mixed, and classical error correcting codes. This relation allowed us to systematically construct AME states.

We showed that k-UNI states derived through our constructions are stabiliser states. Further, we showed how starting from an AME state one can construct a complete orthonormal basis of AME states. These results can also be found in [RGRA18].

AME states are pure multi-partite generalizations of the bipartite maximally entangled states that will play important roles in many applications. Thus, an important line for future research is finding AME states of n parties and local dimension q that belong to different local unitary (LU) classes. So far, as an example we could find two non-LU equivalent $\mathrm{AME}(5, q)$ states for $GF(q)$ for $q > 4$ [BR20]. This will also lead us to study the graph states of AME states that belong to different LU-equivalent classes.

8.2. New construction for k-UNI and absolutely maximally entangled states

In chapter 4, we have presented a method that combines a classical error correcting code with a basis of k-UNI states to generate a set of k-UNI states. The obtained states are examples of non-minimal support k-UNI states. The structure and associated ingredients we used in our method prove to be particularly fruitful in understanding the structure of these quantum states, and their graph-state representation. This shows the difference between our method from the other systematic construction previously known.

In fact, we showed our construction provides states that cannot be obtained from any state of minimal support by SLOCC and have a different graph-state representation. Another advantage is that our method constructs k-UNI states of n parties with smaller local dimensions q compared to the existing methods. Finally, some examples of AME states with its closed expression, such as $\mathrm{AME}(19, 17)$, $\mathrm{AME}(21, 19)$ and $\mathrm{AME}(7, 4)$ are presented that were unknown so far. These results can also be found in [RTGA19].

We know that changing a given graph state corresponds to performing controlled-Z operator on two parties. In this chapter, we showed that k-UNI state of minimal support can be represented by a complete bipartite graph. One future research is to study the manipulations that one can implement in this graph such that the entanglement property does not change or increases in some cases.

8.3. Entanglement and quantum combinatorial designs

It is always important to explore the connection between related scientific areas like mathematics and quantum physics. This is particularly important because there are lots of overlaps

between them that allow designing methods to construct and study quantum states and their applications.

In chapter 5 we have introduced several classes of quantum combinatorial designs, namely quantum Latin squares, cubes, hypercubes and a notion of orthogonality between them. We have also introduced quantum orthogonal arrays (QOA), generalizing all previous classes of designs. We showed that there is a one to one correspondence between QOA and k-UNI states. We presented new mathematical tools and described original techniques to construct multipartite quantum states with remarkable properties. And then, we summarized the existing relations between the studied concepts and the results derived along the work. These results can also be found in [GRDMZ18].

It is well known that OAs can be classified into two classes, irredundant (IrOA) and redundant (simply denoted as OA). In chapter 5, our main focus was presenting the notion of QOAs and using them to construct k-UNI states, so we didn't introduce any classification for QOAs. In the future, we want to study on different classes of QOAs and present a way of constructing them by concatenating two orthogonal arrays (OA) or one OA and one quantum Latin square (QLS). This might have some overlaps between the results we got in chapter (4), but it can be useful to construct more examples of QOAs, also it will lead to different classes of QOAs, like irredundant QOAs like the classical counterpart [GZ14].

8.4. Optimal quantum error correcting codes from absolutely maximally entangled states

In chapter 6, we explored aspects of multipartite entanglement by drawing connections to quantum error correcting codes. A QECC distinguishes a code space of the Hilbert space of a physical system as the space of admissible code states, that is, quantum states of the system that are in a one to one correspondence (via the encoding and decoding maps) with the messages. For the code to be useful, the code space must be chosen such that the expected errors never map a state from the code space to another state. Moreover, it should always take the state out of the code space in such a way that a subsequent correction can bring the system back into its original state.

In the theory of QECCs, stabilisers are a useful tool to construct and analyse codes. The stabiliser group of a code space is the abelian sub-group of the Pauli group that leaves every element from the code space invariant. Conversely every abelian sub-group of the Pauli group that does not contain $-\mathbb{1}$ has a non-trivial subspace spanned by computational basis states that is left invariant.

