Quantum Hypergraph States and the Theory of Multiparticle Entanglement

Dissertation
zur Erlangung des Grades eines Doktors
der Naturwissenschaften

vorgelegt von
MSc. Mariami Gachechiladze

eingereicht bei der Naturwissenschaftlich-Technischen Fakultät
der Universität Siegen
Siegen, 2019

Gutachter:

- Prof. Dr. Otfried Gühne
- PD Dr. Hermann Kampermann

Datum der mündlichen Prüfung: 26.08.2019

Prüfer:

- Prof. Dr. Otfried Gühne (Vorsitz der Prüfungskommission)
- PD Dr. Hermann Kampermann
- PD Dr. Tobias Huber
- PD Dr. Michael Johanning

Dedicated to my grandparents

Abstract

This thesis is devoted to learning different aspects of quantum entanglement theory. More precisely, it concerns a characterization of certain classes of pure multipartite entangled states, their nonlocal and entanglement properties, comparisons with the other well-studied classes of states and, finally, their utilization in certain quantum information processing tasks.

The most extensive part of the thesis explores an interesting class of pure multipartite entangled states, quantum hypergraph states. These states are generalizations of the renowned class of graph states. Here we cover their nonlocal properties in various scenarios, derive graphical rules for unitary transformations and Pauli bases measurements. Using these rules, we characterize entanglement classes of hypergraph states under local operations, obtain tight entanglement witnesses, and calculate entanglement measures for hypergraph states. Finally, we apply all the aforementioned analysis to endorse hypergraph states as powerful resource states for measurement-based quantum computation and quantum error-correction.

The rest of the thesis is devoted to three disjoint problems, but all of them are still in the scope of entanglement theory. First, using mathematical structure of linear matrix pencils, we coarse grain entanglement in tripartite pure states of local dimensions $2 \times m \times n$ under the most general local transformations. In addition, we identify the structure of generic states for every m and n and see that for certain dimensions there is a resemblance between bipartite and tripartite entanglement. Second, we consider the following question: Can entanglement detection be improved, if in addition to the expectation value of the measured witness, we have knowledge of the expectation value of another observable? For low dimensions we give necessary and sufficient criterion that such two product observables must satisfy in order to be able to detect entanglement. Finally, we derive a general statement that any genuine N-partite entangled state can always be projected on any of its k-partite subsystems in a way that the new state in genuine k-partite entangled.

Zusammenfassung

Diese Arbeit ist verschiedenen Aspekten der Verschränkungstheorie gewidmet. Genauer gesagt, beschäftigt sie sich mit der Charakterisierung verschiedener Klassen reiner mehrteilchenverschränkter Zustände, sowie ihrer nicht-lokalen und Verschränkungseigenschaften, Vergleichen mit anderen bekannten Klassen von Zuständen und, letztendlich, ihrer Verwendung in der Quanteninformationsverarbeitung.

Der größte Teil dieser Arbeit beschäftigt sich mit einer interessanten Klasse von reinen mehrteilchenverschränkten Zuständen, den Hypergraphen Zuständen. Diese Zustände bilden eine Verallgemeinerung der weithin bekannten Graphen Zustände. Wir werden ihre nicht-lokalen Eigenschaften untersuchen und graphische Regeln für ihr Verhalten unter unitären Transformationen sowie Messungen in der Pauli Basis herleiten. Unter Verwendung dieser Regeln werden Verschränkungsklassen unter lokalen Operationen charakterisiert, und optimale Verschränkungszeugen sowie Verschränkungsmaße berechnet. Zuletzt wird, unter Berücksichtigung der vorangegangenen Analyse, gezeigt, dass Hypergraphen Zustände eine Ressource für Messungsbasierte Quantencomputer und Quantenfehlerkorrektur bilden.

Der verbleibende Teil dieser Arbeit beschäftigt sich mit drei unterschiedlichen Problemen im Rahmen der Verschränkungstheorie. Zuerst wird die Verschränkung reiner Dreiteilchenzustände mit lokalen Dimensionen $2 \times m \times n$ unter den allgemeinsten Transformationen untersucht. Dazu wird eine spezielle mathematische Struktur verwendet, die so genannten Matrix Pencils. Zudem identifizieren wir die Struktur von generischen Zuständen für alle m und n und wir werden sehen, dass in bestimmten Dimensionen eine Ähnlichkeit zwischen Zweiteilchen- und Dreiteilchenverschränkung besteht. Danach wird der Frage nachgegangen: Kann Verschränkungsdetektion verbessert werden, wenn man zusätzlich zum Erwartungswertes des Verschränkungszeugen noch den Erwartungswert einer anderen Observablen kennt? Für niedrige Dimensionen werden notwendige und hinreichende Bedingungen hergeleitet, die zwei Produktobservablen erfüllen müssen um Verschränkung detektieren zu können. Zuletzt wird die allgemeine Aussage bewiesen, dass jeder echte N-Teilchen verschränkte

Zustand immer auf seine k-Teilchen Subsysteme projiziert werden kann, sodass dieser Zustand echt k-Teilchen verschränkt ist.

Contents

Chapter 1

Introduction

Quantum information theory and quantum computing are products of a rapid development of several key fields of science since the turn of the twentieth century: physics, computer science, information theory, and cryptography. At that time along with gaining more understanding of radiation and the structure of an atom, it was becoming more and more evident that the predictions made by classical physics could not be made consistent with experimental observations by simply adding *ad hoc* hypotheses to classical physics. As a result the new theory, called quantum mechanics was developed, which is accountable for describing nature at its smallest scales of energy levels.

Quantum mechanics offers a mathematical framework for developing the laws that physical systems must comply with. Its main aspects can be given in several postulates: State space postulate, system evolution postulate, quantum measurement postulate, and composite quantum system postulate. The first postulate sets up a mathematical playground for quantum mechanics: A state of an isolated quantum mechanical system is fully specified by a wave function ψ, which mathematically can be represented by a complex vector in a Hilbert space. Then, if one considers a wave function over a composite system of two subsystems, one soon realizes that there exist state vectors in the corresponding composite Hilbert space (in accordance to the last postulate), which cannot be described as a union of any two state vectors over its constituent subsystems. Instead, only the description of the entire global wave function is accessible. To say it yet in another words, the state of one particle cannot be accessed independently of the state of another one, regardless of the distance between them. This striking phenomenon is known as quantum entanglement and was first described by Einstein, Podolsky, and Rosen (EPR) in 1935 [1]. In this paper the authors, however, were rather questioning the completeness of the quantum-mechanical description of

physical reality given by a wave function. To them it was counterintuitive that, given two space-like separated systems, it was possible to measure either the position or momentum of only one system, and to immediately determine the position or momentum, respectively, for the second one. Shortly after, Schrödinger for the first time coined the term entanglement (Verschränkung in German) in his seminal paper [2], nonetheless, he also referred to the findings of EPR as a "*very disconcerting fact*".

In 1964, Bell recognized that, if the *locality assumption* of EPR were indeed true, then the strength of the correlations obtained from the measurements on the composite system, must have been upper-bounded for any complete theory of quantum mechanics [3]. Bounding the strength of correlations, now known as *Bell's theorem*, was indeed an ingenious approach to the problem, as it provided an experimentally verifiable deviations of quantum mechanics from the theories requiring complete local descriptions. In 1972 Bell's theorem was experimentally verified [4] by violating CHSH inequality [5] (discussed in Chapter 2). Along with the rapid development of experimental tools, many other Bell tests were performed [6–9], however, all these experiments had either *detection loophole* or *locality loophole*. Finally, in 2015 the loophole-free experimental violation of Bell inequalities was announced [10–12].

Quantum entanglement has established itself as a central resource in many applications of quantum information theory: quantum teleportation [13], dense coding [14], quantum cryptography [15], measurement-based quantum computation [16], quantum error-correction [17, 18], speed-up in computation [19, 20], the quantum internet [21], precision measurements [22]. Because of its importance, quantum entanglement has been extensively investigated over many years. Even though the phenomenon is fairly well understood for the bipartite scenario, due to its complex structure in multipartite case, its full characterization is unmanageable. Moreover, it has been established that most of the multipartite quantum states are even too entangled to be useful for certain quantum information processing tasks [23–25] and, in addition, it appears that it is more difficult to find resource states for some quantum computing tasks, than quantum computing itself [26]. Taking all these reasons into account, it is crucial to find classes of quantum multipartite states, which are useful for many of the aforementioned applications and at the same time, have easy-to-handle description.

Graph states [27], which are multipartite entangled states, have been utilized in almost all the applications of quantum information theory. Despite their usefulness, this class of states also has its own limitations. To give examples, graph states are fragile against noise and also they need non-Pauli bases measurements as additional resources to guarantee universal measurement-based quantum computation [28]. One of the main

goals of this thesis is to investigate properties of more general pure multipartite entangled states, called hypergraph states and to establish the areas of quantum information processing, where these, more general states, could offer an advantage. The biggest chunk of my thesis is devoted to investigating these states and their applications. See Chapters 3-7.

In Chapter 3, we investigate nonlocality of hypergraph states and derive genuine multipartite Bell inequality specifically for the three-qubit case. The technique is general and can be applied to other hypergraphs. Moreover, we show that certain symmetric N-qubit hypergraph states, in the analogy to the symmetric N-qubit graph states [29], violate Bell inequalities in the exponentially increasing manner with the number of particles. Differently from graph states though, this violation is robust under particle loss. The results on nonlocality of hypergraph states and their connection to the better precision quantum metrology are described in the paper in Ref. [30].

Many insights in entanglement properties of graph states are connected to their graphical representation [27, 31]. In Chapter 4, we generalize some of the known constructions to hypergraph states and derive graphical language to handle useful transformations on hypergraph states. There rules cover local and nonlocal unitary transformations on hypergraph states and Pauli bases measurements. In Chapter 5 we use these results to quantify and detect entanglement present in these states. These results are based on several publications, Refs. [32, 33].

Aforementioned graphical rules also help to construct hypergraph states, which are universal resource states for measurement-based quantum computation. Here hypergraph states have a major advantage that entire computation can be performed using Pauli measurements only. These findings with additional analysis for the depth of universal computation using the new resource state are given in the paper, Ref. [33] and are presented in Chapter 6.

As a last application we investigate whether similarly to graph states, we can use hypergraphs for quantum error-correcting codes [34, 35]. We find several curious statements in this direction. Graph states seems to be more efficient when constructing higher distance codes. However, hypergraph states can be used to describe new nonadditive quantum error-correcting codes. See derivations and results in Chapter 7.

The rest of the thesis is dealing with three different aspects of entanglement theory: classification of entanglement in Chapter 8, entanglement detection in Chapter 9, and Bell nonlocality in Chapter 10.

In entanglement theory it is very important to characterize which quantum states can be transformed to one another under operations in local laboratories. For example, it

is known that in order to perfectly teleport an unknown quantum state from Alice to Bob, it is necessary that these two parties share a so-called two qubit Bell state. Any other state which cannot be obtained from a Bell state under local unitary operations, cannot be a perfect resource for the same task. A Bell state is also called a maximally entangled stated. In multipartite case, entanglement classifications becomes harder, since there are infinite number of quantum states in the corresponding Hilbert space. One way to handle the problem is to consider coarse graining of some of the classes together. In this direction, in Chapter 8 we investigate coarse graining of entanglement in the systems consisting of three parties of unequal local dimensions. As a result, we identify the most powerful states for various tasks. These results are based on the publication, Ref. [36].

Entanglement witnesses are a very important tool in experiments. In Chapter 9 we study how one can improve entanglement detection and estimation, using a witness observable L on the state, when additional data is known from the experiment, such as an expectation value of another observable C. For low-dimensional systems, we derive a necessary and sufficient condition for the product observables $L = L_A \otimes L_B$ and $C = C_A \otimes C_B$ to detect entanglement. The findings are based on the publication, Ref. [37].

Finally, we consider a general question: Which pure quantum states are nonlocal? In 1992 Popescu and Rohrlich showed that any genuine N-partite entangled state can be projected on a two qubit entangled state, using projective measurements on the rest of $(N-2)$ parties [38]. That being the case, there exists a Bell inequality that this two-qubit state violates [39]. The original proof had a flaw, but the statement could still be proven [40]. In addition, we generalize the original theorem of Popescu and Rohrlich by showing that, if the original N-qubit state is genuine multipartite entangled, then one can project on any k qubits via measuring the rest of $(N-k)$ qubits in Pauli bases, such that the remaining state is also genuine k-partite entangled. These findings can be partially found in the publication, Ref. [40].

To sum up, this thesis is based on six publications [30, 32, 33, 36, 37, 40] and several derivations of the work in progress.

Chapter 2

Preliminaries

This chapter is devoted to the introduction of the notions and definitions used later in the thesis. It also presents related results and constructions from the literature, which both, motivate and help explain my work.

2.1 Quantum states and their entanglement

Any quantum system is identified with a finite or infinite dimensional Hilbert space $\mathcal{H}$. In this thesis we will be only concerned with the finite case. A d-dimensional *pure quantum state* mathematically can be described by a vector living in a Hilbert space $\mathcal{H} = \mathbb{C}^d$. For $d = 2$, we refer to quantum states as *qubit* states and if the dimension is higher, as *qudit* states. A pure state is a normalized vector and is called a *ket* vector $|\psi\rangle \in \mathbb{C}^d$. Its dual vector is called a *bra* vector $\langle\psi|$, where $\langle\psi| = |\psi\rangle^\dagger$. A pure state $|\psi\rangle$ can be expressed as a linear combination of some orthonormal basis $\{|a_i\rangle\}_{i=0}^{d-1}$:

$$|\psi\rangle = \sum_{i=0}^{d-1} c_i |a_i\rangle, \tag{2.1}$$

where due to the normalization constraint, $\langle\psi|\psi\rangle = 1$, which corresponds to the algebraic inner product between two complex vectors, the complex-valued coefficients c_i satisfy the following constraint, $\sum_{i=0}^{d-1} |c_i|^2 = 1$. If the basis $\{|a_i\rangle\}_{i=0}^{d-1}$ correspond to the standard basis in linear algebra, $\{|i\rangle\}_{i=0}^{d-1}$, they are called *computational basis* and each element of the basis set $|i\rangle$ is then a *computational basis element*. On the other hand, the square of the absolute value of each coefficient c_i, corresponds to the probability of obtaining an outcome a_i, if the system was measured in the basis $\{|a_i\rangle\}_{i=0}^{d-1}$.

Often it happens that one does not have an exact information about a state of a quantum system, but rather knows that with some probability p_i the system is in a pure state $|\psi_i\rangle$. In this case entire physical system is in a *mixed state* and can be described by a *density matrix* ρ:

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|. \tag{2.2}$$

Since p_i's are probabilities, that is $p_i \geq 0$ and $\sum_i p_i = 1$, it follows that $\mathrm{tr}(\rho) = 1$. At the same time, each matrix $|\psi_i\rangle\langle\psi_i|$ is hermitian and positive. Hence, a density matrix ρ is a complex-valued trace-one matrix with non-negative real eigenvalues, $\rho \geq 0$. Moreover, any trace-one semidefinite matrix is a density matrix describing a mixed state. From here it follows that the set of all quantum states is a closed convex set with pure states on its boundary.

Until now we regarded a quantum system as a single system living in a d-dimensional Hilbert space $\mathcal{H}^d$. However, we can consider a system containing N quantum states, each with a respective Hilbert space dimension, $d_1, \dots d_N$. Then a pure state $|\psi\rangle$ is a state vector in a composite Hilbert space, denoted by the tensor product $\mathcal{H}^{d_1} \otimes \mathcal{H}^{d_2} \otimes \dots \otimes \mathcal{H}^{d_N}$:

$$|\psi\rangle = \sum_{i_1,\dots,i_N=0}^{(d_1-1),\dots,(d_N-1)} c_{i_1\dots i_N} |i_1\rangle \otimes \dots \otimes |i_N\rangle = \sum_{i_1,\dots,i_N=0}^{(d_1-1),\dots,(d_N-1)} c_{i_1\dots i_N} |i_1 \dots i_N\rangle, \tag{2.3}$$

where the right hand side is a short hand notation, first, omitting the tensor product and then merging two ket vectors into one: $|a\rangle \otimes |b\rangle \equiv |a\rangle|b\rangle \equiv |ab\rangle$.

2.1.1 Bipartite entanglement

In this subsection we discuss the properties of composite quantum systems more closely. We start by considering bipartite systems.

Let us assume that a *bipartite* pure state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ is shared between two laboratories A and B. Having a mathematical description of the entire system, we can wonder what are the local pure states present in each laboratory: $|\psi_A\rangle \in \mathcal{H}_A$ and $|\psi_B\rangle \in \mathcal{H}_B$. It appears that given a global physical state, such a local description cannot always be guaranteed [2].

Definition 2.1. A pure state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ is called a product state if can be written as a tensor product of two local pure states $|\psi_A\rangle \in \mathcal{H}_\mathcal{A}$ and $|\psi_B\rangle \in \mathcal{H}_\mathcal{B}$:

$$|\psi\rangle = |\psi_A\rangle \otimes |\psi_B\rangle. \tag{2.4}$$

Otherwise, the state $|\psi\rangle$ is entangled.

The simplest and most famous example of pure entanglement is the two-qubit Bell state:

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}. \tag{2.5}$$

There is a very powerful tool to describe entanglement present in bipartite systems, called *Schmidt decomposition*:

Lemma 2.2. *Let $|\psi\rangle = \sum_{i,j=1}^{d_A,d_B} c_{ij}|a_i b_j\rangle$ be a bipartite state in $\mathcal{H}_A \otimes \mathcal{H}_B$. Then there exists an orthonormal basis $|\alpha_i\rangle \in \mathcal{H}_A$ and an orthonormal basis $|\beta_i\rangle \in \mathcal{H}_B$, such that the following statement holds*

$$|\psi\rangle = \sum_{k=1}^{D} \lambda_k |\alpha_k \beta_k\rangle \tag{2.6}$$

for positive real λ_k, called Schmidt coefficients, D is called Schmidt rank of $|\psi\rangle$ and is equal to the number of non-zero λ_k's.

The concept of a bipartite entanglement can also be generalized to mixed states.

Definition 2.3. A mixed state ρ of a composite system is called separable, if it can be written as a probabilistic mixture of local mixed states ρ_i^A and ρ_i^B:

$$\rho = \sum_i p_i \rho_i^A \otimes \rho_i^B. \tag{2.7}$$

Otherwise, the state is called entangled.

From the definition of separability follows that the convex combination of two or more separable states is again a separable state. Therefore, the set of all separable states is a convex subset of the set of all states with its extremal points being pure product vectors belonging to the boundary of the entire state space.

Given a density matrix, it is interesting to know, if it is separable or not. Although there exist several criteria to decide the separability for some bipartite states [41–44], no general solution for the problem is known.

2.1.2 Multipartite entanglement

Composite systems get more complicated with the increasing number of parties, as there exist different notions of entanglement in multipartite systems. The first notion captures no entanglement present in a quantum state: An N-partite pure state $|\psi\rangle$ is called a product state, if it can be written as a tensor product of local pure states:

$$|\psi\rangle = |\psi_A\rangle \otimes |\psi_B\rangle \otimes \cdots \otimes |\psi_N\rangle. \tag{2.8}$$

Otherwise, the state is called entangled.

Definition 2.4. If a pure multipartite state $|\psi\rangle$ cannot be written as a tensor product of any of its subsystems, then we say that the state is not biseparable or, otherwise, the state is genuine multipartite entangled.

Examples of three-qubit genuine multipartite entangled states are Greenberger-Horne-Zeilinger (GHZ)- [45, 46] and so-called W-states [47]:

$$|GHZ\rangle = \frac{|000\rangle + |111\rangle}{\sqrt{2}}, \qquad |W\rangle = \frac{|001\rangle + |010\rangle + |100\rangle}{\sqrt{3}}. \tag{2.9}$$

2.1.3 Local manipulation of entanglement

Entanglement is a key resource for many applications in quantum information processing. Hence, it is important to classify entangled quantum states in order to learn which states are more powerful. This is done by considering the following questions: Take two quantum states, $|\psi\rangle$ and $|\phi\rangle$, shared between several distant labs. If some local operations are performed on the state $|\psi\rangle$ in these local labs, can the resulting state be equal to the state $|\phi\rangle$? In other words, can $|\psi\rangle$ be transformed to $|\phi\rangle$ using only local operations? And if so, how do such local manipulations change entanglement present in the state?

There are three most studied operations in this direction: Local unitaries (LU), local operations and classical communication (LOCC), and stochastic local operations and classical communication (SLOCC). Here we give a brief overview of each of them:

(i) *LU equivalence*: Two N-partite states, $|\psi\rangle$ and $|\phi\rangle$, are equivalent to each other under local unitary transformations, if there exist unitary matrices $U_1, \ldots, U_N$, such that

$$U_1 \otimes \cdots \otimes U_N |\psi\rangle = |\phi\rangle. \tag{2.10}$$

Note that such operations cannot change any entanglement property of a given quantum state. Therefore, this is the strongest form of local equivalence in the sense that, if the state $|\psi\rangle$ can be used for any quantum information processing task, the same is true for the state $|\phi\rangle$ and the other way around.

The following two-by-two self-adjoint local unitary operations will play an important role throughout the thesis:

$$\text{Pauli-}Z: \quad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \text{Pauli-}X: \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{2.11}$$

We will be denoting them as Z and X. Pauli operators Z and X are the generators for Pauli group P consisting of four elements:

$$P = \{\mathbb{1}, Z, X, Y\}, \tag{2.12}$$

where the self-adjoint Pauli-Y operator is equal to $Y = iXZ = -iZX$.

(ii) *LOCC*: This class of operations is difficult to describe mathematically, however, one can note that under LOCC action entanglement present in the state cannot increase. We will discuss this more closely when looking at entanglement measures in the next section.

(iii) *SLOCC equivalence*: These are probabilistic LOCC. To say otherwise, we want to transform state $|\psi\rangle$ to the state $|\phi\rangle$ via LOCC with a non-zero probability. The set of LOCC are the strict subset of the set of SLOCC. These general stochastic operations seem physically less motivated at the first sight, as they can indeed change entanglement quantifiers of states they are acting on. However, they have the major advantage that their mathematical description is quite simple and this helps to reveal a rich structure of multipartite entanglement. Mathematically an action of SLOCC on a d-dimensional Hilbert space is represented by a $d \times d$ general invertible matrix in GL_d. Two N-partite states $|\psi\rangle$ and $|\phi\rangle$ are SLOCC equivalent, if there exist invertible operations $A, B, \ldots N$ acting on respective subsystems such that

$$A \otimes B \otimes \cdots \otimes N|\psi\rangle = |\phi\rangle. \tag{2.13}$$

These operations define equivalence classes for quantum states. For example, every two-qubit entangled state is SLOCC equivalent to a Bell state, given in Eq. (2.5). In other words, there is a single SLOCC equivalence class in two-qubit state space. Situation changes drastically with the increasing number of particles. Already for three qubits there are two SLOCC classes of genuine tripartite entangled states, which cannot be transformed to each other via SLOCC [47]. Their representatives are GHZ- and W-states, given in Eq. (2.9). In four qubits there are already infinitely many SLOCC classes [48]. This classification of entanglement underlines that the bipartite entanglement is very different from a highly complicated multipartite case.

More generally than all three classes of operations discussed above, in terms of the resource theory of entanglement, one wishes to study *non-entangling maps* or, alternatively, *separability-preserving maps* in different scenarios. These are the largest classes of quantum operations, which map separable states to separable states and have been

extensively investigated qualitatively and quantitatively [49–52], but these kind of general maps are outside of the scope this thesis.

2.1.4 Entanglement measures

Entanglement measure $E(\rho)$ is used to quantify amount of entanglement in the state ρ and fulfills several properties:

(i) If the state ρ is separable, then it vanishes, $E(\rho) = 0$.

(ii) Entanglement measure is invariant under local unitary transformations:

$$E(\rho) = E(U_1 \otimes \cdots \otimes U_N \; \rho \; U_1^\dagger \otimes \cdots \otimes U_N^\dagger). \tag{2.14}$$

(iii) Given a positive map Λ_{LOCC} mathematically describing LOCC operations, entanglement measure cannot increase under such a map:

$$E[\Lambda_{LOCC}(\rho)] \leq E(\rho). \tag{2.15}$$

To learn more about entanglement measures and their properties see reviews [53, 54].

One of the examples of multipartite entanglement measures is the *geometric measure of entanglement* E_G [55, 56]. This entanglement measure quantifies the distance between a given state and a set of separable states. For pure states it is defined to be one minus the maximal squared overlap between a given state and the closest product state:

$$E_G(|\psi\rangle) = 1 - \max_{|\phi\rangle = |a\rangle|b\rangle|c\rangle \ldots} |\langle\phi|\psi\rangle|^2. \tag{2.16}$$

Geometric measure of entanglement of many pure states has been calculated using different techniques and algorithms [55, 57–61]. However, since one needs to optimize over increasing number of parameters in multipartite case, the problem is still challenging for general states. On the other hand, if the given state is permutation symmetric one can make the optimization problem significantly easier.

Theorem 2.5. *[62] Given an N-partite permutation symmetric pure state $|\psi\rangle_{symm}$, where $N \geq 3$, the closest product state maximizing the overlap with this state must necessarily be permutation symmetric:*

$$E_g(|\psi\rangle_{symm}) = 1 - \max_{|a\rangle} |\langle a|^{\otimes N} |\psi\rangle_{symm}|^2. \tag{2.17}$$

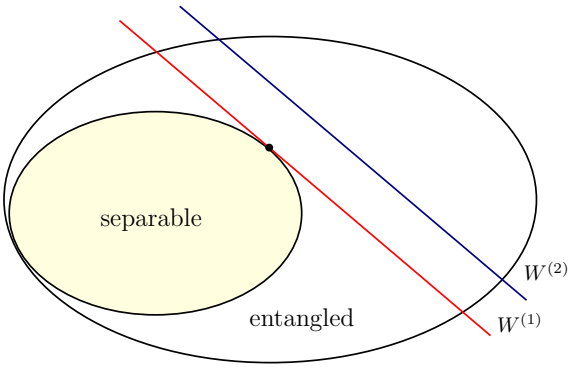


FIGURE 2.1: Schematic representation of the convex set of all states and the nested convex set of separable states. The hyperplanes $W^{(1)}$ and $W^{(2)}$ are entanglement witnesses. We refer to the former as a *tight* witness, as $\mathrm{tr}(W^{(1)}\rho_s) = 0$ for some pure product state ρ_s.

Moreover, if all the coefficients of the state $|\psi\rangle_{symm}$ are positive real numbers, it is straightforward to see that the closest product state can also be chosen to be real-valued. For permutation symmetric qubit states this construction reduces calculations to a single parameter optimization problem.

2.1.5 Entanglement Witnesses

In the previous section we saw quantifiers of entanglement. Here we introduce a construction to detect entanglement, entanglement witnesses [63]. There is a subtle difference between entanglement measures and witnesses. When quantifying entanglement using, for example, geometric measure, we need to know the exact description of the multipartite quantum state in order to find out its distance to the separable states and only then deduce, whether it is entangled or not. On the other hand, entanglement witnesses correspond to observables, which can be directly measured in experiments. Alone from the measurement results and statistics one can deduce, if the measured unknown state was entangled.

Definition 2.6. An observable W is called an entanglement witness, if the following holds

$$\mathrm{tr}[W\rho_s] \geq 0, \quad \text{for all separable states } \rho_s \text{ and}$$

$$\mathrm{tr}[W\rho_e] < 0, \quad \text{for at least one entangled state } \rho_e.$$

Therefore, if in the experiment one obtains $\mathrm{tr}[W\rho] < 0$, one can conclude that ρ is entangled.

In order to understand entanglement witnesses, it is instructive to keep the geometrical picture in mind, see Fig. 2.1. Here we denote the set of all states and the set of separable states as a nested convex structure. The expectation value of an observable depends linearly on the state and, therefore, lines cutting the entire state space are defined by the hyperpnales of the type $\mathrm{tr}\,(O\rho) = c$, for some observable O and a constant value $c \in \mathbb{R}$. However, by definition not all such hyperplanes are entanglement witnesses, but only the ones which have non-negative expectation values for all separable states. In Fig. 2.1 the hyperplanes $W^{(1)}$ and $W^{(2)}$ correspond to witnesses. Any state on the right hand side of the hyperplane $W^{(2)}$ can be detected by this witness. The hyperplane $W^{(1)}$ can also detect all these states and, in addition, the ones between $W^{(1)}$ and $W^{(2)}$. One can conclude that $W^{(1)}$ is more powerful witness than $W^{(2)}$. Moreover, since the witness $W^{(1)}$ is touching the set of separable states, or to say it otherwise, since $\mathrm{tr}\,(W^{(1)}\rho_s) = 0$ for some separable state ρ_s, we say that the witness $W^{(1)}$ is *tight*. However, tight witnesses as are not necessarily the most powerful ones. From the geometrical picture the following statement follows.

Theorem 2.7. *[42] For every entangled state ρ_e exists an entanglement witness that detects it.*

The main question now is: Given some entangled quantum state, how to construct an entanglement witness, which detects it and how to make sure that this witness is tight?

Construction of witnesses

In this subsection we consider the construction of entanglement witnesses. There are many ways to construct entanglement witnesses, see Ref. [64] for an overview. One possible way to design a witness for any state $|\psi\rangle$ is to consider the following observable

$$\mathcal{W} = \alpha\mathbb{1} - |\psi\rangle\langle\psi|. \tag{2.18}$$

The main task then is to determine minimal $\alpha \in \mathbb{R}^+$, such that $\mathcal{W}$ is still positive on all separable states. However, since the set of separable states is defined as a convex hull of all pure product states, the optimization can be done only over pure product states. Therefore, α in Eq. (2.18) is the maximal overlap between the state $|\psi\rangle$ and the pure biseparable states. This can be computed by the maximal squared Schmidt coefficient occurring when computing the Schmidt decomposition with respect to all bipartitions,

$$\alpha = \max_{bipartitions} \{\max_{\lambda_k^{BP}} \{[\lambda_k^{BP}]^2\}\}. \tag{2.19}$$

This optimization is in general a difficult problem. However, we shall see later that for special classes of states the optimization can be fully understood. On the other hand, finding α helps us not only detect, but also quantify entanglement, more precisely, to lower-bound the value of the geometric measure of entanglement for a given state $|\psi\rangle$.

2.2 Nonlocality

In this section we take a different approach from the previous ones to detect entanglement in a so-called device-independent way using Bell inequalities. The main idea here is to derive a set of inequalities, which must be satisfied by any local realistic theory, but can be violated in quantum mechanics. Mathematically local theory can be described by *local hidden variable (LHV)* models. Throughout this section we explain LHV theories and its incompatibility with quantum mechanics for various scenarios.

2.2.1 Bell inequalities

Bipartite case

We introduce the setup on a bipartite system shared between Alice and Bob. Both parties make local measurements on their respective subsystems. If one assumes local realism, or otherwise, one assumes that measurement outcomes existed locally before the measurements were made and that no superluminal signaling is possible, one can derive bounds on two-body correlations obtained from two space-like separated measurements. However, one can perform a quantum mechanical experiment, where these bounds are surpassed by the correlations obtained from a shared entangled system. Therefore, measurement results of such experiment cannot be described by LHV models.

Local hidden variable models

Here first we introduce a Bell scenario for two parties, each having two measurement settings with two outcomes. Consider a system shared between Alice and Bob as shown in Fig. 2.2. Alice and Bob both can measure two quantities each on their respective parties. Alice can choose between measurements A_1 and A_2 and Bob between B_1 and B_2. Results of experiments are $a \in \{+1, -1\}$ for Alice and similarly $b \in \{+1, -1\}$ for Bob. Correlations for each choice of measurements can be calculated

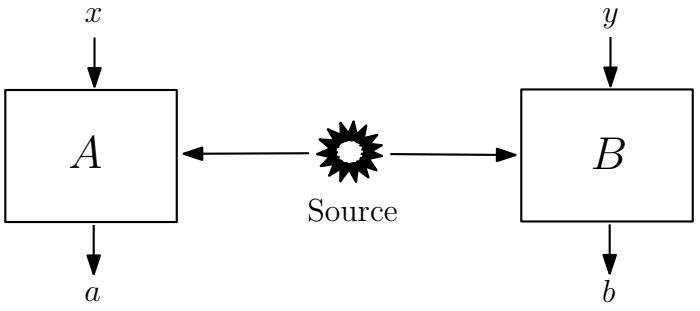


FIGURE 2.2: A schematic representation of a Bell scenario. A source produces an entangled pair of particles and sends each to labs of Alice and Bob. Alice and Bob choose their measurement settings x and y, respectively and get outcomes a and b.

as follows

$$\langle A_i B_j \rangle = p(++|A_i B_j) - p(+-|A_i B_j) - p(-+|A_i B_j) + p(--|A_i B_j). \tag{2.20}$$

Here $p(+-|A_i B_j)$ corresponds to a joint probability of Alice measuring A_i and obtaining outcome $a = +1$ and Bob measuring B_j and obtaining outcome $b = -1$. LHV models assign for every value of the hidden variable, λ, results to all measurements of the parties in a local manner, meaning that for a fixed LHV Alice's probabilities cannot depend on Bob's choice of measurement and vice versa. Therefore, the probabilities, described by the response functions χ for a given value of hidden variable factorize:

$$p(a, b|A_i, B_j) = \int d\lambda p(\lambda) \chi^A(a|A_i, \lambda) \chi^B(b|B_j, \lambda), \tag{2.21}$$

where $a, b \in \{+, -\}$ correspond to possible outcomes and the hidden variable λ occurs with probability $p(\lambda)$. One can always assume that LHV assigns deterministic values 0 or 1 to the response functions $\chi^A(a|A_i, \lambda)$ and $\chi^B(b|B_j, \lambda)$ for a fixed value of λ [65].

From the deterministic nature of LHV model and its predictions for probabilities, one can directly see that the following inequality is always satisfied on the level of probabilities [66]:

$$p(--|A_1 B_1) + p(+-|A_1 B_2) + p(-+|A_2 B_1) - p(--|A_2 B_2) \geq 0. \tag{2.22}$$

One can similarly choose to work on the level of expectation values:

$$\langle A_i B_j \rangle = \int d\lambda p(\lambda) \mathcal{U}(A_i, \lambda) \mathcal{U}(B_j, \lambda), \tag{2.23}$$

where $\mathcal{U}(A_i, \lambda) = \chi^A(+|A_i, \lambda) - \chi^A(-|A_i, \lambda)$ and rewrite the inequality in Eq. (2.22)

accordingly. As a result, the well known Clauser-Horne-Shimony-Holt (CHSH) inequality comes out [5, 67]:

$$\langle A_1 B_1 \rangle + \langle A_1 B_2 \rangle + \langle A_2 B_1 \rangle - \langle A_2 B_2 \rangle \leq 2. \tag{2.24}$$

Similarly to the case of probabilities, one can also easily check all possible deterministic assignments to the expectation values in the inequality in order to prove the LHV bound. Therefore, local hidden variable predictions satisfy these inequalities, called *Bell inequalities* [3], whether they are written on the level of probabilities or expectation values.

To shift ourselves to quantum mechanics, we choose measurements on Alice's side to be quantum mechanical observables $A_1 = -X$ and $A_2 = -Y$, Bob's observables to be $B_1 = (X + Y)/\sqrt{2}$ and $B_2 = (X - Y)/\sqrt{2}$. Here X and Y correspond to Pauli spin operators. Consequently, we define a so-called Bell operator [68]

$$\mathcal{B} = A_1 \otimes B_1 + A_2 \otimes B_1 + A_1 \otimes B_2 - A_2 \otimes B_2. \tag{2.25}$$

Then, if we look for the maximum expectation value that quantum states can attain over this operator, we get that

$$\max_{|\psi\rangle} \langle \psi | \mathcal{B} | \psi \rangle \leq 2\sqrt{2}, \tag{2.26}$$

where the value $2\sqrt{2}$ corresponds to the largest eigenvalue of the operator $\mathcal{B}$. The corresponding eigenstate is a two-qubit singlet state $|\Psi^-\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$, which is LU equivalent to the maximally entangled state in Eq. (2.5). It appears that $2\sqrt{2}$ is the maximal violation quantum mechanics allows for such a Bell scenario and is known as the Tsirelson bound [69].

The violation of Bell inequalities have been extensively tested in experiments [70, 71]. The conclusions that one can draw from these results is that the constraints that local hidden variable theories put on the point behaviour $p(a, b|A_i, B_j)$ are not compatible with nature, which is quantum mechanical.

Multipartite case

The concept of bipartite Bell inequalities can be easily generalized to the multipartite case. Let us assume that there are N different parties in N distinct labs measuring some observables on a shared system. Then the measurement outcomes and their correlations are described by fully local hidden variable models, if for any choice of

measured quantity we can express its expectation value in the following fashion,

$$\langle A_i B_j C_k \dots \rangle = \int d\lambda p(\lambda) \mathcal{U}(A_i, \lambda) \mathcal{U}(B_j, \lambda) \mathcal{U}(C_k, \lambda) \dots, \tag{2.27}$$

where $\mathcal{U}(A_i, \lambda)$ is described as before. The violation of this inequality certifies entanglement in the measured multipartite quantum system.

2.2.2 Genuine multipartite nonlocality

So far we only considered hidden variable models where all the probabilities factorized. Now for multipartite case we go beyond this restricted type of models to the so-called *hybrid* models [45]. The hybrid model is similar to the definition of the biseparability, since one asks if the given correlations can be explained by hidden variable model where one party (let us say party A) is local with respect to the other parties (let us say B and C together), or otherwise, if the joint probability factorizes as follows:

$$p(a, b, c|A_i, B_j, C_k) = \int d\lambda p(\lambda) \chi^A(a|A_i, \lambda) \chi^{BC}(b, c|B_j, C_k, \lambda). \tag{2.28}$$

Here $\chi^{BC}(b, c|B_j, C_k, \lambda)$ is a nonlocal response function for party B and C together. In order to prevent direct conflict with relativity, we assume that the response function $\chi^{BC}(b, c|B_j, C_k, \lambda)$ does not allow instantaneous signaling. Put differently, the joint probability distribution for Bob and Charlie is limited by no-signaling constraints formally expressed as:

$$\begin{aligned} \sum_c p(b, c|B_j, C_k) &= \sum_c p(b, c|B_j, C'_k), \quad \text{for all } b,\ B_j,\ C_k,\ C'_k\ . \\ \sum_b p(b, c|B_j, C_k) &= \sum_b p(b, c|B'_j, C_k), \quad \text{for all } c,\ C_k,\ B_j,\ B'_j\ . \end{aligned} \tag{2.29}$$

Physically these constraints impose that the local marginals of Bob's probabilities must be independent of Charlie's choice of measurement settings and vice versa. Together with the positivity and normalization constraints of probabilities, no-signaling constraints form a no-signaling polytope. A polytope can be fully described as a convex hull of finite set of vertices. For the Bell-scenario with two measurements and two outcomes there are 24 such vertices, 16 of which are the local deterministic ones, but the rest of 8 are nonlocal vertices, all described by so-called *PR-boxes* and are equivalent up to some relabeling of measurement settings and outcomes:

$$p(b, c|B_j, C_k) = \begin{cases} 1/2, & \text{if } \frac{b+1}{2} \oplus \frac{c+1}{2} = (j-1)(k-1), \\ 0, & \text{otherwise,} \end{cases} \tag{2.30}$$

where $j,k \in \{1,2\}$ are choice of measurement settings. It is straightforward to check that the correlations of PR-box surpasses the maximal value of CHSH-inequality violation for quantum mechanics $2\sqrt{2}$ and attains the algebraic maximum, 4, for the inequality. See Ref. [72] for the review on the topic.

As a next step we consider taking probabilistic mixture of the hybrid scenario for all possible bipartitions. Then for the tripartite case this would lead to a hidden variable model explaining the following correlations:

$$\begin{aligned}\langle A_i B_j C_k \rangle = p_1 \int d\lambda p(\lambda)\mathcal{U}(A_i,\lambda)\mathcal{U}(B_j,C_k,\lambda) \\ + p_2 \int d\lambda p'(\lambda)\mathcal{U}'(B_j,\lambda)\mathcal{U}'(A_i,C_k,\lambda) \\ + p_3 \int d\lambda p''(\lambda)\mathcal{U}''(C_k,\lambda)\mathcal{U}''(A_i,B_j,\lambda),\end{aligned} \tag{2.31}$$

where $p_1 + p_2 + p_3$=1. If such a description of correlations cannot replicate results obtained in experiments, we say that the measured state reveals *genuine tripartite nonlocality*.

Here we review how to detect genuine multiparticle nonlocality using linear programming techniques. Having fixed the number of measurement settings and outcomes, probabilities arising from a hybrid local-nonsignalling model for the splitting $A|BC$, form a polytope whose extremal points are given by combinations of deterministic local assignments for the party A and extremal nonsignalling assignments, i.e., local deterministic and PR-boxes [72], for the parties BC. In order to detect genuine multiparticle nonlocality, one has to consider all combinations of probabilities arising from this and the other local-nonsignalling splittings, namely $C|AB$ and $B|AC$. Geometrically, this corresponds to taking the convex hull of the three polytopes associated with the three different splittings. Let us denote such polytopes as $P_{A|BC}$, $P_{C|AB}$, $P_{B|AC}$ and their convex hull as P_{L-NS}. By definition of a convex hull, every vector $\vec{p} \in P_{L-NS}$ can be written as a convex combination of its extremal points, denoted by $\vec{v}_{A|BC}$, $\vec{v}_{B|AC}$, and $\vec{v}_{AB|C}$.

Hence, in order to check whether a given point $\vec{p}$ belongs to the polytope P_{L-NS}, we need to solve the following membership problem formulated as a *linear program (LP)* [72]:

$$\begin{aligned}\text{maximize:} \quad & \vec{\kappa}\cdot\vec{p} - C \\ \text{subject to:} \quad & \vec{\kappa}\cdot\vec{v}_i - C \leq 0, \quad \text{for all } \vec{v}_i \\ & \vec{\kappa}\cdot\vec{p} - C \leq 1.\end{aligned} \tag{2.32}$$

The variables of the LP are $\{\vec{\kappa}, C\}$, where $\vec{\kappa}$ represents the coefficient of a Bell inequality, detecting genuine multiparticle nonlocality, and C the corresponding local-nonsignalling bound. The LP optimizes the coefficients $\vec{\kappa}$ to obtain the maximal value (at most $C+1$) for the quantum probabilities, while keeping the local-nonsignaling bound equal to C. As a consequence, the vector $\vec{p}$ can be written as a convex combination of $\{\vec{v}_i\}$, if and only if the optimal value of the LP is 0.

2.2.3 Hardy-type argument

Just like in standard Bell tests, in Hardy argument the parties generate the conditional statistics in the form of the correlations. The distinctive feature of Hardy-type nonlocality proofs is that we are only concerned whether these probabilities are strictly positive or exactly zero, corresponding to possible and impossible results, respectively. Let us recall the original Hardy argument for bipartite systems, with two measurement settings $A_{1,2}$ and $B_{1,2}$ and two outcomes $\{+,-\}$ [73]. The essence of the argument is that the following four expressions can not be simultaneously satisfied in any local realistic theory:

$$\begin{aligned} p(+,+|A_1,B_1) &= 0, \\ p(-,+|A_1,B_2) &= 0, \\ p(+,-|A_2,B_1) &= 0, \\ p(+,+|A_2,B_2) &> 0. \end{aligned} \tag{2.33}$$

This, then, implies that the event of observing $(+,+)$ having measured A_2 and B_2 is impossible in local realistic theory, while measurements on a quantum system can exhibit such correlations [73]. Hardy-type arguments for many states have been studied and it is known that almost all entangled states reveal such a contradiction with local realism [74].

2.3 Quantum computation

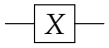
One of the main applications of quantum information theory is quantum computation. Here we review quantum computation and its elementary building blocks.

2.3.1 Quantum Circuits

A quantum computer is built in a resemblance to its classical counterpart. Rather having electrical circuits composed of wires and logic gates, quantum computation is carried out via quantum circuits built with quantum "wires", carrying quantum information, and quantum gates modifying this information. Quantum circuits consist of compositions of quantum gates, which themselves are mathematically described by unitary operations acting on quantum information, in general, expressed in computational basis. An example of a quantum gate in an analogy with its classical equivalent is a NOT-gate, implemented by Pauli-X operator:

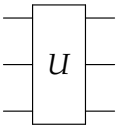
$$X|0\rangle = |1\rangle \quad \text{and} \quad X|1\rangle = |0\rangle. \tag{2.34}$$

In a circuit model this gate is represented as follows:

Pauli-X gate: 

It is conventional to assume that information flows from left to right. In order to express multi-qubit gates, the gate must have multiple inputs and outputs, represented by parallel wires:

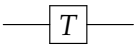
Multi-qubit Gate



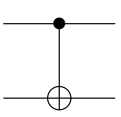
Any unitary operation is a quantum gate, but there are several conventionally important quantum single- and multi-qubit gates that we introduce here, both, algebraically and diagrammatically:

Hadamard

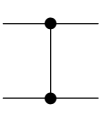
T Gate



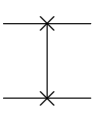
CNOT Gate



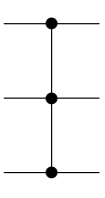
CZ Gate



Swap Gate



CCZ Gate



In a matrix notation these gates look as follows:

$$\text{Single qubit gates:} \quad H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \qquad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}. \tag{2.35}$$

Two-qubit gates:

$$CZ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \quad CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad SWAP = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \tag{2.36}$$

and the three-qubit CCZ gate

$$CCZ = \mathbb{1} - 2|111\rangle\langle 111|. \tag{2.37}$$

Another important single qubit gate is a square-root of Pauli-Z operator and is called a *phase-gate*. Note also its connection with T-gate, $\sqrt{Z} = T^2$.

In general, the length of a quantum computation is expressed by the depth of a quantum circuit implementing this computation. The depth increases when unitary gates in a given circuit do not commute as they cannot be implemented in one time step of a computation.

2.3.2 Universal gate sets

In classical computation a small set of gates can be used to decompose an arbitrary classical function. Such sets of gates are called *universal*. The same concept can be adopted in quantum computation.

Definition 2.8. A quantum gate-set is said to be universal, if a quantum circuit built up using the gates from this gate-set can approximate any unitary operation to an arbitrary accuracy.

Here we introduce two of the most popular universal gate-sets:

Theorem 2.9. *[75] A gate-set $\{CNOT, H, T\}$ is universal for quantum computation.*

Theorem 2.10. *[76] A gate-set $\{CCZ, H\}$ is universal for quantum computation.*

In addition to the universality, there exists an insightful hierarchy of unitary gates, called *Clifford hierarchy*. The Pauli group, $P = \{\mathbb{1}, X, Y, Z\}$, corresponds to the first level in this hierarchy, $\mathcal{C}_1$. The unitary gates in the k-th level of the Clifford hierarchy $\mathcal{C}_k$ are defined inductively using the Pauli-group:

$$\mathcal{C}_{k+1} = \{U |\ \forall U_P \in \mathcal{C}_1,\ UU_PU^\dagger \in \mathcal{C}_k\}. \tag{2.38}$$

The gates in the second level $\mathcal{C}_2$ form a finite group, so-called *Clifford group*. This group is generated by gates $\{CNOT, H, \sqrt{Z}\}$ and is the normalizer of the Pauli group, that is, it preserves the Pauli group elements under conjugation.

The Clifford group is not universal for quantum computation. What is more, there is a famous theorem called the *Gottesman-Knill Theorem*, which states that

Theorem 2.11. *[28] A quantum unitary evolution using only the following elements can be efficiently simulated on a classical computer:*

- *Initialization of a quantum state in any of the computation bases element, e.g.* $|0 \dots 0\rangle$.
- *Evolving the initial state with the unitaries from Clifford group.*
- *Measuring the resulting state in computational basis.*

To sum the discussion of universality, in both theorems, Theorem 2.9 and Theorem 2.10, the universal gate sets contain gates from the Clifford group and, in addition, a single gate from the third level of Clifford hierarchy. In case of Theorem 2.9, $T \in \mathcal{C}_3$ is needed for universality and for latter, $CCZ \in \mathcal{C}_3$.

2.3.3 Quantum error-correcting codes

Introduction to error-correction

Coping with noise and correcting errors in information processing is one of the most important tasks. In classical information theory error detection and correction has been broadly studied. The key idea here is to *encode* the message into some bigger message in a way that, even if errors have occurred, there is enough redundancy in the encoded message to recover original message. We call this last step *decoding*. To give a simple and a standard classical example, suppose we wish to send a single bit message, but the communication channel is not perfect. That is, with a probability $p > 0$ the message will arrive unchanged, but with a probability $(1 - p)$ the bit we are sending might get flipped. One way to improve our chances of communicating a right message is to send three copies of the message in the following way:

$$0 \mapsto 000 \tag{2.39}$$

$$1 \mapsto 111. \tag{2.40}$$

The bit strings 000 and 111 are called logical 0 and 1, respectively. We say that an original message is encoded in the logical subspace. All three bits are sent through the noisy communication channel as described above. The receiver at the end of the channel gets a possibly corrupted message. Nevertheless, now he/she can decide with the majority voting, whether the original message was 0, or 1. This simple error correction code is called a *repetition code*.

More complicated and effective error correcting techniques have been developed in classical case, however, here we switch out attention to quantum error-correction codes. There are subtle differences between classical and quantum information processing that one can already grasp from the simple repetition code example. These dissimilarities necessitate new techniques to make quantum error-correction realizable. We shortly describe them here:

- *No cloning:* Quantum state cannot be copied. Consequently, there cannot be the direct quantum analog to the repetition code.

- *Continuous errors:* In classical information processing, when error occurs, a value of a classical bit gets flipped. In quantum information processing on the other hand, there can be other kind of errors, e.g., the phase-flip error. Any one-qubit operator corresponds to an error that can occur on a single quantum bit. Therefore, errors in quantum information processing are continuous.
- *Measurement destroys quantum information:* In quantum mechanics after a measurement is made on a states, the state is projected in one of the eigenstates of the measured observable. As a consequence, information about the original state is impossible to be recovered.

Fortunately, it is possible to circumvent all these challenges that quantum mechanics brings in. In order to see this, we consider the simplest quantum error-correcting code in the analogy of the repetition code: Encode a singe qubit state $a|0\rangle + b|1\rangle$ in three qubits as $a|000\rangle + b|000\rangle$. The encoded space is the logical space spanned by two basis vectors, the logical zero, $|0_L\rangle \equiv |000\rangle$ and the logical one, $|1_L\rangle \equiv |111\rangle$. Then the encoded qubits are passed through the noisy channel, which with the probability p performs the so-called bit-flip, Pauli-X operation on the qubit and with the probability $(1-p)$, leaves it untouched. If the error occurs on one or less qubits, then it can be corrected with the following procedure:

- (i) *Error-detection:* For error-detection measurements must be performed on the received message. Since it is assumed that $p < 1/2$, the measurements are only required to check, whether no error or one error has occurred. This can be done using the projectors of the following form:

$$P_0 = |000\rangle\langle 000| + |111\rangle\langle 111|, \tag{2.41}$$
$$P_1 = |001\rangle\langle 001| + |110\rangle\langle 110|, \tag{2.42}$$
$$P_2 = |010\rangle\langle 010| + |101\rangle\langle 101|, \tag{2.43}$$
$$P_3 = |100\rangle\langle 100| + |011\rangle\langle 011|. \tag{2.44}$$

  It is noteworthy that these projective measurements do not change the state received and moreover, their outcome cannot reveal any information about the value of the encoded state. This step only helps identify where the bit-flip error has occurred.
- (ii) *Recovery:* Once the location of the flipped bit is identified, it can be perfectly reversed back to the original state.

This example demonstrated that all the difficulties quantumness brings into error-correction can be coped with. Similarly to the bit-flip case, one can design an error-correcting code for the phase-flip. Moreover, one can even extend this analysis to an arbitrary single qubit error E by considering its decomposition into Pauli matrices:

$$E = e_o \mathbb{1} + e_1 X + e_2 Z + e_3 XZ. \tag{2.45}$$

Then, if the single error happens on one of the qubits in the logical subspace $E_i|\psi_L\rangle = E_i(a|0_L\rangle + b|1_L\rangle$, one can first write out the new corrupted state as a superposition of four

possible scenarios: no error, bit-flip error, phase-flip error, and bit and phase-flip errors together. Then one can apply error-detecting procedures to decide which of these four errors has occurred. As a result, one can resolve correcting a continuum of errors in a discrete manner.

Conditions for quantum error-correction

In the previous section we learned elementary concepts for quantum error-correction. Now we formalize the conditions, which guarantee that the logical subspace, we encode the message in, can detect or correct certain amount of errors. At this point, some very broad assumptions are in order. First, we assume that the noise can be described by some quantum operation $\mathcal{E}$ and, second, the complete error-correction step can be captured by a trace-preserving quantum operation $\mathcal{R}$. Here we must note that certain codes can only have power to detect existence of errors, but they cannot correct them. Hence, naturally, the operation $\mathcal{R}$ can be thought as a two step procedure: Error-detection and error-correction. Finally, given an error-correcting code, formally defined as a subspace C of some Hilbert space, the error-correction to be successful, the following requirement must be fulfilled for any state ρ with its support in C

$$(\mathcal{R} \circ \mathcal{E}(\rho)) \propto \rho. \tag{2.46}$$

Not every subspace C is useful for the error-detection/correction. If we want to detect/correct errors using a subspace C, it must satisfy certain conditions. Knill and Laflamme formulated these conditions for the general case [77]:

Theorem 2.12 (Knill-Laflamme)**.** *Let $C \subset \mathcal{H}$ be a quantum code and P the projector onto C. Suppose $\mathcal{E}$ is a quantum noise operator with elements $\{E_i\}$. Then there exists a recovery operator $\mathcal{R}$, if and only if the following conditions hold*

$$PE_i^\dagger E_j P = \alpha_{ij} P, \quad \forall\, i, j \tag{2.47}$$

and for some Hermitian matrix α.

In this thesis we assume that the noise model is local and independent on each Hilbert space. Thus, it can be expressed as a tensor product of errors acting on the respective local dimensions. We will be only discussing codes over qubit systems and therefore, we can express errors in Pauli operator basis as in Eq. (2.45). We say that noise is acting trivially on some qubit, if the identity gate, $E_0 = \mathbb{1}$, is applied on this qubit. Number of non-trivial errors acting on the subspace is called the *weight* of errors and is denoted by $w(E)$.

Now, we are ready to define a *distance d* quantum error-correcting code:

Definition 2.13. A distance d quantum error-correcting code C on a system of n parties, each of local dimension D is defined as a K-dimensional subspace C and is conventionally denoted as $((n, K, d))_D$. Then, any of its orthonormal bases, $\{|c_i\rangle\}$ satisfies the Knill-Laflamme conditions

for all errors $\{E_k\}$ of weight less than d, $w(E_k) < d$,

$$\langle c_l|E_k|c_m\rangle = \begin{cases} 0, & \text{for } l \neq m, \\ \alpha_k, & \text{for } l = m. \end{cases} \tag{2.48}$$

In addition, we say that the code is pure if $\alpha_k = \mathrm{tr}\,(E_k)/D^N$ and we refer to this restricted version of Knill-Laflamme conditions as strict Knill-Laflamme conditions.

A code with distance d can either correct any errors acting non-trivially on at most $(d-1)/2$ qubits, or can detect errors on at most $(d-1)$ qubits. Importantly, the parameters of code C, $((n, K, d))_D$ cannot take arbitrary values.

Theorem 2.14. *(Singleton bound) [78] Let C be a quantum code with parameters $((n, K, d))_D$. Then the following inequality must hold,*

$$K \leq D^{n-2d+2}. \tag{2.49}$$

The Singleton bound underlines that, for example, it is not possible to demand correcting arbitrarily many errors, having fixed the number of particles and the code subspace dimension. Many conditions, constructions, and restrictions exist in a similar spirit to rule out existence of quantum error-correcting codes of certain number of qubits, dimensions, and distance [34, 79–84]. There exist tables presenting already discovered codes and alongside describing the parameters for still many unknown cases [85].

Most prominent examples of the codes are stabilizer codes. For the purpose of this thesis, we do not need a detailed introduction of these codes, but see Refs. [34, 35] for an overview. Stabilizer codes are also called *additive*, due to the connection to classical codes. Qubit stabilizer codes are related to classical additive codes over the finite field $GF(4)$. But more interestingly to us, they are also referred to as *graph* codes, since their basis can be chosen to be multipartite entangled states, called graph states. We introduce graph states in Section 2.4.1 and explain their exact role in quantum error-correcting codes.

Nevertheless, here we give a brief insight, why multipartite entanglement is desirable for error-correction. If a pure code has a distance d, then any state in that code has $(d-1)$ qubit reduced density matrices (RDMs) maximally mixed. States complying with this requirements are highly entangled across any bipartition [17, 18]. Therefore, ideally one looks for an n-particle state with all of its $\lfloor n/2 \rfloor$ RDMs maximally mixed. Such states are called *absolutely maximally entangled (AME)* states. For qubits they do not exist for $n = 4$ and $n > 6$ [86]. And the ones that exist can be described by graph states, as we will see in the subsequent section.

As it is often impossible for a given number of particles n and local dimensions D to find an AME state, one investigates an optimal number k, such that exists at least one state of n qudits, with maximally mixed k marginals. In the literature such states are sometimes called *k-uniform* states. However, this naming conflicts with some other notation in the thesis. So, we will be instead using the k RDMs or k marginals, interchangeably.

2.4 Multipartite pure states and their applications

Due to its possible applications in quantum information processing, multiparticle entanglement is under intensive research. Its characterization has, however, turned out to be difficult. One problem hindering the exploration of multiparticle entanglement is the exponentially increasing dimension of the Hilbert space. This implies that making statements about general quantum states is difficult. So, one has to concentrate on families of multiparticle states with an easier-to-handle description. In fact, symmetries and other kinds of simplifications seem to be essential for a state to be a useful resource. Random states can often be shown to be highly entangled, but useless for quantum information processing [23–25]. One of the objectives in this field is the identification of families of states, which are useful in applications, but nevertheless, can be described by a simple formalism. In this section we introduce concepts and definitions for three classes of pure multipartite entangled states, then we discuss their properties and applications.

2.4.1 Graph states

An interesting class of multi-qubit quantum states is given by pure states called graph states [27]. Mathematically a graph $G = (V, E)$ is described by its set of vertices V and set of edges E. The set E contains an element $e = \{v_1, v_2\}$, if the vertices $v_1, v_2 \in V$ are connected by an edge. Physically vertices correspond to particles and edges represent two-body interactions between them. We will be assuming that we are working with the qubit systems.

2.4.1.1 Constructing graph states

A graph state $|G\rangle$ corresponds to a graph $G = (V, E)$ in a following manner:

- For each vertex $v \in V$, we initialize the physical system in the "+1" eigenstate of Pauli-X operator, $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$. Thus, the N-vertex graph state is initialized as $|+\rangle^{\otimes N}$, where $N = |V|$ is the cardinality of the vertex set.
- For each edge in the graph G, $e = \{v_1, v_2\}$, we apply the two-qubit entangling unitary, represented by a diagonal CZ_e gate, between qubits v_1 and v_2 of the initialized state $|+\rangle^{\otimes N}$. As a result we get a graph state corresponding to the graph G:

$$|G\rangle = \prod_{e \in E} CZ_e |+\rangle^{\otimes |V|}, \tag{2.50}$$

  where CZ gates are diagonal commuting unitaries, $CZ = \mathbb{1} - 2|11\rangle\langle 11|$.

The simplest non-trivial example of a graph state corresponds to the two-vertex graph in Fig. 2.3 (a). The state has a single CZ gate and is equal to:

$$|G_{(a)}\rangle = CZ_{12}|+\rangle_1|+\rangle_2 = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle) \tag{2.51}$$

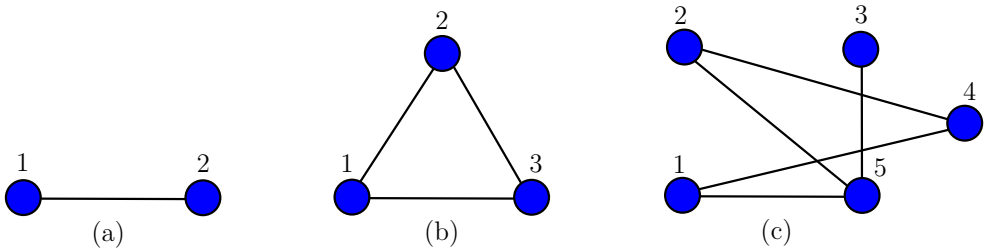


FIGURE 2.3: Graphs representing graph states: (a) The simplest non-trivial graph state, with two vertices and a single edge. This state is local unitary equivalent to the Bell-state. (b) Multipartite graph state with three vertices and three edges. This state is local unitary equivalent to the GHZ-state. (c) An arbitrary five-qubit graph state.

and is a maximally entangled state. To say it otherwise, it is local unitary equivalent to the Bell-state in Eq. (2.5). Note that the state is permutation symmetric as well as the graph is invariant under vertex relabeling.

As a second example we consider a three-qubit graph state in Fig. 2.3 (b). This graph has three vertices and three edges between them and can be written as follows:

$$|G_{(b)}\rangle = CZ_{12}CZ_{13}CZ_{23}|+\rangle_1|+\rangle_2|+\rangle_3 \tag{2.52}$$

$$= \frac{1}{2\sqrt{2}}(|000\rangle + |001\rangle + |010\rangle - |011\rangle + |100\rangle - |101\rangle - |110\rangle - |111\rangle). \tag{2.53}$$

One can see that this is too a permutation symmetric state, as the graph itself is invariant under vertex relabeling. The state $|G_{(b)}\rangle$ is local unitary equivalent to the GHZ-state in Eq. (2.9).