In this chapter, under a conjecture for which we provide numerical evidence, this construction

produces an infinite family of quantum error correcting codes for $\tilde{k} = 1$ and arbitrary large n that achieve the maximum distance allowed by the quantum Singleton bound, i.e., the no-cloning theorem. For n mod 4 = 3 these codes can correct arbitrary errors on the same number t of subsystems as a QMDS code with the same n and $\tilde{k}$. These results can also be found in [RGRA18].

8.5. Quantum codes from highly entangled states

In chapter 7, we focused more on the remarkable relation between classical optimal codes, maximally multipartite entangled states, and quantum error correcting codes. This study, in general, can lead to the construction of optimal quantum error correcting codes from highly entangled subspaces. We have presented a method that starts from a k-UNI state and by removing one party constructs a set of stabiliser QECCs. Our construction provided the list of codewords besides presenting the stabiliser formalism. We extended the connection between classical codes, k-UNI states and quantum codes to provide codes with larger code subspace compared to the existing constructions. We have shown how to modify this method to produce QECCs starting from an AME state without removing any party. Our method, called the Modified-Shortening construction, is explicit, physically motivated and works with a smaller local dimension than previous codes with similar parameters. This has led us to construct stabiliser QECCs starting from AME states that encode q logical qudits into a subspace spanned by AME states, i.e., constructing quantum codes with parameters $[\![n, 1, \lfloor n/2 \rfloor]\!]_q$ starting from an AME state or alternatively quantum code $[\![n, 0, \lfloor n/2 \rfloor + 1]\!]_q$. These results can also be found in [Rai20].

Using the modified-Shortening method we can construct $[\![n, 1, \lfloor n/2 \rfloor]\!]_q$ from a given AME state constructed from MDS codes. In the future, we want to take r steps forward and construct QECCs with code parameters $[\![n, r, \lfloor n/2 \rfloor + 1 - r]\!]_q$.

8.6. Future research

In this section we present other future research plans based on and stimulated by the results of this thesis.

8.6.1. Holographic states and codes

AME states are the fundamental building blocks for the construction of holographic codes using tensor networks [ADH15, LS15, PYHP15]. We showed that AME states can be classified into different locally unitary equivalent classes, therefore, a fundamental question will be comparing tensor network constructed from those set of states. We will also develop ten-

sor networks to construct optimal quantum error correction codes with subspace spanned by entangled tensor networks. The advantage will be having quantum codes with larger code subspace. Moreover, based on the stabilizer formalism we want to search for new encoding and decoding techniques for transmitting both quantum and classical information (hybrid codes).

8.6.2. Characterizing quantum networks

Studying networks is one of the most challenging and fundamental problems in science. The problem is especially very important in the quantum case. Therefore, we want to work on graph states represented in different quantum networks. We want to characterize them by their robustness against losses and local noises. It is also our plan to find a list of figure of merits to specify purity for different networks like regular, random, small-world, and scale-free networks. Characterizing the figure of merits will be based on the clustering coefficients, average degree and degree distribution, network diameter, and average path length of the different networks.

8.6.3. Locally maximally entangled states

We will consider pure states such that its subsystem dimensions are different, and with the property that all reduced states of at most k of the system size are maximally mixed, called locally maximally entangled states. The general case of constructing these states is still open [GBZ16, BLRVR19]. These states are useful for algebraic geometry and geometric invariant theory [WDGC13, BLRVR19]. We realized that it is possible to extend the construction method, stabilizer formalism, and graph representation we have for AME states to construct and formulate locally maximally entangled states.

APPENDICES

A. Appendix of Chapter 7: *Stabilisers group of the code state space*

A.1. Stabilisers group of the code state space

The k-uniform state of minimal support constructed from MDS code, recall

$$|\psi\rangle = \sum_{\vec{v}\in GF(q)^k} |\vec{v}\, G_{k\times n}\rangle \,, \tag{A.1}$$

is the plus one eigenstate of n stabilizer operators. The generators are divided into two sets, X stabilizers, S_X, and Z stabilizers, S_Z,

$$S \coloneqq \begin{cases} S_X = \bigotimes_{j=1}^{n} X^{g_{i,j}} & 1 \le i \le k \\ S_Z = \bigotimes_{j=1}^{n} Z^{h_{i,j}} & 1 \le i \le n-k \end{cases}, \tag{A.2}$$

where the matrix elements of $G_{k\times n}$ are denoted by $g_{i,j}$ and that of the code's parity check matrix $H_{(n-k)\times n}$ by $h_{i,j}$. The first k generators involve the X operators (the X stabilizers). This forms a set of stabilizers, because adding the same codeword to all other codewords is just a relabeling of the terms in the summation. Another set of stabilizers, $n-k$ of them, can be constructed from the Z operators (the Z stabilizers). The action of product of stabilizers S_Z leave state $|\psi\rangle$ invariant because of the fact that $G_{k\times n}(H_{(n-k)\times n})^T = 0$, (see also [RGRA18, Got97]).

The stabiliser formalism of the state $|\psi_0\rangle$, Eq. (7.2), can be found by taking advantage of the connection to the classical coding theory. Therefore, based on Eq. (A.2), one can find $n-1$ generators of the stabilizers of the state $|\psi_0\rangle$,

$$S^{\psi_0} \coloneqq \begin{cases} \bigotimes_{j=1}^{n-1} X^{\overline{g}_{i,j}} & 1 \le i \le k-1 \\ \bigotimes_{j=1}^{n-1} Z^{\overline{h}_{l,j}} & k \le i \le n-1 \end{cases}, \tag{A.3}$$

where the matrix elements of $G_{\widehat{k}}$ are denoted by $\overline{g}_{i,j}$ and that of the code's parity check matrix by $\overline{h}_{i,j}$.

For the code $\mathcal{C} \coloneqq \mathrm{span}(\{|\psi_m\rangle_{m\in[q]}\}) \subset \mathbb{C}_q^{\otimes n-1}$ with $|\psi_m\rangle = M^m|\psi_0\rangle$, Eq. (7.4) to be a stabilizer code, we need to generate a stabilizer group that stabilizes the given subspace. The set of the stabilizers $S^{\mathcal{C}}$ should satisfy the following equality

$$\forall i, m\colon \quad S_i^{\mathcal{C}}\, M^m\, |\psi_0\rangle = M^m\, |\psi_0\rangle \,. \tag{A.4}$$

The above condition implies that every $S_i^{\mathcal{C}} \in S^{\mathcal{C}}$ must commute with M (and hence M^m) operator and stabilize the state $|\psi_0\rangle$. The M operator is a vector of exponents of the X operators. Therefore, the $k-1$ generators of the stabilizer group of the state $|\psi_0\rangle$ that involve X operators, $S_X^{\psi_0}$, (first equation of Eq. (A.7)), commute with M and hence leave the state

$|\psi_m\rangle$ invariant. In order to find the stabilizers $S_i^{\mathcal{C}}$ that involve the Z operators, we first consider direct computation for any two Pauli strings. For two Pauli strings A and B the commutator follows

$$A\,B = \omega^{\vec{A}\odot\vec{B}}\,B\,A\,, \tag{A.5}$$

where $\vec{A} = (\vec{A}_X, \vec{A}_Z)$ and $\vec{b}$ is defined in the same way and,

$$\vec{A}\odot\vec{B} \coloneqq \vec{A}_Z\cdot\vec{B}_X - \vec{A}_X\cdot\vec{B}_Z\,. \tag{A.6}$$

This implies that the stabilizers of $|\psi_0\rangle$ that involves Z operators,$S_Z^{\psi_0}$ (the second equation of Eq. (A.7)), satisfies the Eq. (A.4) if for all m it holds that $m\vec{m}_X\cdot\vec{S}_Z^{\psi_0} = 0 \mod q$. This is also equivalent to just having $\vec{m}_X\cdot\vec{S}_Z^{\psi_0} = 0 \mod q$, where the vector $\vec{m}_X$ represent the vector of exponents in the M operator. The vector of exponents $S_Z^{\psi_0}$ of the Z stabilizers is constructed from linear combination of the rows of the parity check matrix $\overline{H}_{(n-k)\times(n-1)}$. Therefore, $\vec{S}_Z^{\psi_0} = \vec{v}\overline{H}$, represent the vector of exponents of the $S_Z^{\psi_0}$, where $\vec{v}\in GF(q)^{n-k}$. The string of Z operators that leave $|\psi_m\rangle = M^m|\psi_0\rangle$ invariant are those vector of exponents such that $\vec{m}_X\,.\,\vec{v}\overline{H} = 0$. In general, the generator $S^{\mathcal{C}}$ of the stabilizer groups of $\mathcal{C}$ are