The state in Fig. 2.3 (c) represents an arbitrary five-vertex graph state. In general, when we consider N-vertex or N-qubit graph states, we will assume that the graph is connected, unless stated otherwise. That means, there is a connected path between any two vertices of a graph. Finally, we say that the graph state is (permutation) symmetric if it corresponds to a fully connected graph.

2.4.1.2 Stabilizer Formalism

There exists an alternative and a very fruitful definition of graph states, called a *stabilizer formalism.* Given an N-qubit graph state corresponding to a graph $G = (V, E)$, where $V = \{1, 2 \ldots, N\}$, for every vertex $i \in V$ we say that the function $\mathcal{N}(i)$ gives the neighbourhood of the vertex i, that is the set of all the vertices i is adjacent to. Then for each vertex $i \in V$ we can define the operator g_i consisting of the tensor product of Pauli-X on the vertex i and Pauli-Z's on $\mathcal{N}(i)$:

$$g_i = X_i \bigotimes_{j \in \mathcal{N}(i)} Z_j. \tag{2.54}$$

The operators g_i, $0 \leq i \leq N$ form a commutative group and the graph state $|G\rangle$ is their unique common eigenstate with eigenvalue "+1":

$$g_i|G\rangle = |G\rangle \qquad \text{for all } i \in V. \tag{2.55}$$

The stabilizer formalism and its properties have turned out to be very fruitful in studying graph states. We review some of its application is the consequent subsections.

2.4.1.3 Local unitary equivalent graph states

Given two N-qubit graph states $|G_1\rangle$ and $|G_2\rangle$, it is interesting to learn under which local transformations they are equivalent to each other. It turned out that for graph states LU operations are as powerful as SLOCC operations.

Lemma 2.15. *[31] Two N-qubit graph states $|G_1\rangle$ and $|G_2\rangle$ are SLOCC equivalent, if and only if they are LU equivalent.*

From Lemma 2.15 we directly understand that for two-qubits, as expected, there is only the single local unitary equivalence class of graph states. The graph state in Fig. 2.3 (b) corresponds to the GHZ-state and it appears that all other three-qubit graph states are also in the GHZ-class. Therefore, all other graphs with three vertices represent the same state up to LU equivalence. In the following we review a graphical rule of how to transform one graph state to another under local unitaries.

We use local Clifford group operators which correspond to the square-roots of Pauli matrices:

$$\sqrt{X}^{\pm} = \begin{pmatrix} \frac{1\pm i}{2} & \frac{1\mp i}{2} \\ \frac{1\mp i}{2} & \frac{1\pm i}{2} \end{pmatrix} = |+\rangle\langle +| \pm i|-\rangle\langle -|, \quad \sqrt{Z}^{\pm} = \begin{pmatrix} 1 & 0 \\ 0 & \pm i \end{pmatrix}, \tag{2.56}$$

where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ is a "± 1" eigenstate of Pauli-X. Recall that, the Clifford group is a normalizer of the Pauli group. Hence, for graph state equivalence local Clifford group operations play an outstanding role.

An N-qubit graph state $|G\rangle$ can be transformed to another N-qubit graph state $|G'\rangle$ by means of local Clifford group actions, if and only if the graph G' can be obtained from the graph G by a series of *local complementations* [87]. The local complementation on a graph G works as follows: One picks a vertex $i \in V$ and complements a subgraph induced over the neighbourhood $\mathcal{N}(i)$. To complement a subgraph means to erase all the edges in the subgraph, but instead connect the vertices which were originally disconnected. For some time it was conjectured that the rule of local complementation was exhausting all local unitary equivalences between two graph states [87], however, it was later disproved by counterexamples [88, 89]. The local complementation over the vertex $i \in V$ can be physically achieved by the following local unitary transformation:

$$\tau_i(G) = \sqrt{X_i}^{\pm} \bigotimes_{j\in\mathcal{N}(i)} \sqrt{Z_j}^{\mp}. \tag{2.57}$$

See Fig. 2.4 for examples of local complementations.

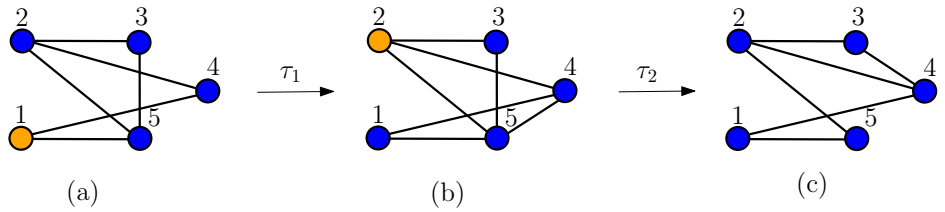


FIGURE 2.4: Graphical rule of local complementation: (a) Local comp lementation is applied to the vertex 1, τ_1. Neighbourhood of the vertex 1 induces a subgraph on vertices $\mathcal{N}(1) = \{4, 5\}$. These vertices get connected as a result of LC. (b) Local comelemntation is applied on the vertex 2, τ_2. Neighbourhood of the vertex 2 induces a subgraph on vertices $\mathcal{N}(1) = \{3, 4, 5\}$. The vertices 4 and 5 were connected as well as 3 and 5. As a result of LC, they both get disconnected. The vertices 3 and 4 were disconnected before the LC, therefore, after the action of LC, they get connected and we get graph in (c).

2.4.1.4 Pauli measurement rules for graph states

Next we review how a given graph state changes if one of its vertex is measured in Pauli bases. It appears that the post- measurement state is always local unitary equivalent to a graph state and moreover, one can derive graphical rules for a given graph $G = (V, E)$:

- Pauli-Z basis measurement: If a qubit $i \in V$ is measured in Pauli-Z basis, the vertex and all of its edges are removed from the graph. Formally, a post-measurement state is:

$$PZ_i(s)|G\rangle \mapsto U_s|G - \{i\}\rangle, \tag{2.58}$$

  where $PZ_i(s)$ expresses Pauli-Z basis measurement on qubit i for the outcome $s \in \{0, 1\}$ and the notation $|G - \{i\}\rangle$ indicates that the vertex i is deleted from the graph G. The post-measurement state can be described by $|G - \{i\}\rangle$ up to local unitary U_s corrections:

$$U_0 = \mathbb{1}, \qquad U_1 = \bigotimes_{j \in \mathcal{N}(i)} Z_j. \tag{2.59}$$

- Pauli-Y basis measurement: If a qubit $i \in V$ is measured in Pauli-Y basis, first the local complementation is done over the vertex i and then i with all of its edges is removed from the graph:

$$PY_i(s)|G\rangle \mapsto U_s|\tau_i(G) - \{i\}\rangle, \tag{2.60}$$

  where for outcomes $s \in \{+, -\}$, the unitary corrections are given by

$$U_+ = \bigotimes_{j \in \mathcal{N}(i)} \sqrt{-iZ_j}, \qquad U_- = \bigotimes_{j \in \mathcal{N}(i)} \sqrt{iZ_j}. \tag{2.61}$$

- Pauli-X basis measurement: This is the most involving rule as it includes a set of three local complementations. If a qubit $i \in V$ is measured in Pauli-X basis, first, the local complementation is done over one of the vertices in the neighbourhood of i, $j \in \mathcal{N}(i)$. Second, the local complementation is done over the vertex i. Third, the vertex i is removed with all of its edges and finally, the local complementation is done over the

vertex j again:

$$PX_i(s)|G\rangle \mapsto U_s|\tau_j(\tau_i(\tau_j(G)) - \{i\})\rangle, \tag{2.62}$$

where for outcomes $s \in \{+, -\}$, the unitary corrections are given by

$$U_+ = \sqrt{iY}_j \bigotimes_{k\in\mathcal{N}(j)\setminus(i\cup\mathcal{N}(i))} Z_k, \qquad U_- = \sqrt{-iY}_j \bigotimes_{k\in\mathcal{N}(j)\setminus(i\cup\mathcal{N}(i)} Z_k. \tag{2.63}$$

At the first step of Pauli-X measurement on vertex i, the choice of the vertex in the neighbourhood $j \in \mathcal{N}(i)$ is not unique, but the post-measurement graph states for any choice of j are LU equivalent.

2.4.1.5 Bell inequalities for graph states

There have been multiple constructions and approaches to derive Bell inequalities for graphs states [90–92]. Here we review so-called Mermin inequalities derived for N-qubit symmetric graph state, which is LU equivalent to the N-qubit GHZ-state. The inequality is violated by an amount that grows exponentially with N. In the original paper, in Ref. [29] the following local variation of N-qubit GHZ-state was considered to reach the aforementioned violation:

$$|\psi_N\rangle = \frac{1}{\sqrt{2}}(|00\ldots0\rangle + i|11\ldots1\rangle). \tag{2.64}$$

The state $|\psi_N\rangle$ is an eigenstate of the Pauli stabilizer operator

$$g_1|\psi_N\rangle = Y_1X_2X_3\ldots X_N|\psi_N\rangle \tag{2.65}$$

and due to the symmetry, the same holds for all other permuted stabilizers g_i too, $1 \leq i \leq N$. Here skip writing tensor products, $A_1 \otimes A_2 \otimes \cdots \otimes A_N \equiv A_1A_2\ldots A_N$.

We take a product of three distinct stabilizer operators, e.g., g_1, g_2, and g_3,

	g_1	$Y_1X_2X_3X_4\ldots X_N$
$\times$	g_2	$X_1Y_2X_3X_4\ldots X_N$
	g_3	$X_1X_2Y_3X_4\ldots X_N$
	$g_1g_2g_3$	$-Y_1Y_2Y_3X_4\ldots N_N$

Then it follows that $Y_1Y_2Y_3X_4\ldots X_N|\psi_N\rangle = -|\psi_N\rangle$. Due to the symmetry every permutation of such operator would give the same eigenvalue equation. Similarly, we can take a product of five stabilizers and one can be easily convinced that the $Y_1Y_2Y_3Y_4Y_5X_6\ldots X_N|\psi_N\rangle = |\psi_N\rangle$.

Therefore, we get an alternating sing for the eigenvalue equation. Interestingly, one can combine all such products with its permutations and reach the so-called Mermin operator [29]:

$$\begin{aligned}\mathcal{M} =& Y_1X_2X_3X_4\dots X_N + \text{ permutations}\\ &-Y_1Y_2Y_3X_4\dots X_N - \text{ permutations}\\ &+Y_1Y_2Y_3Y_4Y_5X_6\dots X_N + \text{ permutations}\\ &-Y_1Y_2Y_3Y_4Y_5Y_6Y_7X_8\dots X_N - \text{ permutations}\\ &+\dots.\end{aligned} \tag{2.66}$$

From the eigenvalue equations and an alternating sign it directly follows that the N-qubit GHZ-like state is an eigenstate of each summand in the Mermin operator, with the eigenvalue having also the alternating sign. That being the case, quantum value of the Mermin operator is equal to the number of terms in the summand:

$$\langle\psi_N|\mathcal{M}|\psi_N\rangle = \sum_{i \text{ odd}} \binom{N}{i} = 2^{N-1}. \tag{2.67}$$

However, if one considers the local hidden variable model, the maximal classical value that the Mermin operator can attain is equal to

$$\langle\mathcal{M}\rangle_{LHV} = 2^{\lfloor N/2\rfloor}. \tag{2.68}$$

From here one sees that graph states can attain exponentially increasing violation of local realism with the number of parties.

The quantum value of Mermin inequality obtained by the GHZ-like state is not robust under particle loss, since the GHZ-state becomes fully separable, in case even a single qubit gets traced out. Therefore, the noisy state does not violate the separability inequalities [93]. The separability inequalities are, in general, violated exponentially stronger than the local reality inequalities by entangled states.

2.4.1.6 Measurement-based quantum computation

Measurement-based quantum computation (MBQC) is a popular scheme of universal quantum computation and differs from the usual circuit model of computation in several key aspects. First, entangling unitary gates are not available during computation on a fly. Instead, all entanglement used during the computation is prepared in a form of a particular many-body highly entangled quantum state before any computation starts. This state is referred to as a *resource state* for universal MBQC. Then an input quantum state is encoded in the resource state. A computational algorithm is executed on this input by performing local measurements on a resource state with the side classical computer analyzing past measurement outcomes in order to predict the future measurement bases.

To show that such measurement-based scheme is universal, one has to prove that a chosen resource state can implement all the gates from some universal gate-set via local measurements.

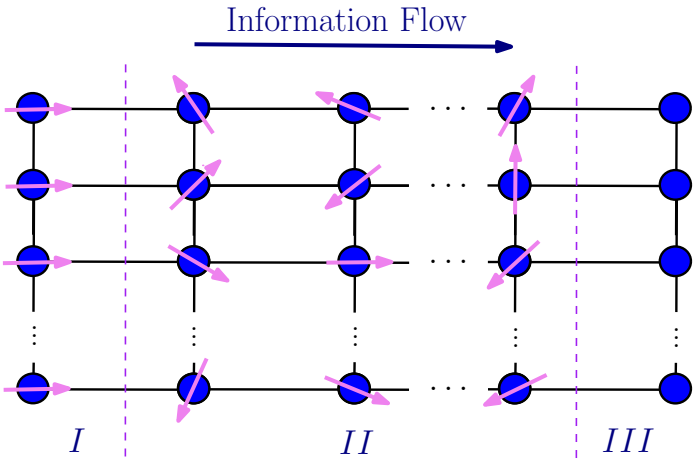


FIGURE 2.5: Cluster state – an universal resource for MBQC. This multiqubit graph state can be divided in three parts: I - input part, where quantum input state is encoded via Bell-bases measurements. II - middle part, where measurements are made in order to implement quantum circuit on an encoded input state. III - output part where the final output state is prepared. Information flows from left to right.

If this is the case we call this state an *universal resource state*. Some classes of universal resource states and their properties have been investigated in the literature [16, 26, 94–98]. Here we review the most conventional universal resource state, the 2D-cluster state and its computational scheme [94]. The 2D cluster state is a particular graph state built on a 2D lattice using the nearest neighbour interactions (See Fig. 2.5).

Having fixed some universal resource state, it is important to characterize physical resources required for computations: the entangling gates needed to prepare the state and the required class of measurements enabling computation. Cluster states are constructed using CZ gates, which are unitaries in the second Clifford hierarchy. Then, due to Gottesman-Knill Theorem 2.11, Pauli measurements cannot suffice to perform universal quantum computation. Therefore, non-Pauli measurements constitute physical resources for cluster state MBQC.

In order to discuss the complexity of MBQC, one needs to consider three aspects. The first is the adaptation of measurement bases, namely whether the choice of some measurement bases should depend on the results of previous measurements. Second, this naturally induces the notion of parallelism and logical depth. Some classes of gates can be carried out by simultaneous measurements, but for implementing other gates one needs to adapt the measurement bases, increasing the logical depth of an underlying circuit. Third, due to intrinsic randomness in the measurement outcomes, there are always random unwanted unitaries, so-called called *byproduct operators*, needed to be corrected, in order to make MBQC deterministic. While it is known that the correction of Pauli operators can be accumulated to the end of computation by classical feed-forwarding of measurement outcomes, one may need to adapt measurement bases and perform additional gates, in general. This step is referred to as a correction step.

The universal gate-set, Clifford group plus T gate from Theorem 2.9 is implemented on a cluster state. Pauli measurements implement Clifford group gates up to random Pauli errors. Since the Clifford group is the normalizer of the Pauli group, Pauli errors can be propagated

	Cluster State
Preparation gates	$CZ \in \mathcal{C}_2$
Measurements	Pauli + $\mathcal{C}_2$
Implemented gates	$\downarrow$ $\mathcal{C}_2$ $\quad$ $\downarrow$ $\mathcal{C}_3$
Byproduct	$\{X, Z\}$
Parallelized gates	$\mathcal{C}_2$

TABLE 2.1: Summary of features of MBQC scheme on cluster states.

in a computation in a closed form. To say it otherwise, if one does not correct Pauli errors directly and keeps Clifford group calculations on a "corrupted" quantum information, the accumulated errors at the end of the Clifford group computation will still be elements of the Pauli group. Therefore, Clifford group unitaries can be implemented without any adaptation of measurement basis, so these gates can be all parallelized in a single step of computation.

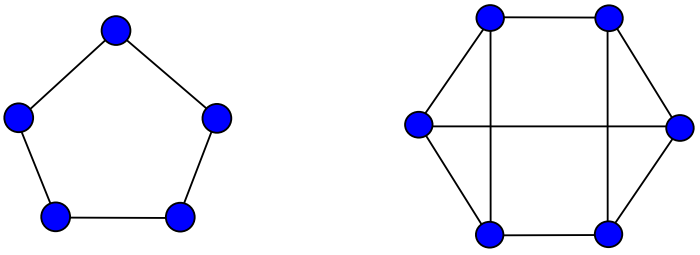
As Clifford group gates are not universal, more general measurements in the $X - Y$-plane of the Bloch sphere must be performed to generate $T \in \mathcal{C}_3$. The direction of measurements are chosen according to accumulated Pauli errors. Therefore, depth of a circuit increases when implementing a T gate. Such time ordering is referred to as a *T-depth* and has been investigated for many circuits as a measure of a cost of its implementation [99–103]. The random byproduct group after implementing the T gates remains to be generated by the Pauli operators X and Z. See Table 2.1 for the general summary of a computational scheme on cluster states.

2.4.1.7 Graph states in quantum error-correction

Given a pure quantum error-correcting code $((n, K, d))_2$, all of its basis states must have all $(d - 1)$ reduced density matrices maximally mixed. Thus, it is interesting to investigate states with such properties. In the following, we give examples of $((n, 1, d))_2$ codes, which corresponds to n-qubit graph states with all of their $(d - 1)$ RDMs being maximally mixed.

To start with, note that any connected graph state has all of its 1 RDMs maximally mixed. But it appears one can do much better. Namely, every possible AME state in qubits corresponds to a graph state. For two-qubits it is a Bell state as in Fig. 2.3 (a). For three qubits, it is the GHZ-state, as in Fig. 2.3 (b). No AME state exists for four qubits [18]. Five and six qubit AME states are presented in Fig. 2.6.

An usual approach to construct an error-correcting code, having found an AME state, or some other entangled state with all of its $(d - 1)$ RDMs maximally mixed, is to use this state and its LU equivalent states as codewords. We will take this approach when studying hypergraph state based error-correcting codes.



(a) (b)

FIGURE 2.6: Absolutely maximally entangled (AME) states. (a) The five-qubit graph state which is an AME state. (b) The six-qubit graph state which is an AME state.

2.4.2 Hypergraph states

Hypergraph states [104–106] correspond to mathematical structures of hypergraphs $H = (V, E)$ and are generalizations of graph states. These states have been recognized as special cases of the so-called locally maximally entangleable (LME) states [104]. Hypergraph states have turned out to play a role for search algorithms in quantum computing [107], quantum fingerprinting protocols [108, 109] and have been investigated in condensed matter physics as ground states of spin models with interesting topological properties [97]. Quantum state verification problem has also been extensively studied for this class of states [110–112].

2.4.2.1 Constructing hypergraph states

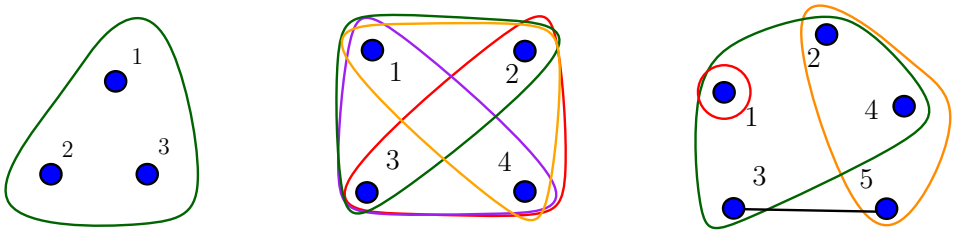
A hypergraph state $|H\rangle$ corresponding to a hypergraph $H = (V, E)$, defined over a set of vertices V and a set of hyperedges E, which may connect more than two vertices. A hypergraph state is constructed in a following manner:

- For each vertex $v \in V$ we initialize the physical system in the "+1" eigenstates of Pauli-X operator, $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$. Thus, the N-vertex hypergraph state is initialized as $|+\rangle^{\otimes N}$, where $N = |V|$ is the cardinality of the vertex set.
- For each hyperedge $e \in E$ in the hypergraph H, we calculate edge cardinality $|e|$ and we apply the $|e|$-qubit entangling unitary, represented by the diagonal gate C on the qubits in the hyperedge e of the initialized state $|+\rangle^{\otimes N}$. As a result we get a hypergraph state corresponding to the hypergraph H:

$$|H\rangle = \prod_{e \in E} C_e |+\rangle^{\otimes |V|}, \tag{2.69}$$

  where C_e gates are generalized CZ gates on $|e|$ qubits and are defined as follows $C_e = \mathbb{1} - 2|11\ldots1\rangle\langle11\ldots1|$.

The simplest non-trivial example of a hypergraph state corresponds to a three-vertex hypergraph with a single hyperedge containing all three vertices (See Fig. 2.7 (a)) and as a state



(a) (b) (c)

FIGURE 2.7: Hypergraph states. (a) A three-vertex hypergraph with a single hyperedge $E = \{\{1,2,3\}\}$. (b) The four-vertex three-uniform complete hypergraph that is every three vertex is connected with a hyperedge: $E = \{\{1,2,3\},\{1,2,4\},\{1,3,4\},\{2,3,4\}\}$. (c) An arbitrary five-vertex hypergraph, containing hyperedges of different cardinality: $E = \{\{1\},\{3,5\},\{2,4,5\},\{1,2,3,4\}\}$.

vector it looks as follows:

$$|H_3^3\rangle = C_{\{1,2,3\}}|+\rangle^{\otimes 3} = CCZ|+\rangle^{\otimes 3} \tag{2.70}$$

$$= \frac{1}{\sqrt{8}}\big(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle - |111\rangle\big). \tag{2.71}$$

Definition 2.16. We call a hypergraph state k-uniform if all of its hyperedges $\forall e \in E$ act exactly on k vertices, or otherwise, all hyperedges have the cardinality $|e| = k$. We say that a hypergraph is complete/fully connected k-uniform if it has every possible hyperedge of the cardinality k. See Fig.2.7 (b) for a 3-uniform example.

To give an example, every graph state is a 2-uniform hypergraph state. The state in Fig. 2.7 (b) is a 3-uniform complete hypergraph state. The state in Fig. 2.7 (c) is an example of a hypergraph state with mixed cardinality edges.

Hypergraph states as state vectors correspond to equally weighted real-valued superposition of all computational basis elements. Alternatively they can be also viewed as states capable of encoding Boolean functions $f(\mathbf{x})$:

$$|H\rangle = \frac{1}{2^{N/2}} \sum_{\mathbf{x}\in\{0,1\}^N} (-1)^{f(\mathbf{x})}|\mathbf{x}\rangle. \tag{2.72}$$

There is a one-to-one correspondence between hypergraph states and such Boolean function encodings. For example, one can easily check that the hypergraph state in Eq. (2.70) can be expressed by the function $f(\mathbf{x}) = x_1x_2x_3$, where $\mathbf{x} = (x_1, x_2, x_3)$. On the other hand, graph states correspond to functions with only two variables. For example, the graph state in Fig. 2.3 (b) is described by the function of the form $f(\mathbf{x}) = x_1x_2 + x_2x_3 + x_1x_3$. This already indicates that there are significantly more hypergraph states than graph states.

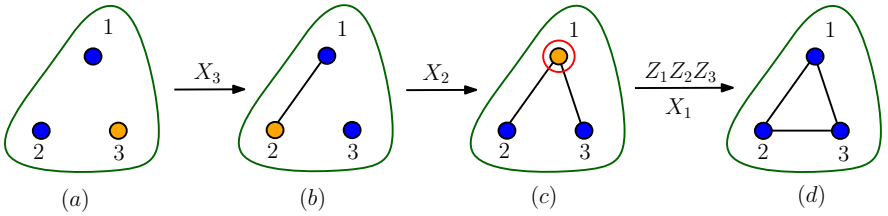


FIGURE 2.8: All three qubit hypergraph states with at least one hyperedge are local Pauli equivalent. Pauli-X on a vertex i, adds all the hyperedges in the adjacency of i. X_3 is applied to the hypergraph state in (a) and the state in (b) is obtained, since the adjacency of the vertex 3 is $\{1,2\}$. X_2 is applied to the hypergraph state in (b) and since the adjacency of vertex 2 is given by $\{\{1\},\{1,3\}\}$, these hyperedges are found in addition in (c). Finally, applying X_1 to the qubit one and $Z_1Z_2Z_3$ to all three qubits, gives the state in (d).

2.4.2.2 Nonlocal stabilizer formalism

Hypergraph states also have an alternative definition using stabilizer formalism, however, the stabilizer is not given by a tensor product of local operators [113]. It turns out that even a nonlocal stabilizer description can be fruitful for investigating entanglement properties of hypergraph states.

Given an N-qubit hypergraph state corresponding to a hypergraph $H = (V, E)$, first we introduce a term that can be regarded as a generalization of the term neighbourhood from graph theory. We call it adjacency of a vertex $i \in V$ and denote it by $\mathcal{A}(i) = \{e - \{i\} | e \in E \text{ with } i \in e\}$. The elements of $\mathcal{A}(i)$ are sets of vertices which are adjacent to i via some hyperedge. To give an example, the adjacency of the vertex $i = 2$ in hypergraph in Fig. 2.7 (c), is given by $\mathcal{A}(2) = \{\{4,5\},\{1,3,4\}\}$. Then for each vertex $i \in V$ we can define the operator h_i, consisting of the tensor product of Pauli-X on the vertex i and generalized controlled-Z gates on the adjacent qubits:

$$h_i = X_i \bigotimes_{e_j \in \mathcal{A}(i)} C_{e_j}. \tag{2.73}$$

The operators h_i, $0 \leq i \leq N$ form a commutative group and the hypergraph state $|H\rangle$ is their unique common eigenstate with the eigenvalue "+1":

$$h_i|H\rangle = |H\rangle \qquad \text{for all } i \in V. \tag{2.74}$$

To given an example, we write down some of the nonlocal stabilizer operators of the hypergraph in Fig. 2.7 (c) explicitly:

$$h_1 = X_1 \otimes C_{\{\}} C_{\{2,3,4\}} = -X_1 \otimes C_{\{2,3,4\}}. \tag{2.75}$$

$$h_5 = X_5 \otimes C_{\{3\}} C_{\{2,4\}}. \tag{2.76}$$

Note that the vertex 1 is included in hyperedges $\{\{1\},\{1,2,3,4\}\}$, and, therefore, its adjacency contains an empty hyperedge $\{\} \in \mathcal{A}(1)$. An empty hyperedge itself corresponds to a global

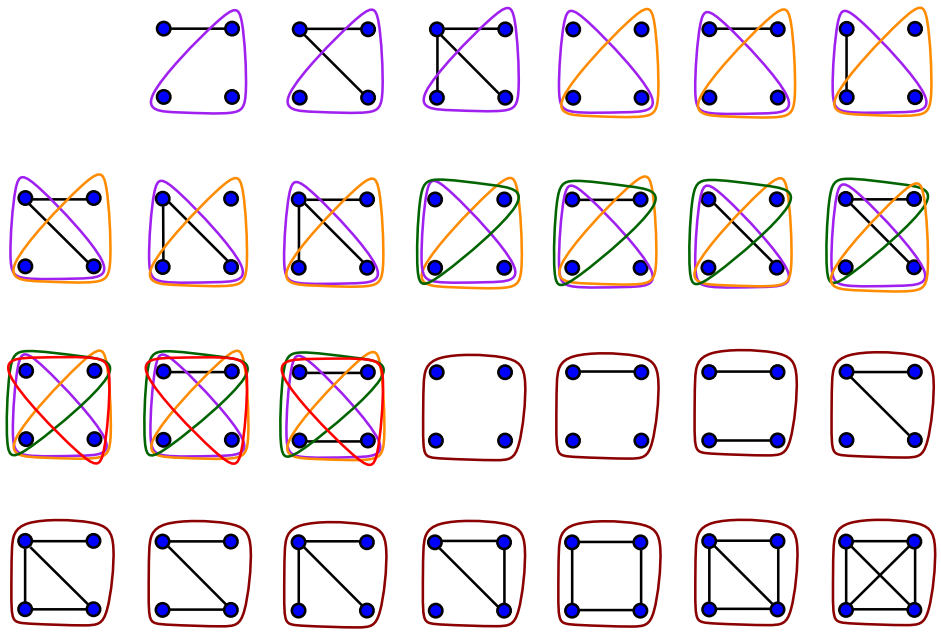


FIGURE 2.9: 27 local unitary equivalence of four-qubit hypergraph states with at least one hyperedge. It appears that local Pauli operations are enough to distinguish these entanglement classes.

sign, -1, as seen in Eq. (2.75). For the sake of a simpler notation, sometimes where it is clear we will skip the tensor product, brackets, and commas in the description of generalized controlled-Z gates and instead write: $h_5 = X_5 C_3 C_{24}$.

2.4.2.3 Local Pauli equivalences of hypergraph states

Similar to graph state case, it is interesting to investigate which hypergraphs are local unitary equivalent. In Ref. [113] it was shown that in case of three-qubit hypergraph states, containing a least one hyperedge, there is a single local unitary equivalence class. This equivalence can be unraveled by investigating local Pauli-X and -Z actions on hypergraph states.

From nonlocal stabilizer equations Eq. (2.73), one can directly derive the graphical rule for Pauli-X operations on hypergraph states:

$$X_i \bigotimes_{e_j \in \mathcal{A}(i)} C_{e_j} |H\rangle = |H\rangle \qquad \Rightarrow \qquad X_i |H\rangle = \bigotimes_{e_j \in \mathcal{A}(i)} C_{e_j} |H\rangle. \tag{2.77}$$

Pauli-X operator on qubit i adds all the edges defined over adjacency of i to the hypergraph. On the other hand, Pauli-Z operator is much more trivial, since it just adds a local C_i to the qubit it is applied to.

Hence, in three-qubit case there are totally two LU inequivalent classes of hypergraph states: GHZ-state and $|H_3^3\rangle$. The former corresponds to a graph state as we have seen previously and is the representative of one of the SLOCC classes. The latter can be transformed with local Pauli operations to any other three-qubit hypergraph states that contain a hyperedge $\{1, 2, 3\}$.

See Fig. 2.8 for the exact transformations. Finally, three-qubit GHZ-state and $|H_3^3\rangle$ are not LU equivalent but they are in the same SLOCC equivalence class.

In four-qubit case the situation changes drastically as there are totally 29 LU inequivalent classes of hypergraph states: Two out of 29 classes are graph states, but the rest of the 27 classes are given in Fig. 2.9 and they have at least one hyperedge. Note that, similar to the three-qubit case, local Pauli operations are able to identify all LU equivalences.

2.4.3 Linear matrix pencil states

In this subsection we review entanglement classification of tripartite pure states $|\psi\rangle$ in non-homogeneous Hilbert space of local dimensions $\mathcal{H} = \mathbb{C}^2 \otimes \mathbb{C}^m \otimes \mathbb{C}^n$, where $m \leq n$ under SLOCC transformations. For $m = n = 2$ we already saw that there are two genuine multiparty entangled SLOCC classes, the W-class and the GHZ-class. Interestingly, the problem of SLOCC classification for arbitrary m and n can be solved using mathematical structures of *linear matrix pencils* [114].

A tripartite state $|\psi\rangle$ in Hilbert space $\mathcal{H}$ shared between Aline (A), Bob (B), and Charlie (C) can be expressed as

$$|\psi\rangle = |0\rangle_A|R\rangle_{BC} + |1\rangle|S\rangle_{BC} \tag{2.78}$$

$$= \big[|0\rangle_A(R \otimes \mathbb{1}) + |1\rangle_A(S \otimes \mathbb{1})\big]|\Phi_n^+\rangle \tag{2.79}$$

$$= \big[|0\rangle_A(\mathbb{1} \otimes R^T) + |1\rangle_A(\mathbb{1} \otimes S^T)\big]|\Phi_m^+\rangle, \tag{2.80}$$

where $|\Phi_k^+\rangle = \frac{1}{\sqrt{k}}\sum_{i=0}^{k-1}|ii\rangle$ is a k-dimensional Bell-state and R and S are complex $m \times n$ matrices. A pair of matrices R and S form a linear matrix pencil $\mathcal{P}(R,S) = \mu R + \lambda S$, a homogeneous matrix polynomial of degree 1 in variables μ and λ. In this thesis we use notation $\mathcal{P}(R,S)$, $\mathcal{P}(\mu,\lambda)$, and simply $\mathcal{P}$ interchangeably. Linear matrix pencils and pure quantum states in $2 \times m \times n$ are in one-to-one correspondence. In Ref. [114] the connection between SLOCC classification of states in $2 \times m \times n$ systems was connected to the normal form of matrix pencils. In the following we review this connection. Without loss of generality, we assume that all the states are of the full local ranks.

Since the SLOCC operations are characterized by Alice's, Bob's, and Charlie's invertible actions A, B, and C on a state $|\psi\rangle$, respectively, we investigate their effects on a corresponding matrix pencil individually. We start by Alice's action: Alice has the smallest of the local dimensions. Her invertible operation can be represented by an arbitrary 2×2 matrix A with a non-zero determinant:

$$A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}. \tag{2.81}$$

Then A transforms the state $|\psi\rangle$ to a new state

$$A \otimes \mathbb{1} \otimes \mathbb{1}|\psi\rangle = |0\rangle_A(\alpha|R\rangle_{BC} + \beta|S\rangle_{BC}) + |1\rangle_A(\gamma|R\rangle_{BC} + \delta|S\rangle_{BC}). \tag{2.82}$$

Alternatively, we can say that a pencil $\mathcal{P}(R,S) = \mu R + \lambda S$ is transformed to a new pencil with new variables $\tilde{\mu} = \alpha\mu + \gamma\lambda$ and $\tilde{\lambda} = \beta\mu + \delta\lambda$,

$$\mathcal{P}(\tilde{\mu},\tilde{\lambda}) = (\alpha\mu + \gamma\lambda)R + (\beta\mu + \delta\lambda)S. \tag{2.83}$$

Action of Bob and Charlie can be discussed together:

$$\begin{aligned} \mathbb{1} \otimes B \otimes C|\psi\rangle =& [|0\rangle_A(BR \otimes C) + |1\rangle_A(BS \otimes C)]|\Phi_n^+\rangle & (2.84)\\ =& [|0\rangle_A(BRC^T \otimes \mathbb{1}) + |1\rangle_A(BSC^T \otimes \mathbb{1})]|\Phi_n^+\rangle. & (2.85) \end{aligned}$$

Therefore, a matrix pencil $\mathcal{P}(R,S)$ is transformed to $\mathcal{P}(BRC^T, BSC^T)$. From these discussions it is evident that the classification of matrix pencils are in order.

Definition 2.17. Two $m \times n$ matrix pencils $\mathcal{P}$(R,S) and $\mathcal{P}(\tilde{R},\tilde{S})$ are said to be strictly equivalent to each other if there exist invertible general linear operators $B \in GL_m$ and $C \in GL_n$, such that

$$BRC^T = \tilde{R} \qquad \text{and} \qquad BSC^T = \tilde{S}. \tag{2.86}$$

It follows that, if two states are SLOCC equivalent under B and C, then their pencils can be made strictly equivalent too. Luckily, there exists the normal form to identify strict equivalence of matrix pencils.

Lemma 2.18. *Two matrix pencils are strictly equivalent to each other if and only if they correspond to the same Kronecker canonical form.*

Kronecker canonical form (KCF) is a generalization of well-known Jordan normal form. A matrix pencil, which is reduced to its KCF is denoted by $\mathcal{P}_{KCF}$. KCF of a $m \times n$ full-rank matrix pencil has a Block-diagonal form:

$$\mathcal{P}_{KCF} = \{L_{\epsilon_1}, \ldots, L_{\epsilon_a}, L_{\nu_1}^T, \ldots L_{\nu_b}^T, J\}. \tag{2.87}$$

Here L_ϵ, and L_ν^T are called *right* and *left null-space* blocks, respectively and indices $\epsilon_1, \ldots \epsilon_a$, $\nu_1, \ldots \nu_b$ are *minimal indices* of a pencil. J is very a similar square matrix to a Jordan matrix and is referred to as *divisor block*. It is filled-up with blocks specified by the so-called *elementary divisors* or, equivalently, with the so-called pencil eigenvalues, $x_i \in \mathbb{C} \cup \{\infty\}$. There are specific steps in order to determine eigenvalues and minimal indices of a matrix pencil. We review them here.

First, we define a rank of a matrix pencil to be the largest integer r, such that there exists a nonvanishing r-minor for any choice of variable μ and λ. A k-minor of matrix is a determinant of a matrix obtained by erasing all but its k rows and k columns. Note that, defining rank of a pencil in this way also incorporates Alice's action. Then we define $D_k(\mu,\lambda)$ for $1 \leq k \leq r$ to be the greatest common divisor of all k-minors of a pencil $\mathcal{P}(R,S)$. More formally, a polynomial $D_k(\mu,\lambda)$ is calculated as

$$D_k(\mu,\lambda) = gcd[minors[\mathcal{P}(R,S),k]]. \tag{2.88}$$

By convention $D_0 = 1$ and $D_k = 0$ for $k > r$. The polynomials $D_k(\mu, \lambda)$ uniquely factorize as a product of eigenvalues of a matrix pencil:

$$D_r(\mu, \lambda) = \mu^{q-t} p_1 \dots p_t, \tag{2.89}$$

where $t \leq q$ and $q \leq r$ and $p_i = \mu x_i + \lambda$, for $x_i \in \mathbb{C}$ are called a *finite eigenvalue* of a pencil and the factor μ is called an *infinite eigenvalue* of a pencil sometimes denoted by $\{\infty\}$. The infinite eigenvalue has an algebraic multiplicity $(q - t)$ denoted by e_μ, while for distinct finite eigenvalues p_i, we denote the corresponding algebraic multiplicity by e_i.

Next step is to calculate *invariant polynomials* of a matrix pencil for $1 \leq k \leq r$:

$$E_k(\mu, \lambda) = \frac{D_k(\mu, \lambda)}{D_{k-1}(\mu, \lambda)}. \tag{2.90}$$

Since by definition $D_{k-1}(\mu, \lambda)$ always divides $D_k(\mu, \lambda)$, an invariant polynomial $E_k(\mu, \lambda)$ is a homogeneous polynomial. Then using distinct we define a *size signature* for each eigenvalue p_i to be a sequence of r integers $s_i = (e_1^i, \dots, e_r^i)$, where e_j^i is a maximal integer power of p_i, such that $(p_i)^{e_j^i}$ divides the invariant polynomial $E_j(\mu, \lambda)$, for $r \geq j \geq 1$. A size signature for an infinite divisor is defined in the same way and $s_\mu = (e_1^\mu, \dots, e_r^\mu)$.

We can already look at the full structure of J blocks assuming that a pencil has $l \leq r$ distinct finite divisors:

$$J = \{M^{e_1^1}(x_1), \dots, M^{e_r^1}(x_l), N^{e_1^\mu}, N^{e_2^\mu}, \dots, N^{e_r^\mu}\}, \tag{2.91}$$

where $M^{e_j^i}$ and $M^{e_j^\mu}$ are $e_j^i \times e_j^i$ and $e_j^\mu \times e_j^\mu$ matrices:

$$M^{e_j^i}(x_i) = \overset{\overset{e_j^i}{\longleftrightarrow}}{\begin{pmatrix} \mu x_i + \lambda & \mu & 0 & \dots & 0 \\ 0 & \mu x_i + \lambda & \mu & & \\ \vdots & & \ddots & \ddots & 0 \\ & & & \mu x_i + \lambda & \mu \\ 0 & & \dots & 0 & \mu x_i + \lambda \end{pmatrix}} \Bigg\updownarrow e_j^i \quad \text{and} \tag{2.92}$$

$$N^{e_j^\mu} = \overset{\overset{e_j^\mu}{\longleftrightarrow}}{\begin{pmatrix} \mu & \lambda & 0 & \dots & 0 \\ 0 & \mu & \lambda & & \\ \vdots & & \ddots & \ddots & 0 \\ & & & \mu & \lambda \\ 0 & & \dots & 0 & \mu \end{pmatrix}} \Bigg\updownarrow e_j^\mu \quad . \tag{2.93}$$

The total size of eigenvalue blocks is $q = \sum_j (\sum_i e_j^i) + e_j^\mu$. The rest of the $m \times n$ pencil is filled up with null-space blocks, which we review next.

A right null-space of a pencil $\mathcal{P}$ corresponds to vectors of homogeneous polynomials in variables λ and μ

$$\vec{y}_i = \sum_{j=0}^{\epsilon_i} y_{ij} \mu^{\epsilon_i - j} \lambda^j, \tag{2.94}$$

where $y_{ij} \in \mathbb{C}$ and the vector satisfies the constraint

$$(\mu R + \lambda S)\vec{y}_i = 0. \tag{2.95}$$

Let a be the number of linearly independent vectors for which Eq. (2.95) holds. We choose linearly independent vectors $\vec{y}_i$ of minimal degree, ϵ_i and order them by degree in the ascending order, $(\epsilon_1, \dots \epsilon_a)$, obtaining the unique set of right minimal indices of a matrix pencil. The integer values of the right minimal indices are sufficient to define L_ϵ blocks:

$$L_\epsilon = \overset{\overset{\epsilon+1}{\longleftrightarrow}}{\begin{pmatrix} \lambda & \mu & 0 & \dots & 0 \\ 0 & \lambda & \mu & & \\ \vdots & & \ddots & \ddots & 0 \\ & & & \lambda & \mu \end{pmatrix}} \Big\updownarrow \epsilon \quad . \tag{2.96}$$

The left null-space block is defined in an analogous way, but instead of the constraint in Eq. (2.95), the vectors have to satisfy the transposed one:

$$(\mu R^T + \lambda S^T)\vec{y}_i = 0, \tag{2.97}$$

uniquely defining b left minimal indices ordered in the ascending order, $(\nu_1, \dots \nu_b)$. Respectively the left null-space block L_ν^T has dimensions $(\nu + 1) \times \nu$. This finishes the description of KCF of a matrix pencil. For a more detailed overview of matrix pencil theory see Refs. [114, 115].

We now get back to the SLOCC classification of $2 \times m \times n$ states. Lemma 2.18 says that two states are SLOCC equivalent under transformation $\mathbb{1} \otimes B \otimes C$, if and only if their corresponding matrix pencils have the same KCF. Finally, we unify this result with Alice's transformation A in Eq. (2.83). By redefining pencil variables, $(\mu, \lambda) \mapsto (\tilde{\mu}, \tilde{\lambda})$, Alice cannot change left or right minimal indices [114, 115], but she can alter eigenvalues of a pencil, whether finite or infinite, in the following way:

$$x_i \mapsto \begin{cases} \frac{\alpha x_i + \beta}{\gamma x_i + \delta}, & \text{if } \gamma x_i + \delta \neq 0 \\ \infty, & \text{if } \gamma x_i + \delta = 0 \end{cases} \quad \text{and} \quad \infty \mapsto \begin{cases} \frac{\alpha}{\gamma}, & \text{if } \gamma \neq 0 \\ \infty, & \text{if } \gamma = 0 \end{cases} \quad . \tag{2.98}$$

From this transformation it follows that Alice can transform at most arbitrary three distinct eigenvalues, finite or infinite to other three eigenvalues. This implies that Alice can always map an infinite eigenvalue to some other finite one. Thus, we only have to make statements about finite eigenvalues from now on and the full SLOCC classification theorem under $A \otimes B \otimes C$ transformations can now be stated as:

Theorem 2.19. *Two $2 \times m \times n$-dimensional pure states $|\psi\rangle$ and $|\phi\rangle$ with corresponding matrix pencils having only finite eigenvalues are SLOCC equivalent, if and only if they have the same minimal indices, matching eigenvalue size signatures, and the eigenvalues $\{x_i\}$ and $\{\tilde{x}_i\}$, respectively, are related by a linear fractional transformation*

$$\frac{\alpha x_i + \beta}{\gamma x_i + \delta} = \tilde{x}_i \tag{2.99}$$

for $\alpha\delta - \beta\gamma \neq 0$.

We can shortly discuss some examples of pencils and implications of Theorem 2.19. First, since there is a one-two-one correspondence between SLOCC classes in $2 \times m \times n$ systems and the number of possible KCFs for $m \times n$ matrix pencils, for small m and n, one can directly enumerate all the classes. For example, in case $m = n = 2$, since we restrict ourselves to the full-rank pencils, there cannot be a left or right null-space block in the pencil. As for the eigenvalues, they can either correspond to a distinct eigenvalue case or to the single eigenvalue with an algebraic multiplicity of two:

$$\mathcal{P}_W = \begin{pmatrix} \lambda & \mu \\ 0 & \lambda \end{pmatrix} \qquad \text{and} \qquad \mathcal{P}_{GHZ} = \begin{pmatrix} \mu & 0 \\ 0 & \lambda \end{pmatrix}. \tag{2.100}$$

As the labels of these pencils indicate, one can directly write out representatives of SLOCC classes in three-qubit systems: the W-state and the GHZ-state as defined in Eq. (2.9). To go beyond the three-qubit case, in $2 \times 2 \times 3$ systems there are also two SLOCC classes with the corresponding pencils given in KCF:

$$\mathcal{P}_1 = \begin{pmatrix} \lambda & 0 & 0 \\ 0 & \lambda & \mu \end{pmatrix} \qquad \text{and} \qquad \mathcal{P}_2 = \begin{pmatrix} \lambda & \mu & 0 \\ 0 & \lambda & \mu \end{pmatrix}. \tag{2.101}$$

The first pencil $\mathcal{P}_1$ has a single eigenvalue and the null-space block L_1. The second one has no divisors and only the single null-space block L_2. No other block structure can fit in a full-rank 2×3 pencil. The full enumeration of SLOCC classes in $2 \times 3 \times n$ systems was also provided in Refs. [114, 116]. Note that there are discrete number of SLOCC classes in these dimensions. However, in $2 \times 4 \times 4$ systems there are infinite number of SLOCC classes. One can directly see it by considering the 4×4 matrix pencil with four distinct divisors:

$$\mathcal{P}_{4\times4} = \begin{pmatrix} \lambda & 0 & 0 & 0 \\ 0 & \lambda + \mu & 0 & 0 \\ 0 & 0 & \mu & 0 \\ 0 & 0 & 0 & \mu x_1 + \lambda \end{pmatrix}. \tag{2.102}$$

Alice can only fix any three divisors out of four, leaving one finite divisor with an arbitrary parameter $x_1 \in \mathbb{C}$. So, each value of x_1 corresponds to a new SLOCC class in $2 \times 4 \times 4$. Therefore, $\mathcal{P}_{4\times4}$ describes a single parameter family of pure states in $2 \times 4 \times 4$.

Until now we reviewed how the SLOCC classes in $2 \times m \times n$ can be characterized via matrix pencils. Here, we go one step beyond that and recall the necessary and sufficient condition for the existence of a local (non–invertible) transformation from a state $|\psi\rangle$ with local ranks

$2 \times m \times n$ to a state $|\phi\rangle$ with local ranks $2 \times m \times k$ where $k < n$. We consider now a (non-invertible) SLOCC transformation on a state with local rank $2 \times m \times n$ to a state with local rank $2 \times m \times (n-1)$. The general case can be deduced from that by iterating the process. Note that such a transformation requires a non-invertible SLOCC operation performed by C. The necessary and sufficient conditions for the existence of this operation are stated in the following theorem which is presented in [114]. Here and in the following, we will denote the matrix pencil that is associated to a state $|\psi\rangle$ by $\mathcal{P}_\psi$.

Theorem 2.20 ([114]). *Let $|\psi\rangle$ and $|\phi\rangle$ be states with local ranks $2 \times m \times n$ and $2 \times m \times (n-1)$ and let $c_1, c_2, \ldots, c_n$ denote the columns of the pencil $\mathcal{P}_\psi(\mu, \lambda)$. Then $|\psi\rangle$ can be mapped to $|\phi\rangle$ via some non-invertible SLOCC operators iff for some $1 \leq i \leq n$, there exist constants $a_1, a_{i-1}, a_{i+1}, \ldots, a_n$ and some invertible linear transformation $(\mu, \lambda) \mapsto (\hat{\mu}, \hat{\lambda})$ such that the pencil $\mathcal{P}_{\psi_i}(\hat{\mu}, \hat{\lambda}) = [c_1 + a_1 c_i, \ldots, c_{i-1} + a_{i-1} c_i, c_{i+1} + a_{i+1} c_i, \ldots, c_n + a_n c_i]$ is strictly equivalent to $\mathcal{P}_\phi(\mu, \lambda)$.*

Let us remark here, that in the transformation from $|\psi\rangle$ to $|\phi\rangle$, the pencil $[c_1 + a_1 c_i, \ldots, c_{i-1} + a_{i-1} c_i, c_{i+1} + a_{i+1} c_i, \ldots, c_n + a_n c_i]$ is obtained by the third party, Charlie, applying an operator C that is given via the $(n-1) \times n$ matrix

$$C = P_{n-1}(\mathbb{1} + |\phi\rangle\langle i|), \tag{2.103}$$

where P_{n-1} denotes the projector onto the $(n-1)$ dimensional subspace spanned by all standard basis vectors, but $\vec{e}_i$ and $|\phi\rangle = \sum_{j \neq i} a_j |j\rangle$. The intuition behind the theorem is that any matrix $\tilde{C}$ can be brought to its so-called *reduced row echelon form* C using invertible row operations, i.e., matrices that act on the left, only [117].

Similarly, transformations from states of local rank $2 \times m \times n$ to states with local rank $2 \times (m-1) \times n$ can be achieved by some non-invertible operation B performed by Bob. Non-invertible operators applied by Alice are not considered as they would always leave Alice disentangled with the rest of the parties.

Chapter 3

Extreme violation of local realism in quantum hypergraph states

Hypergraph states form a family of multiparticle quantum states that generalizes the well-known concept of Greenberger-Horne-Zeilinger states, cluster states, and more broadly graph states. In this chapter we study the nonlocal properties of quantum hypergraph states. We demonstrate that the correlations in hypergraph states can be used to derive various types of nonlocality proofs, including Hardy-type arguments and Bell inequalities for genuine multiparticle nonlocality. Moreover, we show that hypergraph states allow for an exponentially increasing violation of local realism which is robust against loss of particles. Our results suggest that certain classes of hypergraph states are novel resources for quantum metrology and a certain scheme of measurement-based quantum computation.

3.1 Introduction

Learning nonlocal properties of multipartite quantum states is important due to their applications in quantum information processing tasks. In this chapter we show that hypergraph states violate local realism in an extreme manner, but in a way that is robust against the loss of particles. We demonstrate that this leads to applications of these states in quantum metrology and quantum computation. We see that the stabilizer formalism describing hypergraph states, despite being nonlocal, can be used to derive Hardy-type nonlocality arguments [73], Bell inequalities for genuine multiparticle entanglement [45], or a violation of local realism with a strength exponentially increasing with the number of particles. Our approach starts precisely with the properties of the stabilizer, in order to identify the useful correlations provided by quantum mechanics. This is in contrast to previous approaches that were either too general, e.g., Bell inequalities for general multiparticle states [38, 40, 118, 119], or too restricted, considering only a few specific examples of hypergraph states and leading to nonrobust criteria [113]. The violation of local realism is the key to further applications in information processing. Indeed, it is well known that violation of a Bell inequality leads to advantages, in

distributed computation scenarios [72, 120]. In addition, we will explicitly show that certain classes of hypergraph states lead to Heisenberg scaling in quantum metrology and advantages in measurement-based quantum computation.

3.2 Local correlations from nonlocal stabilizer

The key observation for the construction of our nonlocality arguments is that the stabilizer of hypergraph states, despite being nonlocal, predicts perfect correlations for some local measurements. In the following, we explain this for the three-qubit hypergraph state $|H_3^3\rangle$ given in Fig. 2.7 (a) and in Eq. (2.70) as a state vector, but the method is general. The nonlocal stabilizer operators for the hypergraph $|H_3^3\rangle$ are:

$$h_1 = X_1 \otimes C_{23}, \qquad h_2 = X_2 \otimes C_{13}, \qquad \text{and} \qquad h_3 = X_3 \otimes C_{12}. \tag{3.1}$$

Since the hypergraph state is permutation symmetric, we can derive correlations only from one of the generators of nonlocal stabilizer group and then permute them afterwards for another qubits. So, let us write one of the generators more explicitly:

$$h_1 = X_1 \otimes \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}. \tag{3.2}$$

It will be useful to note that the diagonal elements of the CZ_{23} operator can be viewed as the projections on the four subspaces corresponding to four measurement outcomes if Pauli-Z basis measurements were made on qubits 2 and 3: $|00\rangle\langle 00|$, $|01\rangle\langle 01|$, $|10\rangle\langle 10|$, $-|11\rangle\langle 11|$, respectively. Then, if the first party decides to make quantum measurement in Pauli-X basis and gets an outcome "$+$", keeping in mind the eigenvalue equation,

$$h_1|H_3^3\rangle = +|H_3^3\rangle, \tag{3.3}$$

the second and third party when measuring in Pauli-Z direction can never both obtain outcomes 1 and 1, since this would correspond to projecting on the "$-$" sign. One can translate this statement into deterministic probability for hypergraph state:

$$P(+--|XZZ) = 0. \tag{3.4}$$

Just for the sake of notation, we also denote Pauli-Z measurement outcomes also by "$\pm$". Next, we can try to repeat the argumentation when the first party measures in Pauli-X basis but gets the outcome "$-$". Then the only possibility for parties 2 and 3 measuring in Pauli-Z basis, is to project on $-|11\rangle\langle 11|$. Therefore, $P(---|XZZ) = 1$ for the hypergraph state $|H_3^3\rangle$. From here other three deterministic assignments follow for the probablilities:

$$P(-++|XZZ) + P(--+|XZZ) + P(-+-|XZZ) = 0. \tag{3.5}$$

Since the three-qubit hypergraph state is symmetric, the permuted correlations can be obtained by considering eigenvalue equations using h_2 and h_3:

$$P(--+|ZXZ) + P(---|ZZX) = 0. \tag{3.6}$$

$$P(+-+|ZXZ) + P(--+|ZXZ) + P(+--|ZXZ) = 0. \tag{3.7}$$

$$P(++-|ZZX) + P(-+-|ZZX) + P(+--|ZZX) = 0. \tag{3.8}$$

So, totally we obtain twelve perfect correlations for the three-qubit hypergraph state.

Derivation of perfect correlations can be extended to other hypergraph states too. Here we give an example for $|H_N^N\rangle$ state, which is an N-qubit hypergraph state with the single cardinality N hyperedge. Then the correlation from Eqs. (3.4-3.5) directly generalize to

$$P(+--\cdots-|XZZ\ldots Z) = 0 \tag{3.9}$$

and

$$P(-+\cdots+|XZ\ldots Z) + P(-+\cdots+-|XZZ\ldots Z) + \cdots + P(---\cdots-+|XZ\ldots Z) = 0. \tag{3.10}$$

Note that the state $|H_N^N\rangle$ is also permutation symmetric, so, the correlations obtained for the first qubit can directly be permuted for every other.

3.3 Hardy-type arguments and nonlocality proofs

In this section we would like to show that the perfect correlations obtained from the stabilizer equations can first lead to a Hardy-type arguments, which then we translate to Bell nonlocality arguments for fully local hidden variable models. Recall that such models assign for any value of the HV λ results to all measurements of the parties in a local manner, meaning that the probabilities for a given HV factorize. First we consider the tripartite case. If we denote by r_i the result and by s_i the measurement setting on the ith particle, respectively, then the probabilities coming from local models are of the similar form as discussed in Eq. (2.21) but for more parties

$$P(r_1r_2r_3|s_1s_2s_3) = \int d\lambda p(\lambda)\chi^A(r_1|s_1,\lambda)\chi^B(r_2|s_2,\lambda)\chi^C(r_3|s_3,\lambda). \tag{3.11}$$

For probabilities of this form it suffices to consider deterministic models for a given λ. Considering such LHV models and twelve perfect correlations obtained for the three qubit hypergraph state one can reach a Hardy-type contradiction.

Theorem 3.1. *If a fully local hidden variable model satisfies the conditions from Eqs. (3.4-3.5) and their symmetric correlations coming from the permutations, then it must fulfill the following perfect correlations too*

$$P(+--|XXX) + P(-+-|XXX) + P(--+|XXX) = 0. \tag{3.12}$$

The proof of this statement is done by exhausting all possible local deterministic assignments. The Harty-type contradiction comes from the fact that for the three-qubit hypergraph state $|H_3^3\rangle$ the following statement holds,

$$P(+--|XXX) = \frac{1}{16}. \tag{3.13}$$

Due to symmetry the same holds for other two correlations from Eq. (3.12).

Our method shows how the correlations of the nonlocal stabilizer can be used for Hardy-type arguments. We recall that Hardy-type arguments have been obtained for all permutation-symmetric states [121, 122]. However, they involved different settings and have no direct connection with the stabilizer formalism, making a generalization complicated. In contrast, we will see that our measurements can even be used to prove genuine multiparticle nonlocality of the hypergraph state. First, we translate the Hardy-type argument into a Bell inequality:

Theorem 3.2. *Putting together all the null terms derived from the stabilizer formalism and subtracting the terms causing a Hardy-type argument, we obtain the Bell inequality*

$$\begin{aligned}\langle \mathcal{B}_3^{(1)} \rangle = {} & P(+--|XZZ) + P(-++|XZZ) + P(--+|XZZ) + P(-+-|XZZ) \\ & + P(-+-|ZXZ) + P(+-+|ZXZ) + P(--+|ZXZ) + P(+--|ZXZ) \\ & + P(--+|ZZX) + P(++-|ZZX) + P(-+-|ZZX) + P(+--|ZZX) \\ & - P(+--|XXX) - P(-+-|XXX) - P(--+|XXX) \geq 0.\end{aligned} \tag{3.14}$$

Proof. This Bell inequality follows from the Hardy argument: If a deterministic local model predicts one of the results with the minus signs, it also has to predict at least one of the results corresponding to the terms with a plus sign, otherwise, it contradicts with the Hardy argument. In addition, all the terms with a minus sign are exclusive, so a deterministic LHV model can predict only one of them. □

The hypergraph state $|H_3^3\rangle$ violates this inequality with the value $\langle \mathcal{B}_3^{(1)} \rangle_Q = \frac{3}{16}$.

We can get similar Hardy-type argument and Bell inequality from the stabilizer correlations in Eqs. (3.9-3.10):

Theorem 3.3. *If a fully local hidden variable model satisfies the conditions from Eqs. (3.9-3.10) and their symmetric correlations coming from the permutations, then it must imply all the following perfect correlations too, for any possible set of results $\{r_i\}$, where one $r_{i_1} = +1$ and two $r_{i_2} = r_{i_3} = -1$*

$$P(r_1 r_2 \dots r_N | XX \dots X) = 0. \tag{3.15}$$

the proof of this statement again relies on all possible local deterministic assignments. But for the N-qubit hypergraph state $|H_N^N\rangle$ the value of probability in Eq. (3.15) is equal to $1/2^{(2N-2)}$, which is exponentially decreasing with the number of parties. This Hardy-type argument leads to a Bell inequality as in Eq. (3.14), which is violated by the state with a value of $-(2^N - N - 2)/2^{(2N-2)}$.

Clearly, the violation of the Bell inequality is not strong, as it does not increase with the number of particles. Nevertheless, Theorem 3.3 shows that the nonlocal stabilizer formalism allows one to easily obtain nonlocality proofs. In fact, one can directly derive similar arguments for other hypergraph states (e.g., states with one hyperedge of cardinality N and one further arbitrary hyperedge).

3.4 Genuine multiparticle nonlocality

So far, we considered only fully local models, where for a given HV all the probabilities factorize. Now we go beyond these restricted types of models to the so-called hybrid models [45]. We consider a bipartition of the three particles, say $A|BC$, and consider a model of the type presented in Eq. (2.28). Here, Alice is separated from the rest, but χ^{BC} may contain correlations, e.g., coming from an entangled state between B and C. In order to be physically reasonable, however, we still request χ^{BC} not to allow instantaneous signaling.

It turns out that even this kind of more general model, even if different bipartitions are mixed as in Eq. (2.31), cannot explain the correlations of the hypergraph state, meaning that the hypergraph state is genuine multiparticle nonlocal. First, one can see by direct inspection that the stabilizer conditions from Eqs. (3.4-3.5) are not compatible with the hypergraph correlations

$$P(---|XXX) = \frac{1}{16} \qquad \text{and} \qquad P(---|ZZZ) = \frac{1}{8}. \tag{3.16}$$

Since these quantities are symmetric, one can construct a Bell-Svetlichny inequality [45] valid for all the different bipartitions and arrive to one of the main results of this chapter:

Theorem 3.4. *Putting all the terms from the hypergraph stabilizer formalism and the correlations $P(---|XXX)$ and $P(---|ZZZ)$ together, we obtain the following Bell-Svetlichny inequality for genuine multiparticle nonlocality,*

$$\begin{aligned}\langle \mathcal{B}_3^{(2)} \rangle = {} & P(+--|XZZ) + P(-++|XZZ) + P(--+|XZZ) + P(-+-|XZZ) \\ & + P(-+-|ZXZ) + P(+-+|ZXZ) + P(--+|ZXZ) + P(+--|ZXZ) \\ & + P(--+|ZZX) + P(++-|ZZX) + P(-+-|ZZX) + P(+--|ZZX) \\ & + P(---|XXX) - P(---|ZZZ) \geq 0,\end{aligned} \tag{3.17}$$

which is violated by the state $|H_3^3\rangle$ with the amount of $-1/16$.