$$S^{\mathcal{C}} \coloneqq \begin{cases} \bigotimes_{j=1}^{n-1} X^{\overline{g}_{i,j}} & 1\le i\le k-1 \\ \bigotimes_{j=1}^{n-1} Z^{\sum_{l=1}^{n-k} v_l\,\overline{h}_{l,j}} & \text{where } \vec{m}_X\,.\,\vec{v}\overline{H} = 0,\ \vec{v}\in GF(q)^{n-k} \end{cases}. \tag{A.7}$$

The number of generators for the stabilizers group that involve X operators is $k-1$ and that involve Z operators is $n-k-1$, in total, they are $n-2$ generators.

Bibliography

[ABO97] D. Aharonov and M. Ben-Or. Fault-tolerant quantum computation with constant error. In: *Proceedings of the Twenty-ninth Annual ACM Symposium on Theory of Computing*, STOC '97, 176–188. ACM, New York, NY, USA (1997).

[AC13] L. Arnaud and N. J. Cerf. Exploring pure quantum states with maximally mixed reductions. *Phys. Rev. A* **87**, 012319 (2013).

[ADH15] A. Almheiri, X. Dong and D. Harlow. Bulk locality and quantum error correction in ads/cft. *Journal of High Energy Physics* **2015**, 163 (2015).

[AK01] A. Ashikhmin and E. Knill. Nonbinary quantum stabilizer codes. *IEEE Transactions on Information Theory* **47**, 3065 (2001).

[ame] https://github.com/cgogolin/ame.

[AR95] D. Alsina and M. Razavi. Absolutely maximally entangled states, quantum maximum distance separable codes, and quantum repeaters. *arXiv:1907.11253 [quant-ph]* (1995).

[BB06] M. Bahramgiri and S. Beigi. Graph states under the action of local clifford group in non-binary case. *arXiv:quant-ph/0610267* (2006).

[BBC+93] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres and W. K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.* **70**, 1895 (1993).

[BBD+09a] H. J. Briegel, D. E. Browne, W. Dür, R. Raussendorf and M. van den Nest. Measurement-based quantum computation. *Nature Phys* **5**, 19 (2009).

[BBD+09b] H. J. Briegel, D. E. Browne, W. Dür, R. Raussendorf and van den Nest M. Measurement-based quantum computation. *Nature Phys* **5**, 19 (2009).

[BBFM06] S. C. Benjamin, D. E. Browne, J. Fitzsimons and J. J. L. Morton, Brokered. graph-state quantum computation. *New J. Phys.* **8**, 141 (2006).

[BBPS96] C. H. Bennett, H. J. Bernstein, S. Popescu and B. Schumacher. Concentrating Partial Entanglement by Local Operations. *Phys. Rev. A* **53**, 2046 (1996).

[BBRV02] S. Bandyopadhyay, P. O. Boykin, V. Roychowdhury and F. Vatan. A New Proof for the Existence of Mutually Unbiased Bases. *Algorithmica* **34**, 512 (2002).

[Ber17] A. Bernal. On the Existence of Absolutely Maximally Entangled States of Minimal Support. *Quant. Phys. Lett.* **6**, 1 (2017).

[BGM+10] P. Barreiro, J. T.and Schindler, O. Gühne, T. Monz, M. Chwalla, C. F. Roos, M. Hennrich and R. Blatt. Experimental multiparticle entanglement dynamics induced by decoherence. *Nature Physics* **6**, 943 (2010).

[BLRVR19] I. Bryan, S. Leutheusser, Z. Reichstein and M. Van Raamsdonk. Locally Maximally Entangled States of Multipart Quantum Systems. *Quantum* **3**, 115 (2019).