Proof. The proof is done by an exhaustive assignments of nonsignaling and local models. □

To investigate the noise tolerance of inequality (3.17), we consider mixing white noise with the hypergraph state

$$\rho = (1-\epsilon)|H_3^3\rangle\langle H_3^3| + \frac{\epsilon}{8}\mathbb{1}. \tag{3.18}$$

We ask how much noise can be added, while the inequality is still violated by ρ. The white noise tolerance of inequality (3.17) is $\epsilon = 1/13$ and is optimal in the sense that for larger values

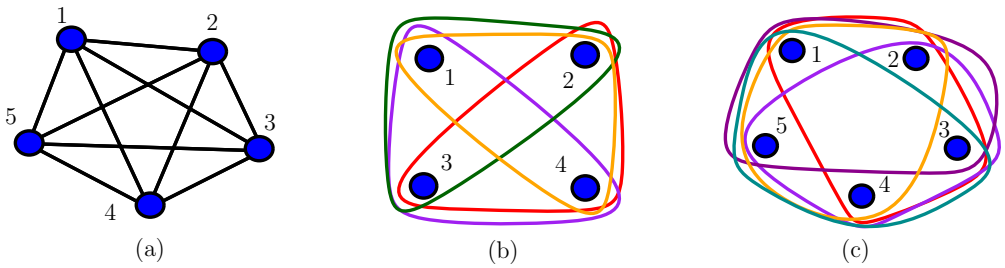


FIGURE 3.1: Complete hypergraph states. (a) Two-uniform fully connected hypergraph state – a complete graph state, LU equivalent to GHZ-state. (b) Three-uniform fully connected hypergraph state – every combination of three vertices are connected by a hyperedge. (c) Four-uniform fully connected hypergraph state – every combination of four vertices are connected by a hyperedge.

of noise a hybrid model can be found, which explains all possible measurements of X and Z (within numerical precision). The existence of such a model can be shown by solving membership problem using linear programming as discussed in Eq. (2.32). With the same method we can also prove that the state becomes fully local with respect to X and Z measurements for $\epsilon \geq 2/3$.

3.5 Extreme violation in complete three-uniform states

In this section we extend our analysis of nonlocality to hypergraph states with a larger number of particles. In the spirit of the exponential violation derived in Chapter 2, Subsection 2.4.1.5 using the N-qubit GHZ-state, we try to get the similar violation of Bell inequalities with the increasing number of parties for hypergraph states. Such a behaviour has previously been observed only for GHZ-states and some cluster states [90, 91].

The N-qubit GHZ state corresponds to the N-vertex complete graph state as in Fig. 3.1 (a), i.e., fully connected two-uniform hypergraph states. The first natural generalization is to investigate the case, where instead of all cardinality two edges, we consider the states with all cardinality three hyperedges. Thus, we take the N-vertex three-uniform complete hypergraph state, $|H_N^3\rangle$ as in Fig. 3.1 (b) and we investigate its nonlocal properties. Similarly to the Mermin operator in Eq. (2.66) we write down a new Bell operator for our state:

$$\begin{aligned}\mathcal{B}_N = &- Z_1Z_2Z_3Z_4\ldots Z_N \\ &+ X_1X_2Z_3Z_4\ldots Z_N + \text{ permutations} \\ &- X_1X_2X_3X_4Z_5\ldots Z_N - \text{ permutations} \\ &+ X_1X_2X_3X_4X_5X_6Z_7\ldots Z_N + \text{ permutations} \\ &- \ldots.\end{aligned} \tag{3.19}$$

These operator is constructed using sums of tensor products of Pauli operators, it is permutation symmetric, has 2^{N-1} terms and an alternating sign in front of the terms with different number of Pauli-X or Pauli-Y matrices. So, the operator $\mathcal{B}_N$ can be obtained from the Mermin one by the change of bases. On the other hand, changing bases cannot alter the maximum classical value the operator can attain. Therefore, one directly concludes that the LHV bound for the new Bell operator can be derived from the bound of the Mermin operator. If N is odd, our Bell inequality is exactly the rotated Mermin inequality $\mathcal{B}_N^M$. If N is even, $\langle \mathcal{B}_N \rangle_{LHV} = \langle Z \cdot \mathcal{B}_{N-1}^M + X \cdot \tilde{\mathcal{B}}_{N-1}^M \rangle_{LHV} \leq 2 \langle \mathcal{B}_{N-1}^M \rangle_{LHV}$, where $\tilde{\mathcal{B}}$ denotes the inequality where Pauli-X and Pauli-Z are exchanged, and the claim follows.

$$\langle \mathcal{B}_N \rangle_{LHV} \leq 2^{\lfloor N/2 \rfloor}. \tag{3.20}$$

Now we calculate the value of the new operator for the three-uniform complete hypergraph state $|H_N^3\rangle$.

Theorem 3.5. *The N-qubit fully connected three-uniform hypergraph state, $|H_N^3\rangle$ violates the classical bound of the operator $\mathcal{B}_N$, by an amount that grows exponentially with the number of qubits, namely*

$$\langle \mathcal{B}_N \rangle_Q \equiv \langle H_N^3 | \mathcal{B}_N | H_N^3 \rangle \geq 2^{N-2} - \frac{1}{2}. \tag{3.21}$$

Proof. The proof is done by direct calculation of the expectation value of the operator, similarly to the GHZ-state case. However, our state is no longer an eigenstate of each summand in the operator $\mathcal{B}_N$ with the eigenvalue ± 1. Instead, for each summand we obtain the following expectations values. On N qubits and for even m with $1 < m < N$

$$\langle \underbrace{X \dots X}_{m} Z \dots Z \rangle = \begin{cases} +\frac{1}{2} & \text{if } m = 2 \bmod 4, \\ -\frac{1}{2} & \text{if } m = 0 \bmod 4. \end{cases} \tag{3.22}$$

Moreover, if $m = N$, then the correlations are given by

$$\langle \underbrace{XX \dots XX}_{N} \rangle = \begin{cases} 0 & \text{if } N = 0 \bmod 4, \\ 1 & \text{if } N = 2 \bmod 4. \end{cases} \tag{3.23}$$

Finally, we always have $\langle ZZ \dots ZZ \rangle = 0$. The derivations of these equations are rather lengthy and require diligent calculations, which we shift to the Appendix A. The key result here corresponds to the fact that terms in Eq. (3.22) have an alternating sign, precisely corresponding to the alternating sign we saw before, when evaluating the Mermin operator for the GHZ-state. The only difference is the factor of $1/2$, which is independent of the number of parties. This guarantees an exponentially growing violation of local realism using three-uniform hypergraph states. In particular, for odd N, we have

$$\langle \mathcal{B}_N \rangle_Q = \sum_{k \, even}^{N} \binom{N}{k} \frac{1}{2} = 2^{N-2}. \tag{3.24}$$

If $N = 0 \bmod 4$, then

$$\langle \mathcal{B}_N \rangle_Q = \sum_{k\ even}^{N-1} \binom{N}{k} \frac{1}{2} - \langle X \dots X \rangle = 2^{N-2} - 1/2 \tag{3.25}$$

and for $N = 2\ mod\ 4$, we have

$$\langle \mathcal{B}_N \rangle_Q = \sum_{k\ even}^{N-1} \binom{N}{k} \frac{1}{2} - \langle X \dots X \rangle = 2^{N-2} + 1/2. \tag{3.26}$$

This finalizes the proof. For the exact derivations and techniques used, see Appendix A.1. □

3.6 Extreme violation in complete four-uniform states

In this section we extend our analysis of extreme nonlocality even further to the hypergraphs with all cardinality four hyperedges, $|H_N^4\rangle$. See Fig. 3.1 (c) for an example of the four-uniform complete hypergraph. For them, the correlations of measurements are not as simple as in Eq. (3.22): They are not constant and depend on number of Pauli-X operators, m as well as on number of particles N. Nevertheless, they can be explicitly computed and also lead to an exponentially increasing violations of local realism.

Theorem 3.6. *The N-qubit complete four-uniform hypergraph state violates local realism by an amount that grows exponentially with the number of qubits. More precisely, one can find a Mermin-like Bell operator $\langle \mathcal{B}_N \rangle$ such that*

$$\frac{\langle \mathcal{B}_N \rangle_Q}{\langle \mathcal{B}_N \rangle_{LHV}} \overset{N\to\infty}{\sim} \frac{(1+\frac{1}{\sqrt{2}})^{N-1}}{\sqrt{2}^{N+3}} \approx \frac{1.20711^N}{2\sqrt{2}+2}, \tag{3.27}$$

where $\langle \mathcal{B}_N \rangle_Q \equiv \langle H_N^4 | \mathcal{B}_N | H_N^4 \rangle$.

Proof. The proof is done by direct calculation of the expectation value of the operator, similar to the three-uniform complete hypergraph state case. However, it is much more involving. In order to make it more evident that hypergraph states behave very differently with local Pauli stabilizers than graph states do, here we give a summary of values of individual correlations. Luckily, it turns out that these states for every value of N reveal correlations from which exponential violation of Mermin-like Bell inequalities can be derived. The same fails to hold for higher cardinality hyperedges.

The following statements hold for N-qubit, four-uniform complete hypergraph states:

1. For the case $N = 8k-2$ or $N = 8k-1$, or $8k$, we have:
   (i)

$$\langle \underbrace{X \dots X}_{m} Z \dots Z \rangle = \begin{cases} +\frac{2^{\lfloor N/2 \rfloor - m + 1}}{2^{\lfloor N/2 \rfloor - \lfloor m/2 \rfloor}} & \text{if } (m-1) = 0 \bmod 4, \\ -\frac{2^{\lfloor N/2 \rfloor - m + 1}}{2^{\lfloor N/2 \rfloor - \lfloor m/2 \rfloor}} & \text{if } (m-1) = 2 \bmod 4. \end{cases} \tag{3.28}$$

(*ii*) For $N = 8k - 1$, we have:

$$\langle \underbrace{XX\ldots XX}_{N} \rangle = -1. \tag{3.29}$$

For $N = 8k - 2$ or $N = 8k$, these correlations will not be needed.

2. For $N = 4k + 1$, we have:

$$\langle \underbrace{X\ldots X}_{m} Z\ldots Z \rangle = \begin{cases} +\frac{1}{2^{\lceil m/2 \rceil}}, & \text{if } (m-1) = 0 \ mod\ 4, \\ -\frac{1}{2^{\lceil m/2 \rceil}}, & \text{if } (m-1) = 2 \ mod\ 4, \\ \frac{1}{2^{\lfloor N/2 \rfloor}}, & \text{if } m = N. \end{cases} \tag{3.30}$$

3. For $N = 8k + 2$ or $8k + 4$, we have for even m:
(i)

$$\langle \underbrace{X\ldots X}_{m} Z\ldots Z \rangle = \begin{cases} +\frac{2^{m/2-1}}{2^{N/2}} & \text{if } (N-m) = 0 \ mod\ 4, \\ -\frac{2^{m/2-1}}{2^{N/2}} & \text{if } (N-m) = 2 \ mod\ 4. \end{cases} \tag{3.31}$$

(ii)

$$\langle XX\ldots XX \rangle = \frac{2^{\frac{N}{2}-1}+1}{2^{\frac{N}{2}}}. \tag{3.32}$$

4. For $N = 8k + 3$, $\langle \underbrace{X\ldots X}_{m} \underbrace{Z\ldots Z}_{N-m-1} \mathbb{1} \rangle$ for even m gives the same exact result as the part 3, so we have:

$$\langle \underbrace{X\ldots X}_{m} \underbrace{Z\ldots Z}_{N-m-1} \mathbb{1} \rangle = \begin{cases} +\frac{2^{m/2-1}}{2^{M/2}} & \text{if } (M-m) = 0 \ mod\ 4, \\ -\frac{2^{m/2-1}}{2^{M/2}} & \text{if } (M-m) = 2 \ mod\ 4, \end{cases} \tag{3.33}$$

where $M = N - 1$.Note that for this last case the full correlation functions do not have the structure required for exponential violation, but if we consider tracing out one of the parties, Eq. (3.33) emerge. For the exact derivations see Appendix A.2

Having established the correlations, we sum them up for calculating the violation. We take either the Bell inequality in Eq. (3.19), or the original Mermin operator, $\langle \mathcal{B}_N^M \rangle$, but we fix instead of Y, Pauli-X and Pauli-Z for X. The choice of the Bell operator depends on the number of qubits: From the correlations above in Eq. (3.6) for a given N either the correlations for an even m or an odd m are given. If m is even, we choose Eq. (3.19) and $\langle \mathcal{B}_N^M \rangle$, otherwise.

From the correlations, it is evident that we need to consider separate cases for different N. However, here we choose the one which encounters the smallest growth in the violation and this is naturally the $N = 8k + 3$ case. Other cases just encounter different factors in the growth

or are greater. For the $N = 8k + 3$, the strategy consists of measuring the Bell operator from Eq. (3.19) on $M = N - 1$ qubits. Then we have:

$$\begin{aligned}\langle \mathcal{B}_N \rangle_Q &\geq \sum_{m=2,4\ldots}^{M} \binom{M}{m} \left(\frac{1}{\sqrt{2}}\right)^{M-m+2} = \frac{1}{2}\Big[\sum_{m\ even}^{M} \binom{M}{m} \left(\frac{1}{\sqrt{2}}\right)^{M-m}\Big] - \left(\frac{1}{\sqrt{2}}\right)^{M+2} \\ &= \frac{1}{4}\left[\left(1+\frac{1}{\sqrt{2}}\right)^{M} - \left(1-\frac{1}{\sqrt{2}}\right)^{M}\right] - \left(\frac{1}{\sqrt{2}}\right)^{M+2}.\end{aligned} \tag{3.34}$$

Checking the ratio of the quantum and classical values, we have that

$$\frac{\langle \mathcal{B}_N \rangle_Q}{\langle \mathcal{B}_N \rangle_C} \overset{N\to\infty}{\sim} \frac{\frac{1}{4}\left(1+\frac{1}{\sqrt{2}}\right)^{N-1}}{2^{\frac{N-1}{2}}} = \frac{\left(1+\frac{1}{\sqrt{2}}\right)^{N-1}}{\sqrt{2}^{N+3}} \approx \frac{1.20711^N}{2\sqrt{2}+2}. \tag{3.35}$$

Looking at the expectation values from Eq. (3.6), it is straightforward to see that in all other cases of N, correlations are stronger than in the $N = 8k + 3$ case, so the quantum violation increases. □

3.7 Robustness of violation

So far, we have shown that the three- and four-uniform hypergraph states violate local realism comparable to the GHZ-states. A striking difference is, however, that the entanglement and Bell inequality violation of hypergraph states is robust under particle loss. This is in stark contrast with the GHZ-states, which become fully separable if a particle is lost. We already got a glimpse at this advantageous property of hypergraph states when looking at the correlations for $N = 8k + 3$ four-uniform complete hypergraph states. Now we extend our analysis to more general cases.

For the three-uniform complete hypergraph states we can prove that the reduced states are highly entangled, as they violate inequalities testing for separability [93] exponentially.

Theorem 3.7. *The N-qubit (except when $N = 4k$) three-uniform HG state violates the separability inequality exponentially after tracing out a single qubit.*

Proof. First we calculate correlations for the reduced density matrices. Alternatively, we measure $(N-1)$-partite correlations. Then the following statements hold for the three-uniform complete hypergraph states:

(i) For $N = 8k + 5$, $N = 8k + 6$, or $N = 8k + 7$:

$$\langle \underbrace{X\ldots X}_{m}\underbrace{Z\ldots Z}_{N-m-1}\mathbb{1}\rangle = \begin{cases} -\frac{1}{2^{\left\lfloor \frac{N-1}{2} \right\rfloor}} & \text{if } (m-1) = 0 \ mod\ 4, \\ +\frac{1}{2^{\left\lfloor \frac{N-1}{2} \right\rfloor}} & \text{if } (m-1) = 2 \ mod\ 4. \end{cases} \tag{3.36}$$

# k	Quantum Value	Separability Bound	≈Ratio
0	511.5	$\sqrt{2}$	361.69
1	16	$\sqrt{2}$	11.31
2	8	$\sqrt{2}$	5.66
3	4	$\sqrt{2}$	2.83
4	2	$\sqrt{2}$	1.414

TABLE 3.1: Violation of the separability inequalities [93] for the $N = 11$ qubit three-uniform complete hypergraph state. Here k is the number of traced out qubits. When $k = 0$, the Mermin-like inequality is violated as expected.

(ii) For $N = 8k + 1$, $N = 8k + 2$, or $N = 8k + 3$:

$$\langle \underbrace{X \dots X}_{m} \underbrace{Z \dots Z}_{N-m-1} \mathbb{1} \rangle = \begin{cases} +\frac{1}{2^{\lfloor \frac{N-1}{2} \rfloor}} & \text{if } (m-1) = 0 \ mod\ 4, \\ -\frac{1}{2^{\lfloor \frac{N-1}{2} \rfloor}} & \text{if } (m-1) = 2 \ mod\ 4. \end{cases} \tag{3.37}$$

(iii) For $N = 4k$:

$$\langle \underbrace{X \dots X}_{m} \underbrace{Z \dots Z}_{N-m-1} \mathbb{1} \rangle = 0 \tag{3.38}$$

See Appendix A.4 for the exact derivations. We consider only one case, $N = 8k + 5$, as others are analogous. Here $M = N - 1$:

$$\langle \mathcal{B}_N \rangle_Q = \sum_{m \ odd}^{M} \binom{M}{m} \left(\frac{1}{\sqrt{2}}\right)^M = 2^{M-1} \cdot 2^{-M/2} = \sqrt{2}^{N-3}. \tag{3.39}$$

Separability bound is $\sqrt{2}$ [93] and it does not depend on the number of qubits. □

This violation decreases with the number of traced out qubits, but persists even if several qubits are lost. See Table. 3.1 for the example of $N = 11$ qubit state, where four qubits are traced out. This suggests that this class of hypergraph states is more robust than GHZ states. One can also check that after particle loss three-uniform complete hypergraph states no longer violate Mermin-like inequalities. Despite the structural differences, this property resembles of the W state, which is itself less entangled but more robust than the GHZ state [123].

The four-uniform complete hypergraph states turn out to be even more robust under particle loss:

Theorem 3.8. *The N-qubit complete four-uniform hypergraph state preserves the violation of the local realism even after loss of one particle. More precisely for for $N = 8k + 4$, we have*

$$\frac{\langle \mathcal{B}_{N-1} \rangle_Q}{\langle \mathcal{B}_N \rangle_Q} \overset{N \to \infty}{\sim} \frac{1}{\sqrt{2}+1}. \tag{3.40}$$

As the fraction is independent of N, the reduced state shows the same exponential scaling of the Bell inequality violation as the original state.

#k	Quantum Value	Classical Bound	Separability Bound	≈Ratio
0	**153.141**	**64**		**2.39283**
1	89.7188	32		2.78125
2	37.1563	32		1.16113
3	15.4219	-	$\sqrt{2}$	10.9049
4	6.375	-	$\sqrt{2}$	4.50781
5	2.70313	-	$\sqrt{2}$	1.9114

TABLE 3.2: Violation of Bell (for odd m) and Separability inequalities in the $N = 12$ qubit four-uniform complete HG state. Here k is the number of traced out qubits. The red line represents that when $k = 1$, or equivalently one qubit is traced out, the violation of Bell inequalities increases. This is caused by decrease in the classical bound [29].

Proof. Similar to the last case, the proof is again based on the direct inspection of correlations. The following statement holds for $N = 8k + 4$ qubit four-uniform complete hypergraph states:

$$\langle \underbrace{X \dots X}_{m} \underbrace{Z \dots Z}_{N-m-1} \mathbb{1} \rangle = \begin{cases} -\left(\frac{1}{\sqrt{2}}\right)^{N-m+2} & \text{if } m = 0 \ mod\ 4, \\ +\left(\frac{1}{\sqrt{2}}\right)^{N-m+2} & \text{if } m = 2 \ mod\ 4. \end{cases} \tag{3.41}$$

See exact derivations in Appendix A.3. We can summarize the correlations to derive the quantum value for expectation value. Denote $M \equiv N - 1$. Then

$$\begin{aligned} \langle \mathcal{B}_{N-1} \rangle_Q &= \sum_{m=2,4\dots}^{M} \binom{M}{m} \left(\frac{1}{\sqrt{2}}\right)^{M-m+3} = \frac{1}{2\sqrt{2}} \left[\sum_{m \ even}^{M} \binom{M}{m} \left(\frac{1}{\sqrt{2}}\right)^{M-m} \right] - \left(\frac{1}{\sqrt{2}}\right)^{M+3} \\ &= \frac{1}{4\sqrt{2}} \left[\left(1 + \frac{1}{\sqrt{2}}\right)^{M} - \left(1 - \frac{1}{\sqrt{2}}\right)^{M} \right] - \left(\frac{1}{\sqrt{2}}\right)^{M+3}. \end{aligned} \tag{3.42}$$

Checking the ratio of the quantum and classical values, we have that

$$\frac{\langle \mathcal{B}_{N-1} \rangle_Q}{\langle \mathcal{B}_{N-1} \rangle_C} \overset{N \to \infty}{\sim} \frac{\frac{1}{4\sqrt{2}} \left(1 + \frac{1}{\sqrt{2}}\right)^{N-1}}{2^{\frac{N-2}{2}}} = \frac{\left(1 + \frac{1}{\sqrt{2}}\right)^{N-1}}{\sqrt{2}^{N+3}} \approx \frac{1.20711^N}{2\sqrt{2} + 2}. \tag{3.43}$$

Note that the same value for the $N = 8k + 4$ qubit four-uniform complete HG state is

$$\frac{\langle \mathcal{B}_N \rangle_Q}{\langle \mathcal{B}_N \rangle_C} \overset{N \to \infty}{\sim} \approx \frac{1.20711^N}{4}. \tag{3.44}$$

Summing up all the ratios, we arrive to the statement of the theorem. Hence, after tracing out a single qubit, the local realism violation decreases with the small constant factor. □

It is important to note that the similar violation is maintained after tracing out more than one qubits. For example, one can calculate for $N = 12$, that if one takes a Bell inequality with the odd number of X measurements, instead of the even ones as we have chosen in the proof, an

exponential violation is maintained after tracing out two qubits. But even if five qubits are traced out, the state is still entangled and this can be verified using the separability inequality [93]. Exact violations for the 12-qubit case is given in Table 3.2.

3.8 Applications and Outlook

The exponential violation of Mermin-like inequalities is not only interesting for proving extreme nonlocality of the state, but from the violation one can deduce that some quantum computational tasks can avail themselves of such states. A first application of our results is *quantum metrology*. In the standard scheme of quantum metrology one tries to make a high resolution measurement M_θ on a quantum system and estimate some physical parameter θ [22, 124]. In classical estimation theory the average error in a measurement outcome can be brought down by an amount proportional to $n^{-1/2}$, when measurement is made n times. Quantum multipartite entanglement can offer the advantage of reducing the error rate farther by an amount proportional to n^{-1}.

In quantum metrology first an N-partite quantum state is prepared. If the state admits local description, we can write it as an N-fold tensor product, $\rho^{\otimes N}$, then in each local quantum state a parameter θ in encoded by some local evolution $\rho(\theta) = e^{-iH\theta}\rho e^{iH\theta}$. Next step is to perform quantum measurements on the state $\rho(\theta)^{\otimes N}$ and try to recover the value of a continuous phase parameter θ. When the initial state is a product state, from the measurement M_θ on each particle one obtains a signal

$$\langle M_\theta \rangle \sim \cos(\theta), \tag{3.45}$$

repeating the measurement on all N particles allows to determine θ with the so-called standard quantum limit accuracy $\delta\theta \sim 1/\sqrt{N}$. However, if one takes instead the N-qubit GHZ state, one can observe

$$\langle (M_\theta)^{\otimes N} \rangle \sim \cos(N\theta). \tag{3.46}$$

This phase superresolution itself allows to reach the Heisenberg limit $\delta\theta \sim 1/N$. For a general state ρ, it has been shown that the visibility of the phase superresolution is given by the expectation value of the Mermin-type inequality [124],

$$V = \mathrm{tr}(\mathcal{B}_N \rho)/2^{N-1}. \tag{3.47}$$

And since the three-uniform complete hypergraph staes violate these inequalities exponentially, the visibility is $V \sim 1/2$, independently of the number of parties. As a result one can summarize that hypergraph states can be used for Heisenberg-limited metrology and from our results they can be expected to have the advantage of being more robust to noise and particle losses.

A second application of exponential violation of Bell inequalities is a nonadaptive measurement based quantum computation with linear side-processing (NMQC$_\oplus$) [125]. The NMQC$_\oplus$ is a non-universal model of quantum computation, where linear classical side-processing is combined with quantum measurements in a nonadaptive way, i.e., the choice of settings is

independent of previous outcomes. In Ref. [125] the authors connect the expectation value of a full-correlation Bell expression [118] with the success probability of computing a Boolean function, specified as a function of the inequality coefficients via $\mathrm{NMQC}_{\oplus}$. In particular, the exponential violation of generalized *Svetlichny inequalities* [123] (equal to Mermin inequalities for even N) corresponds to a constant success probability P_{succ} of computing the pairwise AND on N bits extracted from a uniform distribution, whereas in the classical case this probability decreases exponentially with N. As a consequence, the exponential violation of the full-correlation Bell expression can be directly related to an exponential advantage for computation tasks in the $\mathrm{NMQC}_{\oplus}$ framework. Moreover, in several cases, e.g., four-uniform hypergraph states of $N = 6 \bmod 8$ qubits, also the Svetlichny inequality is violated exponentially, providing advantage for computation of the pairwise AND discussed in Ref. [125].

In summary, we have shown that hypergraph states are very interesting class of multipartite entangled states violating local realism in many ways. These states are also useful for quantum information theoretic tasks in a robust manner and this, supposedly, makes them interesting for experimentalists. In our work, we focused only on some classes of hypergraph states, but for future research, it would be desirable to identify classes of hypergraph states which allow for an all-versus-nothing violation of local realism or which are strongly genuine multiparticle nonlocal. As for a more specific task, it would be interesting to find inequalities for hypergraphs with higher cardinality hyperedges, which such states can also violate with an increasing amount. According to our observations, the correlations coming from such states (e.g., five- or six- uniform complete hypergraph states) for Mermin-like summands do not behave as nicely as the ones from three- and four- uniform case. Therefore, trying some new inequalities are in order.

Chapter 4

Graphical rules for transformations on hypergraph states

Hypergraph states form an interesting family of multiparticle quantum states and have an insightful graphical representation. In this chapter we give a collection of transformations on hypergraph states, which also have a nice graphical rule. Such actions include local and nonlocal unitary transformations between hypergraph states. This leads to a generalization of local complementation and graphical rules for various gates, such as the $CNOT$ gate and the Toffoli gate. As an application, we show that already for five qubits local Pauli operations are not sufficient to check local equivalence of hypergraph states. Next we study Pauli bases measurement rules for hypergraph states, for Pauli-Z this rule is rather simple and was given in Ref.[113]. We give a sufficient criteria when Pauli-X measurements do not leave hypergraph state space.

4.1 Introduction

Multipartite quantum states known as hypergraph states generalize several features of graph states as seen in Chapter 2. First, they admit the stabilizer description (See subsection 2.4.2.2) and they also violate local realism exponentially (See subsection 2.4.1.5 for graph states and Chapter 3 for the generalizations). Most relevantly for this chapter, they have nice graphical rules for Pauli equivalences (See subsection 2.4.2.3). Since different graphs and hypergraphs may lead to quantum states with the same entanglement properties, it is important to study the action of local and nonlocal unitary transformations between these states. For graph states, the local complementation plays a very important role (See subsection 2.4.1.3). Physically this map is implemented by local unitaries, which correspond to the square-roots of a local Pauli stabilizer. Likewise, we derive the graphical rule for the action of the square-roots of a nonlocal stabilizer. The unitaries obtained this way are not necessarily local, but we give several constructions for which one can manage to restrict these operations to local Clifford transformations.

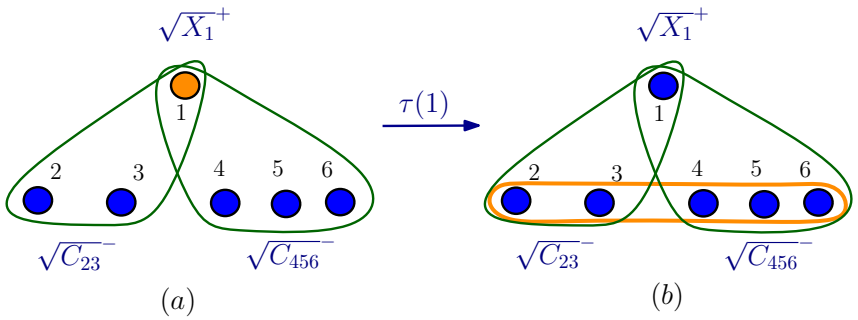


FIGURE 4.1: Generalized local complementation. Transformation $\tau(1)$ is applied to the hypergraph (a). The adjacency of the vertex 1 is $\mathcal{A}(1) = \{\{2,3\},\{4,5,6\}\}$. As a result the new hyperedge $\{2,3,4,5,6\}$ is added to the hypergraph.

Since the hypergraph states are equally weighted Boolean function encoded states as defined in Eq. (2.72), transposing some of the computational basis elements map hypergraph states to hypergraph states. Pauli-X operation is the simplest such transformation. We express general transpositions in the form of multiqubit controlled-NOT unitaries and derive graphical rules for hypergraph states. These rules find applications in several directions of quantum information theory. First, they are one of the core transformations when deriving entanglement witnesses for hypergraphs states (See Chapter 5). Second, they are used when deriving graphical rules for Pauli-X basis measurements (we give these derivations in this chapter), which are themselves crucial to construct measurement-based quantum computation protocols using hypergraph states (See Chapter 6).

To sum up, this chapter is denoted to deriving new graphical rules on hypergraph states.

4.2 Local complementation in hypergraph states

We introduce the concept of a *local edge-pair complementation* in hypergraphs around a vertex $a \in V$. Let us define first the set of adjacency pairs of vertex a to be the set

$$\mathcal{A}_2(a) = \{\{e_1, e_2\} | e_1 \neq e_2, e_1 \in \mathcal{A}(a), e_2 \in \mathcal{A}(a)\} \tag{4.1}$$

of all distinct pairs in the adjacency set. The local edge-pair complementation around a vertex a complements the edges in the multiset $P = \{e_1 \cup e_2 | \{e_1, e_2\} \in \mathcal{A}_2(a)\}$. Notice that P is a multiset and only the edges appearing with odd multiplicity are be affected. Complementation of the edges in this multiset means that they are deleted from the hypergraph, if they were already present, and the are added, if they were not present.

The local complementation or a local edge-pair complementation is implemented over some vertex $a \in V$ of a hypergraph $H = (V, E)$ by applying the square-roots of the stabilizer h_a, defined in Eq. (2.73). Note that the signs of the square-roots have to be chosen in a particular way:

$$\tau(a) = \sqrt{X_a}^{\pm} \bigotimes_{e \in \mathcal{A}(a)} \sqrt{C_e}^{\mp}. \tag{4.2}$$

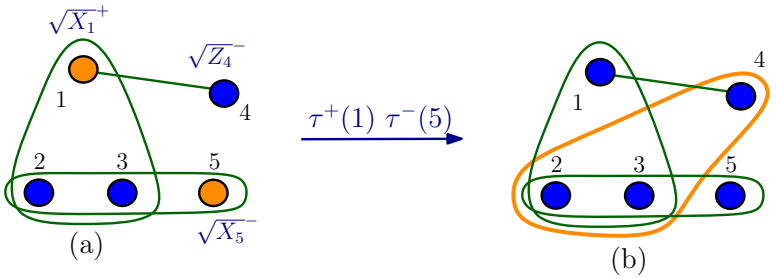


FIGURE 4.2: Local Clifford equivalence of two five-qubit hypergraph states. (a) Application of two local Clifford operators, which effectively implement two local complementations over vertices 1 and 5. Importantly the signs of local complementations shall be chosen to be different from one another. These two maps commute and, moreover, square-roots of adjacent operators on qubits 2 and 3 cancel out. (b) Additional hyperedge $\{2,3,4\}$ is obtained as a result of local complementation over the first vertex. This example shows that for five-qubit hypergraph states local Pauli operators are not enough to classify local unitary equivalences.

Here $\sqrt{C_e}^{\pm} = \mathbb{1} - (1 - (\pm i))|11\ldots1\rangle\langle11\ldots1|$ is a diagonal operator acting on $|e|$ vertices. We are ready to formulate the generalized local complementation theorem

Theorem 4.1. *For any hypergraph state corresponding to a hypergraph $H = (V, E)$, the transformation $\tau(a)$ around a vertex $a \in V$ performs a local edge-pair complementation on its corresponding hypergraph.*

Proof. See the proof in Ref. [32]. □

Note that the transformation τ is a nonlocal map, so it can change entanglement properties of the state. The name, generalized local complementation, shall not be interpreted as if the map is local. For an examples of generalized local complementation see Figs. 4.1 and 4.2.

In Chapter 2, subsection 2.4.2.3 we saw that for the four-qubit hypergraph states Pauli operators are necessary and sufficient to describe local unitary equivalences. Here we investigate local Clifford operations and their actions on hypergraph states. It appears that one can take advantage of the generalized local complementation rule by applying it over different vertices in the way that all the nonlocal unitary actions cancel out. Then a new hypergraph state is obtained only as a result of local Clifford operations. To give an example, consider the five-vertex hypergraph state $H_5 = (V, E)$, with hyperedges, $E = \{\{1,2,3\},\{1,4\},\{2,3,5\}\}$. See also Fig. 4.2. Then one can write explicitly that the local complementation over the vertex 1 can be implemented by several local Clifford gates:

$$\begin{aligned}\tau^+(1)|H_5\rangle =& \tau^+(1)\tau^-(5)|H_5\rangle = \tau^-(5)\tau^+(1)|H_5\rangle \\ =& \sqrt{X_1}^+\sqrt{Z_4}^-\sqrt{C_{23}}^-\sqrt{X_5}^-\sqrt{C_{23}}^+|H_5\rangle \\ =& \sqrt{X_1}^+\sqrt{X_5}^-\sqrt{Z_4}^-(\sqrt{C_{23}}^-\sqrt{C_{23}}^+)|H_5\rangle \\ =& \sqrt{X_1}^+\sqrt{X_5}^-\sqrt{Z_4}^-|H_5\rangle = C_{234}|H_5\rangle.\end{aligned} \tag{4.3}$$

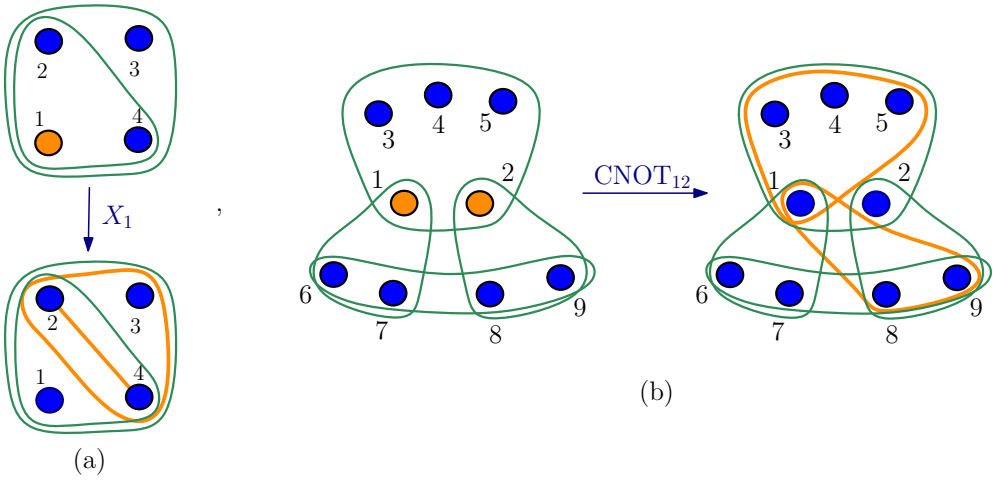


FIGURE 4.3: Examples of transpositions on hypergraph states. (a) Pauli-X transposition is applied to the vertex 1 and as a results new hyperedges are added to the hypergraph. (b) $CNOT_{12}$ is applied to the hypergraph state. Adjacency of the target qubit is $\mathcal{A}(2) = \{\{1,3,4,5\},\{8,9\}\}$, when getting united with the controlled qubit, 1, the new hyperedges, $E_{new} = \{\{1,3,4,5\},\{1,8,9\}\}$, are added to the state.

This example shows that already for five qubits, one needs a bigger class of local unitaries than local Pauli operators in order to classify local unitary equivalent states.

4.3 Graphical rules for permutation unitaries on hypergraph states

In the previous section we considered the extension of local complementation for hypergraph states. In this section we investigate a different family of unitary transformations, we call them permutation unitaries. These transformations permute the vectors of the computational basis. Such permutations are obviously unitary and from Eq. (2.72) it is clear that they map hypergraph states to hypergraph states, so there must be a graphical description.

The simplest example of such a permutation unitary is Pauli-X (or NOT) gate, action of which was studied before as discussed in Chapter 2, see also Fig. 4.3 for an example. A nonlocal example of a permutation unitary is the $CNOT$ gate as seen in Eq. (2.36). This is a nonsymmetric gate in its input, so one has to clarify which qubit is a controlled qubit, c and which one is a target one, t:

$$CNOT_{ct} : |10\rangle \leftrightarrow |11\rangle \tag{4.4}$$

Its extension to three-qubits is the Toffoli gate, $CCNOT_{c_1c_2t} : |110\rangle \leftrightarrow |111\rangle$. The Toffoli gate is itself a conjugated CCZ gate: $CCNOT_{c_1c_2t} = H_3CCZH_3$. Clearly, it is not necessary to consider all permutations, as any permutation can be viewed as a sequence of transpositions. For two-qubit permutations, one can easily see that NOT and $CNOT$ are enough to cover all possible permutations. Additionally, it is known that every permutation on $\{0,1\}^N$ can be realized by means of a reversible circuit using the NOT, $CNOT$ and $CCNOT$ basis and

at most one ancilla bit [126]. It is possible to derive a graphical rule of how such maps transform hypergraph states. Here we give rules explicitly only for the two-qubit *CNOT* and its multiqubit extensions, but the methodology can be applied to derive any arbitrary permutation unitary, if the exact graphical transformation is needed.

Theorem 4.2. *Applying the $CNOT_{ct}$ gate on hypergraph state, where c is the control qubit and t is the target one, introduces/deletes the hyperedges of the form $E_t = \{e_t \cup \{c\} | e_t \in \mathcal{A}(t)\}$.*

Proof. Without loss of generality we assume that $CNOT_{12}$ acts on the first two qubits. We write a hypergraph state $|H\rangle$ in the *expanded form over* vertices 1 and 2 as follows:

$$
\begin{aligned}
|H\rangle = &|00\rangle|H(E_{00})\rangle && E_{00} = \{e | e \in E, e \cap c = \emptyset, e \cap t = \emptyset\}, && (4.5)\\
&+|01\rangle|H(E_{00} + E_{01})\rangle && E_{01} = \{e | e \in \mathcal{A}(t), e \cap c = \emptyset\}, && (4.6)\\
&+|10\rangle|H(E_{00} + E_{10})\rangle && E_{10} = \{e | e \in \mathcal{A}(c), e \cap t = \emptyset\}, && (4.7)\\
&+|11\rangle|H(E_{00} + E_{01} + E_{10} + E_{11})\rangle && E_{11} = \{e | e \in \mathcal{A}(\{c,t\})\}. && (4.8)
\end{aligned}
$$

The $CNOT_{12}$ gate then swaps $|10\rangle$ and $|11\rangle$, or alternatively Eq. (4.7) and Eq. (4.8), but leaves the other parts invariant. Therefore we obtain the following relations between the old and new hyperedges:

$$
\begin{aligned}
E_{00}^{\text{new}} &= E_{00}. && (4.9)\\
E_{00}^{\text{new}} + E_{01}^{\text{new}} = E_{00} + E_{01} \quad &\Rightarrow \quad E_{01}^{\text{new}} = E_{01}. && (4.10)\\
E_{00}^{\text{new}} + E_{10}^{\text{new}} = E_{00} + E_{01} + E_{10} + E_{11} \quad &\Rightarrow \quad E_{10}^{\text{new}} = E_{01} + E_{10} + E_{11}. && (4.11)\\
E_{00}^{\text{new}} + E_{01}^{\text{new}} + E_{10}^{\text{new}} + E_{11}^{\text{new}} = E_{00} + E_{10} \quad &\Rightarrow \quad E_{11}^{\text{new}} = E_{11}. && (4.12)
\end{aligned}
$$

Equations (4.9-4.12) show that only the hyperedges containing the control qubit can play role. More precisely, Eq. (4.11) shows that the new hyperedges that are added/deleted are of the form $E_t = \{e_t \cup c | e_t \in \mathcal{A}(t)\}$. □

An example of this rule is shown in Fig. 4.3. We can directly generalize this rule to extended *CNOT* gates, such as the Toffoli gate, the proof is essentially the same.

Corollary 4.3. *Applying the extended $CNOT_{Ct}$ gate on a hypergraph state, where a set of control qubits C controls the target qubit t, introduces or deletes the set of hyperedges $E_t = \{e_t \cup C | e_t \in \mathcal{A}(t)\}$.*

Moreover, as mentioned above every permutation can be constructed using *NOT*, *CNOT*, and *CCNOT* and at most one ancilla qubit. An ancilla qubit is necessary to construct the multiqubit gate set, $\mathcal{T} = \{C^0NOT, CNOT, \ldots, C^kNOT\}$ [127] and the set $\mathcal{T}$ is enough to realize any permutation on k indices. As $\mathcal{T}$ exactly consists of the gates with graphical rules from above, we can state:

Corollary 4.4. *Every permutation unitary maps a hypergraph state to a hypergraph state and its graphical action can be seen as a composition of rules from $\mathcal{T} = \{C^0NOT, CNOT, \ldots, C^kNOT\}$ graphical rules.*

It is interesting to note how the different rules change the cardinality of edges. If m is the cardinality of the largest edge in the hypergraph, the *NOT* gate can only create/erase edges with a cardinality strictly smaller then m. The *CNOT* gate can create/erase edges with cardinality smaller or equal to m. However, the CCNOT can create hyperedges with cardinality larger than m, since it controls two vertices and if these vertices are disjoint with the adjacency present in the highest cardinality edge of a target qubit, then the new biggest hyperedge will have the cardinality $(m+1)$. We will see the use of a general CNOT action on hypergraph states in various derivations in the subsequent sections.

4.4 Pauli measurement rules on hypergraph states

In this section we discuss graphical rules for Pauli measurements on hypergraph states. The rule for Pauli-Z is rather simple and we start by introducing it. Then we derive Pauli-Y and -X measurements rules. Both of those heavily use generalized local complementation and transposition rules for hypergraphs states.

Definition 4.5. Given a hypergraph state $|H\rangle$ corresponding to a hypergraph $H = (V, E)$. If we write this hypergraph state as follows,

$$|H\rangle = \frac{1}{\sqrt{2}}|0\rangle_a|H_0\rangle + \frac{1}{\sqrt{2}}|1\rangle_a|H_1\rangle, \tag{4.13}$$

we say that hypergraph state is expanded over a vertex $a \in V$. By definition $|H_0\rangle$ and $|H_1\rangle$ are also hypergraph states respectively corresponding to hypergraphs H_0 and H_1 with hyperedges $E_0 = \{e \in E | a \notin e\}$ and $E_1 = E_0 \cup \mathcal{A}(a)$. If we choose a subset of vertices $V_x \subset V$ instead of a vertex a, we say that hypergraph state is expanded over a set of vertices $V_x \subset V$ and expansion is done iteratively for every vertex in V_x.

For example, if we want to expand the hypergraph state $|H\rangle$ over vertices a and b, we first expand it over a and then we expand hypergraphs $|H_0\rangle$ and $|H_1\rangle$ separately over b resulting in

$$|H\rangle = \frac{1}{\sqrt{2}}|0\rangle_a\Big(|0\rangle_b|H_{00}\rangle + |1\rangle_b|H_{01}\rangle\Big) + \frac{1}{\sqrt{2}}|1\rangle_a\Big(|0\rangle_b|H_{10}\rangle + |1\rangle_b|H_{11}\rangle\Big). \tag{4.14}$$

The Pauli-Z measurement rule directly follows from the expansion of a hypergraph state. In Eq. (4.13) if the vertex a is measured in Z direction, then both outcomes occur with equal probability. The outcome 0 corresponds to projecting on a hypergraph state $|H_0\rangle$ and the outcome 1 on a hypergraph state $|H_1\rangle$ and the vertex a is removed from the hypergraph H. Formally, denoting Pauli-Z measurement by PZ, one gets:

$$PZ_a(s)|H\rangle \mapsto U_s|H - \{a\}\rangle, \tag{4.15}$$

where according to outcome $s \in \{0, 1\}$, random unitaries are applied:

$$U_0 = \mathbb{1}, \qquad U_1 = \bigotimes_{e \in \mathcal{A}(i)} C_e \tag{4.16}$$

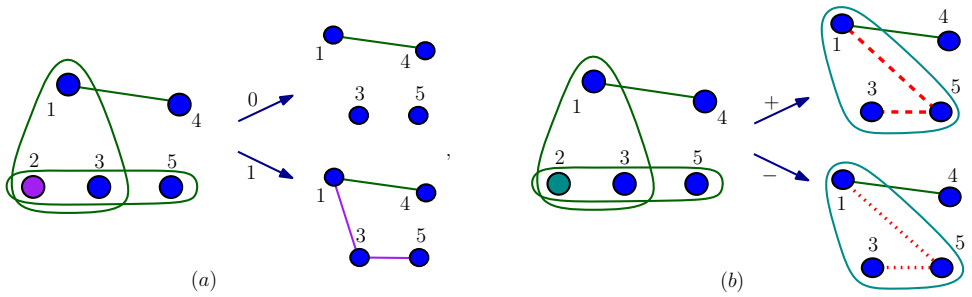


FIGURE 4.4: Graphical rules for Pauli measurements. (a) The vertex 2 is measured in Pauli-Z basis and as a result it gets removed from the hypergraph. For the outcome 0 all the hyperedges containing 2 get removed and for the outcome 1, all hyperedges in $\mathcal{A}(2)$ get added. (b) The vertex 2 is measured in Pauli-Y basis, first generalized LC is performed over the vertex 2 and then the vertex 2 gets removed from the hypergraph. Dashed and dotted lines correspond to the different signs of square-root of all hyperedges in $\mathcal{A}(2)$. Dashed ones correspond to the positive sign and dotted one to negative. Note that post-measurement states are not LU equivalent.

The rule is analogous to the graph state case. See Eq. (2.58).

The Pauli-Y measurement rule can be derived as a combination of generalized local complementation and Pauli-Z basis measurement rule. One can directly observe this by writing down the eigenvectors of Pauli-Y operator as follows:

$$\sqrt{X}^{-}|0\rangle \propto |0\rangle + i|1\rangle \equiv |y_+\rangle \qquad \text{and} \qquad \sqrt{X}^{-}|1\rangle \propto |0\rangle - i|1\rangle \equiv |y_-\rangle. \tag{4.17}$$

Then measuring a vertex a in Pauli-Y basis first corresponds to applying $\sqrt{X}_a^{+}$ and then measuring a in Pauli-Z basis in the full analogy to the graph state Pauli-Y measurement rule in Eq. (2.60).

Lemma 4.6. *Given a hypergraph state corresponding to a hypergraph $H = (V, E)$, Pauli-Y measurement rule on a vertex $a \in V$ can be expressed as follows:*

$$PY_a(s)|H\rangle \mapsto U_s|\tau_a(H) - \{a\}\rangle, \tag{4.18}$$

where unitary corrections U_s depend on a measurement outcome s and correspond to the different signs of square-roots of adjacency phase-gates of the vertex a:

$$U_+ = \bigotimes_{e\in\mathcal{A}(a)} \sqrt{C_e}^{+}, \qquad U_- = \bigotimes_{e\in\mathcal{A}(a)} \sqrt{C_e}^{-}. \tag{4.19}$$

Proof. One can directly observe the structure of the post-measurement states taking into account the identities in Eq. (4.17). □

For the examples of Pauli-Z and Pauli-Y measurements see Fig. 4.4. Note that unlike for graph states, for hypergraph states post-measurement states for a given measurement basis are not in general LU equivalent, therefore, they possess different entanglement properties.

Next we discuss the rule for Pauli-X measurements on hypergraph states. This is the trickiest of all three bases rules, since Pauli-X measurements lead, in general, out of the hypergraph state space. To give an example let us consider the three qubit hypergraph state $|H_3\rangle$ as in Fig. 2.7 (a). Then measuring any of its vertex in Pauli-X bases with an outcome $\langle +|$ gives the post-measurement state proportional to:

$$|00\rangle + |01\rangle + |10\rangle \quad - \text{ not LU equivalent to a hypergraph state.} \tag{4.20}$$

Thus, in the rest of the section we give a sufficient criterion for Pauli-X measurements on a hypergraph state to project on a post-measurement state, which is LU equivalent to some other hypergraph state. Curiously, this criteria entirely captures the rule for graph states.

Let us again consider a hypergraph state expanded over its vertex a as in Eq. (4.13). If the vertex a is measured in Pauli-X basis, then the post-measurement state is proportional to the equally weighted superposition of two hypergraph states, $\propto (|H_0\rangle \pm |H_1\rangle)$ and is not always local unitary equivalent to a hypergraph state. To check if for a given hypergraph state measuring a vertex a or a set of vertices V_a in Pauli-X basis gives a state local unitary equivalent to a hypergraph state, one can expand an original hypergraph state over a vertex a or a set of vertices V_a and check if all the possible equally weighted superpositions of expanded hypergraph states give some other hypergraph state or a state which is local unitary equivalent to a hypergraph state. Here we give a sufficient criterion for the equally weighted superpositions of two hypergraph states being a hypergraph state up to local unitary operations and derive the graphical rule for such cases:

Theorem 4.7. *Let $H_\alpha = (V, E)$ and $H_\beta = (V, E \cup \{a\} \cup \tilde{E})$, where $\tilde{E}$ are hyperedges not containing a vertex $a \in V$. Then the equally weighted superpositions of two hypergraph states $|H_\alpha\rangle$ and $|H_\beta\rangle$ up to the Hadamard gate acting on the vertex a, H_a are still hypergraph states denoted by $|H_+\rangle$ and $|H_-\rangle$:*

$$H_a|H_+\rangle \equiv H_a(|H_\alpha\rangle + |H_\beta\rangle) \propto \prod_{e' \in E'} C_{e'} \prod_{e_a \in \mathcal{A}^\alpha(a)} \prod_{\tilde{e} \in \tilde{E}} C_{e_a \cup \tilde{e}} C_{\tilde{e} \cup a} |+\rangle^{\otimes N}, \tag{4.21}$$

$$H_a|H_-\rangle \equiv H_a(|H_\alpha\rangle - |H_\beta\rangle) \propto C_a \prod_{e' \in E'} C_{e'} \prod_{e_a \in \mathcal{A}^\alpha(a)} C_{e_a} \prod_{\tilde{e} \in \tilde{E}} C_{e_a \cup \tilde{e}} C_{\tilde{e} \cup a} |+\rangle^{\otimes N}. \tag{4.22}$$

Here $\mathcal{A}^\alpha(a)$ is the adjacency of the vertex a in hypergraph H_α and $E' = \{e' | a \notin e',\ e' \in E\}$ and $C_a = Z_a$.

Proof. Let us assume that $a = 1$. Then we get:

$$H_1|H_+\rangle = H_1(|H_\alpha\rangle + |H_\beta\rangle) \tag{4.23}$$

$$= H_1(|H_\alpha\rangle + Z_1 \prod_{\tilde{e} \in \tilde{E}} C_{\tilde{e}} |H_\alpha\rangle) \tag{4.24}$$

$$= H_1(\prod_{e \in E} C_e \left(|+\rangle^{\otimes N} + Z_1 \prod_{\tilde{e} \in \tilde{E}} C_{\tilde{e}} |+\rangle^{\otimes N} \right) \tag{4.25}$$

$$= H_1 \prod_{e \in E} C_e H_1 H_1 \left(\left[|+\rangle + |-\rangle \prod_{\tilde{e} \in \tilde{E}} C_{\tilde{e}} \right] |+\rangle^{\otimes N-1} \right) \tag{4.26}$$

$$= H_1 \prod_{e' \in E'} C_{e'} \prod_{e'' \in E''} C_{e''} H_1 H_1 \left(\left[|+\rangle + |-\rangle \prod_{\tilde{e} \in \tilde{E}} C_{\tilde{e}} \right] |+\rangle^{\otimes N-1} \right) \tag{4.27}$$

$$= \prod_{e' \in E'} C_{e'} H_1 \prod_{e'' \in E''} C_{e''} H_1 H_1 \left(\left[|+\rangle + |-\rangle \prod_{\tilde{e} \in \tilde{E}} C_{\tilde{e}} \right] |+\rangle^{\otimes N-1} \right) \tag{4.28}$$

$$= \prod_{e' \in E'} C_{e'} \prod_{e_1 \in \mathcal{A}^\alpha(1)} CNOT_{e_1,1} \left(\left[|0\rangle + |1\rangle \prod_{\tilde{e} \in \tilde{E}} C_{\tilde{e}} \right] |+\rangle^{\otimes N-1} \right) \tag{4.29}$$

$$\propto \prod_{e' \in E'} C_{e'} \prod_{e_1 \in \mathcal{A}^\alpha(1)} CNOT_{e_1,1} \prod_{\tilde{e} \in \tilde{E}} C_{\tilde{e} \cup 1} |+\rangle^{\otimes N} \tag{4.30}$$

$$= \prod_{e' \in E'} C_{e'} \prod_{e_1 \in \mathcal{A}^\alpha(1)} \prod_{\tilde{e} \in \tilde{E}} C_{e_1 \cup \tilde{e}} C_{\tilde{e} \cup 1} |+\rangle^{\otimes N} \tag{4.31}$$

In Eq. (4.26) we decompose a set of hyperedges E into two parts: E', hyperedges which do not contain the vertex 1 and E'' hyperedges which contain the vertex 1. In Eq. (4.27) the set of hyperedges $\prod_{e' \in E'} C_{e'}$ commute with H_1 and going to Eq. (4.28), $H_1 \prod_{e'' \in E''} C_{e''} H_1 = \prod_{e_1 \in \mathcal{A}^\alpha(1)} CNOT_{e_1,1}$, since Hadamard gate H_1 changes Z_1 to X_1 and, therefore, generalized Controlled-Z gates become generalized $CNOT$ gates.

In Eq. (4.28), H_1 is applied to $|\pm\rangle$ and in Eq. (4.29) a new hypergraph state is obtained, which is written in an expanded form over vertex 1. If we write this hypergraph state we get Eq. (4.30):

$$\left(\left[|0\rangle + |1\rangle \prod_{\tilde{e} \in \tilde{E}} C_{\tilde{e}} \right] |+\rangle^{\otimes N-1} \right) \propto \prod_{\tilde{e} \in \tilde{E}} C_{\tilde{e} \cup 1} |+\rangle^{\otimes N}. \tag{4.32}$$

Then generalized $CNOT$ gates are applied to a new hypergraph state in Eq. (4.30). The action of generalized $CNOT$ gate was already described in the previous section.

In Eq. (4.30) the generalized $CNOT$ gate is applied to the hypergraph state which corresponds to the hypergraph $(V, \{\tilde{e} \cup \{1\} | \tilde{e} \in \tilde{E}\})$. The target qubit in the generalized $CNOT$ gate is the vertex 1 and its adjacency is, therefore, given by edge-set $\tilde{E}$. The control qubits are presented by the edge-set $\mathcal{A}^\alpha(1)$, which correspond to the adjacency of the vertex 1 in the hypergraph H_α. The action of generalized $CNOT$ gate takes the pairwise union of hyperedges in $\mathcal{A}^\alpha(1)$ and $\tilde{E}$ and adds or deletes new hyperedges:

$$\prod_{e_1 \in \mathcal{A}^\alpha(1)} \prod_{\tilde{e} \in \tilde{E}} C_{e_1 \cup \tilde{e}}. \tag{4.33}$$

Inserting these hyperedges in Eq. (4.31), we get the final hypergraph states:

$$H_1(|H_+\rangle) \propto \prod_{e' \in E'} C_{e'} \prod_{e_1 \in \mathcal{A}^\alpha(1)} \prod_{\tilde{e} \in \tilde{E}} C_{e_1 \cup \tilde{e}} C_{\tilde{e} \cup 1} |+\rangle^{\otimes N}. \tag{4.34}$$

In case of the minus superposition $H_1|H_-\rangle$, the derivations are very similar to $H_1|H_+\rangle$ up to Eq. (4.29): In particular, due to the minus sign in the superposition, we get a different hypergraph state from the one in Eq. (4.32):

$$H_1(|+\rangle - |-\rangle \prod_{\tilde{e}\in\tilde{E}} C_{\tilde{e}})|+\rangle^{\otimes N-1} = (|0\rangle - |1\rangle \prod_{\tilde{e}\in\tilde{E}} C_{\tilde{e}})|+\rangle^{\otimes N-1} = C_1 \prod_{\tilde{e}\in\tilde{E}} C_{\tilde{e}\cup 1}|+\rangle^{\otimes N} \tag{4.35}$$

Now we apply generalized *CNOT* gate to the hypergraph state in Eq. (4.35) :

$$\prod_{e_1\in\mathcal{A}^{\alpha}(1)} CNOT_{e_1,1} C_1 \prod_{\tilde{e}\in\tilde{E}} C_{\tilde{e}\cup 1}|+\rangle^{\otimes N}. \tag{4.36}$$

The hypergraph state in Eq. (4.35) has the additional edge C_1 and this means that the adjacency of the vertex 1 in Eq. (4.36) is given by the edge-set $\{\tilde{E}\cup\{\emptyset\}\}$. The action of generalized *CNOT* gate takes the pairwise union of hyperedges in $\mathcal{A}^{\alpha}(1)$ and $\{\tilde{E}\cup\{\emptyset\}\}$ and introduces new hyperedges of the form in the hypergraph:

$$\prod_{e_1\in\mathcal{A}^{\alpha}(1)} C_{e_1} \prod_{\tilde{e}\in\tilde{E}} C_{e_1\cup\tilde{e}} \tag{4.37}$$

Inserting these hyperedges in the original derivations, gives us the final hypergraph state:

$$H_1|H_-\rangle \propto C_1 \prod_{e'\in E'} C_{e'} \prod_{e_1\in\mathcal{A}^{\alpha}(1)} C_{e_1} \prod_{\tilde{e}\in\tilde{E}} C_{e_1\cup\tilde{e}} C_{\tilde{e}\cup 1}|+\rangle^{\otimes N}. \tag{4.38}$$

This finishes the derivations. □

It appears that there is a graphical way to derive the post-measurement states and it is very similar to the Pauli-X measurement rule for graph states in Eq. (2.62). Let the original hypergraph state be written as

$$|H_B\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle_B|H_{\alpha}\rangle + |1\rangle_B|H_{\beta}\rangle\Big), \tag{4.39}$$

where $|H_{\alpha}\rangle$ and $|H_{\beta}\rangle$ satisfy the sufficient conditions of Theorem 4.7. Then we can formulate a nice graphical rule for the post-measurement states obtained as a result of measuring B in Pauli-X basis.

Theorem 4.8. *Given a hypergraph state $|H_B\rangle$ corresponding to a hypergraph $H_B = (V_B, E_B)$ as in Eq.(4.39), then the post-measurement states of Pauli-X basis measurement on the vertex B is derived by three actions of generalized local complementations as follows:*

$$U_{x,\pm}|\tilde{\tau}_a(\tilde{\tau}_B\circ\tilde{\tau}_a(|H_B\rangle)) - \{B\}\rangle, \tag{4.40}$$

where a and B are contained in the same graph edge, $\{a, B\}\in E_B$ and

$$U_{x,+} = \mathbb{1} \qquad \textit{and} \qquad U_{x,-} = C_a \prod_{e_i\in\mathcal{A}^{H_{\alpha}}(a)} C_{e_i}. \tag{4.41}$$

Here $\mathcal{A}^{H_{\alpha}}(a)$ means that the adjacency of qubit a must be taken from the hypergraph H_{α}.

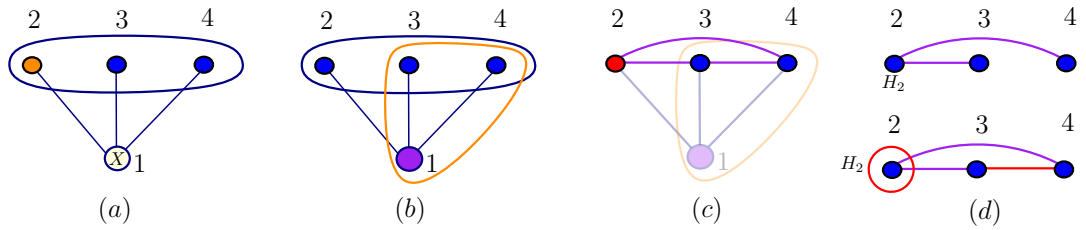


FIGURE 4.5: Post-measurement rule for Pauli-X basis measurement on a hypergraph state. (a) The vertex 1 is to be measured. So, we chose one of its neighbours e.g., $2 \in \mathcal{N}(1)$ and we apply the generalized local complementation over 2. (b) The result of LC on vertex 2. Now we apply LC over the vertex 1. (c) as a result we obtain (c), but we need to remove the vertex 1 with all of its hyperedges. These hyperedges are blurred in the Figure. Finally, LC over the vertex 2 is in order. (d) Post-measurement states corresponding to different outcomes.

Proof. From Theorem 4.7 we know that the hypergraphs have the following structure: $H_\alpha = (V, E)$ and $H_\beta = (V, E \cup \{a\} \cup \tilde{E})$, where $\tilde{E}$ are hyperedges not containing a vertex $a \in V$. Therefore, the hypergraph H_B indeed contains an edge $\{a, B\}$ and there is no other hyperedge in H_B containing both a and B together.