[BPB+07] A. Borras, A. R. Plastino, J. Batle, C. Zander, M. Casas and A. Plastino. Multiqubit systems: highly entangled states and entanglement distribution. *Journal of Physics A: Mathematical and Theoretical* **40**, 13407 (2007).

[BR20] A. Burchardt and Z. Raissi. Stochastic Local Operations with Classical Communication of Absolutely Maximally Entangled States. *accepted for publication in Phys. Rev. A* (2020).

[BSSB05] I. D. K. Brown, S. Stepney, A. Sudbery and S. L. Braunstein. Searching for highly entangled multi-qubit states. *Journal of Physics A: Mathematical and General* **38**, 1119 (2005).

[Bus52] K. Bush. Orthogonal arrays of index unity. *Ann. Math. Statist.* **23**, 426 (1952).

[BW92] C. H. Bennett and S. J. Wiesner. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Phys. Rev. Lett.* **69**, 2881 (1992).

[CC97] N. J. Cerf and R. Cleve. Information-theoretic interpretation of quantum error-correcting codes. *Phys. Rev. A* **56**, 1721 (1997).

[CGL99] R. Cleve, D. Gottesman and H.-K. Lo. How to share a quantum secret. *Phys. Rev. Lett.* **83**, 648 (1999).

[CRSS98] A. Calderbank, E. Rains, P. Shor and N. Sloane. Quantum error correction via codes over GF(4). *IEEE Trans. Inform. Theory* **44**, 1369 (1998).

[CS96] A. R. Calderbank and P. W. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A* **54**, 1098 (1996).

[CZKH97] J. I. Cirac, P. Zoller, H. J. Kimble and M. H. Quantum state transfer and entanglement distribution among distant nodes in a quantum network. *Phys. Rev. Lett.* **78**, 3221 (1997).

[DC00a] W. Dür and J. I. Cirac. Activating bound entanglement in multi-particle systems. *Phys. Rev. A* **62**, 022302 (2000).

[DC00b] W. Dür and J. I. Cirac. Multiparty teleportation. *J. Mod. Opt.* **47**, 247 (2000).

[DC02] W. Dür and J. I. Cirac. Equivalence classes of non-local unitary operations. *Quant. Info. and Comp.* **2**, 240 (2002).

[DM72] H. Dym and H. P. McKean. Fourier Series and Integrals. *Academic Press. New York* (1972).

[Dur05] T. Durt. About mutually unbiased bases in even and odd prime power dimensions. *Journal of Physics A: Mathematical and General* **38**, 5267 (2005).

[DVC00] W. Dür, G. Vidal and J. I. Cirac. Three qubits can be entangled in two inequivalent ways. *Phys. Rev. A* **62**, 062314 (2000).

[dVSK13] J. I. de Vicente, C. Spee and B. Kraus. Maximally Entangled Set of Multipartite Quantum States. *Phys. Rev. Lett.* **111**, 110502 (2013).

[EB01] J. Eisert and H. Briegel. The Schmidt Measure as a Tool for Quantifying Multi-Particle Entanglement. *Phys. Rev. A* **64**, 022306 (2001).

[Fad95] L. D. Faddeev. Discrete Heisenberg-Weyl Group and Modular Group. *Phys. Rev. A* **34**, 249 (1995).

[FFM+10] P. Facchi, G. Florio, U. Marzolino, G. Parisi and S. Pascazio. Classical statistical mechanics approach to multipartite entanglement. *Journal of Physics A: Mathematical and Theoretical* **43**, 225303 (2010).

[FFPP08] P. Facchi, G. Florio, G. Parisi and S. Pascazio. Maximally multipartite entangled states. *Phys. Rev. A* **77**, 060304 (2008).

[GAL+15] D. Goyeneche, D. Alsina, J. I. Latorre, A. Riera and K. Życzkowski. Absolutely maximally entangled states, combinatorial designs, and multiunitary matrices. *Phys. Rev. A* **92**, 032316 (2015).

[GBR04a] M. Grassl, T. Beth and M. Roetteler. On optimal quantum codes. *International Journal of Quantum Information* **2**, 55 (2004).