Let us then consider the action of the first generalized local complementation $\tilde{\tau}(a)$. Note again that a is only contained in the hyperedges $E \cup \{a, B\}$:

$$\begin{aligned}\tilde{\tau}(a)|H_B\rangle =& \tilde{\tau}(a) C_{aB} \prod_{\tilde{e}_i \in \tilde{E}} C_{\tilde{e}_i \cup B} |+\rangle_B |H_\alpha\rangle \\ =& C_{aB} \prod_{e_i \in \mathcal{A}^{H_\alpha}(a)} C_{e_i \cup B} \prod_{e_j \in \mathcal{A}^{H_\alpha}(a), i<j} C_{e_i \cup e_j} \prod_{\tilde{e}_i \in \tilde{E}} C_{\tilde{e}_i \cup B} |+\rangle_B |H_\alpha\rangle.\end{aligned} \tag{4.42}$$

Now we consider the second action, when $\tilde{\tau}(B)$ is applied to the new hypergraph. Note that the vertex B is now contained in three types of hyperedges: the every hyperedge in $\mathcal{A}^{H_\alpha} \cup$ in every hyperedge in $\tilde{E} \cup$ finally in $\{a, B\}$. We have to take a pairwise union between the types of the hyperedges and also the pairwise union within each type too:

$$\tilde{\tau}(B) \circ \tilde{\tau}(a)|H_B\rangle = C_{aB} \prod_{e_i \in \mathcal{A}^{H_\alpha}(a)} C_{e_i \cup B} \prod_{\tilde{e}_i \in \tilde{E}} C_{\tilde{e}_i \cup B} C_{\tilde{e}_i \cup a} C_{\tilde{e}_i \cup e_i} \prod_{\tilde{e}_j \in \tilde{E}, i<j} C_{\tilde{e}_i \cup \tilde{e}_j} \prod_{e' \in E'} C_{e'} |+\rangle^{\otimes |V_B|}, \tag{4.43}$$

where E' are hyperedges in H_α, which do not contain the vertex a. Next step is to remove the vertex B and all the hyperedges it is adjacent to:

$$|\tau_B \circ \tau_a(|H_B\rangle)) - \{B\}\rangle = \prod_{e_i \in \mathcal{A}^{H_\alpha}(a)} \prod_{\tilde{e}_i \in \tilde{E}} C_{\tilde{e}_i \cup a} C_{\tilde{e}_i \cup e_i} \prod_{\tilde{e}_j \in \tilde{E}, i<j} C_{\tilde{e}_i \cup \tilde{e}_j} \prod_{e' \in E'} C_{e'} |+\rangle^{\otimes |V_B|-1}. \tag{4.44}$$

#	Outcome	Post-measurement state
1.	$\langle + + +\vert_{123}$	$\propto (\vert H_\alpha\rangle + \vert H_\beta\rangle)$
2.	$\langle + + -\vert_{123}$	$\propto (\vert H_\alpha\rangle - \vert H_\beta\rangle)$
3.	$\langle + - -\vert_{123}$	0
4.	$\langle - - -\vert_{123}$	$\propto -(\vert H_\alpha\rangle - \vert H_\beta\rangle)$

TABLE 4.1: All possible post-measurement states for Pauli-X measurements on qubits $1, 2, 3$ in Eq. (4.47). Case 2 and 4 are equivalent up to a global sign.

And finally, the generalized local complementation over the vertex a gives:

$$|\tau_a(\tau_B \circ \tau_a(|H_B\rangle)) - \{B\}\rangle = \prod_{e' \in E'} C_{e'} \prod_{\tilde{e}_i \in \tilde{E}} C_{\tilde{e}_i \cup a} \prod_{e_i \in \mathcal{A}^{H_\alpha}(a)} C_{\tilde{e}_i \cup e_i} |+\rangle^{\otimes |V_B|-1}. \tag{4.45}$$

This expression exactly corresponds to the one in Eq. (4.21), the post-measurement state for the positive superposition. For the negative outcome we just fix the correction term $U_{x,-}$:

$$U_{x,-}|\tau_a(\tau_B \circ \tau_a(|H_B\rangle)) - \{B\}\rangle = C_a \prod_{e' \in E'} C_{e'} \prod_{\tilde{e}_i \in \tilde{E}} C_{\tilde{e}_i \cup a} \prod_{e_i \in \mathcal{A}^{H_\alpha}(a)} C_{\tilde{e}_i \cup e_i} C_{e_i} |+\rangle^{\otimes |V_B|-1}, \tag{4.46}$$

which exactly corresponds to the post-measurement state for negative superposition in Eq. (4.22). □

To see an example of the rule of Pauli-X basis measurement on a hypergraph state using local complementation rule, see Fig. 4.5.

The results above and the general hypergraphs considered in Eq. 4.39 guaranteed that the original hypergraph had at least one graph edge. Here we ask an inquisitive question, whether it is possible to start from a hypergraph state with hyperedges of the minimal cardinality three and still project on a hypergraph state after making Pauli-X basis measurements.

To resolve this question, let us consider particular cases of hypergraph states $|H\rangle$, which when expanded over three vertices $1, 2, 3$, give eight new hypergraphs satisfying the following constraints $H_{000} = H_{001} = H_{010} = H_{100} \equiv H_\alpha$ and $H_{111} = H_{110} = H_{101} = H_{011} \equiv H_\beta$. Then the expanded state can be written as follows:

$$\begin{aligned} |H\rangle = \frac{1}{\sqrt{8}} \Big(& (|000\rangle + |001\rangle + |010\rangle + |100\rangle)_{123} \otimes |H_\alpha\rangle \\ & + (|111\rangle + |110\rangle + |101\rangle + |011\rangle)_{123} \otimes |H_\beta\rangle \Big). \end{aligned} \tag{4.47}$$

If qubits $1, 2, 3$ are all measured in Pauli-X basis, due to the symmetry of the first three qubits, there are only four possible post measurement states presented in Table 4.1. We see from Table 4.1 that outcome $\langle + - -|$ never occurs and outcomes $\langle + + -|$ and $\langle - - -|$ are equivalent to each other up to the global sign. Therefore, if we measure the first three qubits of the hypergraph state $|H\rangle$ as presented in Eq. (4.47), there are only two possible post-measurement states and they correspond to the equally weighted superposition of two hypergraph states

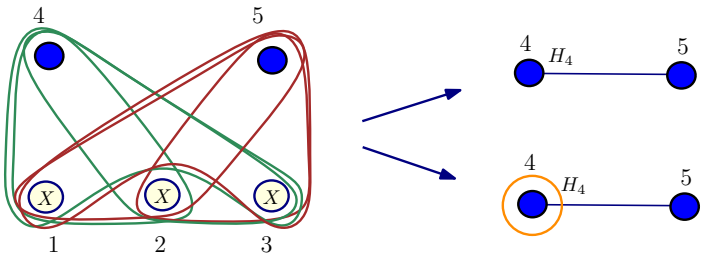


FIGURE 4.6: The five-qubit three-uniform hypergraph state is the smallest hypergraph state with no usual graph edges which can project on a Bell state deterministically. It has hyperedges $E = \{\{1,2,4\},\{1,2,5\},\{1,3,4\},\{1,3,5\},\{2,3,4\},\{2,3,5\}\}$. The qubits $1,2,3$ are measured in X-basis and the post-measurement state is a graph state with a Hadamard correction on the vertex 4. The graph state is obtained with unit probability but up to Pauli-Z_4 random unitary. The probabilistic Pauli-Z_4 appears with the probability $4/5$ when the product of Pauli-X measurement outcomes is -1.

$(|H_\alpha\rangle \pm |H_\beta\rangle)$. Below we consider three examples, where we measure these three qubits but we vary the hypergraphs H_α and H_β and check if new emerging hypergraphs H_α and H_β satisfy the condition of Theorem 4.7.

For now we restrict ourselves to three-uniform hypergraph states and focus on cases when post-measurement states are graph states regardless of the measurement outcomes, in general, this is not the case.

Example 4.1. *The smallest three-uniform hypergraph state which after measuring the first three qubits in Pauli-X basis can deterministically project on a Bell state is (see Fig. 4.6) :*

$$\begin{aligned}|H_5\rangle =& C_{124}C_{125}C_{134}C_{135}C_{234}C_{235}|+\rangle^{\otimes 5}\\ =& \frac{1}{2\sqrt{2}}\Big((|000\rangle+|001\rangle+|010\rangle+|100\rangle)|+\rangle^{\otimes 2}\\ &+(|011\rangle+|110\rangle+|101\rangle+|111\rangle)|-\rangle^{\otimes 2}\Big).\end{aligned} \tag{4.48}$$

The state $|H_5\rangle$ is given in the expanded form over vertices $1,2,3$ as in Eq. (4.47) and $|H_\alpha\rangle = |+\rangle^{\otimes 2}$ and $|H_\beta\rangle = |-\rangle^{\otimes 2} = Z^{\otimes 2}|+\rangle^{\otimes 2}$.

We fix a to be vertex 4, H_α to have hyperedges $E_\alpha = \{\}$ and H_β to have hyperedges $E_\beta = \{\{4\}\cup\tilde{E}\}$, where $\tilde{E} = \{\{5\}\}$. These two hypergraphs satisfy condition of Theorem 4.7. So, measuring qubits $1,2,3$ in Pauli-X basis gives two possible post-measurement hypergraph states $H_4|H_+\rangle \propto |+\rangle^{\otimes 2} + |-\rangle^{\otimes 2}$ with the probability $1/5$ and $H_4|H_-\rangle \propto |+\rangle^{\otimes 2} + |-\rangle^{\otimes 2}$ with the probability $4/5$. Using Theorem 4.7 we derive these post-measurement states:

$$H_4|H_+\rangle \propto H_4\Big(|+\rangle^{\otimes 2} + |-\rangle^{\otimes 2}\Big) \propto C_{45}|+\rangle^{\otimes 2}, \tag{4.49}$$

$$H_4|H_-\rangle \propto H_4\Big(|+\rangle^{\otimes 2} - |-\rangle^{\otimes 2}\Big) \propto C_{45}C_4|+\rangle^{\otimes 2}. \tag{4.50}$$

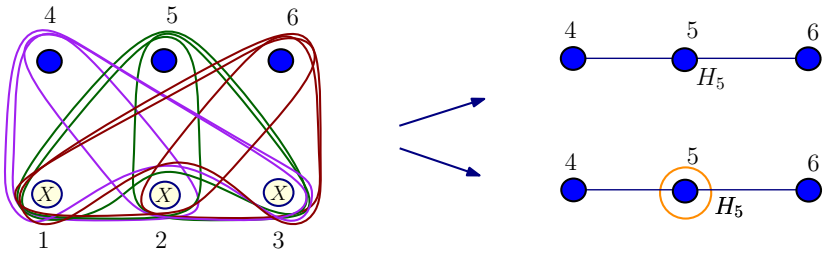


FIGURE 4.7: Pauli-X measurements on the three-uniform hypergraph state. Vertices $1, 2$, and 3 are measured in Pauli-X basis and the post-measurement state is a graph state on $4, 5$, and 6 up to a Hadamard gate. A Random Z_5 appears, if the product of Pauli measurement outcomes is -1. Post-measurement states are LU equivalent.

Example 4.2. *Let us consider the six-qubit hypergraph state $|H_6\rangle$ presented in Fig. 4.7. After measuring qubits $1, 2, 3$ in X-basis we project on the three-qubit graph state. To see this, we write $|H_6\rangle$ directly in the expanded form over vertices $1, 2, 3$:*

$$|H_6\rangle \propto (|000\rangle + |001\rangle + |010\rangle + |100\rangle)\otimes \quad 4\bullet \quad 5\bullet \quad 6\bullet$$
$$+(|110\rangle + |101\rangle + |011\rangle + |111\rangle)\otimes \quad 4\bullet \quad 5\bullet \quad 6\bullet \ . \tag{4.51}$$

Here H_α has hyperedges $E_\alpha = \{\}$ and H_β has hyperedges $E_\beta = \{\{4\},\{5\},\{6\}\}$ and we fix to apply the Hadamard correction on the vertex $a = 5$. We can use Theorem 4.7 to derive two post-measurement states up to Hadamard gate applied to the vertex 5:

$$H_5|H_+\rangle \propto C_{45}C_{56}|+\rangle^{\otimes 3} \quad \textit{and} \quad H_5|H_-\rangle \propto C_{45}C_{56}C_5|+\rangle^{\otimes 3}. \tag{4.52}$$

Example 4.3. *Let us consider more complicated six-qubit hypergraph state $|H_6\rangle$ presented on Fig. 4.8. We write this state expanded over vertices $1, 2, 3$:*

$$|H_6\rangle \propto (|000\rangle + |001\rangle + |010\rangle + |100\rangle)\otimes \quad 4\bullet \quad 5\bullet \quad 6\bullet$$
$$+(|110\rangle + |101\rangle + |011\rangle + |111\rangle)\otimes \quad 4\bullet \quad 5\bullet \quad 6\bullet \ . \tag{4.53}$$

Here H_α has hyperedges $E_\alpha = \{\{1,2,3\}\}$ and H_β has hyperedges $E_\beta = \{\{1,2,3\},\{4\},\{5\},\{6\}\}$ and we fix to apply the Hadamard correction on the vertex $a = 5$. We can use Theorem 4.7 to derive two post-measurement states up to Hadamard gate applied to qubit 5:

$$H_5|H_+\rangle \propto C_{45}C_{56}|+\rangle^{\otimes 3} \quad \textit{and} \quad H_5|H_-\rangle \propto C_{45}C_{56}C_{46}C_5|+\rangle^{\otimes 3}. \tag{4.54}$$

As a closing remark on Pauli-X basis measurement, we can increase the number of vertices that we measure in Pauli-X and generalize the result to higher cardinality edges. Let us expand a hypergraph state over m-qubits, where $3 \leq m \leq N-2$ is an odd number, in the following way:

$$|H_N\rangle \propto \left(\sum_x |x\rangle\right) \otimes |H_\alpha\rangle + \left(\sum_y |y\rangle\right) \otimes |H_\beta\rangle, \tag{4.55}$$

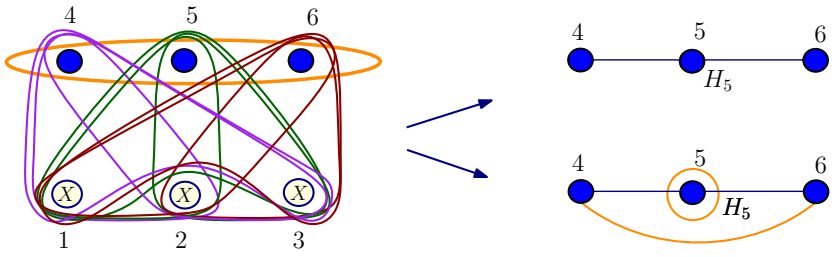


FIGURE 4.8: Pauli-X measurements on the three-uniform hypergraph state. Vertices $1, 2$, and 3 are measured in Pauli-X basis and the post-measurement state is a graph state on $4, 5$, and 6 up to a Hadamard gate. The random gates here include CZ and Z_5 gates and they appears, if the product of Pauli measurement outcomes is -1. Post-measurement states are LU equivalent.

where $x, y \in \{0,1\}^m$ and the first sum runs over all computational bases elements with the weight $w(x) \leq \lfloor m/2 \rfloor$ and the second sum runs over all computational bases elements with the weight $w(y) > \lfloor m/2 \rfloor$.

If all the first m vertices are measured in Pauli-X bases, then we again get two possible measurement outcomes $|H_\alpha\rangle \pm |H_\beta\rangle$. However, it is of our interest how original hypergraph state looks.

For simplicity let us fix $|H_\alpha\rangle = |+\rangle^{\otimes |N-m|}$ and $|H_\beta\rangle = |-\rangle^{\otimes |N-m|}$. Then smallest hyperedges that connect first m vertices to the rest of the hypergraph have a cardinality equal to $\lceil m/2 \rceil + 1$. But for some cases of m with this construction the first m vertices can be connected to the rest of the hypergraph with different sizes of hyperedges.

To illustrate this let us consider an example of $|H_7\rangle$, where $m = 5$ and $|H_\alpha\rangle = |+\rangle^{\otimes 2}$ and $|H_\alpha\rangle = |-\rangle^{\otimes 2}$. Then the smallest cardinality hyperedge in the hypergraph is of a size four - the smallest weight of vector $|y\rangle$ is equal to $\lceil 5/2 \rceil = 3$ and plus 1. However, these are not all the hyperedges in the hypergraph: The vectors with the weight four are in the second summand and they are tensored with $|-\rangle^{\otimes 2}$. However, if we choose any four vertices among m, then every three from them are connected to both vertices $m+1$ and $m+2$, but $\binom{4}{3} = 4$, which is an even number. So, the hypergraph must have additional cardinality 5 edges. Similarly we have to check the weight of the last term in the sum: $\binom{5}{3} + \binom{5}{4} = 15$ is an odd number and, therefore, there is no cardinality six edges in the hypergraph. Therefore, first five qubits are connected with the rest of the hypergraph with four- and five- qubit hyperedges in a symmetric manner.

4.5 Summary and outlook

In this chapter we reviewed several graphical rules on hypergraph states. These transformations make the formalism more attractive and useful, as we will see in the subsequent chapters. There are several directions one could proceed the analysis of graphical transformations. Already in Ref. [89], more general unitary equivalence rules were developed for graphs and hypergraphs, however, it remains unclear whether these unitaries and corresponding rules are also sufficient to decide for LU equivalences for hypergraph states. It is also interesting

to consider a more restrictive question, whether a k-uniform hypergraph state can be transformed to a $\tilde{k}$-uniform one with local unitary operations for $k \neq \tilde{k}$ [106]. It turns out that the transformation is possible with SLOCC operations even for symmetric states but no result is known for unitary operations:

Lemma 4.9. *The N-qubit complete graph state is SLOCC equivalent to the N-qubit hypergraph state with only the single N-cardinality hyperedge.*

Proof. The N-qubit complete graph state is LU equivalent to the GHZ-state. Then one can easily verify that the N-fold tensor product of the invertible operator A maps the GHZ state to $|H_N^N\rangle$ with a non-zero probability, where a and b in

$$A = a(|0\rangle + |1\rangle)\langle 0| + b|1\rangle\langle 1| \tag{4.56}$$

satisfy constraints:

$$a^N = \frac{1}{\sqrt{2}^{N-1}} \quad \text{and} \quad b^N = -2a^N. \tag{4.57}$$

□

This statement emphasizes that for general class of hypergraph states LU transformations constitute strict subset of SLOCC transformations, differently for just graph states case as discussed in Lemma 2.15 [31]. No further connection between graph-theoretic properties of hypergraphs and SLOCC equivalence has been investigated in the literature yet.

As for the measurement rules, they are crucial for deriving MBQC schemes, but apart from that they may find independent applications in deriving entanglement witnesses [32, 128], nonlocality proofs [30, 129, 130], and state verification protocols [110–112] for a large class of hypergraph states.

Chapter 5

Quantifying and detecting entanglement in hypergraph states

Quantum hypergraph states constitute an interesting subclass of pure states. Due to their usefulness it is important to investigate tools to quantify and detect entanglement present in these states. In the first part of this chapter we derive tight entanglement witnesses specifically for hypergraph states. In the process we use the graphical language developed in the previous chapter. The second half of this chapter is devoted to calculating geometric measure of entanglement for many classes of hypergraph states.

5.1 Introduction

The construction of entanglement witnesses for hypergraph states is one of the applications of the graphical rules derived in Chapter 4. We take the existing approach as for graphs states and derive witnesses mostly relying on the graphical reasoning, rather than algebraic derivations. We construct tight witnesses for complete three-uniform hypergraph states. These states are of special interest for MBQC protocols and Bell inequality violations. The Mermin-like inequalities that we considered in Chapter 3 can be used to prove that there is some entanglement in the state exhibiting certain quantum correlations. In this section, we take a different approach and focus on entanglement witnesses for genuine multiparticle entanglement.

Quantifying entanglement is an important task but has been one of the challenges even for pure quantum states. For some graph states different entanglement measures have been connected to certain graph-theoretic properties of a given graph [59]. Here we study geometric measure of entanglement for symmetric hypergraph states and for the states exhibiting certain stabilizer symmetries [131]. We find analytic results that the optimization very often can be simplified by considering real symmetric product states only.

5.2 Entanglement detection for hypergraph states

Recall from Chapter 2 that an entanglement witness is an observable, which for a general state $|\psi\rangle$ can be defined as

$$\mathcal{W} = \alpha \mathbb{1} - |\psi\rangle\langle\psi|, \tag{5.1}$$

where α is the maximal overlap between the state $|\psi\rangle$ and the pure biseparable states (See Eq. 2.19).

For usual graph states the witness can be determined in the following way [132]: First, for any bipartition one can count minimal number of *independent* edges shared between the two parties by considering only local operations with respect to this partition. Here by independence of edges we mean that none of the edges share the same vertex. To say it otherwise, we count how many Bell pairs are shared between this fixed bipartition. We say then that a graph state has been reduced to its *normal form* for a fixed bipartition. On the other hand, one shall keep in mind that during local operations, the maximal Schmidt coefficient can only increase. This proves directly that for any connected graph and for its any bipartition we can upper-bound the squared Schmidt coefficient by $\lambda_k^{\mathrm{BP}} \leq 1/2$, so

$$\mathcal{W} = \frac{1}{2}\mathbb{1} - |G\rangle\langle G| \tag{5.2}$$

is a witness. Using a similar construction, we can write down a witness for three-uniform hypergraph states.

Theorem 5.1. *For any three-uniform hypergraph state $|H_N\rangle$ the operator*

$$\mathcal{W} = \frac{3}{4}\mathbb{1} - |H_N\rangle\langle H_N| \tag{5.3}$$

is an entanglement witness detecting this state.

Proof. The proof is similar to the one for graph states, but in this case the aim is to share the three-qubit hypergraph state between the bipartition. For this state one can directly calculate that the maximal Schmidt coefficient is $\alpha = 3/4$. Given an N-qubit three-uniform state, we consider a bipartition $1, \ldots, p|p+1, \ldots, N$. One can get rid of any edge which entirely belongs to either side of the bipartition. Since the graph is assumed to be connected at least one three-edge remains shared between the two parts. Without loss of generality we can assume that this hyperedge is $e = \{p-1, p, p+1\}$. Now by making measurements in the Pauli-Z basis on every qubit except these three in e, we can disentangle all the qubits from the main hypergraph except $\{p-1, p, p+1\}$ regardless of the measurement outcomes. See Chapter 4 for the measurement rules. Therefore, for all possible measurement results, i.e. with probability one the resulting state is, up to local unitaries, a three-qubit hypergraph state consisting only of the edge e. □

The previous witness can be used for any connected three-uniform hypergraph state, but similarly to the graph state entanglement witness case, it is not necessarily tight. For the

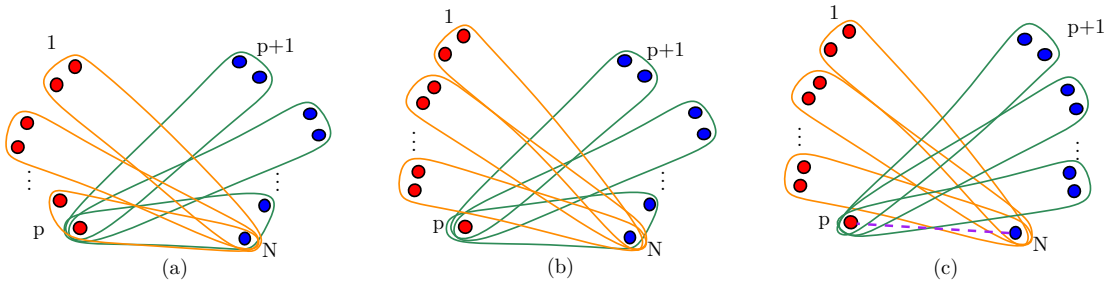


FIGURE 5.1: Different possibilities of the normal forms for the complete three-uniform hypergraph states. (a) The normal form, if p is even and N is even. (b) The normal form, if p is odd and N is odd. (c) The normal form, if p is odd and N is even. We have two cases: (c1) The hypergraph without the edge $\{p, N\}$. This is the normal form, if either both $(p+1) = 2 \mod 4$ and $(N-p+1) = 2 \mod 4$ or if both $(p+1) = 0 \mod 4$ and $(N-p+1) = 0 \mod 4$. (c2) The hypergraph with the edge $\{p, N\}$. This is the normal form, if $(p+1) = 0 \mod 4$ and $(N-p+1) = 2 \mod 4$ or if $(p+1) = 2 \mod 4$ and $(N-p+1) = 0 \mod 4$. The edge $\{p, N\}$ is represented by the dashed line.

special case of complete three-uniform states, where any possible three-edge is present, we derive the tight witnesses. For this we first calculate relevant Schmidt coefficients:

Lemma 5.2. *Consider an N-qubit complete three-uniform hypergraph state. Then, the maximal squared Schmidt coefficient with respect to the bipartition 1 vs. $(N-1)$ qubits, is*

$$\begin{aligned}
\lambda_1 &= \frac{1}{2}, \quad \text{if } N = 4k. \\
\lambda_1 &= \frac{1}{2} + \frac{1}{2^{(N+1)/2}}, \quad \text{if } N = 4k+1 \text{ or } N = 4k+3. \\
\lambda_1 &= \frac{1}{2} + \frac{1}{2^{N/2}}, \quad \text{if } N = 4k+2.
\end{aligned} \tag{5.4}$$

For the 2 vs. $(N-2)$ partition it is $\lambda_2 = \frac{1}{8}(3 + \frac{\sqrt{2^{N+6}+4^N}}{2^N})$.
And for the 3 vs. $(N-3)$ partition it is given by $\lambda_3 = \frac{9}{16}$ if $N = 6$ and for $N > 6$, one has $\lambda_3 < \frac{1}{2}$.

The proof is done by tracing out the parties and calculating the Schmidt coefficients as eigenvalues of the reduced states. Details can be found in Appendix B. Values of Schmidt coefficients calculated here are relevant for determining the tight value of α. But first in the spirit of counting number of Bell pairs shared between any bipartitions for graph states, we also define a normal form for hypergraph states.

Lemma 5.3. *Consider an N-qubit complete three-uniform hypergraph state and a fixed bipartition $1, \ldots, p|p+1, \ldots, N$. Then, using only local actions with respect to this bipartition the hypergraph can be reduced to the form shown in Fig. 5.1. We call this form the normal form of the complete three-uniform hypergraph state respecting the bipartition $1, \ldots, p|p+1, \ldots, N$.*

Proof. The proof consist of an application of a sequence of CNOT gates on both sides of the bipartition. We review the simplest case here to give the idea of how the normal form is obtained in a general case.

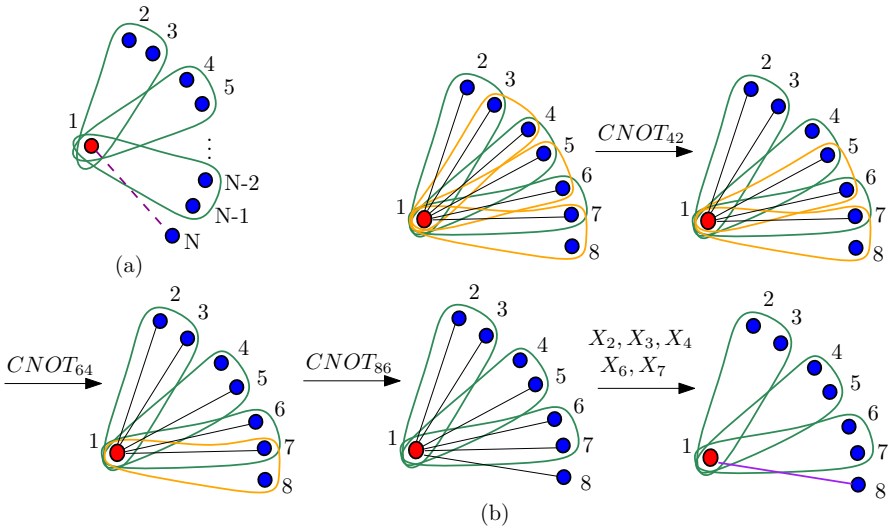


FIGURE 5.2: (a) The normal form hypergraph state for the bipartition $1|2,3,\ldots,N$. (b) An example for the step (c) for obtaining the normal form for the bipartition $1|2,3,\ldots,N$. See the text of the proof for further details.

First we would like to show that the following statement holds: Consider the bipartition $1|2,3,\ldots,N$ for an N-qubit complete three-uniform hypergraph state. Then this state is locally (for the given bipartition) equivalent to the three-uniform hypergraph state where every vertex is contained in only one hyperedge and hyperedges are of the form: $E = \{\{1,i,i+1\} \mid 2 \leq i < N \text{ and } i \text{ is even.}\}$ And only if $N = 4k$, an additional cardinality two edge appears, which is $\{1,N\}$.

Fig. 5.2 (a) represents the goal hypergraph state respecting a bipartition $1|2,3\ldots N$. The algorithm to achieve this state is as follows:

(a) Erase all the edges which only contain subsets of vertices $\{2,3,\ldots N\}$.

All the remaining edges are $\{\{1,i,j\}|i<j, 2\leq i,j\leq N\}$.

(b) Apply $CNOT_{i,i+1}$ for each i, $2 \leq i < N$.

To give an example, we start with the $CNOT_{23}$ gate. The adjacency of 3 is $\mathcal{A}(3) = \{1,i\}$, where $i \neq 3, 2 \leq i \leq N$. The hyperedges introduced by the $CNOT_{23}$ gate are $\{e_t \cup \{2\} | e_t \in \mathcal{A}(3)\}$ and therefore, this action removes all the hyperedges where 2 is contained except of the hyperedge $\{1,2,3\}$ and adds the cardinality two edge $\{1,2\}$.

At this step the remaining edges are $\{\{1,2\},\{1,2,3\},\{1,i,j\}|i<j, 3\leq i,j\leq N\}$.

Since $2 \notin \mathcal{A}(i+1)$ for $i \geq 3$, it is clear that consecutive $CNOT$ gates, presented in this step, do not modify hyperedges containing 2. To give another example, $CNOT_{34}$ erases all the hyperedges where 3 is presented except already established one $\{1,2,3\}$ and the gate where vertices 3 and 4 are presented together $\{1,3,4\}$. It also adds the cardinality two edge $\{1,3\}$. Repeating this procedure:

All the remaining edges are of the form $\{\{1,j,j+1\}|2 \leq j < N\}$ *and cardinality two edges* $\{\{1,i\}|2\leq i<N\}$.

(c) Apply $CNOT_{i+2,i}$, for each even i, $2 \leq i < (N-1)$.

The adjacency of $i = 2 \bmod 4$ right before applying the $CNOT_{i+2,i}$ gate is given by $\mathcal{A}(i) = \{\{1\}, \{1, i+1\}\}$. The $CNOT_{i+2,i}$ gate, therefore, erases/creates hyperedges of the types $\{\{1, i+2\}$ and $\{1, i+1, i+2\}\}$. This means that the adjacency of $i = 0 \bmod 4$ is only $\{1, i+1\}$ and application of $CNOT_{i+2,i}$ gate can only erase a hyperedge $\{1, i+1, i+2\}$. See Fig. 5.2 (b).

To give the final configuration as in Fig. 5.1, here we have to consider three different cases:

1. N is odd:

   All the remaining edges are of the form $\{1, i, i+1\}$, for even $2 \leq i \leq N$ and also $\{1, i\}$ for unless $i = 0 \bmod 4$. It is easy to see that all two edges can be removed by actions of Pauli-X.

2. $N = 2 \bmod 4$:

   The last hyperedge $\{1, N-1, N\}$ is erased and the edge $\{1, N\}$ cannot be created. Therefore, the last qubit is completely disentangled in this case. See Fig.5.2 (a).

3. $N = 0 \bmod 4$

   The last hyperedge $\{1, N-1, N\}$ is erased and the edge $\{1, N\}$ is created. See Fig.5.2 (b) for the exact procedure.

The normal form for other bipartitions are calculated in detail in Appendix B. □

For completeness, we sum up the case of the bipartition $1|2, 3, \ldots, N$. There are three possibilities for the normal form of the hypergraph and it only depends on the number of parties in the hypergraph. If N odd, then every vertex is exactly in one hyperedge. If $N = 4k$, then the final hypergraph corresponds to the one in Fig. 5.2 (a) including the dashed line. Note that this is in agreement with the fact that the maximal Schmidt coefficient for this case is $1/2$ (see Lemma 5.2), as there is a Bell pair shared across the bipartition [91]. In case $N = 4k+2$, the dashed line is missing, therefore, the last qubit can be removed and the result for the maximal Schmidt coefficient matches with the $N = 4k+1$ case from Lemma 5.2.

Theorem 5.4. *The tight witness for the N-qubit complete three-uniform hypergraph state $|H_N^3\rangle$ is given by*

$$\mathcal{W} = \alpha \mathbb{1} - |H_N^3\rangle\langle H_N^3|, \tag{5.5}$$

where $\alpha = \max\{\lambda_1, \lambda_2\}$.

Proof. We have to show that, in general, it is sufficient to consider the 1 vs. $(N-1)$ and 2 vs. $(N-2)$ partitions. As seen in Lemma 5.2 the 3 vs. $(N-3)$ partitions give only smaller Schmidt coefficients. For any other $1, \ldots, p|(p+1), \ldots, N$ bipartition with $p > 3$ we use the normal form in Fig. 5.1. If a resulting hypergraph is reduced either to Fig. 5.1 (b) or (c) [without the dashed edge], then on qubits $1 \ldots (p-3)$ the measurements in the Pauli-Z basis can be made. As a result, the hypergraph state on vertices $(p-2), (p-1), p|(p+1) \ldots N$ is obtained.

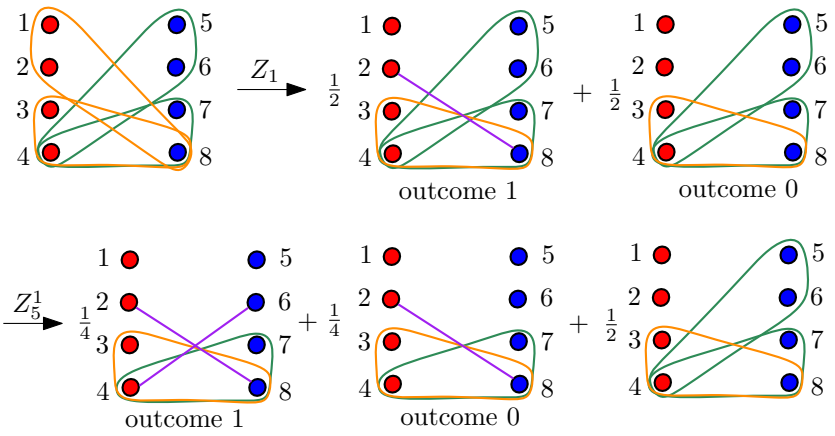


FIGURE 5.3: Estimation of the Schmidt coefficient for a 4 vs. 4 bipartition. See the text for further details.

We know from the Lemma 5.2 that the 3 vs. $(N-3)$ partition has the largest squared Schmidt coefficient less than $1/2$ (unless $N = 6$). Keeping in mind that measurements can never decrease the squared maximal Schmidt coefficient, we reach the conclusion that the bipartition $1,\ldots,p|(p+1),\ldots,N$ cannot contribute to the maximal Schmidt coefficient when $p \geq 3$. If in the normal form in Fig. 5.1 (c) the dashed edge is present, one can make measurements on both sides of the partition to reduce the state to a Bell state between qubits p and N. This clearly gives a squared Schmidt coefficient $\lambda \leq 1/2$.

The final case is the state with a normal form in Fig. 5.1 (a). Here the strategy is as follows: Pauli-Z measurements are made on every qubit but eight of them, namely the qubits $(p-3),(p-2),\ldots,(p+3),(p+4)$ remain untouched. This leaves us with the state given in Fig. 5.3, where the qubits have been relabeled. Then, a Pauli-Z measurement is made on qubit 1. With probability $1/2$ (in case of outcome 1), the edge $\{2,8\}$ is introduced and qubit 1 is disentangled. With probability $1/2$ (outcome 0) both qubits 1 and 2 are disentangled. For the first case (1 outcome), we again make a Pauli-Z measurement on qubit 5, denoted by Z_5^1. This itself gives two possible outcomes with half-half probabilities, the outcome 1 gives the edge $\{4,6\}$ and disentangles qubit 5 and the outcome 0 disentangles qubits 4 and 5. Putting all measurement outcomes together with corresponding probabilities yields as a bound on the Schmidt coefficient

$$\lambda \leq \frac{1}{4}\cdot\frac{1}{4}+\frac{1}{4}\cdot\frac{1}{2}\cdot\frac{1}{8}(3+\sqrt{5})+\frac{1}{2}\cdot\frac{1}{8}(3+\sqrt{2}) \approx 0.420202 < \frac{1}{2}. \tag{5.6}$$

Note that in this estimation it was used that one minus the largest squared Schmidt coefficient can be viewed as the geometric measure of entanglement for this partition, and this measure decreases under local operations even for mixed states. □

5.3 Geometric Measure of hypergraph states

Recall from Chapter 2 Theorem 2.5 that in order to calculate geometric measure of entanglement for permutation symmetric states with $N \geq 3$ particles, one shall optimize its overlap with an N-fold tensor product of a single particle state $|a\rangle = \cos\theta|0\rangle + e^{i\vartheta}\sin\theta|1\rangle$. Therefore, optimization is performed over two parameters only. In this section we calculate such overlaps for several classes of hypergraph states. We show that it is, in addition, sufficient to set the complex parameter to zero, thus, to optimize over only a single parameter θ.

Example 5.1. *As a starting point, let us consider an example of the four-qubit thee-uniform complete hypergraph state $|H_4^3\rangle$, which in the computational basis is given by a state:*

$$|H_4^3\rangle = \frac{1}{4}\sum_{x=0}^{4}(-1)^{\binom{x}{3}}\big(|\underbrace{0\ldots0}_{4-x}\underbrace{1\ldots1}_{x}\rangle + \textit{ permut.}\big). \tag{5.7}$$

Then one can easily check that for $t = 1/2\arctan[1/2(-1+\sqrt{5})]$, application of the real unitary

$$U_4 = \begin{pmatrix} \cos(t) & \sin(t) \\ -\sin(t) & \cos(t) \end{pmatrix} \tag{5.8}$$

brings the state $|H_4^3\rangle$ in the following form:

$$|S_{H_4}\rangle = U_4^{\otimes 4}|H_4^3\rangle = \frac{1}{8}(3-\sqrt{5})\big(|0000\rangle + |1111\rangle\big) + \frac{1}{8}(1+\sqrt{5})(|0011\rangle + \textit{permut.}). \tag{5.9}$$

Here all the coefficients in the state vector are positive and thus, maximization of the overlap can be done over $|a\rangle \in \mathbb{R}$:

$$\begin{aligned}\max_{|a\rangle}\langle a^{\otimes N}|S_{H_4}\rangle =& \max_{\theta}\left(\sin^4(\theta)+\cos^4(\theta)\right) + \frac{6}{8}\left(1+\sqrt{5}\right)\left(\sin^2(\theta)\cos^2(\theta)\right)\\ =& \frac{1}{8}\left(3+\sqrt{5}\right).\end{aligned} \tag{5.10}$$

The last equality follows from taking a derivative of the overlap and finding zero points. Since LU transformations cannot change the value of entanglement measures, it follows that $E_g(|H_4^3\rangle) = \frac{25-3\sqrt{5}}{32} \approx 0.571619$. This value was previously derived in Ref. [113], but only numerically.

Next we consider geometric measure of entanglement for states with a single hyperedge containing all its vertices.

Lemma 5.5. *Geometric measure of entanglement of N-qubit hypergraph state with only the single hyperedge of a cardinality N can be obtained via optimizing over real symmetric states.*

Proof. The statement can be directly checked by applying a Hadamard gate to one of the qubits in the hypergraphs. The resulting state has only non-negative coefficients:

$$H_1|H_N^N\rangle = \frac{1}{\sqrt{2}}H_1(|0\rangle|+\rangle^{\otimes N-1} + |1\rangle|H_{N-1}^{N-1}\rangle) = \frac{1}{\sqrt{2}}(|+\rangle^{\otimes N} + |-\rangle|H_{N-1}^{N-1}\rangle) \in \mathbb{R}^+. \tag{5.11}$$

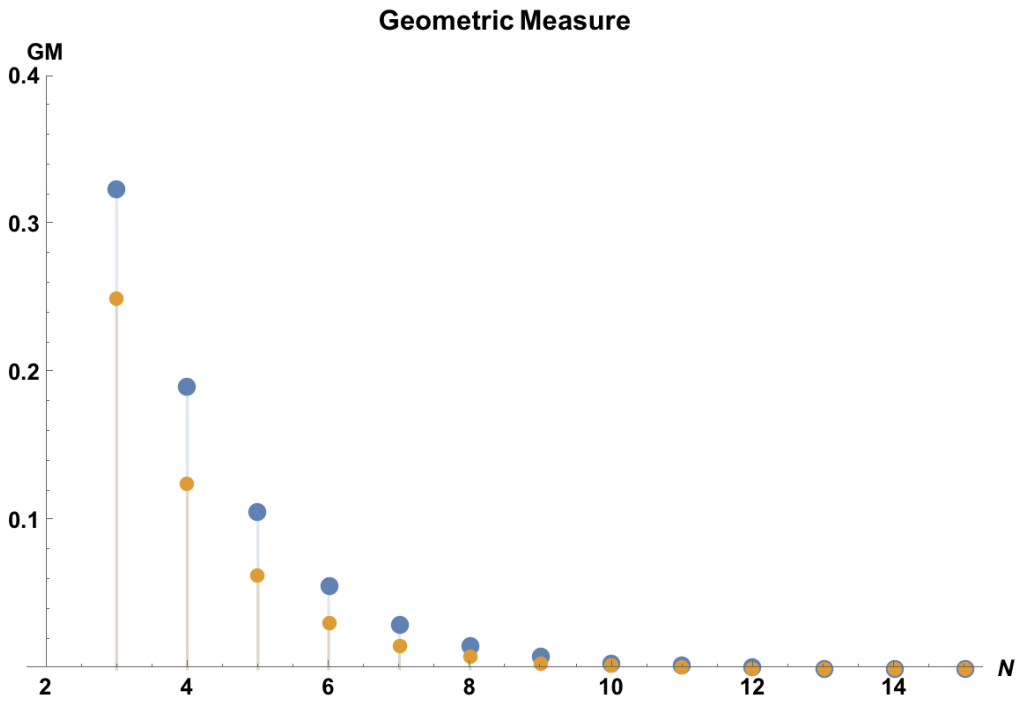


FIGURE 5.4: Geometric measure of $|H_N^N\rangle$. Blue dots represent the result of optimization in over the single real parameter and yellow ones are lower bounds on geometric measure from Ref. [133] obtained by considering bi-partitions. The x-axis shows the number of particles. The lower-bound improves as states get less entangled.

Since Hadamard is also a real unitary operation, the optimal product state can also be chosen to have real coefficients. □

In Ref. [133] lower bounds for geometric measure of entanglement of symmetric hypergraph states were derived by considering entanglement witnesses. i.e., maximal squared Schmidt coefficients. Here we compare the lower bounds for $|H_N^N\rangle$ with our numerical optimization results. For small number of vertices there is a significant difference between the results, however, as the cardinality of hyperedge increases, naturally the state becomes more and more closer to the product state and lower bounds start to become tight. See Fig. 5.4. Note that the optimization is done numerically over a single parameter.

We can generalize Lemma 5.5 to nonsymmetric hypergraph states too:

Lemma 5.6. *Given a hypergraph state $|H_E\rangle$ where every arbitrary edge $e \in E$ contains a vertex $a \in V$. The optimal overlap can always be obtained by real product states.*

Proof. The proof concerns more general case of the result obtained in Lemma 5.5. Without a loss of generality assume that $a = 1$. Then it is always possible to rewrite the hypergraph as follows:

$$|H_1\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle|+\rangle^{\otimes N-1} + |1\rangle|H_{E\setminus\{1\}}\rangle\Big). \tag{5.12}$$

Application of a Hadamard gate on the first qubit maps a hypergraph state to all positive coefficient state. Hence, the overlap is maximized by product states with real coefficients. □

To present other results we need to first introduce a mathematical theorem for hypergraph states, which studies local Pauli stabilizer structures for **k**-uniform hypergraph states. Here $\mathbf{k} = k_1 \dots k_m$ is a vector.

Lemma 5.7. *[131] A symmetric N-qubit **k**-uniform complete hypergraph state is*

(1) a plus one eigenstate of $X^{\otimes N}$ iff

$$\sum_{i=1}^{m} \binom{\omega}{k_i} = \sum_{i=1}^{m} \binom{N-\omega}{k_i}, \quad (mod\ 2) \quad for\ \ 0 \leq \omega \leq N. \tag{5.13}$$

(2) a plus one eigenstate of $-X^{\otimes N}$ iff

$$\sum_{i=1}^{m} \binom{\omega}{k_i} = \sum_{i=1}^{m} \binom{N-\omega}{k_i} + 1, \quad (mod\ 2) \quad for\ \ 0 \leq \omega \leq N. \tag{5.14}$$

(3) a plus eigenstate of $Y^{\otimes N}$ iff

$$\sum_{i=1}^{m} \binom{\omega}{k_i} = \sum_{i=1}^{m} \binom{N-\omega}{k_i} + \omega + \frac{N}{2}, \quad (mod\ 2) \quad for\ \ 0 \leq \omega \leq N. \tag{5.15}$$

Keeping the structure of local Pauli stabilizers, we notice that

Lemma 5.8. *An N-qubit hypergraph state, which is eigenstate of $X^{\otimes N}$ with "$+1$" eigenvalue has real coefficients after the action of $\sqrt{X_{\pm}}^{\otimes N}$. And the one which is eigenstate of $X^{\otimes N}$ with "-1" eigenvalue has all imaginary coefficients after the action of $\sqrt{X_{\pm}}^{\otimes N}$.*

Proof. The proof is straightforward in both cases.

$$X^{\otimes N}|H_N^3\rangle = |H_N^3\rangle \quad \Rightarrow \quad \sqrt{X_{\pm}}^{\otimes N}|H_N^3\rangle = \sqrt{X_{\mp}}^{\otimes N}|H_N^3\rangle. \tag{5.16}$$

Two sides of last equality are complex conjugates of each other and from the equality follows that imaginary part is equal to zero. In a similar manner the second case can be treated:

$$X^{\otimes N}|H_N^3\rangle = -|H_N^3\rangle \quad \Rightarrow \quad \sqrt{X_{\pm}}^{\otimes N}|H_N^3\rangle = -\sqrt{X_{\mp}}^{\otimes N}|H_N^3\rangle. \tag{5.17}$$

Here the minus sign on of the right hand-side implies that the real part of expressions must be zero. □

Interestingly for N-qubit graph state case, when the ± 1 eigenvalue condition of $X^{\otimes N}$ holds, the square-root of Pauli's map graph state to the N-qubit GHZ-state: $\sqrt{X}^{\otimes N}|H_N^2\rangle = |GHZ\rangle_N$. We can apply the same transformations to more general states:

Lemma 5.9. *Given a symmetric hypergraph state that is an eigenstate of $X^{\otimes N}$ with "$+1$" eigenvalue, then it is possible to calculate a coefficient of the computational basis element of a weight e after application of $\sqrt{X}^{\otimes N}$ using the following expression:*

$$k_{|e|} \equiv k_{0\ldots01\ldots1} = \frac{1}{\sqrt{2^N}} - \frac{1}{2^{\frac{3N}{2}-1}} \sum_{\omega} \sum_{m=0}^{|e|} \binom{N-|e|}{\omega-m} \binom{|e|}{m} \Re\left((1+i)^N (-i)^{\omega+|e|-2m}\right), \quad (5.18)$$

here ω depends on the cardinality of hyperedges in a symmetric hypergraph states and sum runs over all the entries with the negative sign in the state vector.

Proof. Let us express an N-qubit hypergraph state which is an eigenstate of $X^{\otimes N}$ with $+1$ eigenvalue as follows:

$$|H\rangle = |+\rangle^{\otimes N} - \frac{1}{\sqrt{2}^{N-2}} \sum_{w}^{N} (|\underbrace{1\ldots1}_{w}0\ldots0\rangle + \text{ permut.}). \quad (5.19)$$

Then the application of $\sqrt{X}^{\otimes N}$ gives,

$$\begin{aligned}
\sqrt{X_+}^{\otimes N}|H\rangle =& \sqrt{X_+}^{\otimes N}\left(|+\rangle^{\otimes N} - \frac{1}{\sqrt{2}^{N-2}} \sum_{\omega}^{N} (|\underbrace{1\ldots1}_{\omega}0\ldots0\rangle + \text{ permut.})\right) \\
=& |+\rangle^{\otimes N} - \frac{1}{\sqrt{2}^{N-2}} \sqrt{X_+}^{\otimes N} \sum_{\omega}^{N} (|\underbrace{1\ldots1}_{\omega}0\ldots0\rangle + \text{ permut.}). \\
=& |+\rangle^{\otimes N} - \frac{1}{\sqrt{2}^{N-2}} \frac{1}{2^N} \left((1+i)\mathbb{1} + (1-i)X\right)^{\otimes N} \sum_{\omega}^{N} (|\underbrace{1\ldots1}_{\omega}0\ldots0\rangle + \text{ permut.})
\end{aligned} \quad (5.20)$$

We will now derive some intermediate steps separately. It is clear that for any binary vector of weight ω_0, $|\underbrace{1\ldots1}_{\omega_0}0\ldots0\rangle$, the following holds for any $0 \leq j \leq N$:

$$\begin{aligned}
X^{\otimes j} \otimes \mathbb{1}^{\otimes N-j} |\underbrace{1\ldots1}_{\omega_0}0\ldots0\rangle =& X^{\otimes j} \otimes \mathbb{1}^{\otimes N-j} X^{\otimes N} |0\ldots0\underbrace{1\ldots1}_{N-\omega_0}\rangle \\
=& \mathbb{1}^{\otimes j} \otimes X^{\otimes N-j} |0\ldots0\underbrace{1\ldots1}_{N-\omega_0}\rangle.
\end{aligned} \quad (5.21)$$

From Lemma 5.7 it is clear that if the vectors with the weight ω have negative sign, than vectors with weight $N-\omega$ have negative sign too and the converse also holds. Let us take a pair of vectors of weight ω and $N-\omega$ related to each other as in Eq.(5.21). Then for any j we get the following term:

$$\begin{aligned}
&(1-i)^j (1+i)^{N-j} X^{\otimes j} \otimes \mathbb{1}^{\otimes N-j} |\underbrace{1\ldots1}_{\omega_0}0\ldots0\rangle + (1-i)^{N-j}(1+i)^j \mathbb{1}^{\otimes j} \otimes X^{\otimes N-j} |0\ldots0\underbrace{1\ldots1}_{N-\omega_0}\rangle \\
=& \left((1-i)^j (1+i)^{N-j} + (1-i)^{N-j}(1+i)^j\right) X^{\otimes j} \otimes \mathbb{1}^{\otimes N-j} |\underbrace{1\ldots1}_{\omega_0}0\ldots0\rangle = 2\Re\left((1-i)^j (1+i)^{N-\mathrm{j}}\right) \\
=& 2\Re\left((-i)^j (1+i)^N\right).
\end{aligned} \quad (5.22)$$

Let us separately derive the coefficients $k_{|e\rangle}$ for computational bases $|e\rangle$ obtained after application of Clifford get on each qubit. We start from the simplest case and then generalize it:

$$k_{0\ldots0} = \frac{1}{\sqrt{2}^N} - \frac{1}{\sqrt{2}^{N-2}\cdot 2^N}\sum_{\omega}^{N}\binom{N}{\omega}\Re\left((-i)^{\omega}(1+i)^N\right). \tag{5.23}$$

Now consider more difficult case, a coefficient of $k_{0\ldots011}$, or otherwise a coefficient of a commutation basis with weight exactly equal to two:

$$\begin{aligned} k_{0\ldots011} =& \frac{1}{\sqrt{2}^N} - \frac{1}{2^{\frac{3N}{2}-1}}\sum_{\omega}^{N}\left(\binom{N-2}{\omega}\Re\left((1+i)^N(-i)^{\omega+2}\right) + 2\binom{N-2}{\omega-1}\Re\left((1+i)^N(-i)^{\omega}\right)\right. \\ &\left. + \binom{N-2}{\omega-2}\Re\left((1+i)^N(-i)^{\omega-2}\right)\right) \\ =& \frac{1}{\sqrt{2}^N} - \frac{1}{2^{\frac{3N}{2}-1}}\sum_{\omega}\sum_{m=0}^{2}\binom{N-2}{\omega-m}\binom{2}{m}\Re\left((1+i)^N(-i)^{\omega+2-2m}\right). \end{aligned} \tag{5.24}$$

From here one can directly generalize that the coefficient of any computational basis element with the weight $|e|$ is given as follows:

$$k_{|e|} \equiv k_{0\ldots01\ldots1} = \frac{1}{\sqrt{2}^N} - \frac{1}{2^{\frac{3N}{2}-1}}\sum_{\omega}\sum_{m=0}^{|e|}\binom{N-|e|}{\omega-m}\binom{|e|}{m}\Re\left((1+i)^N(-i)^{\omega+|e|-2m}\right). \tag{5.25}$$

This finishes the proof. □

Now that we have the general formula for coefficients after action of $\sqrt{X}^{\otimes N}$, we would like to use it to calculate geometric measure of some of the important hypergraph states.

Theorem 5.10. *The geometric measure of N-qubit three-uniform complete hypergraph state, which is an eigenstate of $X^{\otimes N}$ with the $+1$ eigenvalue, can be calculated via optimizing over a single real parameter of the product state $|a\rangle^{\otimes N}$.*

Proof. An N-qubit three-uniform complete hypergraph state is an eigenstate of $X^{\otimes N}$ with $+1$ eigenvalue, if and only if N is of the form $N = 2 \mod 4$ [131]. It is easy to verify that the weight vectors with negative coefficient in $|H_N^3\rangle$ are the ones with the weight $\omega = 3 \pmod 4$:

$$|H_N^3\rangle = |+\rangle^{\otimes N} - \frac{1}{\sqrt{2}^{N-2}}\sum_{w=3,7,\ldots}^{N}\left(|\underbrace{1\ldots1}_{w}0\ldots0\rangle + \text{ permut.}\right). \tag{5.26}$$

Then we evaluate the expression for the coefficients $k_{|e|}$. One can directly observe that in Eq. (5.18) when the weight $|e|$ is odd, since $N/2$ is also an odd number, the following holds,

$$\Re\left((1+i)^N(-i)^{\omega+|e|-2m}\right) = \Re\left((1+i)^N(\pm 1)\right) = \Re\left(\pm(i2)^{N/2}\right) = 0. \tag{5.27}$$

Thus, for all odd $|e|$, the coefficient $k_{|e|} = \frac{1}{\sqrt{2}^N}$.

If the weight $|e|$ is either zero $|e| = 0$, or $|e| = N$, then the expression $k_{|e|}$ simplifies to:

$$k_0 = k_N = \pm\frac{1}{2}. \tag{5.28}$$

For even $|e|$ we have to go through a lengthy combinatorial calculation, which yields the value of coefficients to be zero $k_{|e|} = 0$.

We write $N = 4p + 2$, $p > 0$, $p \in \mathbb{N}$. Then we can simplify the sums in $k_{|e|}$ as follows:

$$\sum_{\omega=3,7\ldots}^{N}\sum_{m=0}^{|e|}\binom{N-|e|}{\omega-m}\binom{|e|}{m}\Re\left((1+i)^N(-i)^{\omega+|e|-2m}\right) \tag{5.29}$$

$$=(-1)^{p+1}\sum_{\omega=3,7\ldots}^{N}\sum_{m=0}^{|e|}\binom{N-|e|}{\omega-m}\binom{|e|}{m}\sqrt{2}^N\Im\left((-i)^{\omega+|e|-2m}\right) \tag{5.30}$$

$$=(-1)^{p}\sum_{\omega=3,7\ldots}^{N}\sum_{m=0}^{|e|}\binom{N-|e|}{\omega-m}\binom{|e|}{m}\sqrt{2}^N\Im\left((-i)^{1+|e|-2m}\right) \tag{5.31}$$

$$=(-1)^{p}\sqrt{2}^N\sum_{\omega=3,7\ldots}^{N}\sum_{m=0}^{|e|}\binom{N-|e|}{\omega-m}\binom{|e|}{m}\begin{cases}(-1)^m & \text{if } |e| \mod 4 = 2.\\ (-1)^{m+1} & \text{if } |e| \mod 4 = 0.\end{cases} \tag{5.32}$$

Let us consider the case when $|e| = 4\tilde{p} + 2$ (the second case works in the analogous way), then we get

$$(-1)^{p}\sqrt{2}^N\sum_{m=0}^{|e|}(-1)^m\binom{|e|}{m}\left[\sum_{\omega=3,7\ldots}^{N}\binom{N-|e|}{\omega-m}\right] \tag{5.33}$$

$$=(-1)^{p}\sqrt{2}^N\sum_{m=0}^{|e|}(-1)^m\binom{|e|}{m}\left[\frac{1}{4}\sum_{j=0}^{3}(2\cos\frac{j\pi}{4})^{N-|e|}\cos\frac{j\pi(N-|e|-2(3-m))}{4}\right] \tag{5.34}$$

$$=(-1)^{p}\sqrt{2}^N\frac{1}{4}\sum_{m=0}^{|e|}(-1)^m\binom{|e|}{m}\times \tag{5.35}$$

$$\left[2^{N-|e|}+2^{\frac{N-|e|}{2}}\left(\cos\frac{\pi(N-|e|-6+2m)}{4}+\cos\frac{3\pi(N-|e|-6+2m)}{4}\right)\right] \tag{5.36}$$

$$=(-1)^{p}\sqrt{2}^N\frac{1}{4}\sum_{m=0}^{|e|}(-1)^m\binom{|e|}{m}\left[2^{N-|e|}-(-1)^q2^{\frac{N-|e|}{2}}(\sin\frac{m\pi}{2}-\sin\frac{3m\pi}{2})\right] \tag{5.37}$$

$$=(-1)^{p+q+\tilde{p}}\sqrt{2}^{2N-|e|-4}\sqrt{2}^{|e|+2}=\sqrt{2}^{2N-2} \tag{5.38}$$

where $q = (N - |e|)/4$. Note here that that $(p + \tilde{p} + q)$ is an even number. Inserting everything in $k_{|e|}$, we get:

$$k_{|e|} = \frac{1}{\sqrt{2}^N} - \frac{1}{\sqrt{2}^{3N-2}}\sqrt{2}^{2N-2} = 0. \tag{5.39}$$

Finally, the entire state can be mapped to

$$\pm\frac{1}{\sqrt{2}}|GHZ\rangle + \frac{1}{\sqrt{2}^N}\sum_{w(x)\ odd}|x\rangle. \tag{5.40}$$

If there is a positive sign in front of GHZ state, we are done. If not N-fold tensor product of Pauli-Z operations introduces a global negative sign for the entire state, which can just be neglected. □

From Eq. (5.40) we write a formula for the geometric measure of entanglement for three-uniform complete hypergraph states:

$$E_G(|H_N^3\rangle) = 1 - \max_t \left[\frac{1}{2}(t^N + \sqrt{1-t^2}^N) + \frac{1}{\sqrt{2}^N}\sum_{j\ odd}\binom{N}{j} t^j \sqrt{1-t^2}^{N-j}\right]^2 \tag{5.41}$$

$$= 1 - \max_t \left[\frac{1}{2}(t^N + \sqrt{1-t^2}^N) + \frac{1}{\sqrt{2}^{N+2}}\left((t+\sqrt{1-t^2})^N - (\sqrt{1-t^2}-t)^N\right)\right]^2. \tag{5.42}$$

The expression above is symmetric under exchange of t and $\sqrt{1-t^2}$, and its derivative vanishes at $t = \frac{1}{\sqrt{2}}$. Inserting this value of t back in the expression of the geometric measure, we get:

$$E_G(|H_N^3\rangle) = \frac{3}{4} - \frac{1}{2^N} - \frac{1}{\sqrt{2}^N}. \tag{5.43}$$

We conjecture that the maximization is indeed attained at the point $t = \frac{1}{\sqrt{2}}$. We have checked this statement up to $N = 4002$ qubits.

5.4 Summary and outlook

In this chapter we have discussed entanglement witnesses and measures for certain classes of hypergraph states. We connected entanglement detection to the graphical transformations on hypergraphs and derived first tight witnesses for three-uniform complete hypergraph states. In the second part we studied geometric measure of entanglement for symmetric hypergraphs. Interestingly, one can often restrict optimization over a single parameter. Moreover, we employed the constructions from local Pauli stabilizers of hypergraphs to derive our results.

Having introduced the formalism for witnesses and simplifications for geometric measures, it would be interesting to investigate entanglement of other hypergraph states, including the non-symmetric ones: E.g. Resource states for MBQC protocols and error correcting codes (See subsequent chapters for applications). Finally, numerical calculations confirm that one can generalize our obtained results to other symmetric states, which are eigenstates of Pauli operators.

Chapter 6

Changing circuit-depth complexity of MBQC with hypergraph states

Measurement-based quantum computation (MBQC) was introduced in Chapter 2 mainly using graph states as resource states. In this chapter we establish that hypergraph states can be new interesting resource states allowing deterministic computational schemes. Our MBQC construction heavily relies on measurement rules derived in Chapter 3. So, for the full understanding of the technical parts in this chapter, we recommend readers to get familiar with the Pauli measurement rules from Chapter 3 first.

6.1 Introduction

A typical way to build a computer, classical or quantum, is to realize a universal set of elementary gates. Consequently, the concept of universality is fundamental in computer science. While the most common choice for the universal gate set in quantum circuits is a two-qubit entangling gate supplemented by certain single-qubit gates (see Theorem 2.9), the universal gate set given by the three-qubit Toffoli gate [or the Controlled-Controlled-Z (CCZ) gate for our case] and the one-qubit Hadamard (H) gate (see Theorem 2.10) is fascinating for several reasons.

First, the Toffoli gate alone is already universal for reversible classical computation. Consequently, the set may give insight into fundamental questions about the origin of quantum computational advantage, in the sense that changing the bases among complementary observables (by the Hadamard gates) brings power to quantum computation [134–138]. Second, this gate set allows certain transversal implementations of fault-tolerant universal quantum computation using topological error correction codes. Transversality means that, in order to perform gates on the encoded logical qubits, one can apply corresponding gates to the physical qubits in a parallel fashion, and this convenience has sparked recent interest on this gate

	Cluster State	Hypergraph State
Preparation gates	$CZ \in \mathcal{C}_2$	$CCZ \in \mathcal{C}_3$
Measurements	Pauli + $\mathcal{C}_2$	Pauli
Implemented gates	$\downarrow$ $\mathcal{C}_2$ $\quad$ $\downarrow$ $\mathcal{C}_3$	$\downarrow$ CCZ, H
Byproduct	$\{X, Z\}$	$\{CZ, X, Z\}$
Parallelized gates	$\mathcal{C}_2$	$\{CCZ^{nn}, SWAP\}$

TABLE 6.1: Features of MBQC schemes using cluster and hypergraph states. Our scheme with a hypergraph state implements all logical CCZ and $SWAP$ gates without adaptation of measurements, leading to a massive parallelization of these.

set [139–142]. Third, the many-body entangled states generated by the CCZ gates correspond to hypergraph states.

Motivated by these observations, we introduce a *deterministic* scheme of MBQC for the gate set of $\{CCZ, H\}$, using multi-qubit hypergraph states. MBQC is a scheme of quantum computation where first a highly-entangled multi-particle state is created as a resource, then the computation is carried out by performing local measurements on the particles only [16, 94]. Compared with the canonical model of MBQC using cluster states generated by Controlled-Z (CZ) gates, our scheme allows to extend substantially several key aspects of MBQC, such as the set of parallelizable gates and the byproduct group to compensate randomness of measurement outcomes (see [96, 143, 144] for previous extensions using tensor network states). Although 2D ground states with certain symmetry-protected topological orders (SPTO) have been shown to be universal for MBQC [97, 145, 146], our construction has a remarkable feature that it allows *deterministic* MBQC, where the layout of a simulated quantum circuit can be predetermined. As a resource state, we consider hypergraph states built only from CCZ unitaries. This is because (i) these states have a connection to genuine 2D SPTO, (ii) it is of fundamental interest if CCZ unitaries alone are as powerful as common hybrid resources by CCZ (or so-called non-Clifford elements) and CZ unitaries, and (iii) they might be experimentally relevant since it requires only one type of the entangling gate, albeit a three-body interaction (cf.[147–149]). On a technical side, we use a complex graphical rule for Pauli-X basis measurements on general hypergraph states, which allows a deterministic MBQC protocol on a hypergraph state, for the first time.

As a remarkable consequence of deterministic MBQC, we demonstrate an N-qubit generalized Controlled-Z ($C^N Z$) gate, a key logical gate for quantum algorithms such as the unstructured database search [150], in a depth logarithmic in N. Although relevant logarithmic implementations of $C^N Z$ have been studied in Refs. [101–103], we highlight a trade-off between space and time complexity in MBQC, namely, reducing exponential ancilla qubits to a polynomial overhead on the expense of increasing time complexity from a constant depth to a logarithmic depth, in this example.

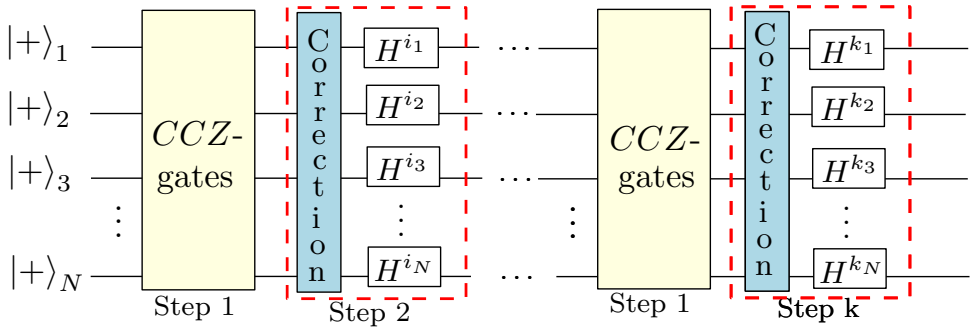


FIGURE 6.1: Any quantum computation can be described as alternative applications of logical CCZ and Hadamard gates. Our MBQC scheme allows a parallelization of all logical CCZ (namely, CCZ^{nn} and $SWAP$) gates and each Hadamard layer increments computational depth, as it requires adaptation of measurement bases to correct prior byproducts.

6.2 Summary of computation scheme

In MBQC, an algorithm is executed by performing local measurements on some entangled resource state. Consequently, two different physical resources, the entangling gates needed to prepare the state and the required class of measurements, characterize the MBQC scheme. In the first column of Table 6.1 cluster state MBQC model is summarized.

As reviewd in Chapter 2, There are three relevant aspects in the complexity of MBQC. First: the adaptation of measurement bases, namely whether the choice of some measurement bases depends on the results of previous measurements. Second: the notion of parallelism and logical depth (cf. [151, 152]) in terms of the ordering of measurements. Third: due to intrinsic randomness in the measurement outcomes, there are byproduct operators sometimes to be corrected. In the canonical scheme of MBQC using the cluster state, Pauli measurements implement Clifford gates in $\mathcal{C}_2$ without adaptation of measurement bases, so these gates are parallelized. As Clifford gates are not universal, more general measurements in the X-Y-plane of the Bloch sphere must be performed to generate unitaries in $\mathcal{C}_3$. The byproduct group is generated by the Pauli operators X and Z.

Our scheme, however, has several key differences summarized in Table 6.1. Our state is prepared using CCZ gates ($CCZ \in \mathcal{C}_3$), but Pauli measurements alone are sufficient for universal computation. We choose $\{CCZ, H\}$ to be the logical gate set for universal computation. Indeed, we can implement all logical CCZ gates at *arbitrary* distance in parallel, by showing that nearest neighbor CCZ gates (CCZ^{nn}) and $SWAP$ gates are applicable without adaptation. Our implementation generates the group of byproduct operators $\{CZ, X, Z\}$, which differs from the standard byproduct group. Since we need Hadamard gates to achieve universality and our byproduct group is not closed under the conjugation with the Hadamard gate, we need to correct all CZ byproducts before the Hadamard gates. Thus, the logical depth grows according to the number of global applications of Hadamard gates, effectively changing the computational bases (see Fig. 6.1).

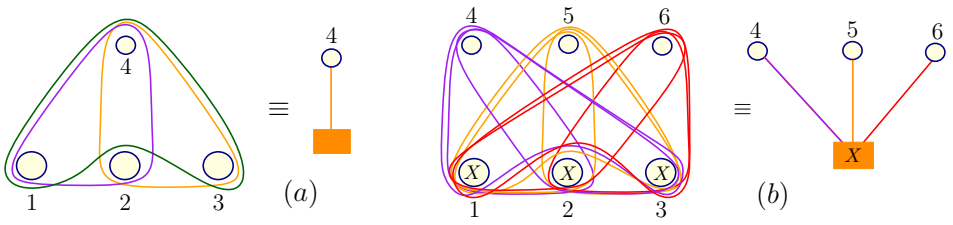


FIGURE 6.2: (a) Denoting the four-qubit hypergraph state with hyperedges $E = \{\{1,2,4\},\{2,3,4\},\{1,3,4\}\}$ with the vertex and the box. (b) Pauli-X measurements on vertices $1,2,3$ by Pauli-X measurement on the box.

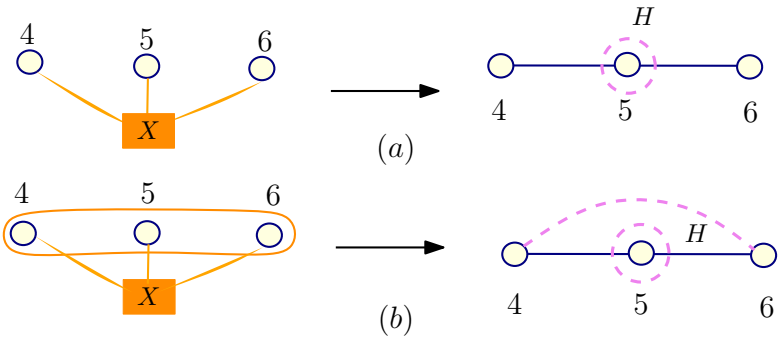


FIGURE 6.3: Pauli-X-measurements on the given hypergraph states result in graph states, with a Hadamard gate applied to its vertex 5. All dashed lines (depicting byproducts) appear additionally if the product of measurement outcomes on vertices $1,2,3$ is -1. (a) Pauli-Z byproduct. (b) Pauli-Z and CZ byproducts.

6.3 Universal three-uniform hypergraph state and deterministic MBQC

We use a three-uniform hypergraphs state as a resource state for MBQC. In MBQC protocols CZ unitaries guarantee information flow via perfect teleportation [94]. Obtaining CZ gates with an unit probability from three-uniform hypergraph states has been a challenge as Pauli-Z measurements always give probabilistic CZ gates. Therefore, only probabilistic or hybrid (where CCZ and CZ gates are available on demand) scenarios have been considered in the literature [97, 142, 153]. However, using a non-trivial Pauli-X measurement rule on three-uniform hypergraph states, we achieve deterministic teleportation via projecting on CZ gates with unit probability. See Chapter 4 and Fig. 4.6 for the simplest such example.

In this section we use two Pauli-X measurement examples as building blocks of our resource state. They were already discussed individually in Fig. 4.7 and Fig. 4.8. For ease of notation, we draw a box instead of three vertices $V = \{1,2,3\}$ and connect it with an edge to another vertex $k\,(\geq 4)$ [see Fig. 6.2 (a)], if every two out of those three vertices are in a three-qubit hyperedge with the vertex k. In addition, we say that a box is measured in the $\mathcal{M}$-basis if all three qubits $\{1,2,3\}$ are measured in the $\mathcal{M}$-basis [see Fig. 6.2 (b), where $\mathcal{M} = X$]. Then the simplified figures for the examples in Fig. 4.7 and Fig. 4.8 can be seen in Fig.6.3.

Now we are ready to formulate the main theorem of the chapter:

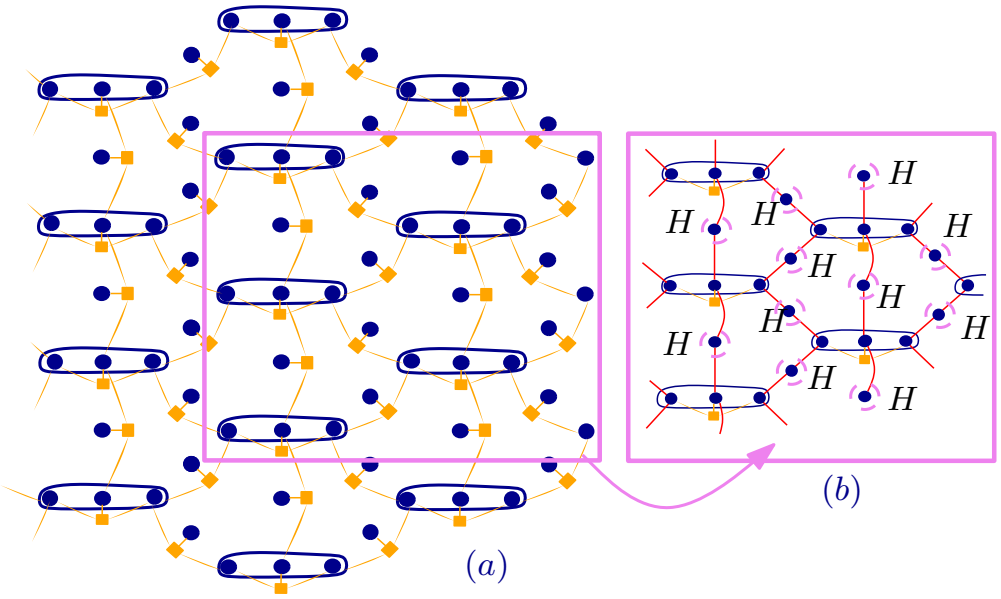


FIGURE 6.4: (a) The universal resource state composed of elements on Fig. 6.3 (a) and (b). (b) Resource state obtained after measuring all boxes in Pauli-X bases, except the ones attached to three qubits surrounded by a hyperedge. All dashed circles represent Pauli-Z byproducts.

Theorem 6.1. *Based on the hypergraph state of Fig. 6.4 (a), we propose MBQC with the following features: (i) it is universal using only Pauli measurements, (ii) it is deterministic, (iii) it allows parallel implementations of all logical CCZ and SWAP gates, among the universal gate set by CCZ, SWAP, and Hadamard gates, and (iv) its computational logical depth is the number of global layers of logical Hadamard gates.*

Proof. We discuss the points in Theorem 6.1 individually: *(i) Universality with Pauli measurements only:* For the universal gate set we choose CCZ and Hadamard gates. We realize the CCZ gate on arbitrary qubits in two steps: a nearest neighbor CCZ gate (CCZ^{nn}) and a *SWAP* gate, swapping an order of inputs. Here we assume that information flows from the bottom to the top differently from the convestion in circuits or previous MBQC schemes.

As a first step we measure almost all boxes in Pauli-X basis, except the ones attached to the horizontal three vertices surrounded by a hyperedge CCZ. As a result we get graph edges connecting different parts of the new state, see the transition from Fig. 6.4 (a) to (b). Getting these graph edges is a crucial step, since it is partially responsible for *(ii) determinism of the protocol.* We use the resource in Fig. 6.5 to implement the CCZ^{nn} gate. For CCZ^{nn} gate

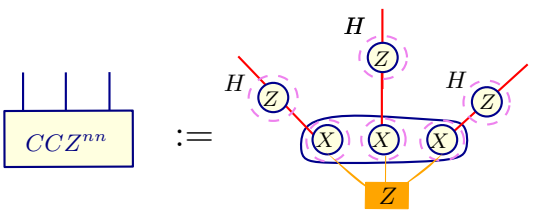


FIGURE 6.5: A nearest-neighbor CCZ gate is implemented up to $\{Z, CZ\}$ byproducts.

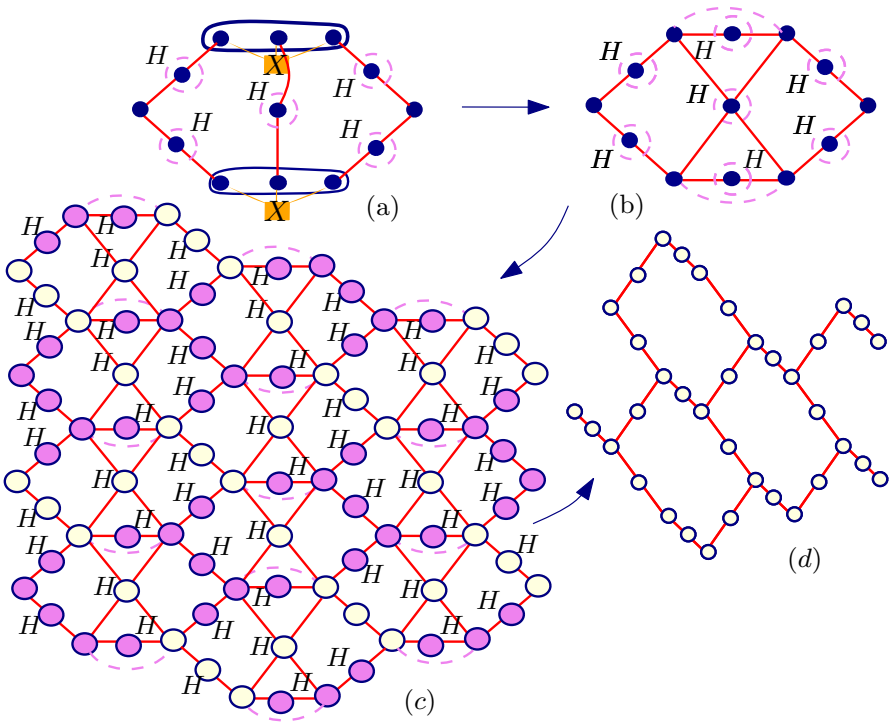


FIGURE 6.6: A *deterministic* graph state to implement *SWAP*, H gates, and correction steps. (a) Gets rid of hyperedges entirely and projects on the graph state with Pauli-Z and CZ byproducts depicted by dashed lines in (b). The hexagonal lattice (d) is obtained deterministically after measuring colored vertices in suitable Pauli bases on (c).

implementation we have to secure independently three inputs and three outputs for CCZ hyperedge in a hypergraph state to be used as a *logical* CCZ gate. The box is measured in the Pauli-Z basis and just gets removed. The three vertices to which the box was attached to are still surrounded by a hyperedge CCZ up to Pauli-Z byproducts. These three qubits are connected to the rest of the state with the graph edges, and performing measurements as shown on Fig. 6.5 teleports the CCZ gate to the output qubits (up to $\{CZ, Z\}$ byproducts). The measurement rules from Chapter 4 have been used for explicit derivations.

Now we need a *SWAP* and a Hadamard (H) gate both contained in $\mathcal{C}_2$. Since some graph states can directly implement Clifford gates with Pauli measurements only, we first get rid of all unnecessary CCZ hyperedges from the resource state by measuring all remaining boxes in Fig. 6.4 (b) in Pauli-X bases resulting to the state in Fig. 6.6 (b) (the full Pauli-X measurement rule is needed for the derivation) and looking at the bigger fragment, we get a graph as in Fig. 6.6 (c). The main idea here is to get rid of all the vertices which might be included in edges corresponding to byproduct CZ's. Then, we make Pauli-Z measurements (qubits to which an H is applied, we measure in the Pauli-X basis) on coloured vertices. As a result, we project to a hexagonal lattice deterministically. This construction is the final step also responsible for *(ii) Determinism of the protocol.* The hexagonal lattice can implement any Clifford gate in parallel up to $\{X, Z\}$ byproducts using Pauli measurements only [95], and therefore, we can implement a *SWAP* gate. *(iii) Parallelization:* The *SWAP* and CCZ^{nn} gates together give a CCZ gate over arbitrary distance, up to $\{CZ, X, Z\}$ byproducts without adaptivity.

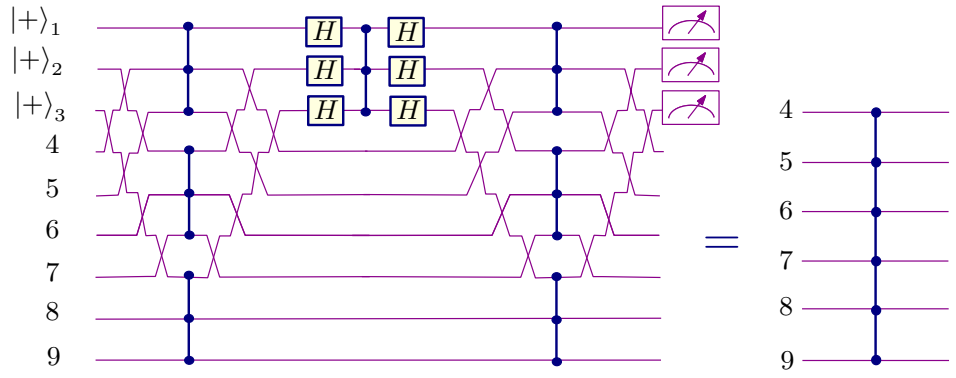


FIGURE 6.7: (a) The circuit identity to create a C^6Z gate. Crossed lines correspond to *SWAP* gates as seen in Chapter 2.3. The first three qubits are measured in Pauli-X basis. The adaptation of measurement bases is needed twice for two Hadamard layers.

(iv) Logical depth: Finally, after every CCZ gate layer, we need to implement the Hadamard layer, which is straightforward [94]. However, since CZ byproducts cannot be fed-forward through Hadamard gates, we need to correct all CZ's. We can again use the hexagonal lattice to perform the correction step, however, the $(k-1)$-th correction step as enumerated in Fig. 6.1 itself introduces $\{X, Z\}$ byproducts which due to the commutation relation, $C_{abc}X_a = X_aC_{abc}C_{bc}$, introduces new CZ byproducts before the k-th correction step. Consequently, the measurement results during the $(k-1)$-th correction must be taken into account to correct all CZ byproducts before the k-th correction step. To sum up, we can parallelize all CCZ gates, but we need to increment the circuit depth for each Hadamard layer in order to correct all CZ byproducts *adaptively*. □

6.4 Applications of computation scheme

We demonstrate that the parallelization in our MBQC protocol may find practical applications, by considering an example of an N-times Controlled-Z (C^NZ) gate. Its implementation has been known either (i) in an $O(\log N)$ non-Clifford T depth with $(8N-17)$ logical T-gates, $(10N-22)$ Clifford gates and $\lceil (N-3)/2 \rceil$ ancillae [101, 103], or (ii) in a constant depth (or constant rounds of adaptive measurements) albeit with $O(\exp N)$ CZ gates in the cluster-state MBQC model and $O(\exp N)$ ancillae [94]. In our approach, a decomposition of the C^NZ gate by CCZ gates and a few number of Hadamard layers is desired.

Theorem 6.2. *An N-times Controlled-Z (C^NZ) gate is feasible in an $O(\log N)$ logical depth of the Hadamard layers (or "Hadamard" depth), using a polynomial spatial overhead in N, namely $(2N-6)$ logical Hadamard gates, $(2N-5)$ CCZ gates and $(N-3)$ ancillae, where $N = 3 \cdot 2^r$ for a positive integer r.*

Proof. We construct a circuit implementing generalized controlled-Z gate complying with the statements of theorem. As a first step, we give the circuit identity for C^6Z gate in Fig. 6.7,

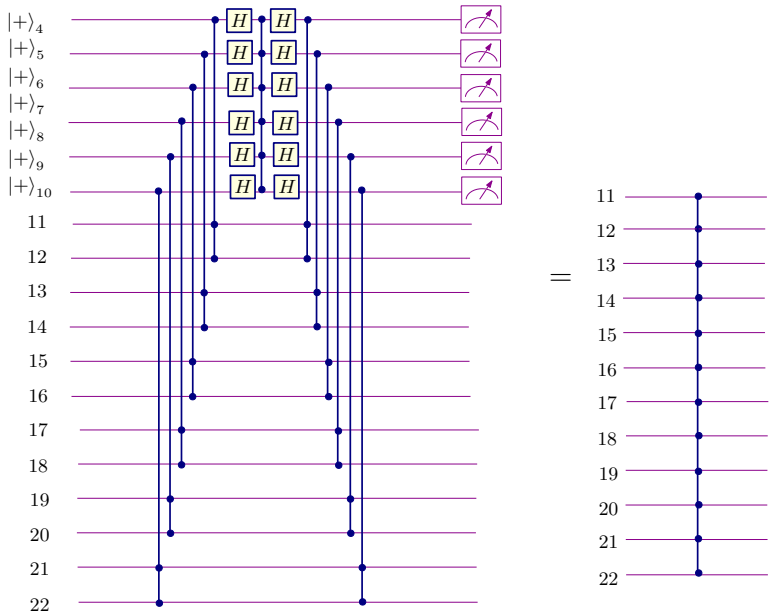


FIGURE 6.8: (a) The circuit identity to create a $C^{12}Z$ gate. The first six qubits are measured in Pauli-X basis. The adaptation of measurement bases is needed additionally twice for two Hadamard layers.

which has only two Hadamard layers. Next we use the new C^6Z gate to create $C^{12}Z$ with only two additional Haramard layers (See Fig. 6.8). Iterating this procedure for implementing a $C^{3\cdot 2^r}Z$ gate, one can directly calculate that we need $2r$ layers of Hadamards only. We also give a brief algebraic derivations of the circuit identity. We first show that the following equality holds for any state $|\psi\rangle$ and sets $i \in e_1$ and $i \in e_2$:

$$C_{e_1} H_i C_{e_2} H_i C_{e_1} |+\rangle_i |\psi\rangle = |+\rangle_i C_{e_1 \cup e_2 \setminus \{i\}} |\psi\rangle. \tag{6.1}$$

Assume that $i = 1$ and denote $e_1' \equiv e_1 \setminus \{1\}$ and $e_2' \equiv e_2 \setminus \{1\}$, then $e_1 \cup e_2 \setminus \{1\} = e_1' \cup e_2'$:

$$C_{e_1} H_i C_{e_2} H_i C_{e_1} |+\rangle_i |\psi\rangle = C_{\{1\}\cup e_1'} CNOT_{e_2',1} C_{\{1\}\cup e_1'} |+\rangle_1 |\psi\rangle. \tag{6.2}$$

We can express an arbitrary multi-qubit state $|\psi\rangle$ in Pauli-X orthonormal basis $|j\rangle$: $|\psi\rangle = \sum_j \phi_j |j\rangle$. Then each vector $|+\rangle_1 |j\rangle$ is itself a hypergraph state.The action of a generalized $CNOT$ gate was already used in the previous sections: Applying the generalized $CNOT_{Ct}$ gate to a hypergraph state, where a set of control qubits C controls the target qubit t, introduces or deletes the set of edges $E_t = \{e_t \cup C | e_t \in \mathcal{A}(t)\}$.

In our example the target qubit $t = 1$ and for each hypergraph state $|+\rangle_1 |j\rangle$ the target qubit $t = 1$ is in a single hyperedge C_{e_1} only. Therefore from linearity follows that:

$$\begin{aligned} C_{\{1\}\cup e_1'} CNOT_{e_2',1} C_{\{1\}\cup e_1'} |+\rangle_1 \left(\sum_j \psi_j |j\rangle \right) &= C_{\{1\}\cup e_1'} C_{e_2\cup e_1'} C_{\{1\}\cup e_1'} |+\rangle_1 \left(\sum_j \psi_j |j\rangle \right) \\ &= C_{e_2\cup e_1'} |+\rangle_1 |\psi\rangle \end{aligned} \tag{6.3}$$

Next we count physical resource necessary to implement $C^N Z$ gate. We saw in Fig. 6.5 that the minimal physical resource for CCZ^{nn} gate is one physical CCZ^{nn} gate, and three CZ gates, and six. The minimal physical resource for a *SWAP* gate is nine CZ gates and eight ancilla qubits as we are implementing conventional *SWAP* gate on a cluster state [94]. Number of total CCZ^{nn} gates can be counted easily from the circuit, it also matches with number of Hadamard gates in the circuit plus one and for implementing $C^{3\cdot 2^r}$ gate is equal to:

$$K_{CCZ} = 3\left(\sum_{k=1}^{r} 2^k\right) + 1 = 2N - 5. \tag{6.4}$$

Here we count number of *SWAP* gates needed. For $C^6 Z$ we need twenty-four *SWAP* gates. In general, to implement a $C^N Z$ gate with our protocol having already created a $C^{N/2} Z$ gate, we need $N(N-2)$ *SWAP* gates. So, in order to create $C^N Z$ gate we need to sum up *SWAP* gates needed at all previous steps of iteration. If $N = 3 \cdot 2^r$, then there are totally $r = \log(N/3)$ iterations in our model from Theorem 6.2. To sum up, totally

$$K_{SWAP} = \sum_{k=1}^{r} (3 \cdot 2^k)(3 \cdot 2^k - 2) = 4N(\frac{N}{3} - 1) \tag{6.5}$$

SWAP gates are needed.

So, to sum up we need $K_{CCZ} = 2N - 5$ physical CCZ^{nn} gates, $3K_{CCZ} + 9K_{SWAP} = 3(2N-5) + 12N^2 - 36N = 12N^2 - 30N - 15$ physical CZ gates, and $6K_{CCZ} + 8K_{SWAP} = \frac{32}{3}N^2 - 20N - 30$ physical qubits. □

Next we look into the standard protocol for creating the $C^N Z$ gate using MBQC with cluster states. It appears that this gate can be implemented in a constant depth, but it has a massive drawback of requiring exponential number of ancillae qubits. In Refs. [94] the 55-qubit cluster state is given to implement three-qubit phase-gates, using Pauli measurements and eigenbasis of operators $U_Z(\pm\frac{\pi}{4})XU_Z(\pm\frac{\pi}{4})^\dagger$. If one extends this result for $C^4 Z$ gate, the initial cluster state must be reduced to the graph state via Pauli measurements implemented in parallel, but now one needs $\sum_{i=1}^{4} \binom{4}{i} = 2^4 - 1$ qubits. And in general, to implement a $C^N Z$ gate in the standard way starting from the cluster state, one would only need to adapt measurement basis twice, which is constant for any N, but number of qubits one would require is $\sum_{i=1}^{N} \binom{N}{i} = 2^N - 1$ which is exponential with the size of the gate implemented [89].

Let us look at the count of a physical qubits in case our gate identity from Theorem 6.2 is implemented on a cluster state. One can directly calculate that totally $8(K_{CCZ} + K_{SWAP}) = \frac{32}{3}N^2 - 16N - 40$ qubits are needed, which is polynomial in N. Therefore, Theorem 6.2 demonstrates a general trade-off between space and time complexity required for quantum algorithms, from the perspective of MBQC.

6.5 Summary and outlook

We introduced a deterministic scheme of MBQC for the gate set of CCZ and H gates, using a three-uniform hypergraph state and Pauli measurements. Our physical implementation enabled us to parallelize massively all long-range CCZ gates and the computational depth depended only on the change computational bases. It would be interesting to study if there exist hypergraph states with simpler planar architecture allowing similar MBQC protocols, since such hypergraph states could also be possessing certain interesting symmetries granting them to be 2D ground states with certain symmetry-protected topological orders (SPTO).

Noise in experiments is one of the major challenges in quantum computing. Along this direction, we have already seen in Chapter 3 that for certain nonlocal tasks hypergraph states can be more robust resources than graph states. Therefore, it would be desirable to investigate how certain realistic noise models affect computations performed using hypergraph resources. Moreover, for Bell inequality violations we saw that four-uniform hypergraph states give significantly more robust results than three- or two- uniform ones. Thus, it could be fruitful to design MBQC protocols using such families of hypergraph states too.

Chapter 7

Quantum error-correction and hypergraph states

Hypergraph states generalize graph states in many ways. Both states violate local realism exponentially, they are both useful for measurement-based quantum computation. Here we investigate whether hypergraph states can be used as bases of quantum-error correcting codes. Doing so, we derive strict Knill-Laflamme conditions specifically for hypergraph states and find the optimal quantum error-correcting codes up to six qubits. Finally, we compare new codes to existing stabilizer codes and show that hypergraph states might offer a new platform for studying nonadditive quantum error-correcting codes.

7.1 Introduction

Quantum error-correcting codes (QECC) constitute an important application of many body quantum entanglement. Since graph states and, more broadly, stabilizer states have proven extremely useful for this task, it is interesting to study whether hypergraph states are similar or better candidates for error-correction. Hence, for the start, it is important to look for hypergraph states with all of their $(d-1)$-marginals maximally mixed. Even though one-dimensional pure quantum codes cannot be used to transmit any information, the notion of distance is still useful in such cases. Every higher-dimensional pure quantum code has to be spanned by such one-dimensional codes. So, we use such states to construct distance d QECC codes and accordingly we call these codes *hypergraph-based quantum error correcting codes.* To differentiate these codes from graph-based codes, we require that each basis states in a code has at least one hyperedge with a cardinality greater or equal to three. In the following we derive conditions on basis hypergraph states to have maximally mixed marginals.

7.2 Conditions for distance two hypergraph-based QECC

In order to study distance $d = 2$ hypergraph-based pure quantum error-correcting codes, we first give conditions for hypergraph states to have all 1 RDMs maximally mixed.

Given a hypergraph state $|H\rangle$ and a vertex $a \in V$, we say that it is written in the expanded form over the vertex a, if it is written in the following form:

$$|H\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle_a|H_{0(a)}\rangle + |1\rangle_a|H_{0(a)} \oplus H_{1(a)}\rangle\big), \tag{7.1}$$

where $|H_{0(a)}\rangle$ and $|H_{0(a)} \oplus H_{1(a)}\rangle$ are also hypergraph states. We will often skip writing the vertex number in the brackets when it is clear from context. Thus, we will denote $|H_{j(a)}\rangle$ by $|H_j\rangle$. The hypergraph state $|H_0\rangle$ corresponds to a hypergraph $H_0 = (V\backslash\{a\}, \{e \in E | a \notin e\})$ and H_1 is also a hypergraph $H_1 = (V\backslash\{a\}, \{e - \{a\} | e \in E \;\&\; a \in e\})$. The notation '$\oplus$' denotes an *overlay* of two hypergraphs, with the same vertex set. It gives a new hypergraph with the same set of vertices and a new edge-set that is obtained by taking the symmetric difference of the edge-sets of original two hypergraphs,

$$(V, E_1) \oplus (V, E_2) = (V, E_1 \Delta E_2). \tag{7.2}$$

Lemma 7.1. *An N-qubit hypergraph state $|H\rangle$ has a^{th}-qubit RDM maximally mixed, if and only if the hypergraph state $|H_1\rangle$ corresponding to the hypergraph H_1 from the expanded form of $|H\rangle$ over the vertex a satisfies the following equality:*

$$\langle +|^{\otimes N}|H_1\rangle = 0. \tag{7.3}$$

Later we will denote $|+\rangle^{\otimes N}$ by $|\emptyset\rangle$, since it is a hypergraph state with an empty set of edges and we will call a hypergraph state *balanced*, if it is orthogonal to $\langle\emptyset|$.

Proof. Let us expand a hypergraph state $|H\rangle$ over the qubit a as in Eq.(7.1). The a^{th}-qubit RDM to be maximally mixed, we need to require that all off-diagonal entries in the RDM must be zero. Due to hermiticity of RDM, we only get a single orthogonality condition:

$$\langle H_0|H_0 \oplus H_1\rangle = 0. \tag{7.4}$$

The following statements are equivalent to Eq.(7.4):

$$\langle\emptyset|C_{H_0}C_{H_0}|\emptyset \oplus H_1\rangle = 0 \quad \Leftrightarrow \quad \langle H_0 \oplus H_0|H_1\rangle = 0 \quad \Leftrightarrow \quad \langle\emptyset|H_1\rangle = 0. \tag{7.5}$$

This finishes the proof. □

We will often use the following identity $\langle H'|H' \oplus H''\rangle = \langle H' \oplus H'|H''\rangle = \langle\emptyset|H''\rangle$ for arbitrary hypergraphs H' and H'' with equal number of vertices.

If every vertex in a hypergraph state $|H\rangle$ satisfies the condition in Lemma 7.1, then $|H\rangle$ has all RDMs maximally mixed, therefore, this state forms a distance $d = 2$ one-dimensional pure code. We can use such states as basis of higher-dimensional codes of distance $d = 2$.

Given two N-qubit hypergraph-based distance $d = 2$ one-dimensional pure codes $|H^{(1)}\rangle$ and $|H^{(2)}\rangle$, we rewrite Knill-Laflamme conditions to get higher-dimensional codes. For any error operator $E \in \{\mathbb{1}, Z, X, Y\}$ the following must hold:

$$\langle H^{(1)}|E|H^{(2)}\rangle = 0. \tag{7.6}$$

We consider each error operator Individually. If $E = \mathbb{1}$, then the two states must be orthogonal.

$$\langle H^{(1)}|H^{(2)}\rangle = \langle \emptyset|H^{(1)} \oplus H^{(2)}\rangle = 0. \tag{7.7}$$

In order to simplify the notation, we denote $H^{(1)} \oplus H^{(2)}$ by dH and call it a *difference* between two hypergraphs.

Next we consider $E = Z_a$, then

$$\langle H^{(1)}|Z_a|H^{(2)}\rangle = \langle \emptyset|Z_a|dH\rangle = \langle \emptyset|(V, \{\{a\}\}) \oplus dH\rangle = 0. \tag{7.8}$$

Therefore, not only the difference between two hyperedges must be balanced, but also any possible addition of a single vertex hyperedge to the difference hypergraph must also keep it balanced.

Next we consider $E = X_a$. Pauli-X error condition is trickier:

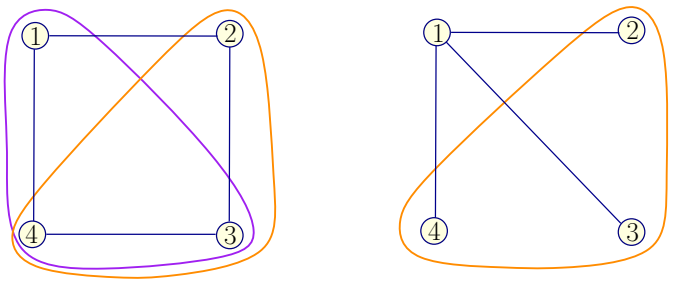
$$\langle H^{(1)}|X_a|H^{(2)}\rangle = \langle H^{(1)}_{1(a)}|dH\rangle = \langle H^{(2)}_{1(a)}|dH\rangle = \langle \emptyset|H^{(1)}_{1(a)} \oplus dH\rangle = \langle \emptyset|H^{(2)}_{1(a)} \oplus dH\rangle = 0. \tag{7.9}$$

Since the two conditions $\langle H^{(1)}_{1(a)}|dH\rangle = 0$ and $\langle H^{(2)}_{1(a)}|dH\rangle = 0$ are equivalent, we only need to check one of them and the other follows.

And finally, if $E = Y_a$, then

$$\langle H^{(1)}|Y_a|H^{(2)}\rangle = \langle H^{(1)}_{1(a)}|Z_a|dH\rangle = \langle \emptyset|(V, \{\{a\}\}) \oplus H^{(1)}_{1(a)} \oplus dH\rangle = 0. \tag{7.10}$$

If all the above orthogonality relations are satisfied for hypergraph basis set, then these basis states constitute codewords in the hypergraph-based pure QECC. In the next section we study such codes.



(a) (b)

FIGURE 7.1: Two examples of base hypergraph states for construction of $((4,4,2))_2$ code. (a) The base hypergraph for the first code. Other three hypergraphs in the code have additional hyperedges: $E_2^{(a)} = \{\{3\},\{4\}\}$, $E_3^{(a)} = \{\{1\},\{2\},\{3,4\}\}$, and $E_4^{(a)} = \{\{1\},\{2\},\{3\},\{4\},\{3,4\}\}$ (b) The base hypergraph for the second code. Other three hypergraphs in the code have additional hyperedges: $E_2^{(b)} = \{\{2\},\{3\}\}$ $E_3^{(b)} = \{\{2\},\{4\}\}$, and $E_4^{(b)} = \{\{3\},\{4\}\}$.

7.3 Hypergraph based codes of distance two

In this section we give examples of hypergraph-based codes of distance $d = 2$. By using the constraints derived in the previous section we search for hypergraph-based codes up to $N = 6$ qubits. We find all hypergraph-based pure codes up to $N = 5$ qubits. We also find some hypergraph-based pure codes for $N = 6$ qubits. In all of these cases the codes saturate the quantum Singleton bound.

For three qubits there is no hypergraph state with at least one hyperedge which satisfies Knill-Laflamme conditions.

Situation changes in four qubits. Already the symmetric case of the four-qubit three uniform complete hypergraph state has all of its 1 RDMs maximally, mixed. However, there also exist other hypergraph states in four qubits with the similar properties and, in addition, these basis states can be used to construct QECCs, which saturate the quantum Singleton bound. In Fig. 7.1 we give two examples of hypergraph states for the construction of $((4,4,2))_2$ codes. With the exhaustive search we also found more codes with the same property, but all their base hypergraph states are local unitary equivalent to one of the base hypergraph states in Fig. 7.1. Here (a) corresponds to the base hypergraph with hyperedges $E_1^{(a)} = \{\{1,2\},\{2,3\},\{3,4\},\{1,4\},\{1,3,4\},\{2,3,4\}\}$ and (b) to the base hypergraph with hyperedges $E_1^{(b)} = \{\{1,2\},\{1,3\},\{1,4\},\{2,3,4\}\}$.

Note that all four-qubit codes saturating the quantum Singleton bound are locally equivalent to the additive/stabilizer QECCs [154].

For five qubits we exhaustively characterize the following optimal hypergraph based codes:

(i) The code $((5,2,2))_2$, where the base code is a three-uniform hypergraph state and the second codeword in the subspace has only single-qubit Pauli-Z decorations. Here by

decorations we mean that the second hyperedge has in addition Pauli-Z gates applied to it.

(ii) The code $((5,4,2))_2$, where the base code is a three-uniform hypergraph state and the other codewords in the subspace are obtained by single-qubit Pauli-Z and graph edge CZ decorations. This is the optimal dimension if we require to have three-uniformity in the base code. The same dimension can be attained by single-qubit Pauli-Z and graph edge CZ and hyperedge CCZ decorations. Decorations of higher cardinalities cannot improve the bound.

(iii) The code $((5,5,2))_2$, where base code is only required to have at least one hyperedge of cardinality three or higher and other codewords can be obtained by single-qubit Pauli-Z decorations. This is again an optimal case since allowing more general decorations cannot increase the dimension of the code, neither when allowing higher cardinality hyperedges in the original codeword. Therefore, in five qubits if requiring to have even a single codeword containing at least one hyperedge of cardinality three or higher, the singleton bound cannot be saturated.

The detailed representatives of all these codes are given in Appendix C.

For graph-based pure codes it is typical that the base code is given by a graph state and other states in the code differ from this graph state only by local Pauli-Z operations. In case of hypergraph-based codes, where we require a base code to have at least one three- or higher cardinality hyperedge, we have seen that the other hypergraphs in the code differ from the base one by not only local Pauli-Z operations, but possibly in addition by CZ's and CCZ's. For $N = 4$-qubit codes we have seen that hypergraphs in the code differ by Pauli-Z and CZ operations and in 5-qubits we have mixture of all, Pauli-Z, CZ and CCZ-gates. Interestingly along this line or search we found that $((6,2,2))_2$ is the smallest hypergraph based pure code, where the base hypergraph state is three-uniform (see Fig. 7.2 (a)) and the difference with the other hypergraph is given by graph edges only (see Fig. 7.2 (b)).

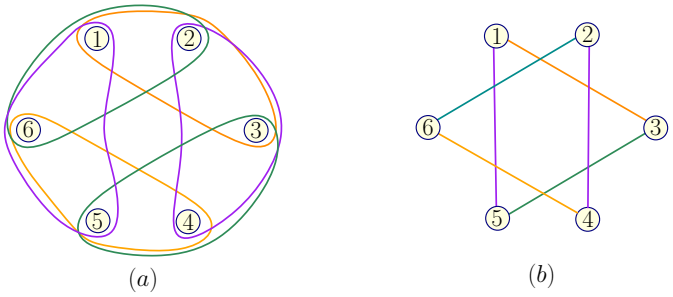


FIGURE 7.2: The hypergraph based pure quantum code $((6,2,2))_2$. (a) In $N = 6$-qubits if we consider three-uniform hypergraphs, there are totally $\binom{6}{3} = 20$ possible three-qubit hyperedges. The base three-uniform hypergraph state for code $((6,2,2))_2$ has every possible three-qubit hyperedge but the ones presented here. (b) The difference with the second hypergraph in the code is given by the six edges $\{\{1,3\},\{3,5\},\{1,5\},\{2,4\},\{4,6\},\{2,6\}\}$.

Already for six qubits an exhaustive search becomes difficult. However, it appears that if one restricts the first base state to be a three-uniform hypergraph state, then it is indeed possible

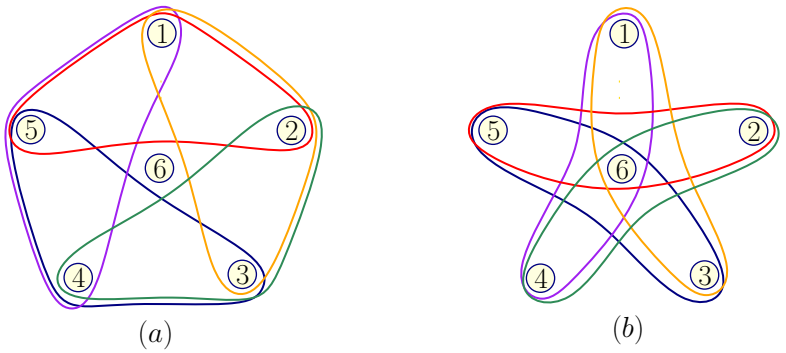


FIGURE 7.3: An overlay of (a) and (b) gives the 3-uniform base code for $((6, 16, 2))$.

to find other 15 codewords, all together building up a $((6, 16, 2))_2$ code. The overlay of two hypergraphs in Fig. 7.3 represents the three-uniform base state. They are drawn separately, in order to make the structure of the base more vivid. See Appendix C for the full description of the code. The code saturates the quantum Singleton bound. In Ref. [79] distance two quantum codes were investigated. It was found that differently from $((4, 4, 2))_2$ case, $2m$-qubit code, $m \geq 3$, which saturates the quantum Singleton bound, need not be additive. The explicit construction of a nonadditive code was given for $m = 3$ case, or otherwise, for 6-qubit case by checking that some quartic invariant differs from that of the additive one with the same parameters [154]. We calculated the same quartic invariants for our hypergraph-based $((6, 16, 2))_2$ code and found that our code is also nonadditive and, moreover, the values of the invariants differ from both, additive case and from the code in Ref. [79]. This demonstrates that hypergraph states might offer a new platform for studying nonadditive QECCs.

7.4 Summary and outlook

To sum up, in this chapter we studied error-correcting codes using hypergraphs states. We derived Knill-Laflamme conditions specifically for hypergraph states, which helped to exhaustively study all the QECC codes up to six qubits. We gave explicitly several interesting codes and the ones saturating the quantum Singleton bound. Finally, we computed quartic invariant for the $((6, 16, 2))_2$ hypergraph-based QECC and concluded that this code in nonadditive. This finding hints that hypergraph states and its stabilizer formalism can be employed to investigate nonadditive codes.

For the future work, it would be nice to derived conditions and constructions to obtain higher distance hypergraph-based codes and also to generalize our findings further to establish the connection between hypergraph states and quantum error-correcting codes.

Chapter 8

Coarse graining of entanglement classes in nonhomogeneous systems

Until now we always considered pure states with equal local dimensions. In this chapter we discuss so-called *coarse graning* of SLOCC classes in $2 \times m \times n$ systems. In general, there are infinitely many SLOCC classes in given dimensions. However, when considering operations from higher- to lower-dimensional Hilbert spaces, an additional hierarchy among the classes can be revealed. We study three-partite pure states in the Hilbert space $\mathbb{C}^2 \otimes \mathbb{C}^m \otimes \mathbb{C}^n$ using the theory of linear matrix pencils and determine generic state set for every dimension. In addition, we show that in order find a resource state capable of transforming to all generic states in $2 \times n \times m$ systems, one just needs to increase local dimension m or n by one. We also investigate optimal resource states, which can be transformed to any state (not excluding any zero-measure set) in the smaller-dimensional Hilbert space. In order to understand mathematical notation and derivations in this section, it is advisable to first read Subsection 2.4.3 from the preliminaries chapter about linear matrix pencils.

8.1 Introduction

Entanglement and especially multiparticle one, has drawn a lot of attention in recent years due to its potential application. Thus, having a better understanding of the phenomenon is one of the main objectives of quantum information theory. Due to its complexity an enormous amount of work has been already devoted to the quantification and qualification of multipartite entanglement. See Refs. [53, 155–157] for the overview. As a state of the art, bipartite entanglement is quite well understood, however, the same cannot be said for multipartite case.

One of the most common ways to get an insight into the structure of multiparticle entanglement, is to establish which of the states can be transformed to each other under local operations and classical communication (LOCC). It is straightforward that, if a state $|\psi\rangle$ can be used in

a certain application, then another state $|\phi\rangle$, which can be transformed to $|\psi\rangle$ under local operations and classical communication, is at least equally good for the same task. Therefore, it is of a great interest to investigate states which can reach other ones with LOCC. In fact, such transformations among pure states are fully characterized in the bipartite case [158]. For this simplest case the maximally entangled state has been identified, which can be transformed into any other state with LOCC. For multiparticle case there does not exist a single maximally entangled state in this spirit (recall that GHZ- and W-states from Chapter 2 are not even probabilistically inter-convertible with LOCC). Instead, one gets a whole set of the maximally entangled states, which has the property that any state outside of this set can be obtained via LOCC from one of the states within the set. Moreover, the set is minimal in the sense that no state inside the sets can be transformed to another. Such sets are very complicated and have been extensively investigated in sequences of publications [159–163] with the conclusion that in general *transformations among pure multipartite entangled states via LOCC are almost never possible* [163].

The results on LOCC transformability suggest the need to consider more general maps, invertible stochastic local operations and classical communication. These transformations divide state space into equivalence classes. Although it is possible to find only two such classes for three-qubit case, already for four qubits there are infinite number of SLOCC classes. The same holds for three-qutrit case and qubit-ququart-ququart case. So, even under the most general maps classification gets difficult.

In this chapter we look for *common resource states* not in the same Hilbert space as the states we would like to transform to, but instead we increase local dimensions and consider non-invertible general operations from higher to lower dimensional Hilbert spaces. More formally, we look for common resource states:

Definition 8.1. A common resource (CR) state for a set of states S is a state that can be transformed probabilistically to any state contained in S. A common resource state $|\psi\rangle$ is called *optimal* common resource state (OCR), if for any other common resource state $|\phi\rangle$ for S, it holds that either $|\phi\rangle$ can be probabilistically transformed to $|\psi\rangle$, or neither $|\psi\rangle$ nor $|\phi\rangle$ can be probabilistically transformed into the other.

We consider the case of $2 \times m \times n$ systems, where linear matrix pencils and their normal form can be used for SLOCC classification (see Chapter 2). The main question then is: Given a set of states, S in Hilbert space $\mathbb{C}^2 \otimes \mathbb{C}^m \otimes \mathbb{C}^n$, each representing different SLOCC class, what is the minimal dimension of the Hilbert space needed in order to find a state $|\psi\rangle$ in it, such that it can be transform to all the states in the set S.

Similar question was already considered before in Ref. [164]: It has been shown that a common resource state always exists, if one of the dimensions is increased sufficiently, in particular it has been shown that given a Hilbert space $\mathcal{H} = \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \otimes \cdots \otimes \mathbb{C}^{d_N}$, where $d_1 \leq d_2 \leq \cdots \leq d_N$, there exists a state which can be transformed to all the other states by LOCC if and only if

$$\prod_{i=1}^{N-1} d_i \leq d_N. \tag{8.1}$$

This result is strong since the common resource state maps to every state in the same- or lower-dimensional Hilbert spaces deterministically, thus the set S contained every state in $\mathcal{H}$. Here we wonder if better optimal bounds can be attained for more restricted set S using SLOCC operations.

8.2 SLOCC classes containing generic states

In this section we characterize a generic set of states in $2 \times m \times n$. In order to do so, we first introduce some lemmata concerning a necessary and sufficient condition for a matrix pencil to be a direct sum of right null-space blocks L_{ϵ_i} only, and a sufficient condition on the matrix pencil corresponding to a state such that the operation applied by the first party can be inverted by a transformation of second and third parties. We use these results for both, the characterization of generic sets of states and to prove that a generic state can always be transformed into any state in a full measure set of states of smaller dimension. Using then the characterization of generic matrix pencils presented in Ref. [165], we show that the union of SLOCC classes of states corresponding to a generic set of matrix pencils is of full measure (see Theorem 8.4). Interestingly, it turns out that this generic set of states (similarly to the generic set of matrix pencils) is characterized by $m - 3$ parameters in case $m = n$ and has no free parameter in case $m \neq n$.

From now on we employee notation for matrix pencils and its Kronecker canonical form (KCF) introduced in the preliminaries subsection 2.4.3. The following lemma plays an important role for subsequent proofs:

Lemma 8.2. *Let $\mathcal{P}(\mu, \lambda)$ denote a $m \times n$ matrix pencil, where $n > m$. Then the following two statements are equivalent.*

1. $D_m = 1$,
2. *$\mathcal{P}(\mu, \lambda)$ is strictly equivalent to a direct sum of right nullspace blocks L_{ϵ_i} only.*

In particular, for an $m \times (m+1)$ matrix pencil $\mathcal{P}(\mu, \lambda)$ we have $D_m = 1$ iff $\mathcal{P}(\mu, \lambda)$ is strictly equivalent to L_m.

Proof. If $\mathcal{P}(\mu, \lambda)$ is strictly equivalent to a direct sum of L_{ϵ_i} blocks, then it is straightforward to see that $D_m = 1$, as one of the m-minors equals μ^m and another one equals λ^m and their greatest common divisor is therefore 1. Let us now prove that the converse also holds. First note, that in case $D_m = 1$ there is no J block present in the pencil's KCF. To see this, note that the rank of the matrix pencil is m, which implies that $D_m = \mu^{e^\mu} \prod_{i, x_i \neq \infty} (x_i \mu + \lambda)^{e^i}$, which can only equal 1 if there exists no eigenvalue and hence no J block. One can also see this by considering the invariant polynomials. Let us assume that a J block is present, which implies that there exist eigenvalues, either finite or infinite. Recall that if this is the case, then there exists an invariant polynomial $E_k = \frac{D_k}{D_{k-1}} = \mu^{e^\mu_k} \prod_{i, x_i \neq \infty} (x_i \mu + \lambda)^{e^i_k} \neq 1$. As D_k divides D_m for all $k \leq m$ and we have at least one k for which $D_k \neq 1$, we also have that $D_m \neq 1$ which

contradicts the assumption that $D_m = 1$. This implies that there is no J block present. We hence have a direct sum of L_{ϵ_i} and $L_{\nu_i}^T$ blocks only. Due to dimensionality reasons, the number of L_{ϵ_i} blocks equals $n - m$ plus the number of $L_{\nu_i}^T$ blocks. We now have to show, however, that there cannot be any left nullspace blocks. Let us assume the contrary, i.e., there is at least one L_ν^T block present. We show that in this case all m-minors vanish implying $D_m = 0$, which contradicts $D_m = 1$. For computing any of the m-minors, there are at most ν vectors which are non-vanishing in the first $\nu + 1$ components. Hence, this $(\nu + 1)$-dimensional subspace can never be spanned by those vectors and thus, the minor vanishes. This completes the proof. The statement about $m \times (m + 1)$ matrix pencils follows immediately from the fact that if $n = m + 1$ there exists no other direct sum of right null space blocks which amounts to the required dimension. □

Note that from the structure of KCF of pencils it is clear that if a matrix contains only nullspace blocks, then Alice's invertible transformation can always be reversed by Bob and Charlie. Hence, $A \in GL_2$ there exist operators $B \in GL_m, C \in GL_n$ such that $A \otimes \mathbb{1} \otimes \mathbb{1}|\psi\rangle = \mathbb{1} \otimes B \otimes C|\psi\rangle$. This property resembles a property of bipartite states as for any bipartite state, $|\phi\rangle$, we have that for any operators A there exist operators B such that $A \otimes \mathbb{1}|\phi\rangle = \mathbb{1} \otimes B|\phi\rangle$.

In Ref. [165] a generic set of matrix pencils has been characterized. TO say otherwise, a set of matrix pencils $G = \{\mathcal{P}_i\}$ has been identified with the property that the union of the orbits of matrix pencils within this set, $\bigcup_i \mathcal{O}(\mathcal{P}_i)$ is of full measure, where $\mathcal{O}(\mathcal{P}_i) = \{B\mathcal{P}_i C^T$, with $B \in GL_m, C \in GL_n\}$. In $m \times m$ it is easy to verify that the set of matrix pencils with distinct eigenvalues is generic [166]. In $m \times n$, with $d = n - m \geq 1$, however, there is only one matrix pencil, whose orbit is generic. It is given by a direct sum of (at most two different) null-space blocks. More precisely, the following theorem has been proven in Ref. [165].

Theorem 8.3. *[165] A generic matrix pencil of dimension $m \times m$ corresponds to the matrix pencil with m distinct divisors. If $d = n - m \geq 1$, the generic matrix pencil is given by $\mathcal{P}(R, S) = (d - (m \bmod d))L_{\lfloor m/d \rfloor} \oplus (m \bmod d)L_{\lceil m/d \rceil}$, where $\lfloor . \rfloor$ ($\lceil . \rceil$) denotes the floor (ceiling) function, respectively.*

Let us mention here that in order to prove this result the codimension of the orbit, $\mathcal{O}(\mathcal{P})$ has been computed. See [165] and references therein. It is defined as the difference between the dimension of the whole space, i.e., $2mn$ (counting complex dimensions), and the dimension of the orbit, $\dim\{\mathcal{O}(\mathcal{P})\}$. It is evident that the codimension is minimal for $n = m$ if there are only distinct divisors (as for such a pencil the dimension of the symmetries, $S_\mathcal{P} = \{(B, C) : B\mathcal{P}C^T = \mathcal{P}\}$, is the smallest). However, in case $d = n - m \geq 1$, it has been shown that the codimension is minimal, in fact vanishes, iff the matrix pencil contains right null-space blocks only and the dimension of the null-space blocks are chosen equal to each other or, if this is not possible, the difference between the two different dimensions of nullspace blocks is at most 1.

We show that the union of SLOCC classes of states corresponding to a generic set of matrix pencils is of full measure. More precisely, we use the lemmata and the theorem above to prove there the following theorem.

Theorem 8.4. *The set of full rank states in $2 \times m \times n$ belonging to a SLOCC class with a representative whose corresponding matrix pencil is generic, is of full measure.*

Proof. The proof of the theorem is presented in the appendix of our paper [36]. The two cases, when $m = n$ and $m < n$ need individual treatment. □

Stated differently, we have that for $n = m$ a generic set of states is given by the union of SLOCC classes whose representatives are given by

$$|\Psi(x_1, \ldots, x_m)\rangle = |0\rangle(D_1 \otimes \mathbb{1})|\Phi_m^+\rangle + |1\rangle(\mathbb{1} \otimes \mathbb{1})|\Phi_m^+\rangle, \tag{8.2}$$

where $D_1 = \mathrm{diag}(x_1, \ldots, x_m)$, where $x_i \neq x_j$ for $i \neq j$. Note that not all states $|\Psi(x_1, \ldots, x_m)\rangle$ correspond to different SLOCC classes, as, e.g., the entries of D_1 could be sorted differently even via local unitaries. Moreover, as mentioned before, the eigenvalues of the matrix pencil, x_i can be altered by an operator applied by A. More precisely, three of the eigenvalues can be fixed, leading to the fact that the representatives constitute a $m - 3$ parameter family. For $n > m$ a generic set of states is given by the SLOCC class of a single state corresponding to the matrix pencil given in Theorem 8.3. For instance, in case $m = 7, n = 10$, the generic matrix pencil is $L_2 \oplus L_2 \oplus L_3$ and the representative of the generic SLOCC class is given by

$$\begin{aligned} |\Psi\rangle = |0\rangle(|01\rangle + |12\rangle + |24\rangle + |35\rangle + |47\rangle + |58\rangle + |69\rangle) \\ +|1\rangle(|00\rangle + |11\rangle + |23\rangle + |34\rangle + |46\rangle + |57\rangle + |68\rangle). \end{aligned} \tag{8.3}$$

For $n = m + 1$, i.e. $d = 1$ the generic matrix pencil is the single nullspace block, L_m. Hence, in this case the generic SLOCC class is represented by the state

$$|\Psi\rangle = |0\rangle \left(\sum_{i=1}^{m} |i-1, i\rangle \right) + |1\rangle|\Phi_m^+\rangle. \tag{8.4}$$

Note that there is only one generic SLOCC class in case $n \neq m$. However, there is a $(m-3)$–parameter family of SLOCC–classes in case $m = n$ whose union constitutes a generic set of states.

8.3 Common resource states for generic states

In this section we look for a common resource states. That means that we study possible transformations from e.g., $2 \times m \times n$ to $2 \times m \times (n-1)$. We show that a random state in $2 \times m \times n$ can be transformed into any state in a full measure set within $2 \times m \times (n-1)$ for any m, n and not only, a random state has a power to reach some other states in $2 \times m \times (n-1)$.

We first study transformations from a generic state in $2 \times m \times (m+1)$ to $2 \times m \times m$.