[GBR04b] M. Grassl, T. Beth and M. Röttler. On optimal quatum codes. *International Journal of Quantum Information* **02**, 55 (2004).

[GBZ16] D. Goyeneche, J. Bielawski and K. Życzkowski. Multipartite entanglement in heterogeneous systems. *Phys. Rev. A* **94**, 012346 (2016).

[GHS90] D. M. Greenberger, M. A. Horne and A. Shimony. Bell's theorem without inequalities. *Am. J. Phys.* **58**, 1131 (1990).

[Got97] D. Gottesman. Stabilizer codes and quantum error correction. *arXiv:quant-ph/9705052* (1997).

[Got09] D. Gottesman. An Introduction to Quantum Error Correction and Fault-Tolerant Quantum Computation. *arXiv:0904.2557 [quant-ph]* (2009).

[GR15] M. Grassl and M. Roetteler. Quantum MDS Codes over Small Fields. *IEEE International Symposium on Information Theory (ISIT)* 1104 (2015).

[Gra] M. Grassl. Code tables: Bounds on the minimum distance of linear codes and quantum codes. Http://www.codetables.de.

[Gra04] M. Grassl. On sic-povms and mubs in dimension 6. *arXiv:quant-ph/0406175* (2004).

[GRDMZ18] D. Goyeneche, Z. Raissi, S. Di Martino and K. Życzkowski. Entanglement and quantum combinatorial designs. *Phys. Rev. A* **97**, 062326 (2018).

[GTB05] O. Gühne, G. Toth and H. J. Briegel. Multipartite entanglement in spin chains. *New J. Phys.* **7**, 229 (2005).

[GW10] G. Gour and N. R. Wallach. All maximally entangled four qubits states. *J. Math. Phys.* **51**, 112201 (2010).

[GZ14] D. Goyeneche and K. Życzkowski. Genuinely multipartite entangled states and orthogonal arrays. *Phys. Rev. A* **90**, 022316 (2014).

[HBB99] M. Hillery, V. Buzek and A. Berthiaume. Quantum secret sharing. *Phys. Rev. A* **59**, 1829 (1999).

[HCL+12] W. Helwig, W. Cui, J. I. Latorre, A. Riera and H. K. Lo. Absolute maximal entanglement and quantum secret sharing. *Phys. Rev. A* **86**, 5 (2012).

[HDE+06] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. Van den Nest and H. J. Briegel. Entanglement in Graph States and its Applications. *arXiv:quant-ph/0602096* (2006).

[HEB04] M. Hein, J. Eisert and H. J. Briegel. Multi-party entanglement in graph states. *Phys. Rev. A* **69**, 062311 (2004).

[Hel13] W. Helwig. Absolutely Maximally Entangled Qudit Graph States. *arXiv:1306.2879 [quant-ph]* (2013).

[HESG18] F. Huber, C. Eltschka, J. Siewert and O. Gühne. Bounds on absolutely maximally entangled states from shadow inequalities, and the quantum MacWilliams identity. *J. Phys. A: Math. Theor.* **51**, 175301 (2018).

[HG20] F. Huber and M. Grassl. Quantum Codes of Maximal Distance and Highly Entangled Subspaces. *Quantum* **4**, 284 (2020).

[HGS17] F. Huber, O. Gühne and J. Siewert. Absolutely maximally entangled states of seven qubits do not exist. *Phys. Rev. Lett* **118**, 200502 (2017).

[HHHH09] R. Horodecki, P. Horodecki, M. Horodecki and K. Horodecki. Quantum entanglement. *Rev. Mod. Phys.* **81**, 865 (2009).

[HNQ+16] P. Hayden, S. Nezami, X.-L. Qi, N. Thomas, M. Walter and Z. Yang. Holographic duality from random tensor networks. *Journal of High Energy Physics* **2016**, 9 (2016).

[HP03] W. C. Huffman and V. Pless. Fundamentals of Error Correcting Codes. *Cambridge University Press* (2003).

[HS00] A. Higuchi and A. Sudbery. How entangled can two couples get? *Phys. Lett. A* **273**, 213 (2000).