Lemma 8.5. *A $2 \times m \times (m+1)$ state $|\psi\rangle$ corresponding to the matrix pencil $\mathcal{P}_\psi = L_m$ is a common resoure state to any $2 \times m \times m$ state $|\phi\rangle$ corresponding to a matrix pencil with m distinct eigenvalues $x_1, \ldots, x_m$, i.e. $\mathcal{P}_\phi = \bigoplus_{i=1}^m J(x_i)$.*

Proof. We consider the matrix pencil consisting of a single L_m block and use Theorem 2.20 to prove the statement. Then there exist local non-invertible transformations which map L_m to the matrix pencil where the last column of L_m is added to the others with coefficients $-a_0, -a_1, \ldots, -a_{m-1} \in \mathbb{C}$ that we will choose later on. That is, there exist local operators accomplishing the transformation

$$L_m = \overset{\longleftarrow\quad m+1\quad\longrightarrow}{\begin{pmatrix} \lambda & \mu & \cdot & \cdot & \cdot & \cdot \\ \cdot & \lambda & \mu & \cdot & \cdot & \cdot \\ \cdot & \cdot & \lambda & \mu & \cdot & \cdot \\ \cdot & \cdot & \cdot & \ddots & \ddots & \cdot \\ \cdot & \cdot & \cdot & \cdot & \lambda & \mu \end{pmatrix}} \Bigg\updownarrow m \quad \longmapsto \tag{8.5}$$

$$\mathcal{P}_m = \overset{\longleftarrow\quad m\quad\longrightarrow}{\begin{pmatrix} \lambda & \mu & \cdot & \cdot & \cdot \\ \cdot & \ddots & \ddots & \cdot & \cdot \\ \cdot & \cdot & \lambda & \mu & \cdot \\ \cdot & \cdot & \cdot & \lambda & \mu \\ -a_0\mu & \cdots & \cdot & -a_{m-2}\mu & -a_{m-1}\mu + \lambda \end{pmatrix}} \Bigg\updownarrow m. \tag{8.6}$$

We calculate the KCF of the pencil $\mathcal{P}_m$. To determine the pencil's KCF, we first evaluate the greatest common divisor of its k-minors, D_k, for $1 \leq k \leq m$. First note that $D_k = 1$ for all $1 \leq k \leq m-1$. This can be seen as follows. Among the $(m-1)$-minors, there is one minor equal to λ^{m-1} and another one equal to μ^{m-1}. Hence, their greatest common divisor equals to 1 and therefore $D_{m-1} = 1$ which implies that $D_k = 1$ for all $1 \leq k \leq m-1$. The m-minor, however, equals the determinant of $\mathcal{P}$ which can be expressed as

$$D_m(\mu, \lambda) = \lambda^m + \sum_{i=0}^{m-1} (-1)^{m-i} a_i \mu^{m-i} \lambda^i. \tag{8.7}$$

As D_m is of degree m, there must exist m (not necessarily distinct) eigenvalues. Recall that this implies that the size of the J block equals $q \times q$ with $q = m$. Hence, the KCF of the matrix pencil contains no nullspace blocks, only the J block is present. Moreover, as $D_m(\mu = 0, \lambda) \neq 0$, all the eigenvalues are finite. Denoting the (here possibly non-distinct) eigenvalues as $x_1, \ldots, x_m$, D_m can, hence, be expressed as

$$D_m = (\mu x_1 + \lambda)(\mu x_2 + \lambda) \ldots (\mu x_m + \lambda). \tag{8.8}$$

The coefficients, $a_0, a_1, \ldots, a_{m-1}$, are thus given by

$$a_k = (-1)^{m-k}\Bigg(\sum_{\substack{i_1,i_2,\ldots,i_m\in\{0,1\}\\ \sum_{j=1}^{m} i_j=(m-k)}} x_1^{i_1} x_2^{i_2}\ldots x_m^{i_m}\Bigg), \tag{8.9}$$

which can be verified by comparing the coefficients of the polynomials in μ and λ in Eq. (8.7) and Eq. (8.8).

Let us denote by $\{\tilde{x}_i\}_i$ the set of distinct eigenvalues. Considering that $D_{m-1} = 1$ and therefore $E_k = 1$ for all $k \leq m-1$, the size signature corresponding to an eigenvalue $\tilde{x}_i$ is $s_i = (0, \ldots, 0, m_i)$, where m_i is the algebraic multiplicity of eigenvalue $\tilde{x}_i$. Hence the KCF of the matrix pencil is of the form

$$\mathcal{P}_{KCF} = \begin{pmatrix} \tilde{x}_1\mu+\lambda & \mu & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \ddots & \ddots & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \tilde{x}_1\mu+\lambda & \mu & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \tilde{x}_1\mu+\lambda & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \tilde{x}_2\mu+\lambda & \mu & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \ddots & \ddots \end{pmatrix} = \bigoplus_i J(\tilde{x}_i) = \bigoplus_i M^{m_i}(\tilde{x}_i), \tag{8.10}$$

where the size of $J(\tilde{x}_i)$ is $m_i \times m_i$.

In case the eigenvalues $x_1, x_2, \ldots, x_m \in \mathbb{C}$ are all distinct, the KCF is diagonal and one can easily determine the matrices B and C^T bringing the given matrix pencil to its KCF, i.e., $B\mathcal{P}C^T = \mathcal{P}_{KCF}$. In order to see that, note that the matrix pencil $\mathcal{P}$ is of the form $\lambda\mathbb{1} + \mu\mathcal{C}$, where $\mathcal{C}$ is the transpose of a so-called companion matrix [117]. We can hence use the Vandermonde matrix

$$V = \begin{pmatrix} 1 & x_1 & x_1^2 & \ldots & x_1^{m-1} \\ 1 & x_2 & x_2^2 & \ldots & x_2^{m-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_m & x_m^2 & \ldots & x_m^{m-1} \end{pmatrix} \tag{8.11}$$

to diagonalize $\mathcal{C}$ as $V\mathcal{C}^TV^{-1} = \mathrm{diag}(x_1, x_2, \ldots, x_m)$, where $\mathrm{diag}(x_1, x_2, \ldots, x_m)$ denotes a diagonal matrix with the entries $x_1, x_2, \ldots, x_m$ [117]. Hence, the matrices bringing $\mathcal{P}$ to its KCF are $B = {V^{-1}}^T$ and $C^T = V^T$. Note that if the eigenvalues, x_i, are degenerate then $\mathcal{C}$ is not diagonalizable. In this case a similarity transformation $\tilde{V}$ can be used, which transforms $\mathcal{C}$ to a block diagonal matrix, where each block is a Jordan block of size given by the algebraic multiplicity of the eigenvalues. Hence, the matrix pencil, $\lambda\mathbb{1} + \mu\mathcal{C}$, can be transformed with this similarity transformation $\tilde{V}$ to its KCF given in Eq. (8.10).

The discussion above tells us how to choose appropriate coefficients $a_0, \ldots, a_{m-1}$ to reach states that correspond to a pencil with finite eigenvalues, $x_1, x_2, \ldots, x_m$ and with a KCF given in Eq. (8.10). In particular, we can reach any state corresponding to a pencil with distinct, finite eigenvalues. Due to Theorem 2.19 infinite eigenvalues do not need to be considered, as the

corresponding states are always SLOCC equivalent to a state with finite eigenvalues. This completes the proof. □

From the proof above we can see that it is also possible to reach states whose corresponding pencils have non-distinct eigenvalues. As $D_{m-1} = 1$, however, the corresponding size signatures cannot be chosen freely, they are given by $s_i = (0, \ldots, 0, m_i)$, where m_i equals the algebraic multiplicity of eigenvalue x_i.

Let us now, conversely, start from an arbitrary state, $|\psi\rangle$, with local ranks $2 \times (m+1) \times (m+1)$ corresponding to a matrix pencil with $m+1$ distinct eigenvalues and consider transformations to states with local ranks $2 \times m \times (m+1)$. Here, we prove that a state $|\phi\rangle$ with $\mathcal{P}_\phi = L_m$ can be reached from any such state $|\psi\rangle$.

Lemma 8.6. *Any state $|\psi\rangle$ in $2 \times (m+1) \times (m+1)$ corresponding to a $(m+1) \times (m+1)$ matrix pencil $\mathcal{P}_\psi$ with $m+1$ distinct eigenvalues can be transformed via local operations to the $2 \times m \times (m+1)$ state $|\phi\rangle$ corresponding to a matrix pencil that consists of one single L_m block, i.e., $\mathcal{P}_\phi = L_m$.*

Proof. Let us denote the eigenvalues of $\mathcal{P}_\psi$ as $x_1, x_2, \ldots, x_m$. Due to Theorem 2.20, there exists a non-invertible matrix B which, applied to $|\psi\rangle$, transforms $|\psi\rangle$ to a state whose corresponding matrix pencil, $\mathcal{P}'$, can be obtained by erasing the first row of the initial pencil after adding it to the other rows with coefficients $a_2, a_3, \ldots, a_{m+1}$. We will prove that the resulting matrix pencil, $\mathcal{P}'$, is strictly equivalent to $\mathcal{P}_\phi = L_m$ for some choice of the coefficients $a_2, a_3, \ldots, a_{m+1}$. The explicit pencils read

$$\mathcal{P}_\psi = \begin{pmatrix} \mu x_1 + \lambda & 0 & \cdot & \cdot \\ \cdot & \mu x_2 + \lambda & \ddots & \cdot \\ \cdot & \cdot & \ddots & 0 \\ \cdot & \cdot & \cdot & \mu x_{m+1} + \lambda \end{pmatrix} \text{ and} \tag{8.12}$$

$$\mathcal{P}' = \overbrace{\begin{pmatrix} a_2(\mu x_1 + \lambda) & \mu x_2 + \lambda & \cdot & \cdot & \cdot \\ a_3(\mu x_1 + \lambda) & \cdot & \mu x_3 + \lambda & \cdot & \cdot \\ \vdots & \cdot & \cdot & \ddots & \cdot \\ a_{m+1}(\mu x_1 + \lambda) & \cdot & \cdot & \cdot & \mu x_{m+1} + \lambda \end{pmatrix}}^{m+1} \Bigg\} m. \tag{8.13}$$

It is straightforward to see that D_m of $\mathcal{P}'$ is given by

$$\begin{aligned} D_m = \quad & \gcd\{(\mu x_2+\lambda)(\mu x_3+\lambda)\cdots(\mu x_{m+1}+\lambda), \\ & -a_2(\mu x_1+\lambda)(\mu x_3+\lambda)\cdots(\mu x_{m+1}+\lambda), \\ & a_3(\mu x_1+\lambda)(\mu x_2+\lambda)(\mu x_4+\lambda)\cdots(\mu x_{m+1}+\lambda), \\ & \vdots \\ & (-1)^m a_{m+1}(\mu x_1+\lambda)(\mu x_2+\lambda)\cdots(\mu x_m+\lambda)\} \\ = \quad & \gcd\{(-1)^{j+1}a_j \prod_{i=1, i\neq j}^{m+1}(\mu x_i+\lambda) \quad | \quad j=1,\ldots,(m+1)\} = 1, \end{aligned} \tag{8.14}$$

where $a_1 = 1$. Note that the last equality holds iff none of the coefficients a_i vanish. This is in fact the only requirement we impose on the choice of coefficients. Using Lemma 8.2 it follows that $\mathcal{P}'$ is strictly equivalent to L_m, which proves the statement. □

Using the lemmata above, we are now in the position to prove one of the main results of this chapter, namely that a generic state in $2\times m\times n$ can be transformed to any state in the generic set of states in $2\times m\times(n-1)$, as stated in the following theorem.

Theorem 8.7. *Any generic state $|\psi\rangle$ in $2\times m\times n$ can be transformed to any generic state $|\phi\rangle$ in $2\times m\times(n-1)$.*

In order to prove this theorem, we make use of the following lemma, which is actually more general than needed for the proof of the theorem above.

Lemma 8.8. *A state $|\psi\rangle$ in $2\times m\times n$ with $\mathcal{P}_\psi = \bigoplus_{i=1}^{n-m} L_{\epsilon_i}$ can be transformed to a state $|\phi\rangle$ in $2\times m\times(n-1)$ with $\mathcal{P}_\phi = \bigoplus_{i=1}^{n-m-1} L_{\epsilon'_i}$ via local operations for any $n \geq m+2$ if the following condition holds. There exists $j\in\{1,\ldots,n-m-1\}$ such that for all $i\in\{1,\ldots,j-1\}$ $\epsilon_i = \epsilon'_i$ and for all $i\in\{j,\ldots,n-m-1\}$ $\epsilon_{i+1}\leq\epsilon'_i$, where we assume $(\epsilon_i)_i$ and $(\epsilon'_i)_i$ to be sorted in ascending order.*

The proof of this lemma can be found in Appendix D. Let us now use it to prove Theorem 8.7.

Proof of Theorem 8.7. Let us write $d = n-m$, where $d\geq 0$. The cases $d=0$ and $d=1$ were discussed and proven above in Lemma 8.6 and Lemma 8.5, respectively. Let us now prove the statement for the case $d\geq 2$. To this end, we consider the matrix pencils $\mathcal{P}_\psi$ and $\mathcal{P}_\phi$ corresponding to the states $|\psi\rangle$ and $|\phi\rangle$ which we assume w.l.o.g. to be in SKCF. As shown in Theorem 8.4, the matrix pencils corresponding to generic states are given by $\mathcal{P}_\psi = (d-(m \bmod d))L_{\lfloor m/d\rfloor}\oplus(m \bmod d)L_{\lceil m/d\rceil}$ and $\mathcal{P}_\phi = (d-1-(m \bmod (d-1)))L_{\lfloor m/(d-1)\rfloor}\oplus(m \bmod (d-1))L_{\lceil m/(d-1)\rceil}$. Note that the matrix pencils contain only L_{ϵ_i} blocks. More precisely, $\epsilon_1=\ldots=\epsilon_{(d-(m \bmod d))}=\lfloor m/d\rfloor$, and if $m \bmod d\neq 0$, $\epsilon_{(d-(m \bmod d)+1)}=\ldots=\epsilon_d=\lceil m/d\rceil$ for $\mathcal{P}_\psi$ and $\epsilon'_1=\ldots=\epsilon'_{(d-1-(m \bmod (d-1)))}=\lfloor m/(d-1)\rfloor$, and if $m \bmod (d-1)\neq 0$, $\epsilon'_{(d-1-(m \bmod (d-1))+1)}=\ldots=\epsilon'_{(d-1)}=\lceil m/(d-1)\rceil$ for $\mathcal{P}_\phi$. Hence, the sizes of the blocks are distributed in such a way that Lemma 8.8 applies proving that $|\psi\rangle$ can be transformed to $|\phi\rangle$, which completes the proof. □

8.4 Common resource states for all states

In the previous section we showed that any generic state in $2 \times m \times (n+1)$ can be transformed probabilistically to any generic state in $2 \times m \times n$. Stated differently, it is sufficient to increase n only by one in order to find a generic state that can be transformed to every generic state in a lower dimensional Hilbert space.

In this section, we extend our result. In particular, we look for common resource states for S containing all states in $\mathcal{H} = \mathbb{C}^2 \times \mathbb{C}^m \times \mathbb{C}^n$ for fixed m and n, i.e., where in addition to the generic set of states also sets of measure zero are included. In the following, we show that in contrast to common resources for a generic set of states, the increase of dimension by one is not sufficient to find common resource states for the full set of states.

To find such common resource states, we consider an increase of the highest dimension, n, i.e., we look for common resource states in $\mathbb{C}^2 \times \mathbb{C}^m \times \mathbb{C}^{\tilde{n}}$, where $\tilde{n} > n$. Due to the bound in Eq. 8.1, it is clear that a common resource state exists in case $\tilde{n} = 2m$. However, the question we address here is whether we can find a common resource state for which $\tilde{n} < 2m$. Again, a difference between the two cases $m = n$ and $m \neq n$ becomes apparent. In the following theorems, we prove that in case $m = n$ such a common resource state exists for $\tilde{n} = 2m - 2$. Moreover, this increase of dimension (of the third system) is optimal. In contrast to that, in case $m \neq n$, the teleportation bound is tight, i.e., there exists no common resource state whenever $\tilde{n} < 2m$.

The following $m \times (m-2)$ matrix pencil will be of relevance throughout the remainder of this section,

$$\mathcal{P}_\psi = (m-3)L_1 \oplus L_2 \oplus M^1(0). \tag{8.15}$$

The reason for that is that this pencil corresponds to the $2 \times m \times (2m-2)$ state $|\psi\rangle$, which turns out to be a common resource for all $2 \times m \times m$ states, which we will show in the following theorem.

Theorem 8.9. *The $2 \times m \times (2m-2)$ state $|\psi\rangle$ that corresponds to the matrix pencil given in Eq. (8.15) is a common resource for $2 \times m \times m$ states, where $m \geq 4$, i.e., $|\psi\rangle$ can be transformed to any $2 \times m \times m$ state via non-invertible SLOCC.*

Proof. Although we could directly prove the statement considering the matrix pencil given in Eq. (8.15), we prove this theorem in three steps for readability. First, we explicitly give a $2 \times m \times 2m$ state which reaches all $2 \times m \times m$ states. Based on this state, we then construct a $2 \times m \times (2m-1)$ state which can be used for the same task. Finally, we argue that the dimension can be reduced by one more by showing that the $2 \times m \times (2m-2)$ corresponding to the matrix pencil $\mathcal{P}_\psi$ given in Eq. (8.15) is a common resource for all $2 \times m \times m$ states.

A common resource $|\psi\rangle$ for $2 \times m \times m$ states can be trivially found in $2 \times m \times 2m$, namely $|\phi_2^+\rangle_{AC} \otimes |\phi_m^+\rangle_{BC}$. Associating $|0\rangle_C \otimes |i\rangle_C$ to $|i\rangle_C$ and $|1\rangle_C \otimes |i\rangle_C$ to $|m+i\rangle_C$, the corresponding

matrix pencil is

$$\mathcal{P}_\psi = \begin{pmatrix} \mu & \cdot & \cdot & \lambda & \cdot & \cdot \\ \cdot & \ddots & \cdot & \cdot & \ddots & \cdot \\ \cdot & \cdot & \mu & \cdot & \cdot & \lambda \end{pmatrix}, \tag{8.16}$$

which is strictly equivalent to its KCF equal to mL_1.

We present now an alternative proof of this statement by considering the corresponding matrix pencils. We show that given the matrix pencil $\mathcal{P}_\psi = mL_1$, any $m \times m$ matrix pencil $\mathcal{P}_\phi$ can be obtained applying Theorem 2.20 m times consecutively. In particular, we explicitly show that the L_1 blocks in $\mathcal{P}_\psi$ can be combined in such a way that arbitrary blocks, L, L^T, and J can be created for $\mathcal{P}_\phi$. Furthermore, we count the number of required L_1 blocks and see that m of them present in $\mathcal{P}_\psi$ suffice.

First note that L_2 can be obtained by adding the first column of some L_1 to the last column of another L_1 block and discarding this column afterwards. This procedure can be iterated to generate L_ϵ, consuming ϵ L_1 blocks. An L_ν^T block can be generated by first generating $L_{\nu+1}$ and then discarding the first and the last column of $L_{\nu+1}$. This procedure consumes $(\nu+1)$ of the L_1 blocks in total. As the matrix pencil $\mathcal{P}_\phi$ is square, we have that the number of L blocks equals the number of L^T blocks in $\mathcal{P}_\phi$. Let us assume w.l.o.g. that the matrix pencil $\mathcal{P}_\phi$ consists of null-space blocks of total dimension $k \times k$, where $k = \sum_{i=1}^a \epsilon_i + \sum_{i=1}^a (\nu_i + 1)$ and of a J block of size $(m-k) \times (m-k)$. As explained above, the null-space blocks can be created by consuming k of the L_1 blocks of $\mathcal{P}_\psi$. We will now show that the $(m-k)$ remaining L_1 blocks can be used to create an arbitrary J block. First note, that due to dimensionality reasons, the size signatures of the eigenvalues sum up to $(m-k)$. An arbitrary finite eigenvalue x_i (infinite eigenvalue) with size signature 1 can be created consuming a single L_1 block by adding the second column to the first one with coefficient x_i and discarding the second column afterwards (discarding the first column), respectively. Moreover, an existing $M^{e_j^i}(x_i)$ block can be enlarged to $M^{e_j^i+1}(x_i)$ consuming a single L_1 block arranged to the upper left, i.e., $L_1 \oplus M^{e_j^i}(x_i)$. To this end, the second column of L_1 is added to the first column of the existing $M^{e_j^i}(x_i)$ block before it is added to the first column of the L_1 block with coefficient x_i and discarded afterwards. Similarly, an $N^{e_j^\mu}$ block can be enlarged. Thus, in total $m-k$ L_1 blocks are consumed in order to create an arbitrary J block of size $(m-k) \times (m-k)$. Hence, $\mathcal{P}_\psi = mL_1$ can be transformed to an arbitrary $m \times m$ matrix pencil and thus, the $2 \times m \times 2m$ state $|\psi\rangle$ can be transformed to any $2 \times m \times m$ state.

Let us now show that the $2 \times m \times (2m-1)$ state $|\psi\rangle$, whose corresponding matrix pencil is

$$\mathcal{P}_\psi = (m-1)L_1 \oplus M^1(0), \tag{8.17}$$

can perform the same task. Note that the first $(m-1)$ L_1 blocks are the same as before. However, the last L_1 block is replaced by $M^1(0)$. We will distinguish the two cases that $\mathcal{P}_\phi$ has eigenvalues and that $\mathcal{P}_\phi$ has no eigenvalues. In both cases we show that $\mathcal{P}_\psi$ given in Eq. (8.17) can be transformed into $\mathcal{P}_\phi$. In the first case, as a first step, Alice's action is used to transform the eigenvalue o present in $\mathcal{P}_\psi$ to some eigenvalue x that is present in $\mathcal{P}_\phi$. From this point on,

the same procedure as described above is used to increase the size signature of the eigenvalue x or to obtain the remaining blocks present in $\mathcal{P}_\phi$. In the second case, the pencil $\mathcal{P}_\phi$ does not contain a J block, hence it is a direct sum of L and L^T blocks only. Due to dimensionality reasons, at least one L^T block is present in $\mathcal{P}_\phi$. It is easy to see that in this case, the $M^1(0)$ block in $\mathcal{P}_\psi$, can be used together with ν L_1 blocks to obtain L_ν^T by first using the ν L_1 blocks to create L_ν as described above and finally adding the $M^1(0)$ block below the last column of the created L_ν bock and discarding the first column of this block. From this point on, the procedure described in the $2 \times m \times 2m$ scenario can be used in order to obtain the remaining blocks present in $\mathcal{P}_\phi$.

Let us now show that we can further reduce the dimension by one by considering the $2 \times m \times (2m-2)$ state $|\psi\rangle$, whose corresponding matrix pencil $\mathcal{P}_\psi$ is given in Eq. (8.15). As it is more involved to see that $|\psi\rangle$ is indeed a common resource to all $2 \times m \times m$ states and, thus, the theorem holds, we will consider the following three classes of matrix pencils separately. Note that each matrix pencil $\mathcal{P}_\phi$ belongs to at least one of these classes,

(i) There is at least one L_ϵ block with $\epsilon \geq 2$ present in $\mathcal{P}_\phi$,

(ii) There is at least one L_1 block present in $\mathcal{P}_\phi$,

(iii) There is no L block present in $\mathcal{P}_\phi$.

Let us first deal with case (i). In that case, the block L_2 together with $\epsilon - 2$ L_1 blocks in $\mathcal{P}_\psi$ can be used to create the block L_ϵ as explained above. Due to dimensionality reasons, there exists also a L_ν^T in $\mathcal{P}_\phi$ and we can use the $M^1(0)$ block together with ν L_1 blocks to create it. We are left with $m - 3 - (\epsilon - 2) - \nu$ L_1 blocks which are used to create the remaining arbitrary $[m - (\epsilon + \nu + 1)] \times [m - (\epsilon + \nu + 1)]$ sized matrix pencil, as explained above. Let us now consider case (ii). We keep one of the L_1 blocks in $\mathcal{P}_\psi$ unchanged, as this block is also present in $\mathcal{P}_\phi$. Again, due to dimensionality reasons, there exists a L_ν^T block in $\mathcal{P}_\phi$, which can be created using L_2 together with $\nu - 1$ L_1 blocks. We are left with $m - 3 - \nu$ L_1 blocks and the $M^1(0)$ block which are used to create the remaining arbitrary $[m - (2 + \nu)] \times [m - (2 + \nu)]$ sized matrix pencil, as explained above in the $[2 \times m \times (2m-1)]$ scenario. In the remaining case, case (iii), no L block and hence (as $\mathcal{P}_\phi$ is square) also no L^T block is present in $\mathcal{P}_\phi$, i.e., it only remains to be shown that $\mathcal{P}_\psi$ can be used to reach an arbitrary J block of size $m \times m$. Due to Theorem 2.19, we only have to consider finite eigenvalues. Let us show that with one exception (we elaborate on that below), $\mathcal{P}_\psi$ can indeed be used to reach an arbitrary J block of size $m \times m$. First, Alice can transform $M^1(0)$ to $M^1(x)$ for an arbitrary x. The L_2 block can either be used to create $M^2(x)$ or $M^1(x_1) \oplus M^1(x_2)$, where $x_1 \neq x_2$ as proven in Lemma 8.5 and right below it. Together with $M^1(0)$, L_2 can also be used to create $M^3(x)$. As explained above, the remaining L_1 blocks can be used to create the remaining part of the J block by either creating new $M^1(x)$ blocks, or by increasing the size signature of existing ones. Let us note here, that with the method explained here, it is possible to reach any J, except pencils of the form $\mathcal{P}_\phi = mM^1(x)$. The reason for that is that L_2 cannot be used to create $M^1(x) \oplus M^1(x)$. However, this is not a problem as this matrix pencil corresponds to a state where Alice is not entangled with the other parties. This completes the proof. □

Let us remark here that Theorem 8.9 does not hold for $m = 3$, as $\begin{pmatrix} \lambda & \mu & \cdot & \cdot \\ \cdot & \lambda & \mu & \cdot \\ \cdot & \cdot & \cdot & \lambda \end{pmatrix}$ can be used to reach any 3×3 matrix pencil except $\begin{pmatrix} \lambda & \mu & \cdot \\ \cdot & \cdot & \mu \\ \cdot & \cdot & \lambda \end{pmatrix}$. Moreover, no other $2 \times 3 \times 4$ state is a common resource for $2 \times 3 \times 3$, which can be easily verified by considering the full SLOCC hierarchy up to $2 \times 3 \times 6$ states which has been derived in Ref. [114, 116]. A common resource for $2 \times 3 \times 3$ states can be found in $\mathbb{C}^2 \otimes \mathbb{C}^3 \otimes \mathbb{C}^5$ instead. For example, the $2 \times 3 \times 5$ state corresponding to the matrix pencil $\begin{pmatrix} \lambda & \mu & \cdot & \cdot & \cdot \\ \cdot & \cdot & \lambda & \mu & \cdot \\ \cdot & \cdot & \cdot & \cdot & \lambda \end{pmatrix}$ can be used to reach any $2 \times 3 \times 3$ state.

We are going to show next that the resource state introduced in Theorem 8.9 is an optimal resource for $\mathbb{C}^2 \otimes \mathbb{C}^m \otimes \mathbb{C}^m$ states.

Theorem 8.10. *The common resource state given in Theorem 8.9 is optimal, i.e., no common resource state which reaches any $2 \times m \times m$ state for $m \geq 4$ exists in $\mathbb{C}^2 \otimes \mathbb{C}^m \otimes \mathbb{C}^{2m-3}$ or lower dimensions.*

Proof. The proof of this theorem is presented in our paper in Ref. [36]. □

Finally, we consider the optimal common resource state for $2 \times m \times n$ states where $n > m$. We see that in contrast to the $2 \times m \times m$ scenario, where we found an optimal resource state in $\mathbb{C}^2 \otimes \mathbb{C}^m \otimes \mathbb{C}^{2m-2}$, here, the trivial $2 \times m \times 2m$ state that can be used to perform teleportation is optimal. In other words, no common resource for $2 \times m \times n$ states exists in $\mathbb{C}^2 \otimes \mathbb{C}^m \otimes \mathbb{C}^{2m-1}$ or lower dimensions.

Theorem 8.11. *A common resource state which reaches any $2 \times m \times n$ state for $m \geq 2$, $n > m$ exists in $\mathbb{C}^2 \otimes \mathbb{C}^m \otimes \mathbb{C}^{2m}$. It is optimal, i.e., no common resource exists in $\mathbb{C}^2 \otimes \mathbb{C}^m \otimes \mathbb{C}^{2m-1}$ or lower dimensions.*

Proof. The complete proof of this theorem is presented in our paper in Ref. [36]. The main idea is that we consider the set of matrix pencils $\mathcal{P}_\psi$ corresponding to $2 \times m \times (2m-1)$ states $|\psi\rangle$ and prove the statement in two steps. First, we show that a common resource $\mathcal{P}_\psi$ may not contain a divisor block. Due to dimensionality reasons, only one candidate remains, which we prove not to be a common resource in the second step. □

8.5 Summary and outlook

In conclusion, we have investigated the hierarchy of pure quantum states representing SLOCC classes in $2 \times m \times n$-systems. We used matrix pencils and their Kronecker canonical form to identify SLOCC classes and to study most general non-invertible transformations between

them [114]. This allowed us to find and parametrize generic SLOCC classes in every dimension and to find possible non-invertible transformations between them. Moreover, we identified resource states in higher dimensions, which can be used to probabilistically generate all possible (including zero measure sets) SLOCC classes in a lower dimensional system. These results lead to a coarse graining of SLOCC classes. The identification of such resource states is also relevant from the point of view of state discrimination as will be explained in the following. It has been shown that if a state $|\Phi\rangle$ on a multipartite high-dimensional system is a resource state for all states in a lower-dimensional multipartite system, then its complex conjugate $|\Phi^*\rangle$ is a universal resource for unambiguous state discrimination in the lower-dimensional system [167]. More precisely, any state out of a fixed set of linearly independent states $\{|\psi_i\rangle\}$ in the low-dimensional system can be correctly identified with non-vanishing probability of success (and a fail to do so can be detected), if the parties share in addition the resource $|\Phi^*\rangle$.

There are several directions in which our work may be generalized. First, it may be useful to find new witnesses or polynomial invariants characterizing the SLOCC classes [168–170]. These invariants can be used to construct entanglement measures such as the so-called three-tangle. Moreover, it would be appealing to use the results obtained here to gain more insight into the entanglement properties of three-partite systems. Apart from the relation among the SLOCC classes which is induced via the hierarchy studied here, a more detailed investigation of entanglement seems possible. In particular, it would be desirable to study the derived resource states further and to understand their entanglement properties better. Furthermore, for some of the considered SLOCC classes it might prove promising to study LOCC transformations within them, as the symmetries of states in those classes indicate that the structure of possible LOCC transformations lies somewhere between the very simple bipartite LOCC structure and truly multipartite LOCC structure. Finally, it would be very interesting to go beyond the somehow artificial restriction of $2 \times m \times n$-dimensional systems and consider general three-partite systems. This, however, probably requires a significant extension of the present theory of matrix pencils.

Chapter 9

Entanglement detection with two observables

Detecting entanglement in experiments is crucial in many areas of quantum information and accordingly various different techniques for constructing witnesses have been derived. In this chapter we are interested how the knowledge of the expectation value of another observable can help improve entanglement detection. We tackle the problem with the method of Legendre transformation, leading even to entanglement quantification. We focus on two product observables and for low dimensions give the necessary and sufficient criteria for entanglement detection.

9.1 Introduction

Entanglement witnesses are the most convenient tools to certify entanglement in experiments. See Chapter 2 for basic introduction. Any entanglement witness can be represented as follows:

$$W = g_s \mathbb{1} - L, \tag{9.1}$$

where L is a measured observable and the value of g_s is given by

$$g_s = \sup_{\sigma} \{ \mathrm{tr}\,(\sigma L) | \sigma \in S_{sep} \}, \tag{9.2}$$

where the optimization can be performed over pure product states.

We go a step further and consider, in addition to $l = \langle L \rangle$, the expectation value $c = \langle C \rangle$ of a second observable C. Under which conditions on L and C can we benefit from such extra knowledge? To give an example, if an observable C is a scalar multiple of an observable L, then, trivially, entanglement detection cannot be improved with such an additional knowledge. More generally, from the knowledge of the expectation value of two observables, one

determines the expectation value of a composite observable $X = \alpha C + \beta L$, where $\alpha, \beta \in \mathbb{C}$. Then the new witness operator depends on α and β and can be expressed as

$$W(\alpha, \beta) = g_s(\alpha, \beta)\mathbb{1} - X. \tag{9.3}$$

Since the separable state space is convex, it follows that if the knowledge of $l = \langle L \rangle$ and $c = \langle C \rangle$ can be used to certify entanglement of some state, then the witness $W(\alpha, \beta)$ can also detect this state for some α and β.

Similar problem, so called, *ultrafine entanglement witnessing* (UEW) was addressed in recent few publications [171–173], but with a different approach. Given an entanglement witness as in Eq. (9.1), one tries to evaluate how the value of g_s changes if the states must satisfy another hyperplane constraint $c = \langle C \rangle$:

$$g_s = \sup_{\sigma} \{ \mathrm{tr}\,(\sigma L) | \sigma \in S_{sep} \text{ and } \mathrm{tr}\,(\sigma C) = c \}. \tag{9.4}$$

It turns out that this problem is more involving as the optimization over pure product states is no longer sufficient [37, 172]. Instead one has to work with rank-two mixed states.

In our work we focus on the witnesses of the type presented in Eq. (9.3). We study a bipartite case and consider the observables which are of the product form: $L = L_A \otimes L_B$ and $C = C_A \otimes C_B$. We analyze entanglement detection using Legendre transformations. The approach itself is not new [174, 175], but it helps to derive analytic results useful to understand the structure of such composite witnesses. Finally, we derive conditions that L and C shall fulfill in order to be able to detect entanglement.

9.2 Formulation with Legendre transformation

In this section using Legendre transformations we want to find a lower bound on the value of some entanglement measure $E(\varrho)$ of the state ϱ knowing the two expectation values $c = \mathrm{tr}\,\{(\varrho C)\}$ and $l = \mathrm{tr}\,\{(\varrho L)\}$ of the observables C and L. That is, we need to compute the minimal value of $E(\varrho)$ over all states compatible with the observed quantities,

$$\varepsilon(c, l) = \inf_{\varrho} \{ E(\varrho) \,|\, \mathrm{tr}\,\{(\varrho C)\} = c \text{ and } \mathrm{tr}\,\{(\varrho L)\} = l \}. \tag{9.5}$$

For the convex entanglement measure $E(\varrho)$, this is a convex function in c and l and, hence, it can be characterized as the supremum over all affine functions below it. Therefore, given c and l, we would like to find the smallest constant $k \in \mathbb{R}$, such that

$$\varepsilon(c, l) \geq \alpha c + \beta l - k \tag{9.6}$$

for arbitrary α and $\beta \in \mathbb{R}$. Rewriting Eq. (9.6), we obtain

$$\begin{aligned} k := \hat{E}(X) &= \sup_{c,l} \{\alpha c + \beta l - \varepsilon(c,l)\} \\ &= \sup_{\varrho} \{\alpha \mathrm{tr}\{(\varrho C)\} + \beta \mathrm{tr}\{(\varrho L)\} - E(\varrho)\}, \end{aligned} \tag{9.7}$$

which is the definition of $\hat{E}$ as the Legendre transform of the entanglement measure E, evaluated for the operator

$$X = \alpha C + \beta L. \tag{9.8}$$

We can use the value of k itself to obtain the supremum over all slopes α and β:

$$\varepsilon(c,l) = \sup_{\alpha,\beta} \{\alpha c + \beta l - \hat{E}(X)\}. \tag{9.9}$$

This on the other hand is a Legendre transform of $\hat{E}(X)$ and as seen before corresponds to a lower bound on the entanglement measure $E(\varrho)$ compatible with the values c and l. From convex geometry one can see that this lower bound is tight, since there exists a state with the values c and l having the entanglement $E(\varrho) = \varepsilon(c,l)$. Also, one shall note the practical difference between Eq. (9.7) and Eq. (9.9): For obtaining a valid lower bound on $E(\varrho)$ one needs the global optimum in the maximization in Eq. (9.7). In Eq. (9.9), however, any pair of values α, β gives a valid lower bound.

Whether one can analytically evaluate Eqs. (9.7, 9.9) depends on the entanglement measure E and the specific form of observables. For measures defined via the convex roof construction,

$$E(\varrho) = \inf_{p_i, |\psi_i\rangle} \sum_i p_i E(|\psi_i\rangle), \tag{9.10}$$

with $\varrho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$, the Legendre transform can be evaluated by optimizing over pure states only [174]:

$$E(X) = \sup_{|\psi\rangle} \{\langle\psi|X|\psi\rangle - E(|\psi\rangle)\}. \tag{9.11}$$

Here, we concentrate on the geometric measure of entanglement E_G [55] defined for pure states as in Eq. (2.16) and for mixed states via a convex roof construction. Thus, we need to evaluate

$$E_G(X) = \sup_{|\psi\rangle} \sup_{|\phi\rangle = |a\rangle|b\rangle|c\rangle \ldots} \{\langle\psi|(X + |\phi\rangle\langle\phi|)|\psi\rangle - 1\}. \tag{9.12}$$

This optimization can be done in practice numerically in an efficient manner [174]. Here, however, we consider a specific case of X where analytical derivations are possible.

Example 9.1. *We choose as observables*

$$C = \sigma_z \otimes \sigma_z, \quad L = \sigma_x \otimes \sigma_x. \tag{9.13}$$

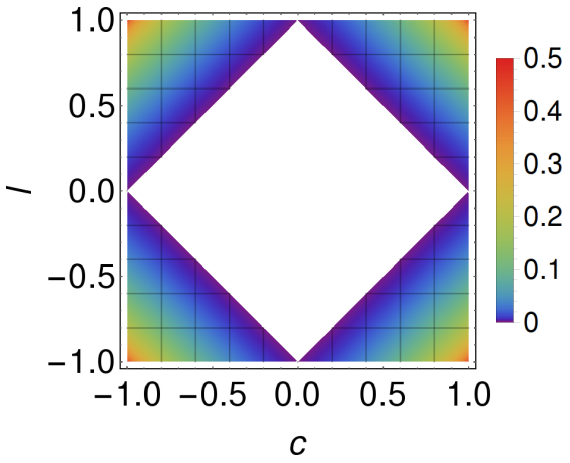


FIGURE 9.1: Lower bounds on the geometric measure of entanglement based on the expectation values $c = \mathrm{tr}(\varrho\sigma_z \otimes \sigma_z)$ and $l = \mathrm{tr}(\varrho\sigma_x \otimes \sigma_x)$. The white inner region corresponds to separable states.

The operator X accordingly is then diagonal in the Bell basis with eigenvalues $(\alpha+\beta, \alpha-\beta, -\alpha+\beta, -\alpha-\beta)$. For such operators, the Legendre transformation of the geometric measure is given by [92]

$$E_G(X) = \frac{\lambda_1 + \lambda_2 - 1}{2} + \frac{1}{2}\sqrt{(\lambda_1 - \lambda_2)^2 + 1}, \tag{9.14}$$

where λ_1 denotes the largest, and λ_2 denotes the second-largest eigenvalue of X. Note that the formula in Ref. [174] is formulated as an upper bound on the Legendre transform, but for the special case of two-qubit Bell states equality holds. This is due to the fact that for any pair of Bell states we can find a product vector having an overlap of $1/2$ with both. Finally, it should be added that Eq. (28) in Ref. [92] contains a typo.

For $c = \mathrm{tr}\{(\varrho C)\}$ and $l = \mathrm{tr}\{(\varrho L)\}$ we can assume without loss of generality that $c \geq l \geq 0$, as this can be achieved for the given observables by local unitary transformations that do not alter the entanglement. In addition, we have $c \leq 1$. It is easy to see that the higher the values of c and l, the more entangled the state is. From this it follows that in Eq. (9.9) the interesting case is if α and β both have positive values.

We have to distinguish between two cases, $\alpha \geq \beta \geq 0$ and $\beta \geq \alpha \geq 0$. First, assume that $\alpha \geq \beta \geq 0$, then

$$\varepsilon(c,l) = \sup_{\alpha,\beta}\left[\alpha(l-1) + \frac{1}{2} + \beta c - \sqrt{\beta^2 + \frac{1}{4}}\right]. \tag{9.15}$$

Taking the partial derivative with respect to α we obtain $\partial_\alpha \varepsilon(c,l) = (l-1) \leq 0$, therefore α must be chosen as small as possible, i.e., $\alpha = \beta$. Inserting this and taking the partial derivative with respect to β we find

$$\partial_\beta \varepsilon(c,l) = (c+l-1) - \frac{\beta}{\sqrt{\beta^2 + \frac{1}{4}}} \stackrel{!}{=} 0, \tag{9.16}$$

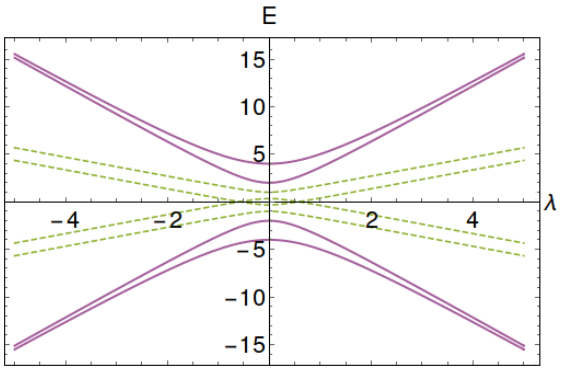


FIGURE 9.2: Eigenvalues of the qubit-ququart operator $X = C + \lambda L$ for different values of λ [see Eqs. (9.19, 9.20)]. This gives a counterexample for the qubit-ququart case.

and consequently $\beta = (c + l - 1)/[2\sqrt{1 - (c + l - 1)^2}]$. *This yields the final result:*

$$E_G \geq \varepsilon(c, l) = \frac{1}{2}\left(1 - \sqrt{1 - (c + l - 1)^2}\right). \tag{9.17}$$

Considering the second case, $\beta \geq \alpha \geq 0$, *the second largest eigenvalue changes from* $\alpha - \beta$ *to* $\beta - \alpha$. *The function to maximize is essentially the same as before, but with* α *and* β *swapped. Therefore, the solution is the same and Eq. (9.17) also holds. The corresponding bounds on the geometric measure are depicted in Fig. 9.1.*

9.3 Criterion for various scenarios

In this section we give a brief overview of the qualitative results on the conditions that the C and L must be satisfying in order to detect entanglement. The proofs and derivations for all the subsequent statements can be found in our paper [37].

Theorem 9.1. *Consider a two-qubit system and product operators* $C = C_A \otimes C_B$ *and* $L = L_A \otimes L_B$. *Then C and B can be used for entanglement detection, if and only if*

$$[C_A, L_A] \neq 0 \quad \textit{and} \quad [C_B, L_B] \neq 0. \tag{9.18}$$

In the proof of the previous theorem perturbation theory was employed and one had to treat degenerate and non-degenerate cases individually. It appears that one can generalize the results to qubit-qutrit observables, but it needs to be ensured that the ground state of C is non-degenerate.

Theorem 9.2. *Consider a qubit-qutrit system and operators* $C = C_A \otimes C_B$ *and* $L = L_A \otimes L_B$ *where the ground state and the most excited state of C are non-degenerate. Then C and L can be used for entanglement detection, if and only if* $[C_A, L_A] \neq 0$ *and* $[C_B, L_B] \neq 0$.

For the case of qubit-ququart similar statement no longer holds. To show this, we present two Hermitean operators $L = L_A \otimes L_B$ and $C = C_A \otimes C_B$ with $[C_A, C_B] \neq 0 \neq [L_A, L_B]$, where

the operator $X = \alpha C + \beta L$ does not have entangled ground or most excited states for any α and β. Thus, no combination of expectation values of $\langle C \rangle$ and $\langle L \rangle$ is useful for entanglement detection. If one chooses observables to be

$$C_A = \sigma_z \quad \text{and} \quad C_B = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & \frac{1}{3} & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 4 \end{pmatrix} \tag{9.19}$$

and

$$L_A = \sigma_x \quad \text{and} \quad L_B = \begin{pmatrix} 3 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix}, \tag{9.20}$$

leads to the eigenvalue structure displayed in Fig. 9.2. Similar counterexample can be obtained in the two-qutrit case too [37].

9.4 Summary and outlook

In this section we considered quantifying and detecting entanglement using data from two observables. We used methods from Legendre transformation for giving quantitative results. In addition, we obtained necessary and sufficient criterion for lower-dimensional two product observables to be able to detect entanglement. Surprisingly we saw that there are counterexamples to the criterion in high dimensions. The statement is interesting and counter-intuitive, since in many situation one expects that in order to derive strong witnesses one is inclined to choose product observables that anticommute locally [128]. It turned out that in higher dimensions this may not be a good strategy. It is, hence, still to be determined under which conditions observables become useful in high-dimensional Hilbert spaces.

Chapter 10

Pure entangled states are Bell nonlocal

Bell inequalities are one of the oldest and most important tools in quantum information as they rule out local hidden variable models (See Chapter 2 for the introduction). The question whether all entangled states exhibit quantum nonlocality is of the great importance. In 1992 in a paper by Popescu and Rohrlich [38] a proof has been presented that any pure entangled state violates some Bell inequality. We point out the gap in the proof, but with additional efforts show that the statement indeed holds. This construction demonstrates how to obtain two qubit entanglement from any multiqubit entangled state by performing local measurements. We generalize the statement further to projecting on genuine multipartite nonlocality.

10.1 Introduction

The question which quantum states violate a Bell inequality and which not is of central importance for quantum information processing. In Ref. [38] it has been shown that any pure multiparticle quantum state violates a Bell inequality. The strategy for proving this statement was the following: First, one can show that for any entangled pure state on N particles one can find projective measurements on $(N-2)$ particles, such that for appropriate results of the measurements the remaining two particles are in an entangled pure state. Then,one can apply the known fact that any pure bipartite entangled state violates some Bell inequality [39].

Here we point out a gap in the proof presented in Ref. [38]. The gap concerns the part where the projective measurements on $(N-2)$ particles are made. It turns out that a certain logical step does not follow from the previous statements and we give an explicit counterexample for a conclusion drawn at the critical point. Luckily it turns out, however, that with a significantly refined and extended argumentation the main statement can still be proven. Independently of the connection to Ref. [38], our results provide a constructive way how a two particle entangled state can be generated from an N-particle state by performing local projections onto $(N-2)$

particles. This may be of interest for the theory of multiparticle entanglement. Finally we generalize the results to projecting on genuine multipartite entangled states if the initial state was genuine multiparticle entangled.

10.2 Discussion of the original argument

The gap concerns the proof of the Lemma on page 296 of Ref. [38]. This lemma states that:

Let $|\psi\rangle$ be an N system entangled state. For any two of the N systems, there exists a projection onto a direct product of state of the other $(N-2)$ systems, that leaves the two systems in an entangled state.

In the following we show that while the Lemma is correct, there is a gap in its original proof. Doing so, in this section we will reformulate the proof in modern language in order to see where the problem is. For simplicity, we first consider only qubits.

The proof from Ref. [38] is a proof by contradiction, so it starts with assuming the opposite. So, orthogonal basis vectors $|b_i\rangle \in \{|0\rangle, |1\rangle\}$ are considered for each qubit i, where the conclusion does not hold. That is,

$$\langle b_3|\langle b_4|\ldots\langle b_N|\psi\rangle = |\alpha\rangle|\beta\rangle, \tag{10.1}$$

where the projections are carried out on the qubits $3,\ldots,N$ and the qubits one and two remain in the product state $|\alpha\rangle|\beta\rangle$ for any possible choice of the $\langle b_3|\langle b_4|\ldots\langle b_N|$. The $\langle b_i|$ can take the values 0 or 1. So, the product vector will in general depend on this choice and it is appropriate to write this dependency as

$$|\alpha\rangle = |\alpha(b_3,\ldots,b_N)\rangle \quad \text{and} \quad |\beta\rangle = |\beta(b_3,\ldots,b_N)\rangle. \tag{10.2}$$

What happens if the value of b_3 changes? The proof in Ref. [38] argues convincingly that then not *both* of the $|\alpha\rangle$ and $|\beta\rangle$ can change: If this were the case, a projection onto the superposition $\langle c_3| = \langle b_3 = 0| + \langle b_3 = 1|$, while keeping $\langle b_4|\ldots\langle b_N|$ constant, projects the system on the first two qubits in an entangled state. So, we have either

$$|\alpha\rangle = |\alpha(\circ, b_4,\ldots,b_N)\rangle \quad \text{or} \quad |\beta\rangle = |\beta(\circ, b_4,\ldots,b_N)\rangle, \tag{10.3}$$

where the "$\circ$" indicates that $|\alpha\rangle$ or $|\beta\rangle$ *for the given values of* $b_4,\ldots,b_N$ does not depend on b_3.

The original proof continues the argument as follows: *Repeating the argument for other subspaces, we conclude that ... each index [b_i] actually appears in either $|\alpha\rangle$ or in $|\beta\rangle$ but not in both.* This conclusion is unwarranted. The point is that for a given set of $b_4,\ldots,b_N$ one of the vectors (say, $|\alpha\rangle$ for definiteness) does not depend on b_3, but for another choice of $b_4,\ldots,b_N$ the other vector $|\beta\rangle$ may be independent on b_3, while $|\alpha\rangle$ may depend on it. So, one cannot conclude that one of the vectors is *generally* independent.

The problem is best illustrated with a counterexample. Consider the four-qubit state

$$|\psi\rangle = \frac{1}{2}(|0000\rangle + |0101\rangle + |0110\rangle + |1111\rangle). \tag{10.4}$$

One can easily check that this is not a product state for any bipartition, so the state is genuine multiparticle entangled. Also, any projection into the computational basis on the particles three and four leaves the first two particles in a product state. We have for the dependencies:

$$|\alpha(00)\rangle = |0\rangle, \quad |\alpha(01)\rangle = |0\rangle, \quad |\alpha(10)\rangle = |0\rangle, \quad |\alpha(11)\rangle = |1\rangle, \tag{10.5}$$

and

$$|\beta(00)\rangle = |0\rangle, \quad |\beta(01)\rangle = |1\rangle, \quad |\beta(10)\rangle = |1\rangle, \quad |\beta(11)\rangle = |1\rangle, \tag{10.6}$$

so neither of these vectors does depend on a single index only.

Of course, if one chooses measurements in other directions on the qubits three and four, that is, one measures vectors like

$$|c_3\rangle = \cos(\gamma)|0\rangle + \sin(\gamma)|1\rangle \text{ and } |c_4\rangle = \cos(\delta)|0\rangle + \sin(\delta)|1\rangle, \tag{10.7}$$

then the remaining state on the qubits one and two is entangled. So the state $|\psi\rangle$ is not a counterexample to the main statement of the Lemma, but it demonstrates that proof requires some extra work.

Finally, if one accepts the step that each index $[b_i]$ occurs only in $|\alpha\rangle$ or $|\beta\rangle$, but not in both, one can conclude as demonstrated in Ref. [38] that the original state has to factorize, so it is not entangled, which would lead to a contradiction.

10.3 Completing the argument

In Ref. [40] we provided a way to add the missing part to the proof. Here we give a short overview to the main construction.

We prove the following statement: *Let* $\mathbf{b}' = (b_3, b_4, \ldots, b_N)$ *with* $b_i \in \{0, 1\}$ *be the basis vectors which are used for the projection on the qubits* $3, \ldots, N$ *and denote the remaining product state on the first two qubits by* $|\alpha(\boldsymbol{b'})\rangle|\beta(\boldsymbol{b'})\rangle$*. Then,* $|\alpha(\cdot)\rangle$ *depends only on some subset of the indices* $\mathbf{b}'$*, while* $|\beta(\cdot)\rangle$ *depends on the complement subset.* This statement implies the correctness of the Lemma in Ref. [38].

The proof is done by assuming the opposite and reaching a contradiction. The opposite claim is that there exists an index i (without the loss of generality, we can take $i = 3$) and two sets of values for the remaining indices

$$\mathbf{b} = b_4, b_5, \ldots, b_N \quad \text{and} \quad \mathbf{B} = B_4, B_5, \ldots, B_N, \tag{10.8}$$

such that

$$|\alpha(0, \mathbf{b})\rangle \neq |\alpha(1, \mathbf{b})\rangle \quad \textit{and} \quad |\beta(0, \mathbf{B})\rangle \neq |\beta(1, \mathbf{B})\rangle, \tag{10.9}$$

meaning that both depend on b_3. Here, $|\alpha(0,\mathbf{b})\rangle$ is a short-hand notation for $|\alpha(b_3=0,\mathbf{b})\rangle$. Also, the inequality symbol here and in the following indicates linear independence, i.e., $|\alpha(0,\mathbf{b})\rangle \neq \lambda|\alpha(1,\mathbf{b})\rangle$ for any $\lambda \neq 0$.

The vectors $\mathbf{b}$ and $\mathbf{B}$ differ in some entries, but in some entries they match. Without loss of generality, we can assume that they differ in the first k entries while the others are the same and equal to zero. More specifically, they can be taken of the form:

$$\begin{aligned}\mathbf{b} &= 0\,0\,0\,\ldots\,0\;\;0\,0\,\ldots\,0,\\ \mathbf{B} &= \underbrace{1\,1\,1\,\ldots\,1}_{k}\;\underbrace{0\,0\,\ldots\,0}_{N-k-3}.\end{aligned} \tag{10.10}$$

Then the proof proceeds via induction on k. The precise statement we want to prove for all k is the following: Let the vectors $\mathbf{b}$ and $\mathbf{B}$ differ by at most at k terms. Then, if $|\alpha(0\mathbf{b})\rangle \neq |\alpha(1\mathbf{b})\rangle$, the equality $|\beta(0\mathbf{B})\rangle = |\beta(1\mathbf{B})\rangle$ must hold. The crucial point here is that on each induction step we need to use the already derived linear dependencies and independencies from all the previous induction steps, i.e. for all $k' < k$.

The base case proof when $k = 0$, or, equivalently, when $\mathbf{b} = \mathbf{B}$, is covered in the original paper [38].

The first $(k = 0 \mapsto k = 1)$ and the second $(k = 1 \mapsto k = 2)$ step of the induction explicitly is given in Ref. [40] and these are used in order to get the idea for the general case. The rest of the proof is given in Ref. [40].

The results can be extended to higher dimensional systems. There are two ways to deal with this issue. First, one can extend the discussion used to for qubits also to the higher dimensions. The point is that in the qubit proof the core conditions were always stating that certain indices are equal or not equal. This, of course, can be formulated also for non-binary indices. A second and more elegant way, however, makes use of the fact that any N-qudit entangled pure state can be projected by local means on an entangled N-qubit entangled state. This can be achieved by the following procedure:

Let $|\psi\rangle$ be a $d \times d \times ... \times d$ entangled state, where d is the dimension of the Hilbert space associated with each system. We start by considering the first subsystem and write down the Schmidt decomposition with respect to the split $1|2,3,4,\ldots,N$:

$$|\psi\rangle = \sum_{i=1}^{d} s_i |i\rangle_1 |i\rangle_{2,3,4,\ldots,N}. \tag{10.11}$$

Then, we proceed as follows:

1. If $|\psi\rangle$ is separable with respect to the $1|2,3,4,\ldots,N$ partition, the sum consists only of one term and we do nothing. Note that effectively the whole state lives on a one-dimensional subspace on Alice's side, so one can view it as a $1 \times d \times \cdots \times d$ state.

2. If $|\psi\rangle$ is entangled with respect to the $1|2,3,4,\ldots,N$ partition, we project locally for Alice onto the two first Schmidt vectors, resulting in the truncated sum:

$$|\psi'\rangle = \sum_{i=1,2} s'_i |i\rangle_1 |i\rangle_{2,3,4,\ldots,N}. \tag{10.12}$$

This state is still entangled with respect to the $1|2,3,4,\ldots,N$ partition and it is a $2 \times d \times \cdots \times d$ state.

Now, we go on and do the same procedure iteratively for particle 2, then particle 3, etc., until we arrive at the last party N. At the end we have a state living in a $2 \times 2 \times \cdots \times 2$-dimensional Hilbert space. If the original state was entangled, then the state $|\psi'\rangle$ is also entangled: when going through the parties, there will be some party, say j, where the last projection according to point (2) above is made. So the final state will be entangled with respect to the $j|\texttt{rest}$ partition (where `rest` denotes all the remaining parties) and it is not a fully separable state. Note that the projection on j may change the separability properties of the $1|\texttt{rest}$ partition, and this partition may become separable. However, at least one entangled partition remains, and as discussed above, this is sufficient to show that the state is not a fully separable state.

So any entangled $d \times d \times \cdots \times d$ pure state can be projected locally onto a pure entangled N-qubit state and for qubit states we already repaired the proof.

A further point worth to discuss is the question whether the state $|\psi\rangle$ considered in the proof has maybe vanishing coefficients in the basis where the projections are made. In fact, the careful reader may have noticed that for the theorem and the proof above to work, it is required all possible projections in the computational basis, especially the states $|\alpha(\cdot)\rangle$ and $|\beta(\cdot)\rangle$ are non-zero. This might not be fulfilled for a given basis.

Of course, for a random choice of the product basis this will be in general fulfilled and this property has been recently utilized to show that genuine multipartite entanglement of all multipartite pure states in arbitrary finite dimension can be detected in a device-independent way by employing bipartite Bell inequalities on states that are deterministically generated from the initial state via random bases measurements [176]. But more constructively, one can ask whether there is a set of local unitaries that, when applied to any initial state $|\psi\rangle$ in the computational basis, give *with certainty* some states where all the coefficients are non-vanishing. Interestingly, this question was brought up as one of the "ten most annoying questions in quantum computing" [177] with the local unitaries being the Hadamard gates and the solution was given in Ref. [178]. We now recall this result in the following lemma with the notation σ_x and σ_z being the Pauli-X and Pauli-Z matrices, respectively.

Lemma [178]. *Given an N-qubit pure state, there is always a way to apply Hadamard gates to some subset of the qubits to make all 2^N computational basis components having non-zero amplitudes. In other words, if one considers the 2^N product bases defined by the eigenstates of the observables $\sigma_{k_1}^{(1)} \otimes \cdots \otimes \sigma_{k_N}^{(N)}$ with $\sigma_k^{(j)} \in \{\sigma_x, \sigma_z\}$, then any state $|\psi\rangle$ has non-vanishing coefficients in at least one of these bases.*

This Lemma guarantees that a suitable basis can be found in a constructive manner. □

10.4 Projecting on genuine multipartite entanglement

The idea of having an entangled multipartite resource state and projecting it onto a smaller entangled state via local operations was developed further since the paper of Popescu and Rohrlich [38]. In Ref. [176] it was proven that given an N-qudit genuine multipartite entangled state, one can project on a genuine multipartite entangled state on $(N-k)$ parties regardless of the outcomes, if the rest of the k parties are measured in random bases. Similar statement was made for projecting on genuine tripartite entanglement using only Pauli-X and -Z bases measurements in Refs. [179, 180]:

Theorem 10.1. *[179, 180] Let $|\psi\rangle$ be an N-qubit entangled state with $N \geq 3$. There exists some choice of three of the N qubits and a projection of the other $(N-3)$ qubits onto a tensor product of computational and Pauli-X bases states that leaves the three qubits in a genuinely entangled state.*

This is a generalization of the result presented in the previous section since the measurement bases are fixed. However, it is still restricted since it only promises the projection on a genuine multipartite entangled state on some subset of qubits. Here we give a proof to the most general result:

Theorem 10.2. *Any N-qubit genuine multipartite entangled state can be projected on k party genuine multipartite entanglement via measurements in X and Z direction on the other $(N-k)$ parties, $3 \leq k \leq (N-1)$.*

Proof. We take a genuine N-qubit entangled state $|\psi\rangle$. Let us consider the simplest case: $N=4$ and $k=3$ and assume the opposite to the theorem. From the original argument of Popescu and Rohrlich we know that it is possible to project on any two entangled qubits. Let us assume that to project on an entangled state on parties 12, we need to measure $\langle m_3|$ and $\langle 0_4|$ on qubits three and four, respectively. Then $\langle 0_4|\psi\rangle \mapsto 12|3$. Similarly, let us assume that to project on qubits $2,4$ such that the state on 24 is entangled, we need to measure $\langle 0_3|$ on qubit 3. Then $\langle 0_3|\psi\rangle \mapsto 1|24$. Thus, if we first measure $\langle 0_4|\psi\rangle \mapsto 12|3$ and after, if we measure $\langle 0_3|$ on the resulting state, we end up either with entangled state on qubits 1 and 2 since

$$\langle 0_3|\psi_{12|3}\rangle \mapsto 12, \tag{10.13}$$

or we get zero, since the post-measurement state on qubit $1,2,3$ might have been of the form $|\psi_{12|3}\rangle = |\psi_{12}\rangle \otimes |1_3\rangle$. However, if we first measure $\langle 0_3|\psi\rangle \mapsto 1|24$ and then $\langle 0_4|$, we end up with a separable state on 1 and 2:

$$\langle 0_4|\psi_{1|24}\rangle \mapsto 1|2 \tag{10.14}$$

and since the state on 24 is entangled, measuring the forth qubit in computational basis cannot give 0. This is a contradiction. Therefore, a genuine multipartite entangled state on three qubits can be obtained by measuring the fourth qubit in either X or Z direction.

Next we generalize the construction to an arbitrary k. For this it is sufficient to show that if the statement is correct for $k=N-2$, then the same follows for $k=N-1$. The proof is very similar to $N=4$ and $k=3$ case.

We start by assuming the opposite. We can project on a genuine multipartite entangled state on the first $(N-2)$ qubits when measuring $\langle m_{N-1}|$ and $\langle 0_N|$ without loss of generality. Then according to the assumption the following must hold

$$\langle 0_N|\psi\rangle \mapsto 12\ldots(N-2)|(N-1). \tag{10.15}$$

On the other hand, there exits a measurement on the qubit $(N-1)$, assume $\langle 0_{N-1}|$, which projects on the configuration

$$\langle 0_{N-1}|\psi\rangle \mapsto 1|23\ldots(N-2)N, \tag{10.16}$$

where the state on qubits $23\ldots(N-2)N$ is genuine multipartite entangled.

Then similarly to the first case, measuring first $\langle 0_N|$ and then $\langle 0_{N-1}|$ gives either a genuine multipartite entangled state on qubits $12\ldots(N-1)$

$$\langle 0_{N-1}|\psi_{12\ldots(N-2)|(N-1)}\rangle \mapsto 12\ldots(N-2), \tag{10.17}$$

or zero. On the other hand, first measuring $\langle 0_{N-1}|$ and then $\langle 0_N|$ would yield

$$\langle 0_N|\psi_{1|2\ldots(N-2)N}\rangle \mapsto 1|2\ldots(N-2), \tag{10.18}$$

where the post-measurement state factorizes for the bipartition 1 versus the rest. The rest can be genuine multipartite entangled or it can itself be separable for some other bipartition, but this is not important for the proof. What is important that it cannot be zero. Since the difference sequences of the same commuting measurements reach to the states with different entanglement properties, we reach the contradiction to the initial assumption. Thus, given any N-qubit entangled pure state, it is possible to project on a genuine multipartite entangled state on any subset of $2 < k < N$ qubits using X or Z bases measurements. □

10.5 Summary and outlook

In this section we discussed the proof of the result that any state can violate some Bell inequality. We started with an N-partite state and showed that using Pauli-X and -Z bases measurements it can be projected on any subset of two-qubit entangled states. We generalized these results to projecting on genuine multipartite entanglement on any arbitrary subset of $2 < k < N$ parties. The original results for two qubits have been previously used to derive Bell inequalities in various scenarios. It would be interesting to employee the more general results in the same direction.

Conclusions and outlook

In this thesis we have considered mainly pure multipartite entanglement and its applications. The biggest part of the thesis, Chapters 3-7, is devoted to quantum hypergraph states, their properties, and applications. We compared all our results with already well-established theory for graph states.

In Chapter 3 we investigated nonlocal properties of hypergraph states. We managed to use existing nonlocal stabilizer formalism to derive genuine multipartite Bell inequalities. Besides, we demonstrated that the symmetric three- and four- uniform hypergraph states violate Mermin-like inequalities in an exponentially growing manner with the number of qubits. This violation is robust under particle loss, in contrast to the results known for the GHZ-states. Due to such violations, we found interesting applications of these states in quantum metrology and nonadaptive measurement-based quantum computation with linear side-processing.

In Chapter 4 we developed graphical rules for transformations on hypergraph states. We started from generalizing the concept of local complementation to hypergraph states. Then we derived graphical rules of how a hypergraph changes, in case some of its computational basis elements are transposed. Finally, we used these two results to develop graphical measurement rules for hypergraph states. These rules curiously correspond to the exact generalizations of graph state measurement rules.

In Chapter 5 we discussed entanglement quantification and detection for hypergraph states. We used graphical rules developed in Chapter 4 to obtain tight entanglement witnesses for three-uniform complete hypergraph states. In the second half of the chapter, we calculated geometric measure of entanglement for many classes of hypergraph states. Most importantly, we connected the properties of having a local Pauli stabilizer to analytic derivations of the value of geometric measure. We believe that these results will have broad further implications for investigating nonlocal properties of hypergraph states.

In Chapter 6 we demonstrated that three-uniform hypergraph states are novel and interesting resource states for measurement-based quantum computation using Pauli measurements only. This is not the only advantage they offer, the entire protocol is deterministic and, as a result, adaptation of measurement basis is only required when basis are changed during computation.

In Chapter 7 we studied pure quantum error-correcting codes with hypergraphs being all the codewords. We derived strict Knill-Laflamme conditions specifically for hypergraph states, exhaustively characterized hypergraph states satisfying this condition up to six qubits. We found that many hypergraphs state codes saturating quantum Singleton bounds. Most interestingly we discovered that such a six-qubit code is a nonadditive code.

There are several directions in which one can extend our work on hypergraph states:

(i) It would be interesting to derive Bell inequalities for more classes of hypergraph states, especially for the ones which are eigenstates of local Pauli stabilizers. Since certain hypergraph states are robust under particle loss, they are also natural candidates to reveal nonlocality even in the condition of low detection efficiency.

(ii) Graph states are SLOCC equivalent iff they are LU equivalent. This result heavily relies on the uniqueness of the SLOCC normal form up to LU operations. Already for three-qubits we saw that for the entire class of hypergraph states this statement does not hold: The 3-qubit GHZ-state is SLOCC equivalent to the three qubit hypergraph state $|H_3^3\rangle$, however, they are not LU-equivalent. Therefore, it is interesting to investigate power of SLOCC transformations in general hypergraph states. This would help to get an idea about the limitations of LU operations on hypergraphs and perhaps can give an insight into deriving new LU equivalence rules.

(iii) We derived a criterion when Pauli-X measurements map hypergraph states to hypergraph states. It is not clear that this criteria is necessary for the measurement rule to hold.

(iv) We used graphical rules for basis transposition to derive tight entanglement witnesses for three-uniform complete hypergraph states. For graph states tight entanglement witnesses have been derived from stabilizer formalism. It would be desirable to combine our analysis with the knowledge of graph state case and study detection of entanglement in hypergraph states in general.

(v) We used several techniques to estimate geometric measure of entanglement of symmetric hypergraph states. All these techniques work for symmetric cases. First, it would be interesting to connect entanglement measures with hypergraph-theoretic properties of examined states, in a resemblance to the construction in graph states [181]. We have already seen on the example of three-uniform complete hypergraph states, that local Pauli stabilizers can be connected to geometric measure of entanglement. This analysis could be extended to other symmetric states.

(vi) We showed that hypergraph states can be used for measurement-based quantum computation. It is interesting to investigate, how the fidelity of gates implemented on our architecture scales with certain noise models in the resource states.

(vii) A lot of work needs to be done in the direction of hypergraph-based quantum error-correcting codes. The code $((6, 16, 2))_2$ is a stimulating example in this direction, since it is an example of a nonadditive code. Also it would be interesting to find hypergraph-based error-correcting codes of higher distance.

The rest of the thesis is devoted to independent topics, however, studying entanglement is still central in all of them.

Chapter 8 is devoted to pure entangled states with non-homogeneous local dimensions, $2 \times m \times n$. We revisited the connection between these states and linear matrix pencils. As a result we characterized generic states for any m and n by showing that the full measure set of states indeed corresponds to the full measure set of pencils in the same local dimension. We studied coarse graining of entanglement present in these states under noninvertible transformations. First we showed that in order to obtain any state in the full measure set for any local dimension $2 \times m \times n$, it is sufficient to take a random state in $2 \times m \times (n+1)$. Then this state is a common resource state for any generic state in $2 \times m \times n$ under noninvertible transformation. We also investigated common resource states to reach all the states in $2 \times m \times m$, including the ones in zero measure set and we found that there is a states in $2 \times m \times (2m-2)$, which can do the job. Indeed one can show that this is the optimal local dimension for the common resource state. Finally the optimal common resource state for all the states in $2 \times m \times n$, when $n > m$ is obtained trivially in $2 \times m \times 2m$. There are several directions in which our work may be generalized. First, it may be useful to find new witnesses or polynomial invariants characterizing the SLOCC classes. These invariants can be used to construct entanglement measures such as the so-called three-tangle. Moreover, it might prove promising to study LOCC transformations within a generic state in $2 \times m \times n$ systems, as similarly to the bipartite case, the representative of this SLOCC class is a single state.

In Chapter 9 we studied a possibility to detect entanglement with two observables. We asked the following natural question, given expectation value of one of the observables, can we improve entanglement detection, if experimental data from some other observable is also known. We tackled the problem with the theory of Legendre transforms, which, in addition to detecting, can also quantify entanglement. Restricting ourselves to two sets of product observables $C = C_A \otimes C_B$ and $L = L_A \otimes L_B$, we found that, if we are dealing either with qubit-qubit or qubit-qutrit case, expectation values of these observables can be used to detect entanglement, if and only if they do not commute locally: $[C_A, L_A] \neq 0$ and $[C_B, L_B] \neq 0$. For higher dimensional cases non-commutativity is not sufficient for detecting entanglement. It is, hence, still to be determined under which conditions product observables become useful in higher dimensional Hilbert spaces.

In Chapter 10 we revisited the proof of the following statement. Two-particle entangled state can be generated from any entangled N-particle state by performing local projections onto $(N-2)$ particles. The original proof had a flaw, which we pointed out by a counterexample, however, the statement itself luckily could be proven with some extra effort. One can indeed show that, it is sufficient to consider Pauli-X and Z measurements. We generalized the proof one step further: Any N-qubit genuine multipartite entangled state can be projected on k party genuine multipartite entanglement via measurements in X and Z direction on the other $(N-k)$ parties, $3 \leq k \leq (N-1)$. It is still unclear, if the statement is true for higher dimensions. Moreover, the original statement has been heavily used in nonlocality proofs and derivations of Bell inequalities. It is desirable to find similar applications for the more general case.

Acknowledgements

First and most of all, I can never thank enough my supervisor, Otfried Gühne for his constant guidance and persistent effort to make me better at what I do. I would like to thank him for giving me a chance to study physics, even though I had absolutely no knowledge of it, when I first arrived in Siegen in 2015. I would like to thanks him for providing me with numerous opportunities to work on very interesting projects, to meet with many interesting scientists, and, most importantly, for taking his time to discuss with me and to teach me many things. Looking back, I value all the discussions we have had over the course of the years. Lastly, I would like to thank him for all the interesting and fun chess games we got to play together.

I would like to thank Barbara Kraus for her supervision when hosting me in her group at the University of Innsbruck, Austria. Special thanks goes to Martin Hebenstreit for the amazing long discussions we have had during my visit. Many thanks to David Sauerwein and Katherina Schwaiger for their hospitality.

Many thanks to Akimasa Miyake for his supervision during my visit at the university of New Mexico, USA. I would like to especially thank him for all the interest that he took in our discussions and for his constant encouragement. Many thanks to CQuIC group and Gloria Cordova for making my stay in Albuquerque unforgettable.

I would like to specially acknowledge my collaborator and a good friend, Nikoloz Tsimakuridze for working with me, discussing with me, teaching me, and inspiring me for many, many years.

I would like to acknowledge my collaborator, an office-mate, and a friend, Nikolai Wyderka. It is always very interesting, inspiring, and efficient to work and discuss with him. Many thanks to his lovely wife Magdalena, little David, and their extended big family for making Siegen very homey place.

I am particularly grateful to my collaborator, Costantino Budroni for providing his fresh and valuable input, when working on my very first project in Siegen.

I would like to acknowledge Cornelia Spee for her input in the proof of Theorem 10.2, for helping with abstract translation, and mostly for always giving her fresh and thoughtful insight. I thank Tristan Kraft for being impossible to offend and for translating the abstract of this thesis; Davide Orsucci for many interesting discussions during our stay in Albuquerque and for being a great swimming teacher; All my friends and at the same time colleagues: Ali Asadian, Ana Cristina Sprotte Costa, Roope

Uola, Jiangwei Shang, Gael Sentís, Timo Simnacher, Yuanyuan Mao, Matthias Kleinmann, Fabian Bernards, Xiao-Dong Yu, Chau Nguyen, Andreas Ketterer, Christina Ritz, Zhen-Peng Xu.

I cannot thank enough Ms. Daniela Lehmann for her constant help with work bureaucracy and not only, for making my life easier since my first day in Siegen. I would like to acknowledge the funding from the Gesellschaft der Freunde und Förderer der Universität Siegen.

Very special thanks to Nikolai Miklin for always cheering me up, for many interesting scientific discussions, for his constant support and love.

I would like to thank my hard-working parents, my amazing brother and an awesome sister for letting me have this time off from our lives together.

List of publications

(A) Mariami Gachechiladze, Costantino Budroni and Otfried Gühne
Extreme violation of local realism in quantum hypergraph states
Phys. Rev. Lett. **116**, 070401 (2016)

(B) Mariami Gachechiladze, Nikoloz Tsimakuridze and Otfried Gühne
Graphical description of unitary transformations on hypergraph states
J. Phys. A: Math. Theor. **50**, 19LT01 (2017)

(C) Mariami Gachechiladze and Otfried Gühne
Completing the proof of "Generic quantum nonlocality"
Phys. Lett. A **381**, 1281 (2017)

(D) Martin Hebenstreit, Mariami Gachechiladze, Otfried Gühne and Barbara Kraus
Coarse graining of entanglement classes in $2 \times m \times n$ *systems*
Phys. Rev. A **97**, 032330 (2018)

(E) Mariami Gachechiladze, Nikolai Wyderka and Otfried Gühne
The structure of ultrafine entanglement witnesses
J. Phys. A: Math. Theor. **51**, 365307 (2018)

(F) Mariami Gachechiladze, Otfried Gühne and Akimasa Miyake
Changing the circuit-depth complexity of measurement-based quantum computation with hypergraph states
Phys. Rev. A **99**, 052304 (2019)

Appendix A

An Appendix to Chapter 3

Preliminary calculations

Before starting with the actual calculations, we need to settle couple of identities and a look-up table, which we will refer to throughout the main proofs.

The first and probably the most important identity is a commutation relation between multi-qubit phase gates and Pauli X matrices [113],

$$C_e\big(\bigotimes_{i\in K} X_k\big) = \big(\bigotimes_{i\in K} X_k\big)\big(\prod_{f\in\mathcal{P}(K)} C_{e\setminus\{f\}}\big). \tag{A.1}$$

Here, $\mathcal{P}(K)$ denotes the power set of the index set K. Note that the product of the $C_{e\setminus\{f\}}$ may include the term $C_\emptyset$, which is defined to be $-\mathbb{1}$ and leads to a global sign.

Furthermore, it turns out to be useful to recall some basic facts about binomial coefficients, as the appear frequently in the following calculations.

Lemma A.1. *The following equalities hold:*

$$Re\Big[(1+i)^n\Big] = \sum_{k=0,4,\ldots}^{n} \binom{n}{k} - \binom{n}{k+2}, \tag{A.2}$$

$$Im\Big[(1+i)^n\Big] = \sum_{k=0,4,\ldots}^{n} \binom{n}{k+1} - \binom{n}{k+3}. \tag{A.3}$$

Proof. Here we derive (A.2) and (A.3) together:

$$s := (1+i)^n = \sum_{k=0}^{n} \binom{n}{k} i^k = \sum_{k=0,4,\ldots}^{n} \binom{n}{k} + i\binom{n}{k+1} - \binom{n}{k+2} - i\binom{n}{k+3}. \tag{A.4}$$

It is easy to spot that $Re[s]$ and $Im[s]$ indeed leads to the identities (A.2) and (A.3) respectively. □

#	n	$Re\Big[(1+i)^n\Big]$	$Im\Big[(1+i)^n\Big]$	$Re\Big[(1+i)^n\Big]+Im\Big[(1+i)^n\Big]$	$Re\Big[(1+i)^n\Big]-Im\Big[(1+i)^n\Big]$
1.	$n=0 \bmod 8$	$+2^{\frac{n}{2}}$	0	$+2^{\frac{n}{2}}$	$+2^{\frac{n}{2}}$
2.	$n=1 \bmod 8$	$+2^{\frac{n-1}{2}}$	$+2^{\frac{n-1}{2}}$	$+2^{\frac{n+1}{2}}$	0
3.	$n=2 \bmod 8$	0	$+2^{\frac{n}{2}}$	$+2^{\frac{n}{2}}$	$-2^{\frac{n}{2}}$
4.	$n=3 \bmod 8$	$-2^{\frac{n-1}{2}}$	$+2^{\frac{n-1}{2}}$	0	$-2^{\frac{n+1}{2}}$
5.	$n=4 \bmod 8$	$-2^{\frac{n}{2}}$	0	$-2^{\frac{n}{2}}$	$-2^{\frac{n}{2}}$
6.	$n=5 \bmod 8$	$-2^{\frac{n-1}{2}}$	$-2^{\frac{n-1}{2}}$	$-2^{\frac{n+1}{2}}$	0
7.	$n=6 \bmod 8$	0	$-2^{\frac{n}{2}}$	$-2^{\frac{n}{2}}$	$+2^{\frac{n}{2}}$
8.	$n=7 \bmod 8$	$+2^{\frac{n-1}{2}}$	$-2^{\frac{n-1}{2}}$	0	$+2^{\frac{n+1}{2}}$

TABLE A.1: Look-up table for the values of Eq. (A.2) and Eq. (A.3).

The look-up table, Table A.1 represents the values of (A.2) and (A.3) for different n. These values can be derived from the basic properties of complex numbers.

A.1 Complete three-uniform hypergraph correlations

Correlations for Pauli-X and Z operators for fully-connected three-uniform hypergraph states

Proof. Here we present the proof of correlations in Eq. (3.22). We can write:

$$K := \langle HG|X\dots XZ\dots Z|HG\rangle = \langle +|^{\otimes N}\Big(\prod_{e\in E} C_e\Big)X\dots XZ\dots Z\Big(\prod_{e\in E} C_e\Big)|+\rangle^{\otimes N}. \tag{A.5}$$

We can group all the controlled phase gates on the right hand side of the expression (A.5). Note that the operators C_e and X_i do not commute, but we can use the identity $(A.1)$. While regrouping we count the multiplicity of each phase gate. If each phase gate appears even times, we get an identity as $C^2 = \mathbb{1}$, if not, we keep these phase gates with the multiplicity one for the further calculations.

For the purposes which will become apparent shortly, we denote the parties which measure in X direction by $\circledast$ and ones in Z direction by $\triangle$, in a way that, for example, if an arbitrary phase gate acts on $XXXZZ$, it is represented as $\circledast\circledast\circledast\triangle\triangle$. Without loss of generality, we fix one phase gate C_e and consider all the possible scenarios of $\circledast$ and $\triangle$ it can be acting on. Since we work on three-uniform HG states, every phase gate acts on bashes of different three party systems. These parties can be either of type $\circledast$ or $\triangle$ and we have to consider all possible scenarios. Since we are working with symmetric states, we can sort the parties such that we have m $\circledast$'s followed by $(N-m)$ $\triangle$'s:

$$\underbrace{\circledast\cdots\circledast}_{m}\underbrace{\triangle\cdots\triangle}_{N-m} \tag{A.6}$$

and then we can enumerate all the scenarios of one phase gate acting on (A.6):

1. C_eZZZ corresponds to $\triangle\,\triangle\,\triangle$
2. C_eXZZ corresponds to $\circledast\,\triangle\,\triangle$
3. C_eXXZ corresponds to $\circledast\,\circledast\,\triangle$
4. C_eXXX corresponds to $\circledast\,\circledast\,\circledast$

We consider each case separately:

1. $C_eZZZ = ZZZC_e$ as C_e and Z commute. C_e moves on the right side with the multiplicity one. To save us writing in the future, we will denote the multiplicity of the phase gate moving on the right side by $\#e$. In this particular case it is $\#\triangle\,\triangle\triangle = 1$. However, on the right side of the equation (A.5) we have a product of all three-party phase gates. Therefore, we get C_e with the multiplicity of two and $C_e^2 = \mathbb{1}$. Note that, as we have chosen an arbitrary three-qubit phase gate, the same result holds for every such phase gate. So, all three-qubit phase gates coming from the case 1, cancel out. We will see that with the same reasoning all three qubit phase gates cancel out (give an identity).

2. For C_eXZZ, we use the identity (A.1):

$$C_eXZZ = XC_eC_{\{e\setminus X\}}ZZ. \tag{A.7}$$

The three-qubit phase gate C_e, from (A.7), appears with the multiplicity one ($\#\circledast\,\triangle\triangle = 1$) and like in the case 1, it gives an identity when being multiplied by the same three-qubit phase gate at the right side of the expression in (A.5). It is more tricky to calculate the multiplicity of $C_{\{e\setminus X\}}$ ($\#\triangle\,\triangle$ as the $\circledast$ part (or equivalently, X part) is removed from the set of vertices e.). For this we need to fix $\triangle\triangle$ and count all the scenarios when an arbitrary C_e is reduced to $\triangle\triangle$. As we are working with the symmetric case, such scenario repeats $\binom{m}{1} = m$ times, where m is the number of parties measuring in X direction.We shortly denote this as $\#\triangle\,\triangle = \binom{m}{1} = m$. So, as m is an even number, $(C_{\{e\setminus X\}})^m = (C_{\triangle\triangle})^m = \mathbb{1}$.

Note that the gate $C_{\triangle\triangle}$ can only be generated from in case 2.

3. For C_eXXZ, we use the identity (A.1):

$$C_eXXZ = XXC_eC_{\{e\setminus XX\}}\Big[\prod_{\forall X} C_{\{e\setminus X\}}\Big]Z. \tag{A.8}$$

The three-qubit phase gate C_e, from (A.7), appears with the multiplicity one ($\#\circledast\,\circledast\triangle = 1$); therefore, like in the two previous cases, it cancels out on the right side of the expression. A multiplicity of $C_{\{e\setminus XX\}}$ is calculated by fixing a concrete $\triangle$ and counting all possible appearance of arbitrary $\circledast\circledast$. As the number of parties measuring in direction is X is m, this means that it is all combination of two parties with X measurements out of total m parties. So,

$$\#\triangle = \binom{m}{2} = \frac{m(m-1)}{2} = \begin{cases} \text{even, if} \quad m = 0\ mod\ 4 & \Rightarrow C_\triangle \text{ cancels out.} \\ \text{odd, if} \quad m = 2\ mod\ 4 & \Rightarrow C_\triangle \text{ remains.} \end{cases} \tag{A.9}$$

The last one from this case is the multiplicity of $C_{\{e\setminus X\}}$ or $\#\circledast\,\triangle$. Here we fix one qubit from m (X direction) and one from $N-m$ (Z direction) and count the number of such occurrences,

when the third qubit is an arbitrary one of the type $\circledast$, which is exactly $\binom{m-1}{1}$. Therefore,

$$\#\circledast\triangle = \binom{m-1}{1} = m-1, \text{which is odd}, \Rightarrow\ C_{\circledast\triangle}\text{remains.} \tag{A.10}$$

4. For C_eXXX, we use the identity $(A.1)$:

$$C_eXXX = XXXC_e\Big[\prod_{\forall X} C_{\{e\setminus X\}}\Big]\Big[\prod_{\forall X} C_{\{e\setminus XX\}}\Big]C_{\{\}}. \tag{A.11}$$

C_e occurs once and it gives an identity with the other one from the right side like in the previous cases. The multiplicity of $C_{\{e\setminus X\}}$ is $\#\circledast\circledast$. Here we fix two parties in X direction and count the occurrence of this scenario by altering the third party, from the remaining $m-2$, in X direction. Therefore,

$$\#\circledast\circledast = \binom{m-2}{1} = m-2, \text{which is even}, \Rightarrow\ C_{\circledast\circledast}\text{ cancels out.} \tag{A.12}$$

Similarly for $C_{\{e\setminus XX\}}$, we fix one party in X direction and count all possibilities of choosing two parties out of remaining $m-1$. Therefore,

$$\#\circledast = \binom{m-1}{2} = \frac{(m-1)(m-2)}{2} = \begin{cases} \text{odd, if} & m = 0\ mod\ 4 \quad \Rightarrow\ C_{\circledast}\text{ remains.} \\ \text{even if,} & m = 2\ mod\ 4 \quad \Rightarrow\ C_{\circledast}\text{ cancels out.} \end{cases} \tag{A.13}$$

At last, we consider $C_{\{\}}$. This gate determines the global sign of the expectation value and it appears only when C_e acts on systems which are all measured in X direction. Therefore,

$$\#\{\} = \binom{m}{3} = \frac{m(m-1)(m-2)}{2\cdot 3}, \text{which is even} \Rightarrow \quad \text{the global sign is positive .} \tag{A.14}$$

To go on, we need to consider two cases #1: $m = 0$ mod 4 and #2: $m = 2$ mod 4 and calculate the expectation value separately for both:

Case #1: When $m = 0\ mod\ 4$, we write out all remaining phase gates and continue the derivation from equation (A.5):

$$\langle K\rangle := \langle +|^{\otimes N} X\ldots XZ\ldots Z \prod_{\forall\circledast,\forall\triangle} C_{\circledast\triangle}C_{\circledast}|+\rangle^{\otimes N}. \tag{A.15}$$

Using the fact that X is an eigenstate of $\langle +|$, we can get rid of all Xs and then we can write $C_\triangle$ instead of Z:

$$\begin{aligned}\langle K\rangle =&\langle +|^{\otimes N} \prod_{\forall\circledast,\forall\triangle} C_{\circledast\triangle}C_{\circledast}C_{\triangle}|+\rangle^{\otimes N} = \frac{1}{\sqrt{2}^N}\sum_{i=00\ldots00}^{11\ldots11}\langle i| \prod_{\forall\circledast,\forall\triangle} C_{\circledast\triangle}C_{\circledast}C_{\triangle}\frac{1}{\sqrt{2}^N}\sum_{j=00\ldots00}^{11\ldots11}|j\rangle\\ =&\frac{1}{2^N}\Big[\langle 00\ldots00| \prod_{\forall\circledast,\forall\triangle} C_{\circledast\triangle}C_{\circledast}C_{\triangle}|00\ldots00\rangle + \cdots + \langle 11\ldots11| \prod_{\forall\circledast,\forall\triangle} C_{\circledast\triangle}C_{\circledast}C_{\triangle}|11\ldots11\rangle\Big]\\ =&\frac{1}{2^N}Tr\Big[\prod_{\forall\circledast,\forall\triangle} C_{\circledast\triangle}C_{\circledast}C_{\triangle}\Big].\end{aligned} \tag{A.16}$$

In (A.16), to get line two from the line one, note that $\prod_{\forall\circledast,\forall\triangle} C_{\circledast\triangle}C_{\circledast}C_{\triangle}$ is a diagonal matrix.

To evaluate the trace of the given diagonal matrix, we need to find the difference between the number of $+1$ and -1 on the diagonal. We write every row in the computational basis by enumerating it with the binary notation. For each row, we denote by α the number of 1's in binary notation appearing in the first m columns and by β, the same on the rest. For example, for $N = 7$, and $m = 4$, the basis element $|1101110\rangle$ leads to α=3 and $\beta = 2$. Considering the phase gates in the equation (A.16), the expression $(-1)^s$ defines whether in the given row the diagonal element is $+1$ or -1, where :

$$s := \binom{\alpha}{1}\binom{\beta}{1} + \binom{\alpha}{1} + \binom{\beta}{1} = \alpha\beta + \alpha + \beta. \tag{A.17}$$

In s, $\binom{\alpha}{1}\binom{\beta}{1}$ denotes how many $C_{\circledast\triangle}$ acts on the row. Also, $\binom{\alpha}{1}$ determines the number of $C_{\circledast}$ and $\binom{\beta}{1}$, number of $C_\triangle$. Every time when the phase gate acts, it changes the sign of the diagonal element on the row. Therefore, we need to determine the number s:

To see whether s is even or odd, we have to consider the following cases exhaustively:

1. α is even & β is even $\quad (-1)^s = +1$
2. α is even & β is odd $\quad (-1)^s = -1$
$\Rightarrow$ These two cases sum up to zero.

3. α is odd & β is even $\quad (-1)^s = -1$
4. α is odd & β is odd $\quad (-1)^s = -1$
$\Rightarrow$ These two contribute with " $-$ " sign.

From the cases 3 and 4, one can directly calculate the trace:

$$\langle K\rangle = \frac{1}{2^N}\Big[-\sum_{\alpha=1,3,\ldots}^{m}\binom{m}{\alpha}\sum_{\beta=0}^{N-m}\binom{N-m}{\beta}\Big] = -\frac{2^{m-1}2^{N-m}}{2^N} = -\frac{1}{2}. \tag{A.18}$$

So, we get that if m is divisible by 4,

$$\langle \underbrace{X\ldots X}_{m}Z\ldots Z\rangle = -\frac{1}{2}. \tag{A.19}$$

Case #2: We use the identical approach: when $m = 2 \ mod \ 4$, we write out all remaining phase gates and continue the derivation from equation (A.5):

$$\langle K \rangle = \langle + |^{\otimes N} X \dots XZ \dots Z \prod_{\forall \circledast, \forall \triangle} C_{\circledast \triangle} C_{\triangle} |+\rangle^{\otimes N}. \tag{A.20}$$

Again we use the fact that X is an eigenstate of $\langle + |$ and $Z = C_{\triangle}$. As in (A.20), there is already one $(C_{\triangle})$, they cancel. Therefore, we are left with:

$$\langle K \rangle = \langle + |^{\otimes N} \prod_{\forall \circledast, \forall \triangle} C_{\circledast \triangle} |+\rangle^{\otimes N} = \frac{1}{2^N} Tr \Big[\prod_{\forall \circledast, \forall \triangle} C_{\circledast \triangle} \Big]. \tag{A.21}$$

We need to define the sign of the diagonal element by $(-1)^s$, where

$$s = \binom{\alpha}{1} \binom{\beta}{1} = \alpha\beta. \tag{A.22}$$

1. α is even $\quad (-1)^s = +1 \qquad \Rightarrow$ This case contributes with the positive sign in the trace

2. α is odd & β is even $\quad (-1)^s = +1$
3. α is odd & β is odd $\quad (-1)^s = -1$ $\qquad \Rightarrow$ These two give zero contribution together.

As the case 2 and 3 add up to zero, we only consider the case 1:

$$\langle K \rangle = \frac{1}{2^N} \sum_{\alpha = 0,2,\dots}^{m} \binom{m}{\alpha} \sum_{\beta=0}^{N-m} \binom{N-m}{\beta} = \frac{2^{m-1} 2^{N-m}}{2^N} = \frac{1}{2}. \tag{A.23}$$

So, we get that if m is NOT divisible by 4,

$$\langle \underbrace{X \dots X}_{m} Z \dots Z \rangle = \frac{1}{2}. \tag{A.24}$$

This completes the proof. □

Correlations for Pauli-X operators for three-uniform hypergraph states

Proof. In this proof of Eq. (3.23) we employ the notation introduced in details in the proof of the Eq. (3.22).

$$\langle K \rangle := \langle H_3^N | XX \dots XX | H_3^N \rangle = \langle + |^{\otimes N} \Big[\prod_{e \in E} C_e \Big] XX \dots XX \Big[\prod_{e \in E} C_e \Big] |+\rangle^{\otimes N}. \tag{A.25}$$

We use the identity (A.1), to regroup the phase gates on the right hand side of the expression (A.25). Therefore, we count the multiplicity of the remaining phase gates:

$\#\circledast\,\circledast\,\circledast$ Each C_e, where $|e| = 3$, occurs once and cancels with the one on right hand side.

$\#\circledast\circledast$ $= \binom{N-2}{1}$ is even $\Rightarrow C_{\circledast\circledast}$ cancels .

$\#\circledast$ $= \binom{N-1}{2} = \frac{(N-1)(N-2)}{2}$ is $\begin{cases} \text{odd, if } N = 0 \; mod \; 4 & \Rightarrow C_{\circledast} \text{ remains.} \\ \text{even, if } N = 2 \; mod \; 4 & \Rightarrow C_{\circledast} \text{ cancels.} \end{cases}$

$\#\{\}$ $= \binom{N}{3} = \frac{N(N-1)(N-2)}{2\cdot 3}$ is even $\Rightarrow$ global sign GS is positive.

Therefore, we need to consider two cases to continue the derivation of the expression (A.25):

Case #1: If $N = 0 \; mod \; 4$, then

$$\langle K\rangle = \langle +|^{\otimes N} XX\ldots XX \prod_{\circledast\in E} C_{\circledast}|+\rangle^{\otimes N} = \langle +|^{\otimes N} \prod_{\circledast\in E} C_{\circledast}|+\rangle^{\otimes N} = 0. \tag{A.26}$$

Case #2: If $N = 2 \; mod \; 4$, then

$$\langle K\rangle = \langle +|^{\otimes N} XX\ldots XX|+\rangle^{\otimes N} = \Big[\langle +|+\rangle\Big]^N = 1. \tag{A.27}$$

□

A.2 Complete four-uniform hypergraph correlations

Proof. Each part of the equations (3.6) needs a separate consideration. note that the notation and machinery that is employed in the proof is based on the proof of the Eq. 3.22. Therefore, we advise the reader to become familiar with that one first.

Part 1. We consider the cases when $N = 8k-2$, $N = 8k-1$ or $8k$ and odd m together. We prove (i) first:

$$\langle G_1\rangle = \langle H_4^N|\underbrace{X\ldots X}_{m}Z\ldots Z|H_4^N\rangle = \langle +|^{\otimes N}\Big(\prod_{e\in E} C_e\Big)XX\ldots XZ\ldots Z\Big(\prod_{e\in E} C_e\Big)|+\rangle^{\otimes N}. \tag{A.28}$$

We need to use the identity (A.1) to regroup all the phase gates on the right hand side of the expression (A.28). If each phase gate occurs even number of times, they give an identity, otherwise, they are used in the further calculations. We consider each case separately in the following table:

Remark: All four-qubit phase gates move with the multiplicity one to the right side and therefore, cancel out with the same phase gate on the right. The detailed reasoning was discussed in proof of Eq. (3.22) in the Appendix A.1. So, we skipped such scenarios in Table A.2.

Now we consider two cases of $(m-1)$ separately and for each case we fix the global sign (GL) defined in Table A.2.

1. $\#\triangle\,\triangle\,\triangle \quad = \binom{m}{1}$ is odd $\Rightarrow C_{\triangle\triangle\triangle}$ remains.

2. $\#\triangle\triangle \quad = \binom{m}{2} = \frac{m(m-1)}{2}$ is $\begin{cases} \text{even, if } (m-1) = 0 \bmod 4 & \Rightarrow C_{\triangle\triangle} \text{ cancels.} \\ \text{odd, if } (m-1) = 2 \bmod 4 & \Rightarrow C_{\triangle\triangle} \text{ remains.} \end{cases}$

$\#\circledast\,\triangle\,\triangle \quad = \binom{m-1}{1}$ is even $\Rightarrow\ C_{\circledast\triangle\triangle}$ cancels.

3. $\#\triangle \quad = \binom{m}{3} = \frac{m(m-1)(m-2)}{2\cdot 3}$ is $\begin{cases} \text{even, if } (m-1) = 0 \bmod 4 & \Rightarrow C_{\triangle} \text{ cancels.} \\ \text{odd, if } (m-1) = 2 \bmod 4 & \Rightarrow C_{\triangle} \text{ remains.} \end{cases}$

$\#\circledast\,\circledast\,\triangle \quad = \binom{m-2}{1}$ is odd $\Rightarrow C_{\circledast\circledast\triangle}$ remains.

$\#\circledast\triangle \quad = \binom{m-1}{2} = \frac{(m-1)(m-2)}{2}$ is $\begin{cases} \text{even, if } (m-1) = 0 \bmod 4 & \Rightarrow C_{\circledast\triangle} \text{ cancels.} \\ \text{odd, if } (m-1) = 2 \bmod 4 & \Rightarrow C_{\circledast\triangle} \text{ remains.} \end{cases}$

4. $\#\circledast\,\circledast\,\circledast \quad = \binom{m-3}{1}$ is even $\Rightarrow\ C_{\circledast\circledast\circledast}$ cancels.

$\#\circledast\circledast \quad = \binom{m-2}{2} = \frac{(m-2)(m-3)}{2}$ is $\begin{cases} \text{odd, if } (m-1) = 0 \bmod 4 & \Rightarrow C_{\circledast\circledast} \text{ remains.} \\ \text{even, if } (m-1) = 2 \bmod 4 & \Rightarrow C_{\circledast\circledast} \text{ cancels.} \end{cases}$

$\#\circledast \quad = \binom{m-1}{3} = \frac{(m-1)(m-2)(m-3)}{2\cdot 3}$ is even $\Rightarrow\ C_{\circledast}$ cancels.

$\#\{\} \quad = \binom{m}{4} = \frac{(m-1)(m-2)(m-3)(m-4)}{2\cdot 3\cdot 4}$ affects global sign (GL).

TABLE A.2: Counting phase gates for a four-uniform case. m is odd.

Case # 1: $(m-1) = 0 \bmod 4$:

$$\langle G_1\rangle = \pm\,\langle +|^{\otimes N} XX\ldots XZ\ldots Z \prod_{\forall\circledast,\forall\triangle} C_{\triangle\triangle\triangle} C_{\circledast\circledast\triangle} C_{\circledast\circledast} |+\rangle^{\otimes N} \tag{A.29}$$

$$= \pm\,\frac{1}{2^N} Tr\Big(\prod_{\forall\circledast,\forall\triangle} C_{\triangle\triangle\triangle} C_{\circledast\circledast\triangle} C_{\circledast\circledast} C_{\triangle}\Big). \tag{A.30}$$

Remark: We write the '$\pm$' sign as we have not fixed the global sign yet.

To evaluate the trace of the given diagonal matrix, we need to find the difference between the number of $+1$'s and -1's on the diagonal. We write every row in the computational basis by enumerating it with the binary notation. Due to the symmetry of the problem, we assign the first m columns to X measurement ($\circledast$) and the rest to, $Z(\triangle)$. For each row, we denote by α the number of 1's in binary notation appearing in the first m column and by β, the same on the rest. This notation is also adopted. See the proof of Eq. (3.22) for more detailed explanation.

Considering the phase gates in (A.29), the expression $(-1)^s$ defines whether in the given row the diagonal element is $+1$ or -1, where :

$$s := \binom{\beta}{3} + \binom{\alpha}{2}\binom{\beta}{1} + \binom{\alpha}{2} + \binom{\beta}{1} = \frac{\beta(\beta-1)(\beta-2)}{2\cdot 3} + \frac{\alpha(\alpha-1)}{2}(\beta+1) + \beta. \tag{A.31}$$

The sign of the diagonal element is determined at follows:

1. α is even & β is even: if $\alpha = 0 \bmod 4 \Rightarrow (-1)^s = +1$
if $\alpha = 2 \bmod 4 \Rightarrow (-1)^s = -1$

2. α is odd & β is even: if $(\alpha - 1) = 0 \bmod 4 \Rightarrow (-1)^s = +1$
if $(\alpha - 1) = 2 \bmod 4 \Rightarrow (-1)^s = -1$

3. (Any α) & β is odd: if $(\beta - 1) = 0 \bmod 4 \Rightarrow (-1)^s = -1$
if $(\beta - 1) = 2 \bmod 4 \Rightarrow (-1)^s = +1$

Having established the ± 1 values for each row, we can sum them up to find the trace in (A.29). Here we use the identities (A.2) and (A.3) and afterwards the look-up Table A.1 to insert the numerical values where necessary:

$$\begin{aligned}
\langle G_1 \rangle &= \pm \frac{1}{2^N} \Bigg[\sum_{\beta=0,2,4\ldots}^{N-m} \binom{N-m}{\beta} \Big[\sum_{\alpha=0,4,\ldots}^{m} \binom{m}{\alpha} + \binom{m}{\alpha+1} - \binom{m}{\alpha+2} - \binom{m}{\alpha+3} \Big] \\
&\quad + \sum_{\beta=1,5,\ldots} \Big[- \binom{N-m}{\beta} \sum_{\alpha} \binom{m}{\alpha} + \binom{N-m}{\beta+2} \sum_{\alpha} \binom{m}{\alpha} \Big] \Bigg] \\
&= \pm \frac{1}{2^N} \Bigg[\Big[Re\Big[(1+i)^m\Big] + Im\Big[(1+i)^m\Big] \Big] 2^{N-m-1} + 2^m \sum_{\beta=1,5,\ldots}^{N-m} \Big[- \binom{N-m}{\beta} + \binom{N-m}{\beta+2} \Big] \Bigg] \\
&= \pm \frac{1}{2^N} \Bigg[\Big[Re\Big[(1+i)^m\Big] + Im\Big[(1+i)^m\Big] \Big] 2^{N-m-1} - 2^m Im\Big[(1+i)^{N-m}\Big] \Bigg] \equiv \pm \frac{1}{2^N} E.
\end{aligned} \tag{A.32}$$

We have to consider $N = 8k-1$ and $N = 8k$ or $N = 8k-2$ separately to continue the derivation of (A.32):

1. For $N = 8k-1$, using the values from Table A.1:

$$\begin{aligned}
\langle G_1 \rangle &= \pm \frac{1}{2^N} \Big[2^{\frac{m+1}{2}} 2^{N-m-1} - 2^m Im\Big[(1+i)^{N-m}\Big] \Big] \\
&= \pm \frac{2^{\frac{m+1}{2}} 2^{N-m-1} + 2^m 2^{\frac{N-m}{2}}}{2^N} = \pm \frac{2^{\lfloor N/2 \rfloor - m} + 1}{2^{\lfloor N/2 \rfloor - \lfloor m/2 \rfloor}}.
\end{aligned} \tag{A.33}$$

2. For $N = 8k$ or$N = 8k-2$, using the values from Table A.1:

$$\begin{aligned}
\langle G_1 \rangle &= \pm \frac{1}{2^N} \Big[2^{\frac{m+1}{2}} 2^{N-m-1} - 2^m Im\Big[(1+i)^{N-m}\Big] \Big] \\
&= \pm \frac{2^{\frac{m+1}{2}} 2^{N-m-1} + 2^m 2^{\frac{N-m-1}{2}}}{2^N} = \pm \frac{2^{\lfloor N/2 \rfloor - m} + 1}{2^{\lfloor N/2 \rfloor - \lfloor m/2 \rfloor}}.
\end{aligned} \tag{A.34}$$

Therefore,

$$\langle G_1 \rangle = \pm \frac{2^{\lfloor N/2 \rfloor - m} + 1}{2^{\lfloor N/2 \rfloor - \lfloor m/2 \rfloor}}. \tag{A.35}$$

Concerning the sign in (A.35), it is affected by the product of two components: one from the case **4** from Table A.2: GL and the other by E from (A.32). If $(m-1) = 0 \bmod 8$, the equation E has a positive sign and also $GL = +1$. And if $(m-1) = 4 \bmod 8$, E has a negative sign and $GL = -1$. Therefore, in both cases or equivalently, for $(m-1) = 0$ *mod* 4,

$$\langle G_1 \rangle = + \frac{2^{\lfloor N/2 \rfloor - m} + 1}{2^{\lfloor N/2 \rfloor - \lfloor m/2 \rfloor}}. \tag{A.36}$$

Case # 2: $(m-1) = 2 \bmod 4$:

$$\begin{aligned} \langle G_1 \rangle &= \pm \langle + |^{\otimes N} XX \dots XZ \dots Z \prod_{\forall \circledast, \forall \triangle} C_{\triangle\triangle\triangle} C_{\triangle\triangle} C_{\circledast\circledast\triangle} C_{\circledast\triangle} C_{\triangle} | + \rangle^{\otimes N} \\ &= \pm \frac{1}{2^N} Tr(\prod_{\forall \circledast, \forall \triangle} C_{\triangle\triangle\triangle} C_{\triangle\triangle} C_{\circledast\circledast\triangle} C_{\circledast\triangle}). \end{aligned} \tag{A.37}$$

In this case, we apply the same technique to determine the sign:

$$s := \binom{\beta}{3} + \binom{\beta}{2} + \binom{\alpha}{2}\binom{\beta}{1} + \binom{\alpha}{1}\binom{\beta}{1} = \frac{\beta(\beta-1)(\beta-2)}{2 \cdot 3} + \frac{\beta(\beta-1)}{2} + \frac{\alpha(\alpha-1)}{2}\beta + \alpha\beta. \tag{A.38}$$

The sign of s, is determined at follows:

1. β is even & any α — if $\beta = 0 \bmod 4 \Rightarrow (-1)^s = +1$; if $\beta = 2 \bmod 4 \Rightarrow (-1)^s = -1$

2. β is odd & α is even: — if $\alpha = 0 \bmod 4 \Rightarrow (-1)^s = +1$; if $\alpha = 2 \bmod 4 \Rightarrow (-1)^s = -1$

3. β is odd & α is odd: — if $(\alpha - 1) = 0 \bmod 4 \Rightarrow (-1)^s = -1$; if $(\alpha - 1) = 2 \bmod 4 \Rightarrow (-1)^s = +1$

$$\begin{aligned} \langle G_1 \rangle &= \pm \frac{1}{2^N} \Bigg[\sum_{\beta=0,4\dots} \Bigg[\binom{N-m}{\beta} \sum_{\alpha=0}^{m} \binom{m}{\alpha} - \binom{N-m}{\beta+2} \sum_{\alpha=0}^{m} \binom{m}{\alpha} \Bigg] \\ &\quad + \sum_{\beta=1,3,\dots} \binom{N-m}{\beta} \Bigg[\sum_{\alpha=0,4,\dots}^{m} \binom{m}{\alpha} - \binom{m}{\alpha+1} - \binom{m}{\alpha+2} + \binom{m}{\alpha+3} \Bigg] \Bigg] \\ &= \pm \frac{1}{2^N} \Bigg[2^m \sum_{\beta=0,4,\dots} \Bigg[\binom{N-m}{\beta} - \binom{N-m}{\beta+2} \Bigg] + 2^{N-m-1} \Bigg[Re\Big[(1+i)^m\Big] - Im\Big[(1+i)^m\Big] \Bigg] \Bigg] \\ &= \pm \frac{1}{2^N} \Bigg[2^m Re\Big[(1+i)^{N-m}\Big] + 2^{N-m-1} \Bigg[Re\Big[(1+i)^m\Big] - Im\Big[(1+i)^m\Big] \Bigg] \Bigg] \equiv \frac{1}{2^N} E. \end{aligned} \tag{A.39}$$

We have to consider $N = 8k-1$ and $N = 8k$ or $N = 8k-2$ separately to continue the derivation of (A.32):

1. For $N = 8k-1$, using the values from Table A.1:

$$\begin{aligned}\langle G_1\rangle &= \pm\frac{1}{2^N}\left[2^m Re\Big[(1+i)^{N-m}\Big] + 2^{\frac{m+1}{2}}2^{N-m-1}\right] \\ &= \pm\frac{2^m 2^{\frac{N-m}{2}} + 2^{\frac{m+1}{2}}2^{N-m-1}}{2^N} = \pm\frac{2^{\lfloor N/2\rfloor - m}+1}{2^{\lfloor N/2\rfloor - \lfloor m/2\rfloor}}.\end{aligned} \tag{A.40}$$

2. For $N = 8k$ or$N = 8k-2$, using the values from Table A.1:

$$\begin{aligned}\langle G_1\rangle &= \pm\frac{1}{2^N}\left[2^m Re\Big[(1+i)^{N-m}\Big] + 2^{\frac{m+1}{2}}2^{N-m-1}\right] \\ &= \pm\frac{2^m 2^{\frac{N-m-1}{2}} + 2^{\frac{m+1}{2}}2^{N-m-1}}{2^N} == \pm\frac{2^{\lfloor N/2\rfloor - m}+1}{2^{\lfloor N/2\rfloor - \lfloor m/2\rfloor}}.\end{aligned} \tag{A.41}$$

Therefore,

$$\langle G_1\rangle = \pm\frac{2^{\lfloor N/2\rfloor - m}+1}{2^{\lfloor N/2\rfloor - \lfloor m/2\rfloor}}. \tag{A.42}$$

Concerning the sign in (A.42), it is affected by the product of two components: one from the case **4** from Table A.2: GL and the other by E in (A.39).

Hence, if $(m-3) = 0 \bmod 8$, E has a negative sign and $GL = +1$. And if $(m-3) = 4 \bmod 8$, E has a positive sign and $GL = -1$. Therefore, in both cases or equivalently, for $(m-1) = 2\ mod\ 4$,

$$\langle G_1\rangle = -\frac{2^{\lfloor N/2\rfloor - m}+1}{2^{\lfloor N/2\rfloor - \lfloor m/2\rfloor}}. \tag{A.43}$$

This completes the proof of part 1 (i).

Part 1 (ii) For $N = 8k-1$, show that

$$\langle G_2\rangle = \langle \underbrace{XX\ldots XX}_{N}\rangle = -1. \tag{A.44}$$

Here as well we use the identity (A.1) to count the multiplicity of remaining phase gates. Since all the measurements are in X direction, we need to make a new table with the same notations as in the previous case:

Therefore,

$$\langle G_2\rangle = -\frac{1}{2^N}Tr(\mathbb{1}) = -1. \tag{A.45}$$

This finishes the proof of part 1.

1.	$\#\circledast\circledast\circledast\circledast$	every gate occurs only once $\Rightarrow$ every C_e cancels with the C_e.
2.	$\#\circledast\circledast\circledast$	$\binom{8k-4}{1}$ is even $\Rightarrow$ $C_{\circledast\circledast\circledast}$ cancels.
3.	$\#\circledast\circledast$	$\binom{8k-3}{2}$ is even $\Rightarrow$ $C_{\circledast\circledast}$ cancels.
4.	$\#\circledast$	$\binom{8k-2}{3}$ is even $\Rightarrow$ $C_{\circledast}$ cancels.
5.	$\#\{\}$	$\binom{8k-1}{4}$ is odd $\Rightarrow$ we get a global negative sign.

TABLE A.3: Counting phase gates for a four-uniform HG when each system is measured in X direction.

Part 2: We show that, for $N = 4k+1$:

$$\langle G_3\rangle = \langle \underbrace{X\dots X}_{m} Z\dots Z\rangle = \begin{cases} +\frac{1}{2^{\lceil m/2\rceil}}, & \text{if } (m-1) = 0 \ mod\ 4, \\ -\frac{1}{2^{\lceil m/2\rceil}}, & \text{if } (m-1) = 2 \ mod\ 4, \\ \frac{1}{2^{\lfloor N/2\rfloor}}, & \text{if } m = N. \end{cases} \tag{A.46}$$

Since the number of systems measured in the X direction is the same in this part as it was in part 1, we can use the results demonstrated in Table A.2. Therefore, we use equation (A.32) when $m-1 = 0 \bmod 4$ and (A.39), for $m-1 = 2 \bmod 4$.

Case # 1: $(m-1) = 0 \bmod 4$:

$$\langle G_3\rangle = \pm\frac{1}{2^N}\left[\left[Re\left[(1+i)^m\right] + Im\left[(1+i)^m\right]\right]2^{N-m-1} - 2^m Im\left[(1+i)^{N-m}\right]\right] = \pm\frac{1}{2^N}E. \tag{A.47}$$

As $N = 4k+1$, we have that $N-m = 4k+1-m = 4k-(m-1)$, which is divisible by 4. Therefore, $Im\left[(1+i)^{N-m}\right] = 0$ and equation (A.47) reduces to:

$$\langle G_3\rangle = \pm\frac{2^{N-m-1}}{2^N}\left[Re\left[(1+i)^m\right] + Im\left[(1+i)^m\right]\right] = \pm\frac{1}{2^{\lceil m/2\rceil}}. \tag{A.48}$$

We need to fix the global sign GL from Table A.2. For this, we consider two cases. First, if $(m-1) = 0 \bmod 8$, then $GL = +$ and so is the sign E in equation (A.47):

$$\langle G_3\rangle = +\frac{1}{2^{\lceil m/2\rceil}}. \tag{A.49}$$

Second, if $(m-1) = 4 \bmod 8$, then $GL = -$ and so is the sign of$E$ in equation (A.47):

$$\langle G_3\rangle = +\frac{1}{2^{\lceil m/2\rceil}}. \tag{A.50}$$

Case # 2: For $(m-1) = 2 \bmod 4$:

$$\langle G_3 \rangle = \pm \frac{1}{2^N} \left[2^m Re\Big[(1+i)^{N-m}\Big] + 2^{N-m-1} \left[Re\Big[(1+i)^m\Big] - Im\Big[(1+i)^m\Big] \right] \right]. \tag{A.51}$$

As $N = 4k+1$, we have $N - m = 4k + 1 - m = 4k - (m-1)$, which is not divisible by 4 but is an even number. Therefore, $Re\Big[(1+i)^{N-m}\Big] = 0$. So, the equation (A.51) reduces to:

$$\langle G_3 \rangle = \pm \frac{2^{N-m-1}}{2^N} \left[Re\Big[(1+i)^m\Big] - Im\Big[(1+i)^m\Big] \right] \equiv \pm \frac{2^{N-m-1}}{2^N} E. \tag{A.52}$$

We need to fix the global sign GL from Table A.2. For this, we consider two cases. First, if $(m-3) = 0 \bmod 8$, then the global sign is positive but the sign of E in (A.52) is negative. Therefore,

$$\langle G_3 \rangle = -\frac{1}{2^{\lceil m/2 \rceil}}. \tag{A.53}$$

Second, if $(m-3) = 4 \bmod 8$, then the global sign is negative but the sign of E in (A.52) is positive. Therefore,

$$\langle G_3 \rangle = -\frac{1}{2^{\lceil m/2 \rceil}}. \tag{A.54}$$

Case # 3: $m = N$ resembles part 1 (ii). The only difference comes in with the number of qubits we are currently working with:

1	$\#\circledast\circledast\circledast\circledast$	e every gate occurs only once $\Rightarrow$ every C_e cancels with the C_e.
2.	$\#\circledast\circledast\circledast$	$\binom{4k-2}{1}$ is even $\Rightarrow$ $C_{\circledast\circledast\circledast}$ cancels.
3.	$\#\circledast\circledast$	$\binom{4k-1}{2}$ is odd $\Rightarrow$ $C_{\circledast\circledast}$ remains.
4.	$\#\circledast$	$\binom{4k}{3}$ is even $\Rightarrow$ $C_{\circledast}$ cancels.
5.	$\#\{\}$	the global sign depends on k, as $\binom{4k+1}{4} = \frac{(4k+1)4k(4k-1)(4k-2)}{2\cdot 3\cdot 4}$

TABLE A.4: Counting phase gates for a four-uniform HG when each system is measured in X direction.

Back to the expectation value,

$$\langle G_3 \rangle = \pm \frac{1}{2^N} Tr\left[\prod_{\forall \circledast} C_{\circledast\circledast} \right]. \tag{A.55}$$

So, we have to count the difference between the amount of $+1$'s and -1's on the diagonal. As we use exactly the same techniques before, we will skip the detailed explanation. The sign on the diagonal is:

$$(-1)^{\binom{\alpha}{2}} = (-1)^{\frac{\alpha(\alpha-1)}{2}}. \tag{A.56}$$

and it is straightforward to evaluate it for each value of α.

$$\begin{aligned}\langle G_3\rangle &= \pm\frac{1}{2^N}\left[\sum_{\alpha=0,4,\ldots}^{N}\binom{N}{\alpha}+\binom{N}{\alpha+1}-\binom{N}{\alpha+2}-\binom{N}{\alpha+3}\right]\\ &= \pm\frac{1}{2^N}\left[Re\Big[(1+i)^N\Big]+Im\Big[(1+i)^N\Big]\right]\equiv\pm\frac{1}{2^N}E.\end{aligned} \tag{A.57}$$

Keeping in mind that $N = 4k+1$, the global sign from Table A.4 is positive for even k and negative for odd. The sign of E in (A.57) is positive if k is even and negative, otherwise. Therefore,

$$\langle G_3\rangle = \frac{1}{2^{\lfloor N/2\rfloor}}. \tag{A.58}$$

This completes the proof of part 2.

Part 3: We start with (ii). We show that for $N = 8k+2$, or $8k+4$:

(ii)

$$\langle G_4\rangle = \langle XX\ldots XX\rangle = \frac{2^{\frac{N}{2}-1}+1}{2^{\frac{N}{2}}}. \tag{A.59}$$

Although the result seems identical, unfortunately, each case needs a separate treatment. The technique is similar to the previous proofs, though. We just mind the number of qubits we are working with:

For $N = 8k+2$ we find the remaining phase gates as follows:

1	$\#\circledast\circledast\circledast\circledast$	each gate only once; thus, every C_e cancels with the C_e.
2.	$\#\circledast\circledast\circledast$	$\binom{8k-1}{1}$ is odd $\Rightarrow$ $C_{\circledast\circledast\circledast}$ remains.
3.	$\#\circledast\circledast$	$\binom{8k}{2}$ is even $\Rightarrow$ $C_{\circledast\circledast}$ cancels.
4.	$\#\circledast$	$\binom{8k+1}{3}$ is even $\Rightarrow$ $C_{\circledast}$ cancels.
5.	$\#\{\}$	$\binom{8k+2}{4}$ is even times $\Rightarrow$ we get a global positive sign.

TABLE A.5: Counting phase gates for a four-uniform HG when each system is measured in X direction.

Therefore,

$$\langle G_4\rangle = \frac{1}{2^N}Tr\Big[\prod_{\forall\circledast}C_{\circledast\circledast\circledast}\Big]. \tag{A.60}$$

We use $(-1)^s$ to define the sign of the diagonal element and $s = \binom{\alpha}{3}$. So, after considering all possible values of α, it is directly obtained that

$$\begin{aligned}\langle G_4\rangle = \frac{1}{2^N} Tr(C_{\circledast\circledast\circledast}) &= \frac{1}{2^N}\Big[\sum_{\alpha=0,2,\ldots}^{N}\binom{N}{\alpha} + \sum_{\alpha=1,5,\ldots}\Big[\binom{N}{\alpha} - \binom{N}{\alpha+2}\Big]\Big] \\ &= \frac{1}{2^N}\Big[2^{N-1} + Im\big[(1+i)^N\big]\Big] = \frac{2^{\frac{N}{2}-1}+1}{2^{\frac{N}{2}}}.\end{aligned} \tag{A.61}$$

For $N = 8k+4$ we find the remaining phase gates as follows:

1. $\#\circledast\circledast\circledast\circledast$ each gate occurs only once $\Rightarrow$ every C_e cancels with the C_e.
2. $\#\circledast\circledast\circledast$ $\binom{8k+1}{1}$ is odd $\Rightarrow$ $C_{\circledast\circledast\circledast}$ remains.
3. $\#\circledast\circledast$ $\binom{8k+2}{2}$ is odd $\Rightarrow$ $C_{\circledast\circledast}$ remains.
4. $\#\circledast$ $\binom{8k+3}{3}$ is odd $\Rightarrow = C_{\circledast}$ remains.
5. $\#\{\}$ $\binom{8k+4}{4}$ is odd $\Rightarrow$ we get a global negative sign, $GL = -1$.

TABLE A.6: Counting phase gates for a four-uniform case in all X direction.

Therefore,

$$\langle G_4\rangle = -\frac{1}{2^N} Tr\Big[\prod_{\forall\circledast} C_{\circledast\circledast\circledast} C_{\circledast\circledast} C_{\circledast}\Big]. \tag{A.62}$$

We use $(-1)^s$ to define the sign of the diagonal element and $s = \binom{\alpha}{3} + \binom{\alpha}{2} + \binom{\alpha}{1}$. So, after considering all possible values of α, it is directly obtained that

$$\begin{aligned}\langle G_4\rangle = -\frac{1}{2^N} Tr(C_{\circledast\circledast\circledast} C_{\circledast\circledast} C_{\circledast}) &= -\frac{1}{2^N}\Big[\sum_{\alpha=0,4,\ldots}^{N}\Big[\binom{N}{\alpha} - \binom{N}{\alpha+2}\Big] - \sum_{\alpha=1,3,\ldots}^{N}\binom{N}{\alpha}\Big] \\ = -\frac{1}{2^N}\Big[-2^{N-1} + Re\big[(1+i)^N\big]\Big] &= \frac{2^{N-1}+2^{N/2}}{2^N} = \frac{2^{\frac{N}{2}-1}+1}{2^{\frac{N}{2}}}.\end{aligned} \tag{A.63}$$

This finishes the proof of part (i).

(ii) We need to show that

$$\langle G_4\rangle = \langle \underbrace{X\ldots X}_{m} Z\ldots Z\rangle = \begin{cases} +\frac{2^{m/2-1}}{2^{N/2}} & \text{if } (N-m) = 0 \ mod\ 4, \\ -\frac{2^{m/2-1}}{2^{N/2}} & \text{if } (N-m) = 2 \ mod\ 4. \end{cases} \tag{A.64}$$

Note that in this case m is an even number. Therefore, we have to derive again from the scratch how phase gates can be moved to the right hand side of the expression and for this we use the identity $(A.1)$.

Remark: Similarly to previous proofs the four-qubit phase gates cancel out. Therefore, we directly skip the discussion about them.

1. $\#\triangle\,\triangle\,\triangle \;= \binom{m}{1}$ is even $\Rightarrow\ C_{\triangle\triangle\triangle}$ cancels.

2. $\#\triangle\triangle \;= \binom{m}{2} = \frac{m(m-1)}{2}$ is $\begin{cases} \text{even, if } m = 0 \bmod 4 & \Rightarrow C_{\triangle\triangle} \text{ cancels.} \\ \text{odd, if } m = 2 \bmod 4 & \Rightarrow C_{\triangle\triangle} \text{ remains.} \end{cases}$

$\#\circledast\,\triangle\,\triangle \;= \binom{m-1}{1}$ is odd $\Rightarrow C_{\circledast\triangle\triangle}$ remains.

3. $\#\triangle \;= \binom{m}{3} = \frac{m(m-1)(m-2)}{2\cdot 3}$ is even $\Rightarrow\ C_{\triangle}$ cancels.

$\#\circledast\,\circledast\,\triangle \;= \binom{m-2}{1}$ is even $\Rightarrow\ C_{\circledast\circledast\triangle}$ cancels.

$\#\circledast\triangle \;= \binom{m-1}{2} = \frac{(m-1)(m-2)}{2}$ is $\begin{cases} \text{odd, if } m = 0 \bmod 4 & \Rightarrow C_{\circledast\triangle} \text{ remains.} \\ \text{even, if } m = 2 \bmod 4 & \Rightarrow C_{\circledast\triangle} \text{ cancels.} \end{cases}$

4. $\#\circledast\,\circledast\,\circledast \;= \binom{m-3}{1}$ is odd $\Rightarrow\ C_{\circledast\circledast\circledast}$ remains.

$\#\circledast\circledast \;= \binom{m-2}{2} = \frac{(m-2)(m-3)}{2}$ is $\begin{cases} \text{odd, if } m = 0 \bmod 4 & \Rightarrow C_{\circledast\circledast} \text{ remains.} \\ \text{even, if } m = 2 \bmod 4 & \Rightarrow C_{\circledast\circledast} \text{ cancels.} \end{cases}$

$\#\circledast \;= \binom{m-1}{3} = \frac{(m-1)(m-2)(m-3)}{2\cdot 3}$ is $\begin{cases} \text{odd, if } m = 0 \bmod 4 & \Rightarrow C_{\circledast} \text{ remains.} \\ \text{even, if } m = 2 \bmod 4 & \Rightarrow C_{\circledast} \text{ cancels.} \end{cases}$

$\#\{\} \;= \binom{m}{4} = \frac{m(m-1)(m-2)(m-3)}{2\cdot 3\cdot 4}$ affects the global sign (GL).

TABLE A.7: Counting phase gates for the four-uniform HG state, for even m.