[HSS99] A. S. Hedayat, N. J. A. Sloane and J. Stufken. *Orthogonal Arrays: Theory and Applications*. Springer-Verlag, New York (1999).

[HW19] F. Huber and N. Wyderka. Table of AME states. *https://www.tp.nt.uni-siegen.de/+fhuber/ame.html* (2019).

[JX14] L. Jin and C. Xing. A construction of new quantum mds codes. *IEEE Transactions on Information Theory* **60**, 2921 (2014).

[KB98] A. Karlsson and M. Bourennane. Quantum teleportation using three-particle entanglement. *Phys. Rev. A* **58**, 4394 (1998).

[Kim08] H. J. Kimble. The quantum internet. *Nature* **452**, 1023 (2008).

[KKKS06] A. Ketkar, A. Klappenecker, S. Kumar and P. K. Sarvepalli. Nonbinary stabilizer codes over finite fields. *EEE Trans. Info. Theor.* **52**, 4892 (2006).

[KKO15] J. I. Kokkala, D. S. Krotov and P. R. J. Ostergard. On the Classification of MDS Codes. *IEEE Trans. Inf. Theory* **61**, 6485 (2015).

[KL97] E. Knill and R. Laflamme. A Theory of Quantum Error-Correcting Codes. *Phys. Revi. A* **55**, 900 (1997).

[Llo96] S. Lloyd. Universal Quantum Simulators. *Science* **273**, 1073 (1996).

[LMPZ96a] R. Laflamme, C. Miquel, J. P. Paz and W. Zurek. Perfect Quantum Error Correcting Code. *Physical Review Lett.* **77**, 198 (1996).

[LMPZ96b] R. Laflamme, C. Miquel, J. P. Paz and W. H. Zurek. Perfect Quantum Error Correction Code. *Phys. Rev. Lett.* **77**, 198 (1996).

[LS15] J. I. Latorre and G. Sierra. Holographic codes. *arXiv:1502.06618 [quant-ph]* (2015).

[Mar90] T. Maruta. On Singleton arrays and Cauchy matrices. *Discrete Mathematics* **81**, 33 (1990).

[MMS72] F. MacWilliams, C. Mallows and N. Sloane. Generalizations of Gleason's theorem on weight enumerators of self-dual codes. *IEEE Transactions on Information Theory* **18**, 794 (1972).

[MS77] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error Correcting Codes*. North-Holland, Amesterdam (1977).

[Mus17] B. Musto. Constructing Mutually Unbiased Bases from Quantum Latin Squares. *Proc. 13th International Conference on Quantum Physics and Logic, University of Strathclyde* **236**, 108 (2017).

[MV04] A. Miyake and F. Verstraete. Multipartite entanglement in $2 \times 2 \times n$ quantum systems. *Phys. Rev. A* **69**, 012101 (2004).

[MV16] B. Musto and J. Vicary. Quantum Latin squares and unitary error bases. *Quant. Inf. and Comp.* **16**, 1318 (2016).

[NC00] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press (2000).

[Nie99] M. A. Nielsen. Conditions for a class of entanglement transformations. *Phys. Rev. Lett.* **83**, 436 (1999).

[Or𝕝14] R. Orús. A practical introduction to tensor networks: Matrix product states and projected entangled pair states. *Ann. Phys.* **349**, 117 (2014).

[Pip03] N. Pippenger. The inequalities of quantum information theory. *IEEE Transactions on Information Theory* **49**, 773 (2003).

[PYHP15] 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* **2015**, 149 (2015).

[Rai99a] E. M. Rains. Nonbinary quantum codes. *IEEE Transactions on Information Theory* **45**, 1827 (1999).

[Rai99b] E. M. Rains. Quantum shadow enumerators. *IEEE Transactions on Information Theory* **45**, 2361 (1999).

[Rai20] Z. Raissi. Modified-Shortening: Modifying method of constructing quantum codes from highly entangled states. *arXiv:2005.01426 [quant-ph]* (2020).

[Rao46] C. R. Rao. Hypercubes of strenght d leading to confounded designs in factorial experiments. *Bull. Calcutta Math. Soc.* **38**, 67 (1946).

[RB01] R. Raussendorf and H. J. Briegel. A one-way quantum computer. *Phys. Rev. Lett.* **86**, 5188 (2001).

[RGRA18] Z. Raissi, C. Gogolin, A. Riera and A. Acín. Constructing optimal quantum error correcting codes from absolute maximally entangled states. *J. Phys A: Math. and Theor.* **51**, 075301 (2018).

[RS85] R. M. Roth and G. Seroussi. On Generator Matrices of MDS Codes. *IEEE Trans. Inf. Theor.* **31** (1985).

[RTGA19] Z. Raissi, A. Teixidó, C. Gogolin and A. Acín. Constructing new k-uniform and absolutely maximally entangled states. *accepted for publication in Phys. Rev. Research* (2019).

[Sco04] A. J. Scott. Multipartite entanglement, quantum-error-correcting codes, and entangling power of quantum evolutions. *Phys. Rev. A* **69**, 052330 (2004).

[SdVK16] C. Spee, J. I. de Vicente and B. Kraus. The maximally entangled set of 4-qubit states. *J. Math. Phys.* **57**, 052201 (2016).

[Sin64] R. Singleton. Maximum Distance Q-nary Codes. *IEEE Trans. Inf. Theor.* **10**, 116 (1964).

[SK05] P. K. Sarvepalli and A. Klappenecker. Nonbinary quantum reed-muller codes. In: *Proceedings. International Symposium on Information Theory, 2005. ISIT 2005*, 1023–1027 (2005).

[SR86] G. Seroussi and R. M. Roth. On MDS Extensions of Generalized Reed-solomon Codes. *IEEE Trans. Inf. Theor.* **32**, 349 (1986).

[SSC+15] K. Schwaiger, D. Sauerwein, M. Cuquet, J. de Vicente and B. Kraus. Operational multipartite entanglement measures. *Phys. Rev. Lett.* **115**, 150502 (2015).

[Ste96a] A. Steane. Multiple Particle Interference and Quantum Error Correction. *Proc. Roy. Soc. Lond. A* **452**, 2551 (1996).

[Ste96b] A. Steane. Simple Quantum Error Correcting Code. *Phys. Rev. A* **54**, 4741 (1996).

[Sti03] D. R. Stinson. *Combinatorial Designs: Constructions and Analysis*. New York: Springer (2003).

[SW01] D. Schlingemann and R. F. Werner. Quantum error-correcting codes associated with graphs. *Phys. Rev. A* **65**, 012308 (2001).

[Ter15] B. M. Terhal. Quantum Error Correction for Quantum Memories. *Rev. Mod. Phys.* **87**, 307 (2015).

[TGP10] S. Turgut, Y. Gül and N. K. Pak. Deterministic transformations of multipartite entangled states with tensor rank 2. *Phys. Rev. A* **81**, 012317 (2010).

[VDMV02] F. Verstraete, J. Dehaene, B. D. Moor and H. Verschelde. Four qubits can be entangled in nine different ways. *Phys. Rev. A* **65**, 052112 (2002).

[Vid99] G. Vidal. Entanglement of Pure States for a Single Copy. *Phys. Rev. Lett.* **83**, 1046 (1999).

[Vid00] G. Vidal. Entanglement monotones. *Journal of Modern Optics* **47**, 355 (2000).

[WDGC13] M. Walter, B. Doran, D. Gross and M. Christandl. Entanglement Polytopes: Multiparticle Entanglement from Single-Particle Information. *Science* **340**, 6137 (2013).

[Wer89] R. F. Werner. Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model. *Phys. Rev. A* **40**, 4277 (1989).

[Wey50] H. Weyl. *The Theory of Groups and Quantum Mechanics*. Dover Books on Mathematics. Dover Publications (1950).

[WF89] W. K. Wootters and B. D. Fields. Optimal state-determination by mutually unbiased measurements. *Annals of Physics* **191**, 363 (1989).

[WZ82] W. K. Wootters and W. H. Zurek. A Single Quantum Cannot be Cloned. *Nature* **299**, 802 (1982).