We need to consider two cases, when $m = 0 \bmod 4$ and $m = 2 \bmod 4$ for each $N = 8k+2$ and $8k+4$ separately:

Case # 1: If $m = 0 \bmod 4$:

$$\begin{aligned} \langle G_4\rangle &= \pm\langle +|^{\otimes N} XX\ldots XZ\ldots Z \prod_{\forall\circledast,\forall\triangle} C_{\circledast\triangle\triangle} C_{\circledast\triangle} C_{\circledast\circledast\circledast} C_{\circledast\circledast} C_{\circledast} |+\rangle^{\otimes N} \\ &= \pm\frac{1}{2^N} Tr\Big[\prod_{\forall\circledast,\forall\triangle} C_{\circledast\triangle\triangle} C_{\circledast\triangle} C_{\circledast\circledast\circledast} C_{\circledast\circledast} C_{\circledast} C_{\triangle}\Big]. \end{aligned} \tag{A.65}$$

We use $(-1)^s$ to define the sign of the diagonal element and $s = \binom{\alpha}{1}\binom{\beta}{2} + \binom{\alpha}{1}\binom{\beta}{1} + \binom{\alpha}{3} + \binom{\alpha}{2} + \binom{\alpha}{1} + \binom{\beta}{1}$. If s is even, the value on the diagonal is $+1$ and -1, otherwise. We consider all possible values of α and β:

1. α is even & β is even
if $\alpha = 0 \bmod 4 \Rightarrow (-1)^s = +1$
if $\alpha = 2 \bmod 4 \Rightarrow (-1)^s = -1$

2. α is even & β is odd:
if $\alpha = 0 \bmod 4 \Rightarrow (-1)^s = -1$
if $\alpha = 2 \bmod 4 \Rightarrow (-1)^s = +1$

From here one can easily spot that for even α, there is equal number of $+1$ and -1 on the diagonal. So, they do not contribute in the calculations. We now consider the odd α:

3. α is odd & β is even if $\beta = 0 \bmod 4 \Rightarrow (-1)^s = -1$
if $\beta = 2 \bmod 4 \Rightarrow (-1)^s = +1$

4. α is odd & β is odd: if $(\beta - 1) = 0 \bmod 4 \Rightarrow (-1)^s = -1$
if $(\beta - 1) = 2 \bmod 4 \Rightarrow (-1)^s = +1$

We now continue calculation of the trace from $(A.65)$:

$$\begin{aligned}\langle G_4 \rangle &= \pm\frac{1}{2^N}\sum_{\alpha=1,3,5\ldots}\binom{m}{\alpha}\Big[\sum_{\beta=0,4,\ldots}^{N-m} -\binom{N-m}{\beta} - \binom{N-m}{\beta+1} + \binom{N-m}{\beta+2} + \binom{N-m}{\beta+3}\Big] \\ &= \pm\frac{2^{m-1}}{2^N}\Big[- Re\Big[(1+i)^{N-m}\Big] - Im\Big[(1+i)^{N-m}\Big]\Big] = \pm\frac{2^{m-1}}{2^N}\Big(\mp 2^{\frac{N-m}{2}}\Big).\end{aligned} \tag{A.66}$$

We have to take care of the sign which appears from the product of the sign of the sum of real and imaginary part in $(A.66)$ and global sign (GL), which we defined while deriving the remaining phase gates. If m is divisible by 8, $GL = +1$ and since we are in $N = 8k+2$ case, $(N - m = 8k + 2 - m) - 2 \bmod 8$ and therefore:

$$\langle G_4 \rangle = \frac{2^{m-1}}{2^N}\Big(- 2^{\frac{N-m}{2}}\Big) = -\frac{2^{m/2-1}}{2^{N/2}}. \tag{A.67}$$

If m is not divisible by 8, the global sign $GL = -1$, and the sum of real and imaginary part also contribute with a negative sign. Thus,

$$\langle G_4 \rangle = -\frac{2^{m-1}}{2^N}\Big(- (-2^{\frac{N-m}{2}})\Big) = -\frac{2^{m/2-1}}{2^{N/2}}. \tag{A.68}$$

Since the $N = 8k+4$ case is identical, we only have to mind the sign of the sum of the real and imaginary part. Here as well we consider two cases: if m is divisible by 8, then the global sign $GL = +1$, and the sign of the sum of real and imaginary part is $" - "$. Therefore,

$$\langle G_4 \rangle = \frac{2^{m-1}}{2^N}\Big(- (-2^{\frac{N-m}{2}})\Big) = +\frac{2^{m/2-1}}{2^{N/2}}. \tag{A.69}$$

And if m is not divisible by 8, $GL = -1$, and the sign of real and imaginary part is $" + "$. Therefore,

$$\langle G_4 \rangle = -\frac{2^{m-1}}{2^N}\Big(- (+2^{\frac{N-m}{2}})\Big) = +\frac{2^{m/2-1}}{2^{N/2}}. \tag{A.70}$$

Case # 2: If $m = 2 \bmod 4$:

$$\begin{aligned}\langle G_4 \rangle &= \pm\langle +|^{\otimes N} XX\ldots XZ\ldots Z \prod_{\forall\circledast,\forall\triangle} C_{\circledast\triangle\triangle}C_{\circledast\circledast\circledast}C_{\triangle\triangle}|+\rangle^{\otimes N} \\ &= \pm\frac{1}{2^N}Tr(\prod_{\forall\circledast,\forall\triangle} C_{\circledast\triangle\triangle}C_{\circledast\circledast\circledast}C_{\triangle\triangle}C_{\triangle}).\end{aligned} \tag{A.71}$$

We use $(-1)^s$ to define the sign of the diagonal element and $s = \binom{\alpha}{1}\binom{\beta}{2} + \binom{\alpha}{3} + \binom{\beta}{2} + \binom{\beta}{1}$. If s is even, the value on the diagonal is $+1$ and -1, otherwise. We consider all possible values of α and β:

Considering the terms from odd α:

1. α is odd & β is even
if $(\alpha - 1) = 0 \bmod 4 \Rightarrow (-1)^s = +1$
if $(\alpha - 1) = 2 \bmod 4 \Rightarrow (-1)^s = -1$

2. α is odd & β is odd:
if $(\alpha - 1) = 0 \bmod 4 \Rightarrow (-1)^s = -1$
if $(\alpha - 1) = 2 \bmod 4 \Rightarrow (-1)^s = +1$

It is easy to see that these cases adds up to 0.

3. α is even & β is even
if $\beta = 0 \bmod 4 \Rightarrow (-1)^s = +1$
if $\beta = 2 \bmod 4 \Rightarrow (-1)^s = -1$

4. α is even & β is odd:
if $(\beta - 1) = 0 \bmod 4 \Rightarrow (-1)^s = -1$
if $(\beta - 1) = 2 \bmod 4 \Rightarrow (-1)^s = +1$

Therefore,

$$\begin{aligned}\langle G_4 \rangle &= \pm\frac{1}{2^N} \sum_{\alpha=0,2,4\ldots} \binom{m}{\alpha} \left[\sum_{\beta=0,4,\ldots}^{N-m} \binom{N-m}{\beta} - \binom{N-m}{\beta+1} - \binom{N-m}{\beta+2} + \binom{N-m}{\beta+3} \right] \\ &= \pm 2^{m-1} \left[Re\left[(1+i)^{N-m}\right] - Im\left[(1+i)^{N-m}\right] \right] = \pm\frac{2^{m/2-1}}{2^{N/2}}.\end{aligned} \tag{A.72}$$

To fix the sign, we need to first consider $N = 8k+2$, and $(m-2) = 0 \bmod 8$. Then the global sign $GL = +1$ and type of $N - m$ also yields a positive sign. But if $(m-2) = 4 \bmod 8$, global sign in negative and the $N - m$ also yields the negative sign. So,

$$\langle G_4 \rangle = \frac{2^{m/2-1}}{2^{N/2}}. \tag{A.73}$$

$N = 8k+4$ case is identical to $N = 8k+2$, therefore we will just state the result. For $N = 8k+4$

$$\langle G_4 \rangle = -\frac{2^{m/2-1}}{2^{N/2}}. \tag{A.74}$$

To sum up,

$$\langle G_4 \rangle = \begin{cases} +\frac{2^{m/2-1}}{2^{N/2}} & \text{if } (N-m) = 0 \; mod \; 4, \\ -\frac{2^{m/2-1}}{2^{N/2}} & \text{if } (N-m) = 2 \; mod \; 4. \end{cases} \tag{A.75}$$

This finishes the proof of part 3.

Part 4: We show that for $N = 8k+3$, $\langle \underbrace{X \ldots X}_{m} \underbrace{Z \ldots Z}_{N-m-1} \mathbb{1} \rangle$ for even m gives the same exact result as the part 3 (i).

We tackle the problem as follows: We make a measurement on one of the qubits in Z direction and depending on the measurement outcome, we obtain the new $|H^M_{4_{new}}\rangle$ state, where $M := N-1$. Then we consider the expectation values for the all possible measurement outcomes and $|H^M_{4_{new}}\rangle$. From that we conclude the statement in the part 4.

Initial HG state $|H^N_4\rangle$ can be written in the following form as well:

$$\begin{aligned}|H^N_4\rangle =& \prod_e C_e|+\rangle^{\otimes N} = \prod_{e',e''} C_{e'}C_{e''}|+\rangle^{\otimes N} \\ =& \prod_{e',e''}\left[\mathbb{1}_{e'\setminus N}|0\rangle_N\langle 0|_N + C_{e'\setminus N}|1\rangle_N\langle 1|_N\right]C_{e''}|+\rangle^{\otimes N},\end{aligned} \tag{A.76}$$

where e' represents the gates containing the last qubit, N and e'' represents the ones which do not contain N^{th} qubit. And $e = e' + e''$. Then if one makes a measurement in Z basis on the last qubit and obtains outcome $+$,

$$\begin{aligned}|H^{M+}_{4_{new}}\rangle = \langle 0_N|H^N_4\rangle =& \prod_{e',e''}\left[\langle 0|_N\mathbb{1}_{e'\setminus N}|0\rangle_N\langle 0|_N + \langle 0|_N C_{e'\setminus N}|1\rangle_N\langle 1|_N\right]C_{e''}|+\rangle^{\otimes N} \\ =& \prod_{e',e''}\mathbb{1}_{e'\setminus N}\langle 0|_N C_{e''}|+\rangle^{\otimes N} = \langle 0|_N\prod_{e',e''}\mathbb{1}_{e'\setminus N}C_{e''}|+\rangle^{\otimes M}\big(|0\rangle_N + |1\rangle_N\big). \\ =& \prod_{e',e''}\mathbb{1}_{e'\setminus N}C_{e''}|+\rangle^{\otimes M} = \prod_{e''}C_{e''}|+\rangle^{\otimes M}.\end{aligned} \tag{A.77}$$

So, $+$ outcome after measuring in Z direction leaves us with $|H^{M+}_{4_{new}}\rangle$, which is precisely four uniform M-qubit HG state. Now, let us see what is the remaining state if one gets $-$ as an outcome result:

$$\begin{aligned}|H^{M-}_{4_{new}}\rangle = \langle 1_N|H^N_4\rangle =& \prod_{e',e''}\left[\langle 1|_N\mathbb{1}_{e'\setminus N}|0\rangle_N\langle 0|_N + \langle 1|_N C_{e'\setminus N}|1\rangle_N\langle 1|_N\right]C_{e''}|+\rangle^{\otimes N} \\ =& \prod_{e',e''}C_{e'\setminus N}\langle 1|_N C_{e''}|+\rangle^{\otimes N} = \langle 1|_N\prod_{e',e''}C_{e'\setminus N}C_{e''}|+\rangle^{\otimes M}\big(|0\rangle_N + |1\rangle_N\big) \\ =& \prod_{e',e''}C_{e'\setminus N}C_{e''}|+\rangle^{\otimes M}.\end{aligned} \tag{A.78}$$

So, $-$ outcome after measuring in Z direction leaves us with $|H^{M-}_{4_{new}}\rangle$, which is precisely a symmetric M-qubit HG state with all possible edges of cardinality four and three. We will call such HG state a three- and four-uniform HG state.

Therefore, problem boils down to showing that, (i) If the measurement outcome is $+$, we get the $M = 8k+2$ four-uniform HG state and the correlations are given in part 3.
(ii) If the measurement outcome is $-$, we get $M = 8k+2$ three- and fouruniform HG state and the following holds:

$$\langle G^-_5\rangle = \langle H^{M-}_{4_{new}}|\underbrace{X\dots X}_{m}Z\dots Z|H^{M-}_{4_{new}}\rangle = \begin{cases} -\frac{2^{m/2-1}}{2^{M/2}} & \text{if } (M-m) = 0 \ mod\ 4, \\ +\frac{2^{m/2-1}}{2^{M/2}} & \text{if } (M-m) = 2 \ mod\ 4. \end{cases} \tag{A.79}$$

(i) $|H_{4_{new}}^{M+}\rangle$, where $M = 8k+2$ was already considered in part 3.

(ii). For $|H_{4_{new}}^{M-}\rangle$,

$$\langle G_5^- \rangle = \langle + |^{\otimes M} \Big[\prod_{e',e'' \in E} C_{e'} C_{e''} \Big] \underbrace{X \dots X}_{m} Z \dots Z \Big[\prod_{e',e'' \in E} C_e C_{e''} \Big] |+\rangle^{\otimes M}. \tag{A.80}$$

Before, we treated three- and four-uniform cases separately. Now, we just need to put them together.

Case # 1: If $m = 0 \bmod 4$:
Then from equations (A.16) and (A.65), we can directly write down that

$$\langle G_5^- \rangle = \frac{1}{2^M} Tr \Big[\prod_{\forall \circledast, \forall \triangle} C_{\circledast \triangle \triangle} C_{\circledast \circledast \circledast} C_{\circledast \circledast} C_{\triangle} \Big]. \tag{A.81}$$

We check the sign of each term on the diagonal by $(-1)^s$, where $s = \binom{\alpha}{1}\binom{\beta}{2} + \binom{\alpha}{3} + \binom{\alpha}{2} + \binom{\beta}{1}$. For this we need to consider each value of α and β separately.

1. α is even & β is even
$\alpha = 0 \bmod 4 \Rightarrow +1$
$\alpha = 2 \bmod 4 \Rightarrow -1$
$\Rightarrow$ These give zero contribution.

2. α is even & β is odd
$\alpha = 0 \bmod 4 \Rightarrow -1$
$\alpha = 2 \bmod 4 \Rightarrow +1$

3. α is odd & β is even
$\beta = 0 \bmod 4 \Rightarrow +1$
$\beta = 2 \bmod 4 \Rightarrow -1$

4. α is odd & β is odd
$\beta - 1 = 0 \bmod 4 \Rightarrow -1$
$\beta - 1 = 2 \bmod 4 \Rightarrow +1$

$$\begin{aligned} \langle G_5^- \rangle &= \pm \frac{1}{2^M} \sum_{\alpha \ odd}^{m} \binom{m}{\alpha} \Big[\sum_{\beta=0,4}^{M-m} \binom{M-m}{\beta} - \binom{M-m}{\beta+1} - \binom{M-m}{\beta+2} + \binom{M-m}{\beta+3} \Big] \\ &= \pm \frac{2^{m-1}}{2^M} \Big[Re(1+i)^{M-m} - Im(1+i)^{M-m} \Big] = \pm \frac{2^{\frac{m}{2}-1}}{2^{M/2}}. \end{aligned} \tag{A.82}$$

If $m = 0 \bmod 8$, real and imaginary part in (A.82) has a negative sign and the global sign coming from Table A.7, GL is positive. Note from equation (A.14) that three uniform gate moving does not introduce any global signs. And if $m = 4 \bmod 8$, real and imaginary part in (A.82) has a positive sign and the global sign coming from Table A.7, GL is negative.Therefore,

$$\langle G_5^+ \rangle = -\frac{2^{\frac{m}{2}-1}}{2^{M/2}}. \tag{A.83}$$

Case # 2: If $m = 2 \bmod 4$:
Then from equations (A.20) and (A.71), we can directly write down that

$$\langle G_5^- \rangle = \pm \frac{1}{2^M} Tr\Big[\prod_{\forall \circledast, \forall \triangle} C_{\circledast \triangle \triangle} C_{\circledast \triangle} C_{\circledast \circledast \circledast} C_{\triangle \triangle} \Big]. \tag{A.84}$$

We check the sign of each term on the diagonal by $(-1)^s$, where $s = \binom{\alpha}{1}\binom{\beta}{2} + \binom{\alpha}{3} + \binom{\beta}{2} + \binom{\alpha}{1}\binom{\beta}{1}$. For this we need to consider each value of α and β separately.

1.	α is even & β is even	$\beta = 0 \bmod 4 \Rightarrow +1$ $\beta = 2 \bmod 4 \Rightarrow -1$	
2.	α is even & β is odd	$\beta - 1 = 0 \bmod 4 \Rightarrow +1$ $\beta - 1 = 2 \bmod 4 \Rightarrow -1$	
3.	α is odd & β is even	$\alpha - 1 = 0 \bmod 4 \Rightarrow +1$ $\alpha - 1 = 2 \bmod 4 \Rightarrow -1$	$\Rightarrow$ These give zero contribution.
4.	α is odd & β is odd	$\alpha - 1 = 0 \bmod 4 \Rightarrow -1$ $\alpha - 1 = 2 \bmod 4 \Rightarrow +1$	

$$\begin{aligned} \langle G_5^- \rangle &= \pm \frac{1}{2^M} \sum_{\alpha \ even}^{m} \binom{m}{\alpha} \Big[\sum_{\beta=0,4}^{M-m} \binom{M-m}{\beta} + \binom{M-m}{\beta+1} - \binom{M-m}{\beta+2} - \binom{M-m}{\beta+3} \Big] \\ &= \pm \frac{1}{2^M} 2^{m-1} \Big[Re(1+i)^{M-m} + Im(1+i)^{M-m} \Big] = \pm \frac{2^{\frac{m}{2}-1}}{2^{M/2}}. \end{aligned} \tag{A.85}$$

If $m - 2 = 0 \bmod 8$, real and imaginary part in (A.85) has a positive sign and the global sign coming from Table A.7, GL is positive. Note from equation (A.14) that the three uniform gate moving does not introduce any global signs. And if $m - 2 = 4 \bmod 8$, real and imaginary part in (A.85) has a negative sign and the global sign coming from Table A.7, GL is negative.Therefore,

$$\langle G_5^- \rangle = + \frac{2^{\frac{m}{2}-1}}{2^{M/2}}. \tag{A.86}$$

Finally, we can put everything together. Since one can observe that $\langle G_5^- \rangle = -\langle G_5^+ \rangle$,

$$|0\rangle\langle 0|\langle G_5^+ \rangle - |1\rangle\langle 1|\langle G_5^- \rangle = |0\rangle\langle 0|\langle G_5^+ \rangle + |1\rangle\langle 1|\langle G_5^+ \rangle = \mathbb{1}\langle G_5^+ \rangle = \langle \underbrace{X \dots X}_{m} \underbrace{Z \dots Z}_{N-m-1} \mathbb{1} \rangle. \tag{A.87}$$

This completes the proof of part 4. □

A.3 Bell and separability inequalities for noisy four-uniform states

Proof. The derivation of this result is very similar to the combinatorial calculations in the previous subsections. Since m is even, we refer to Table A.7 to see what gates remain after regrouping hyperedges on the right hand side of Eq.(3.41):

Case # 1: If $m = 0 \bmod 4$:

$$\begin{aligned}\langle G_6\rangle &= \pm\langle+|^{\otimes N}\underbrace{X\dots X}_{m}\underbrace{Z\dots Z}_{N-m-1}\mathbb{1}\prod_{\forall\circledast,\triangle,\diamondsuit} C_{\circledast\triangle\triangle}C_{\circledast\triangle}C_{\circledast\triangle\diamondsuit}C_{\circledast\diamondsuit}C_{\circledast\circledast\circledast}C_{\circledast\circledast}C_{\circledast}|+\rangle^{\otimes N}\\ &= \pm\frac{1}{2^N}Tr\Big[\prod_{\forall\circledast,\triangle,\diamondsuit} C_{\circledast\triangle\triangle}C_{\circledast\triangle}C_{\circledast\triangle\diamondsuit}C_{\circledast\diamondsuit}C_{\circledast\circledast\circledast}C_{\circledast\circledast}C_{\circledast}C_{\triangle}\Big].\end{aligned} \tag{A.88}$$

Here $\circledast$ again refers to X operator, $\triangle$ to Z and $\diamondsuit$ to $\mathbb{1}$ and it is denoted as γ. The strategy now is similar to the previous proofs: count the number of +1's and -1's on the diagonal and then their difference divided by 2^N gives the trace.

We use $(-1)^s$ to define the sign of the diagonal element and $s = \binom{\alpha}{1}\binom{\beta}{2} + \binom{\alpha}{1}\binom{\beta}{1} + \binom{\alpha}{1}\binom{\beta}{1}\binom{\gamma}{1} + \binom{\alpha}{1}\binom{\gamma}{1} + \binom{\alpha}{3} + \binom{\alpha}{2} + \binom{\alpha}{1} + \binom{\beta}{1}$. If s is even, the value on the diagonal is $+1$ and -1, otherwise. We consider all possible values of α, β, and γ:

a) If γ is even (that is $\gamma = 0$):

1. α is even & β is even
if $\alpha = 0 \bmod 4 \Rightarrow (-1)^s = +1$
if $\alpha = 2 \bmod 4 \Rightarrow (-1)^s = -1$

2. α is even & β is odd:
if $\alpha = 0 \bmod 4 \Rightarrow (-1)^s = -1$
if $\alpha = 2 \bmod 4 \Rightarrow (-1)^s = +1$

From here one can easily spot that for even α, there is equal number of $+1$ and -1 on the diagonal. So, they do not contribute in the calculations. We now consider the odd α:

3. α is odd & β is even
if $\beta = 0 \bmod 4 \Rightarrow (-1)^s = -1$
if $\beta = 2 \bmod 4 \Rightarrow (-1)^s = +1$

4. α is odd & β is odd:
if $(\beta - 1) = 0 \bmod 4 \Rightarrow (-1)^s = -1$
if $(\beta - 1) = 2 \bmod 4 \Rightarrow (-1)^s = +1$

b) If γ is odd (that is $\gamma = 1$):

The cases **1** and **2** don't change. Therefore, they sum up to 0.

3. α is odd & β is even
if $\beta = 0 \bmod 4 \Rightarrow (-1)^s = +1$
if $\beta = 2 \bmod 4 \Rightarrow (-1)^s = -1$

4. Stays the same as in the previous case.

Therefore the result is:

$$\begin{aligned}\langle G_6\rangle = \pm\frac{1}{2^N}\Big(\sum_{\gamma\ even}\binom{\gamma}{0}\Big[\sum_{\alpha\ odd}^{m}\binom{m}{\alpha}\times \\ \Big[\sum_{\beta=0,4\ldots}^{N-m-1}-\binom{N-m-1}{\beta}-\binom{N-m-1}{\beta+1}+\binom{N-m-1}{\beta+2}+\binom{N-m-1}{\beta+3}\Big]\Big] \\ +\sum_{\gamma\ odd}\binom{\gamma}{1}\Big[\sum_{\alpha\ odd}^{m}\binom{m}{\alpha}\times \\ \Big[\sum_{\beta=0,4\ldots}^{N-m-1}\binom{N-m-1}{\beta}-\binom{N-m-1}{\beta+1}-\binom{N-m-1}{\beta+2}+\binom{N-m-1}{\beta+3}\Big]\Big]\Big) \\ =\pm\frac{2^m}{2^N}\cdot(-Im[(1+i)^{N-m-1}]) = \mp\Big(\frac{1}{\sqrt{2}}\Big)^{N-m+2}.\end{aligned} \tag{A.89}$$

It is time to fix a sign. One needs to keep in mind that the sign of the Eq. (A.89) is negative: if $m = 4 \bmod 8$, the global sign from the Table A.7 is negative, and $Im[(1+i)^{N-m-1}] = -2^{\frac{N-m-2}{2}}$. Therefore, an overall sign in negative. If $m = 0 \bmod 8$, global sign is positive and $Im[(1+i)^{N-m-1}] = 2^{\frac{N-m-2}{2}}$. Therefore, an overall sign in negative.

Case # 2: If $m = 2 \bmod 4$:

$$\begin{aligned}\langle G_6\rangle &= \pm\langle+|^{\otimes N}\underbrace{X\ldots X}_{m}\underbrace{Z\ldots Z}_{N-m-1}\mathbb{1}\prod_{\forall\circledast,\triangle,\diamondsuit}C_{\circledast\triangle\triangle}C_{\circledast\circledast\circledast}C_{\triangle\triangle}C_{\circledast\triangle\diamondsuit}C_{\triangle\diamondsuit}|+\rangle^{\otimes N} \\ &= \pm\frac{1}{2^N}Tr(\prod_{\forall\circledast,\triangle,\diamondsuit}C_{\circledast\triangle\triangle}C_{\circledast\circledast\circledast}C_{\triangle\triangle}C_{\circledast\triangle\diamondsuit}C_{\triangle\diamondsuit}C_{\triangle}).\end{aligned} \tag{A.90}$$

We use $(-1)^s$ to define the sign of the diagonal element and $s = \binom{\alpha}{1}\binom{\beta}{2} + \binom{\alpha}{1}\binom{\beta}{1}\binom{\gamma}{1} + \binom{\alpha}{3} + \binom{\beta}{2} + \binom{\beta}{1}\binom{\gamma}{1} + \binom{\beta}{1}$. If s is even, the value on the diagonal is $+1$ and -1, otherwise. We consider all possible values of α, β, and γ:

a) If γ is even (that is $\gamma = 0$):

Considering the terms from even α:

1. α is even & β is even — if $\beta = 0 \bmod 4 \Rightarrow (-1)^s = +1$; if $\beta = 2 \bmod 4 \Rightarrow (-1)^s = -1$

2. α is even & β is odd: — if $(\beta-1) = 0 \bmod 4 \Rightarrow (-1)^s = -1$; if $(\beta-1) = 2 \bmod 4 \Rightarrow (-1)^s = +1$

Considering odd α:

3. α is odd & β is even if $(\alpha-1) = 0 \bmod 4 \Rightarrow (-1)^s = +1$
if $(\alpha-1) = 2 \bmod 4 \Rightarrow (-1)^s = -1$

4. α is odd & β is odd: if $(\alpha-1) = 0 \bmod 4 \Rightarrow (-1)^s = -1$
if $(\alpha-1) = 2 \bmod 4 \Rightarrow (-1)^s = +1$

It is easy to see that cases **3** and **4** adds up to 0.

b) If γ is odd (that is $\gamma = 1$):

1. Stays the same as in the previous case.

2. Gets an opposite sign, therefore, will cancel out with the a) case **2** in the sum.

3. Stays the same as in the previous case.

4. Stays the same as in the previous case.

Therefore the result is:

$$\langle G_6\rangle = \pm\frac{1}{2^N}2^m\left[\sum_{\beta=0,4..}^{N-m-1}\binom{N-m-1}{\beta} - \binom{N-m-1}{\beta+2}\right] = \pm\frac{2^m}{2^N}Re[(1+i)^{N-m-1}]. \quad \text{(A.91)}$$

It is time to fix a sign: if $m = 2 \bmod 8$, the global sign is positive from Table A.7 and $Re[(1+i)^{N-m-1}] = 2^{\frac{N-m-2}{2}}$. Therefore, an overall sign is positive. If $m = 6 \bmod 8$, overall sign in negative and $Re[(1+i)^{N-m-1}] = -2^{\frac{N-m-2}{2}}$. Therefore, an overall sign in positive. □

A.4 Separability inequality for noisy three-uniform states

Proof. As a starting point, we derive the remaining gates on the right hand side of the equations (3.36), the same derivation turns out to be working for Eq. (3.37) and (3.38). This approach is analogous to the previous proves, but now, m is odd. Consider two cases:

1. If $(m-1) = 0 \bmod 4$:

$$\begin{aligned}\langle G_7\rangle &= \pm\langle+|^{\otimes N}\underbrace{X\ldots X}_{m}\underbrace{Z\ldots Z}_{N-m-1}\mathbb{1}\prod_{\forall\circledast,\triangle,\diamondsuit}C_{\circledast\circledast}C_{\triangle\triangle}C_{\triangle\diamondsuit}|+\rangle^{\otimes N}\\ &= \pm\frac{1}{2^N}Tr\Big[C_{\circledast\circledast}C_{\triangle\triangle}C_{\triangle\diamondsuit}C_{\triangle}\Big].\end{aligned} \quad \text{(A.92)}$$

Here $\circledast$ again refers to X operator, $\triangle$ to Z and $\diamondsuit$ to $\mathbb{1}$ and is denoted by γ. The strategy is similar to the previous case: count the number of +1's and -1's on the diagonal. Their difference divided by 2^N, gives the trace.

We use $(-1)^s$ to define the sign of the diagonal element and $s = \binom{\alpha}{2} + \binom{\beta}{2} + \binom{\beta}{1}\binom{\gamma}{1} + \binom{\beta}{1}$. If s is even, the value on the diagonal is $+1$ and -1, otherwise. We consider all possible values of α, β and γ:

1. $\#\circledast\circledast = \binom{m-2}{1}$ is odd $\Rightarrow$ $C_{\circledast\circledast}$ remains.

2. $\#\circledast = \binom{m-1}{2} = \frac{(m-1)(m-2)}{2}$ is $\begin{cases} \text{even, if } (m-1) = 0 \bmod 4 & \Rightarrow C_{\circledast} \text{ cancels.} \\ \text{odd, if } (m-1) = 2 \bmod 4 & \Rightarrow C_{\circledast} \text{ remains.} \end{cases}$

3. $\#\{\} = \binom{m}{3} = \frac{m(m-1)(m-2)}{2\cdot 3}$ is $\begin{cases} \text{even, if } (m-1) = 0 \bmod 4 & \Rightarrow \text{ gives "+".} \\ \text{odd, if } (m-1) = 2 \bmod 4 & \Rightarrow \text{ gives "-".} \end{cases}$

4. $\#\triangle\triangle = \binom{m}{1}$ is odd $\Rightarrow$ $C_{\triangle\triangle}$ remains.
5. $\#\circledast\triangle = \binom{m-1}{1}$ is even $\Rightarrow$ $C_{\circledast\triangle}$ cancels.
6. $\#\triangle = \binom{m}{2} = \frac{m(m-1)}{2\cdot 3}$ is $\begin{cases} \text{even, if } (m-1) = 0 \bmod 4 & \Rightarrow C_{\triangle} \text{ cancels.} \\ \text{odd, if } (m-1) = 2 \bmod 4 & \Rightarrow C_{\triangle} \text{ remains.} \end{cases}$

TABLE A.8: Counting phase gates for a three-uniform HG when m (m is odd) systems are measured in X direction.

a) If γ is even (that is $\gamma = 0$): Considering the terms from even β:

1. β is even & α is even
if $\alpha = 0 \bmod 4$ and $\beta = 0 \bmod 4 \Rightarrow (-1)^s = +1$
if $\alpha = 0 \bmod 4$ and $\beta = 2 \bmod 4 \Rightarrow (-1)^s = -1$
if $\alpha = 2 \bmod 4$ and $\beta = 0 \bmod 4 \Rightarrow (-1)^s = -1$
if $\alpha = 2 \bmod 4$ and $\beta = 2 \bmod 4 \Rightarrow (-1)^s = +1$

2. β is even & α is odd
if $(\alpha - 1) = 0 \bmod 4$ and $\beta = 0 \bmod 4 \Rightarrow (-1)^s = +1$
if $(\alpha - 1) = 0 \bmod 4$ and $\beta = 2 \bmod 4 \Rightarrow (-1)^s = -1$
if $(\alpha - 1) = 2 \bmod 4$ and $\beta = 0 \bmod 4 \Rightarrow (-1)^s = -1$
if $(\alpha - 1) = 2 \bmod 4$ and $\beta = 2 \bmod 4 \Rightarrow (-1)^s = +1$

Considering odd β:

3. β is odd & α is even
if $\alpha = 0 \bmod 4$ and $(\beta - 1) = 0 \bmod 4 \Rightarrow (-1)^s = -1$
if $\alpha = 0 \bmod 4$ and $(\beta - 1) = 2 \bmod 4 \Rightarrow (-1)^s = +1$
if $\alpha = 2 \bmod 4$ and $(\beta - 1) = 0 \bmod 4 \Rightarrow (-1)^s = +1$
if $\alpha = 2 \bmod 4$ and $(\beta - 1) = 2 \bmod 4 \Rightarrow (-1)^s = -1$

4. β is odd & α is odd
if $(\alpha - 1) = 0 \bmod 4$ and $(\beta - 1) = 0 \bmod 4 \Rightarrow (-1)^s = -1$
if $(\alpha - 1) = 0 \bmod 4$ and $(\beta - 1) = 2 \bmod 4 \Rightarrow (-1)^s = +1$
if $(\alpha - 1) = 2 \bmod 4$ and $(\beta - 1) = 0 \bmod 4 \Rightarrow (-1)^s = +1$
if $(\alpha - 1) = 2 \bmod 4$ and $(\beta - 1) = 2 \bmod 4 \Rightarrow (-1)^s = -1$

b) If γ is odd (that is $\gamma = 1$):

Considering the terms from even β:

1. and **2.** Nothing changes in comparison to a) **1.** and **2.**

3. and **4.** These two terms have opposite sign from a) **3.** and **4.** Therefore, in the sum they cancel (γ is always 1.). Therefore,

$$\begin{aligned}\langle G_7\rangle = \frac{1}{2^{N-1}}\Bigg[\sum_{\beta=0,4..}^{N-m-1}\binom{N-m-1}{\beta} - \binom{N-m-1}{\beta+2}\Bigg]\times \\ \Bigg[\sum_{\alpha=0,4..}^{m}\binom{m}{\alpha} + \binom{m}{\alpha+1} - \binom{m}{\alpha+2} - \binom{m}{\alpha+3}\Bigg] \\ = \frac{1}{2^{N-1}} Re[(1+i)^{N-m-1}]\cdot\Big(Re[(1+i)^m] + Im[(1+i)^m]\Big).\end{aligned} \tag{A.93}$$

Now we can consider each cases separately, for this we use the look-up Table A.1:

(i) If $N = 8k+5$ and if $(m-1) = 4 \bmod 8$, $Re[(1+i)^{N-m-1}] = -2^{\frac{N-m-2}{2}}$ and $Re[(1+i)^m] + Im[(1+i)^m] = 2^{\frac{m+1}{2}}$. Therefore,

$$\langle G_7\rangle = -\frac{2^{\frac{N-m-2}{2}}\cdot 2^{\frac{m+1}{2}}}{2^{N-1}} = -\Big(\frac{1}{2}\Big)^{\frac{N-1}{2}}. \tag{A.94}$$

And, if $(m-1) = 0 \bmod 8$, $Re[(1+i)^{N-m-1}] = +2^{\frac{N-m-2}{2}}$ and $Re[(1+i)^m] + Im[(1+i)^m] = -2^{\frac{m+1}{2}}$. Therefore,

$$\langle G_7\rangle = -\frac{2^{\frac{N-m-2}{2}}\cdot 2^{\frac{m+1}{2}}}{2^{N-1}} = -\Big(\frac{1}{2}\Big)^{\frac{N-1}{2}}. \tag{A.95}$$

Exactly the same is true for $N = 8k+7$. But for $N = 8k+6$ and if $(m-1) = 4 \bmod 8$, $Re[(1+i)^{N-m-1}] = -2^{\frac{N-m-1}{2}}$ and $Re[(1+i)^m] + Im[(1+i)^m] = 2^{\frac{m+1}{2}}$. Therefore,

$$\langle G_7\rangle = -\frac{2^{\frac{N-m-1}{2}}\cdot 2^{\frac{m+1}{2}}}{2^{N-1}} = -\Big(\frac{1}{2}\Big)^{\lfloor\frac{N-1}{2}\rfloor}. \tag{A.96}$$

And, if $(m-1) = 0 \bmod 8$, $Re[(1+i)^{N-m-1}] = 2^{\frac{N-m-1}{2}}$ and $Re[(1+i)^m] + Im[(1+i)^m] = -2^{\frac{m+1}{2}}$. Therefore,

$$\langle G_7\rangle = -\frac{2^{\frac{N-m-1}{2}}\cdot 2^{\frac{m+1}{2}}}{2^{N-1}} = -\Big(\frac{1}{2}\Big)^{\lfloor\frac{N-1}{2}\rfloor}. \tag{A.97}$$

(ii) If $N = 8k+1$ and if $(m-1) = 4 \bmod 8$, $Re[(1+i)^{N-m-1}] = -2^{\frac{N-m-2}{2}}$ and $Re[(1+i)^m] + Im[(1+i)^m] = -2^{\frac{m+1}{2}}$. Therefore,

$$\langle G_7\rangle = \frac{2^{\frac{N-m-2}{2}}\cdot 2^{\frac{m+1}{2}}}{2^{N-1}} = \Big(\frac{1}{2}\Big)^{\frac{N-1}{2}}. \tag{A.98}$$

And, if $(m-1) = 0 \bmod 8$, $Re[(1+i)^{N-m-1}] = 2^{\frac{N-m-1}{2}}$ and $Re[(1+i)^m] + Im[(1+i)^m] = 2^{\frac{m+1}{2}}$. Therefore,

$$\langle G_7\rangle = \frac{2^{\frac{N-m-1}{2}}\cdot 2^{\frac{m+1}{2}}}{2^{N-1}} = \Big(\frac{1}{2}\Big)^{\lfloor\frac{N-1}{2}\rfloor}. \tag{A.99}$$

It is analogous for other two cases as well.

(*iii*) For $N = 4k$, $Re[(1+i)^{N-m-1}] = 0$. Therefore, $\langle G_7 \rangle = 0$.

2. If $(m-1) = 2 \bmod 4$:

$$\begin{aligned}\langle G_7 \rangle &= \langle + |^{\otimes N} \underbrace{X \dots X}_{m} \underbrace{Z \dots Z}_{N-m-1} \mathbb{1} \prod_{\forall \circledast, \triangle, \diamondsuit} C_{\circledast\circledast} C_{\circledast} C_{\triangle\triangle} C_{\triangle\diamondsuit} C_{\triangle} C_{\diamondsuit} | + \rangle^{\otimes N} \\ &= \frac{1}{2^N} Tr\Big[C_{\circledast\circledast} C_{\circledast} C_{\triangle\triangle} C_{\triangle\diamondsuit} C_{\diamondsuit} \Big].\end{aligned} \tag{A.100}$$

Here $\circledast$ again refers to X operator, $\triangle$ to Z and $\diamondsuit$ to $\mathbb{1}$ and is denoted by γ. The strategy is similar to the previous case: count the number of +1's and -1's on the diagonal and their difference divided by 2^N, gives the trace.

We use $(-1)^s$ to define the sign of the diagonal element and $s = \binom{\alpha}{2} + \binom{\alpha}{1} + \binom{\beta}{2} + \binom{\beta}{1}\binom{\gamma}{1} + \binom{\gamma}{1}$. If s is even, the value on the diagonal is $+1$ and -1, otherwise. We consider all possible values of α, β and γ:

a) If γ is even (that is $\gamma = 0$): Considering the terms from even β:

1. β is even & α is even
- if $\alpha = 0 \bmod 4$ and $\beta = 0 \bmod 4 \Rightarrow (-1)^s = +1$
- if $\alpha = 0 \bmod 4$ and $\beta = 2 \bmod 4 \Rightarrow (-1)^s = -1$
- if $\alpha = 2 \bmod 4$ and $\beta = 0 \bmod 4 \Rightarrow (-1)^s = -1$
- if $\alpha = 2 \bmod 4$ and $\beta = 2 \bmod 4 \Rightarrow (-1)^s = +1$

2. β is even & α is odd
- if $(\alpha-1) = 0 \bmod 4$ and $\beta = 0 \bmod 4 \Rightarrow (-1)^s = -1$
- if $(\alpha-1) = 0 \bmod 4$ and $\beta = 2 \bmod 4 \Rightarrow (-1)^s = +1$
- if $(\alpha-1) = 2 \bmod 4$ and $\beta = 0 \bmod 4 \Rightarrow (-1)^s = +1$
- if $(\alpha-1) = 2 \bmod 4$ and $\beta = 2 \bmod 4 \Rightarrow (-1)^s = -1$

Considering odd β:

3. β is odd & α is even
- if $\alpha = 0 \bmod 4$ and $(\beta-1) = 0 \bmod 4 \Rightarrow (-1)^s = +1$
- if $\alpha = 0 \bmod 4$ and $(\beta-1) = 2 \bmod 4 \Rightarrow (-1)^s = -1$
- if $\alpha = 2 \bmod 4$ and $(\beta-1) = 0 \bmod 4 \Rightarrow (-1)^s = -1$
- if $\alpha = 2 \bmod 4$ and $(\beta-1) = 2 \bmod 4 \Rightarrow (-1)^s = +1$

4. β is odd & α is odd
- if $(\alpha-1) = 0 \bmod 4$ and $(\beta-1) = 0 \bmod 4 \Rightarrow (-1)^s = -1$
- if $(\alpha-1) = 0 \bmod 4$ and $(\beta-1) = 2 \bmod 4 \Rightarrow (-1)^s = +1$
- if $(\alpha-1) = 2 \bmod 4$ and $(\beta-1) = 0 \bmod 4 \Rightarrow (-1)^s = +1$
- if $(\alpha-1) = 2 \bmod 4$ and $(\beta-1) = 2 \bmod 4 \Rightarrow (-1)^s = -1$

b) If γ is odd (that is $\gamma = 1$):

1. and **2.** These two terms have opposite sign from a) **1.** and **2.** Therefore, in the sum they cancel (γ is always 1.)

3. and **4.** Nothing changes in comparison to a) **3.** and **4.**Therefore,

$$\begin{aligned}\langle G_7\rangle = \frac{1}{2^{N-1}}\Bigg[\sum_{\beta=0,4..}^{N-m-1}\binom{N-m-1}{\beta+1}-\binom{N-m-1}{\beta+3}\Bigg]\times \\ \Bigg[\sum_{\alpha=0,4..}^{m}\binom{m}{\alpha}-\binom{m}{\alpha+1}-\binom{m}{\alpha+2}+\binom{m}{\alpha+3}\Bigg] \\ = \frac{1}{2^{N-1}}Im[(1+i)^{N-m-1}]\cdot\Big(Re[(1+i)^m]-Im[(1+i)^m]\Big).\end{aligned} \tag{A.101}$$

Now we can consider each cases separately, for this we use the look-up Table A.1:

(i) If $N = 8k+5$ and if $(m-1) = 4 \bmod 8$, $Im[(1+i)^{N-m-1}] = 2^{\frac{N-m-2}{2}}$ and $Re[(1+i)^m] - Im[(1+i)^m] = -2^{\frac{m+1}{2}}$. And the overall sign from Table A.8 is negative. Therefore,

$$\langle G_7\rangle = -\frac{2^{\frac{N-m-2}{2}}\cdot(-2^{\frac{m+1}{2}})}{2^{N-1}} = \Big(\frac{1}{2}\Big)^{\frac{N-1}{2}}. \tag{A.102}$$

And, if $(m-1) = 0 \bmod 8$, $Im[(1+i)^{N-m-1}] = -2^{\frac{N-m-2}{2}}$ and $Re[(1+i)^m] - Im[(1+i)^m] = 2^{\frac{m+1}{2}}$. Overall sign in negative. Therefore,

$$\langle G_7\rangle = -\frac{-2^{\frac{N-m-2}{2}}\cdot 2^{\frac{m+1}{2}}}{2^{N-1}} = \Big(\frac{1}{2}\Big)^{\frac{N-1}{2}}. \tag{A.103}$$

The same holds for $N = 8k+6$ and $N = 8k+7$. Besides, (ii) differs with the sign flip and is trivial to check.It is also trivial to prove (iii), as when $N = 4k$, $Im[(1+i)^{N-m-1}] = 0$. □

Appendix B

An Appendix to Chapter 5

Proof of Lemma 5.2

Proof. First we consider 1 vs. $N-1$ bipartition. To calculate the maximal Schmidt coefficient we compute the reduced density matrix. As the state is symmetric, we only have to take the bipartition $1|2,3,\ldots,N$. We have

$$\varrho_1 = Tr\big(|H\rangle\langle H|\big)_{2\ldots N} = \frac{1}{2^N}\begin{pmatrix} 2^{N-1} & a \\ a & 2^{N-1} \end{pmatrix}. \tag{B.1}$$

The diagonal elements follow directly from the representation of the hypergraph state in Eq. (2.72) and do not depend on the structure of the hypergraph. For computing the off-diagonal entries, we write the hypergraph state as

$$|H\rangle = |0\rangle \sum_x \Big[(-1)^{f_0(x)}|x\rangle\Big] + |1\rangle \sum_x \Big[(-1)^{f_1(x)}|x\rangle\Big]. \tag{B.2}$$

with $x \in \{0,1\}^{(N-1)}$. Since we deal with three-uniform complete hypergraph states, we have $f_0 = \binom{w(x)}{3}$ and $f_1 = \binom{w(x)+1}{3}$, where $w(x)$ is the weight (i.e., the number of "1" entries) of x. We can then write

$$a = \sum_x (-1)^{f_0(x)+f_1(x)}. \tag{B.3}$$

The values of f_0 and f_1 do only depend on $w(x) \mod 4$. Instead of summing over x, we can also sum over all possible $k = w(x)$ in Eq. (B.3) and distinguish the cases of $k \mod 4$. The value for a given k is then up to the sign given by the numbers of possible x with the same $w(x) = k$. We have:

$$\begin{aligned} a =& \sum_{k=0,4\ldots}^{2^{N-1}} \left[\binom{N-1}{k} + \binom{N-1}{k+1} - \binom{N-1}{k+2} - \binom{N-1}{k+3}\right] \\ =& Re\big[(1+i)^{N-1}\big] + Im\big[(1+i)^{N-1}\big]. \end{aligned} \tag{B.4}$$

To give the final result, we have to consider several cases in Eq. (B.4): If $N = 4\ell$, then $a = 0$, therefore, ϱ_1 is maximally mixed and $\lambda_1 = 1/2$. If $N = 4\ell + 1$ or $N = 4\ell + 3$, then $a = \pm 2^{\frac{N-1}{2}}$. Then, it follows that $\lambda_1 = 1/2 + 1/2^{\frac{N+1}{2}}$. Similarly, for $N = 4\ell + 2$, $a = \pm 2^{\frac{N}{2}}$ and therefore $\lambda_1 = 1/2 + 1/2^{\frac{N}{2}}$. This ends the computation of λ_1.

Second, we look at the 2 vs. $N-2$ bipartitions. The idea of the proof very much resembles the previous case. First, we take the bipartition $1,2|3,4,\ldots,N$ and trace out the second part:

$$\varrho_{12} = Tr\big(|H\rangle\langle H|\big)_{3\ldots N} = \frac{1}{2^N}\begin{pmatrix} 2^{N-2} & a_+ & a_+ & 0 \\ a_+ & 2^{N-2} & 2^{N-2} & a_- \\ a_+ & 2^{N-2} & 2^{N-2} & a_- \\ 0 & a_- & a_- & 2^{N-2} \end{pmatrix}. \tag{B.5}$$

For computing the entries, we express a hypergraph state in the following way:

$$\begin{aligned} |H\rangle = |00\rangle \sum_x \Big[(-1)^{f_{00}(x)}|x\rangle\Big] + |01\rangle \sum_x \Big[(-1)^{f_{01}(x)}|x\rangle\Big] \\ + |10\rangle \sum_x \Big[(-1)^{f_{10}(x)}|x\rangle\Big] + |11\rangle \sum_x \Big[(-1)^{f_{11}(x)}|x\rangle\Big]. \end{aligned} \tag{B.6}$$

with $x \in \{0,1\}^{(N-2)}$. The diagonal elements of ϱ_{12} are, as before, easy to determine. This is also the case for the two anti-diagonal terms $|01\rangle\langle 10| = |10\rangle\langle 01|$ as $f_{01} + f_{10}$ is always even. The next term, a_+, is derived as Eqs. (B.3, B.4): $a_+ = Re[(1+i)^{N-2}] + Im[(1+i)^{N-2}]$. For the term $|00\rangle\langle 11|$, $f_{00}(x) + f_{11}(x)$ is even if $w(x)$ is even and is odd if $w(x)$ is odd. Therefore $\sum_x (-1)^{f_{00}+f_{11}} = 0$. For the last term we find $a_- = a - a_+ = Re\big[(1+i)^{N-2}\big] - Im\big[(1+i)^{N-2}\big]$.

Putting all these terms together in the matrix, one can calculate the maximal eigenvalue of ϱ_{12}:

$$\begin{aligned} \lambda_2 &= \frac{1}{8}\Big(3 + \frac{\sqrt{4^N + 128(a_+^2 + a_-^2)}}{2^N}\Big) = \frac{1}{8}\Big(3 + \frac{\sqrt{4^N + 64Abs[(1+i)^N]^2}}{2^N}\Big) \\ &= \frac{1}{8}\Big(3 + \frac{\sqrt{4^N + 2^{N+6}}}{2^N}\Big). \end{aligned} \tag{B.7}$$

Finally, we have to consider the $1,2,3|4\ldots N$ bipartition and write down the reduced density matrix:

$$\varrho_{123} = Tr\big(|H\rangle\langle H|\big)_{4\ldots N} = \frac{1}{2^N}\begin{pmatrix} 2^{N-3} & c & c & 0 & c & 0 & 0 & b \\ c & 2^{N-3} & 2^{N-3} & -b & 2^{N-3} & -b & -b & 0 \\ c & 2^{N-3} & 2^{N-3} & -b & 2^{N-3} & -b & -b & 0 \\ 0 & -b & -b & 2^{N-3} & -b & 2^{N-3} & 2^{N-3} & -c \\ c & 2^{N-3} & 2^{N-3} & -b & 2^{N-3} & -b & -b & 0 \\ 0 & -b & -b & 2^{N-3} & -b & 2^{N-3} & 2^{N-3} & -c \\ 0 & -b & -b & 2^{N-3} & -b & 2^{N-3} & 2^{N-3} & -c \\ b & 0 & 0 & -c & 0 & -c & -c & 2^{N-3} \end{pmatrix}, \tag{B.8}$$

where $c = Re\big[(1+i)^{N-3}\big] - Im\big[(1+i)^{N-3}\big]$ and $b = -Re\big[(1+i)^{N-3}\big] + Im\big[(1+i)^{N-3}\big]$.

From this we can be derive all possible values of maximal Schmidt coefficient λ_3.

If $N \equiv 4k$, then $\lambda_3 = 2^{-2} + 2^{-4k-3}\sqrt{48 \cdot 2^{4k} + 4^{4k}}$. If $N \equiv 4k+1$, then $\lambda_3 = 2^{-2} + 2^{-2k-1} + 2^{-4k-3}\sqrt{16^k(16 + 2^{4k} + 2^{2k+2})}$. If $N \equiv 4k+2$, then $\lambda_3 = 2^{-2} + 2^{-2k-1} + 2^{-4k-3}\sqrt{2^{4k}(2+2^{2k})^2}$ and finally, if $N \equiv 4k+3$, then $\lambda_3 = 2^{-2} + 2^{-2k-2} + 2^{-4k-3}\sqrt{2^{4k}(4 + 2^{4k} + 2^{2k+1})}$. It can be easily seen that λ_3 is decreasing with N and it is only greater than $1/2$ when $N = 6$.

□

Reduction of three uniform hypergraph states to the normal form in Lemma 5.3.

Proof. We continue the proof of Lemma 5.3 by considering other simple bipartitions, where the strategy is the similar and then the final statement follows directly.

We derive the normal form for the bipartition $12|3,4,\ldots,N$ for an N-qubit fully-connected three-uniform hypergraph state. We heavily use the normal form for one versus the rest bipartition. We show that the following statement holds: This state is locally equivalent to the three-uniform hypergraph state already derived from the bipartition $2|3\ldots N$ and in addition has the hyperedge $\{1,2,N\}$.

The steps are very similar to the $1|23\ldots N$ case:

(a) From a hypergraph we remove all the hyperedges which do not contain either party 1, or 2.
All the remaining hyperedges are $\{\{1,i,j\},\{2,i,j\},\{1,2,i\}|2<i<j\leq N\}$

(b) Apply $CNOT_{12}$.
The adjacency of 2 *is* $\mathcal{A}(2) = \{\{i,j\},\{1,i\}\}$ *for* $2 < i < j \leq N\}$. *Augmented by the control qubit* 1, *action of* $CNOT_{12}$ *removes* $\{1,i,j\}$ *and creates* $\{1,i\}$, $3 \leq i \leq N$.
All the remaining hyperedges are $\{\{1,i\},\{2,i,j\},\{1,2,i\}|2<i<j\leq N\}$

(c) Apply X_2.
All the elements in the adjacency $\mathcal{A}(2) = \{\{1,i\},\{i,j\}\}$ *for* $2 < i < j \leq N\}$ *are added as hyperedges to the hypergraph. Thus, all the edges of the type* $\{1,i\}$ *cancel out and* $\{i,j\}$ *can be directly removed.*
All the remaining hyperedges are $\{\{2,i,j\},\{1,2,i\}|2<i<j\leq N\}$

(d) Apply the algorithm from the bipartition $1|2\ldots N$ to the qubits $2|3\ldots N$.
Each of the action of the $CNOT_{i,i+1}$ gate from the algorithm for the bipartition $1|2\ldots N$ step (b), $3 \leq i < N$, removes the hyperedge $\{1,2,i\}$, in addition to the its actions considered for the case of bipartition $1|2\ldots N$. Therefore only the hyperedge $\{1,2,N\}$ remains of this type and other ones resulting from the action algorithm from the bipartition one versus the rest on qubits $2|3\ldots N$.

Considering any bipartition $1\ldots p|(p+1)\ldots N$ of the complete three-uniform hypergraph state, the consecutively applying local CNOT gates (respecting the fixed bipartition) reduces the hypergraph to the union of two hypergraphs as shown on Fig. 5.1: $p|p+1\ldots N$ and $N|1\ldots p$, both already reduced to the normal form by the results of one versus the rest bipartition.

This result is obtained by applying the algorithm from one versus the rest bipartition first to $N|1 \dots p$ and then to $p|(p+1) \dots N$. This ends the proof of Lemma 5.3. □

Appendix C

An Appendix to Chapter 7

Here we give representatives of five- and six-qubit codes as described in the main text:

(i) $((5,2,2))_2$: A three-uniform base code and Pauli-Z decoration for the second codeword respectively are:

$$\{\{1,2,3\},\{1,2,4\},\{1,3,4\},\{2,3,4\},\{2,3,5\},\{2,4,5\},\{3,4,5\}\} \text{ and } \{\{3\},\{4\},\{5\}\}. \tag{C.1}$$

(ii) $((5,4,2))_2$: A three-uniform base code and the decoration for the three other codewords are given respectively:

$$\text{The base code: } \{\{1,2,3\},\{1,2,4\},\{1,3,4\},\{2,3,4\},\{2,3,5\},\{2,4,5\},\{3,4,5\}\} \tag{C.2}$$

$$\text{Decoration \#1: } \{\{2\},\{1,3\},\{4\},\{1,4\},\{3,4\},\{5\},\{3,5\},\{4,5\}\} \tag{C.3}$$

$$\text{Decoration \#2: } \{\{2\},\{1,2\},\{3\},\{4\},\{1,4\},\{2,4\},\{2,5\},\{4,5\}\} \tag{C.4}$$

$$\text{Decoration \#3: } \{\{1\},\{1,2\},\{3\},\{1,3\},\{4\},\{2,4\},\{3,4\},\{2,5\},\{3,5\}\}. \tag{C.5}$$

(iii) $((5,5,2))_2$: One of the base codes with mixed cardinality edges and Pauli-Z decorations for four other codewords respectively are:

$$\text{The base: } \{\{1,3\},\{2,3\},\{2,4\},\{2,5\},\{3,4\},\{3,5\},\{4,5\},\{1,2,4\},\{1,4,5\},\{2,4,5\}\} \tag{C.6}$$

$$\text{Decoration \#1: } \{\{1\},\{2\},\{4\}\} \tag{C.7}$$

$$\text{Decoration \#2: } \{\{1\},\{2\},\{5\}\} \tag{C.8}$$

$$\text{Decoration \#3: } \{\{1\},\{4\},\{5\}\} \tag{C.9}$$

$$\text{Decoration \#4: } \{\{2\},\{4\},\{5\}\}. \tag{C.10}$$

Decorations of $((6,16,2))_2$ code with the base three-uniform hypergraph state is given in Fig. 7.3:

$$\text{The base: } \{\{1,2,3\},\{1,2,4\},\{1,3,5\},\{1,4,6\},\{1,5,6\}, \tag{C.11}$$
$$\{2,3,6\},\{2,4,5\},\{2,5,6\},\{3,4,5\},\{3,4,6\}\} \tag{C.12}$$

are either single-qubit Pauli-Z or graph edges CZ:

$$\#1\text{: } \{\{1\},\{2\},\{3\},\{6\},\{1,2\},\{1,3\},\{1,4\},\{1,5\},\{2,6\},\{3,6\},\{4,6\},\{5,6\}\} \tag{C.13}$$
$$\#2\text{: } \{\{1\},\{2\},\{4\},\{6\},\{1,2\},\{1,6\},\{2,3\},\{2,4\},\{2,5\},\{3,6\},\{4,6\},\{5,6\}\} \tag{C.14}$$
$$\#3\text{: } \{\{1\},\{3\},\{5\},\{6\},\{1,3\},\{1,6\},\{2,3\},\{2,6\},\{3,4\},\{3,5\},\{4,6\},\{5,6\}\} \tag{C.15}$$
$$\#4\text{: } \{\{2\},\{4\},\{5\},\{6\},\{1,4\},\{1,6\},\{2,4\},\{2,6\},\{3,4\},\{3,6\},\{4,5\},\{5,6\}\} \tag{C.16}$$
$$\#5\text{: } \{\{3\},\{4\},\{5\},\{6\},\{1,5\},\{1,6\},\{2,5\},\{2,6\},\{3,5\},\{3,6\},\{4,5\},\{4,6\}\} \tag{C.17}$$
$$\#6\text{: } \{\{1\},\{2\},\{5\},\{6\},\{1,2\},\{1,3\},\{1,4\},\{1,6\},\{2,4\},\{2,5\},\{2,6\},\{3,5\}\} \tag{C.18}$$
$$\#7\text{: } \{\{1\},\{3\},\{4\},\{6\},\{1,2\},\{1,4\},\{1,5\},\{1,6\},\{2,3\},\{3,4\},\{3,5\},\{3,6\}\} \tag{C.19}$$
$$\#8\text{: } \{\{1\},\{4\},\{5\},\{6\},\{1,4\},\{1,5\},\{2,4\},\{2,5\},\{3,4\},\{3,5\},\{4,6\},\{5,6\}\} \tag{C.20}$$
$$\#9\text{: } \{\{2\},\{3\},\{4\},\{6\},\{1,2\},\{1,4\},\{2,3\},\{2,5\},\{2,6\},\{3,4\},\{4,5\},\{4,6\}\} \tag{C.21}$$
$$\#10\text{: } \{\{2\},\{3\},\{5\},\{6\},\{1,2\},\{1,3\},\{2,5\},\{3,4\},\{3,5\},\{3,6\},\{4,5\},\{5,6\}\} \tag{C.22}$$
$$\#11\text{: } \{\{1\},\{2\},\{3\},\{4\},\{1,3\},\{1,4\},\{2,3\},\{2,4\},\{3,5\},\{3,6\},\{4,5\},\{4,6\}\} \tag{C.23}$$
$$\#12\text{: } \{\{1\},\{2\},\{3\},\{5\},\{1,2\},\{1,5\},\{2,3\},\{2,4\},\{2,6\},\{3,5\},\{4,5\},\{5,6\}\} \tag{C.24}$$
$$\#13\text{: } \{\{1\},\{2\},\{4\},\{5\},\{1,3\},\{1,4\},\{1,5\},\{1,6\},\{2,3\},\{2,5\},\{4,5\},\{5,6\}\} \tag{C.25}$$
$$\#14\text{: } \{\{1\},\{3\},\{4\},\{5\},\{1,2\},\{1,3\},\{1,5\},\{1,6\},\{2,4\},\{3,4\},\{4,5\},\{4,6\}\} \tag{C.26}$$
$$\#15\text{: } \{\{2\},\{3\},\{4\},\{5\},\{1,3\},\{1,5\},\{2,3\},\{2,4\},\{2,5\},\{2,6\},\{3,4\},\{3,6\}\}. \tag{C.27}$$

Appendix D

An Appendix to Chapter 8

Here, we restate Lemma 8.8 introduced in the main text in order to prove Theorem 8.7 and present a proof of the lemma.

Lemma 8.8. *A state $|\psi\rangle$ in $2 \times m \times n$ with $\mathcal{P}_\psi = \bigoplus_{i=1}^{n-m} L_{\epsilon_i}$ can be transformed to a state $|\phi\rangle$ in $2 \times m \times (n-1)$ with $\mathcal{P}_\phi = \bigoplus_{i=1}^{n-m-1} L_{\epsilon'_i}$ via local operations for any $n \geq m+2$ if the following condition holds. There exists $j \in \{1, \ldots, n-m-1\}$ such that for all $i \in \{1, \ldots, j-1\}$ $\epsilon_i = \epsilon'_i$ and for all $i \in \{j, \ldots, n-m-1\}$ $\epsilon_{i+1} \leq \epsilon'_i$, where we assume $(\epsilon_i)_i$ and $(\epsilon'_i)_i$ to be sorted in ascending order.*

Proof. First of all, let us note that it suffices to prove the lemma for $j = 1$, as any other case can be reduced to that case by acting trivially on the subspace of $\mathcal{P}_\psi$ which contains the blocks $L_{\epsilon_1}, \ldots, L_{\epsilon_{j-1}}$. Hence, we will assume $j = 1$ in the following, which implies that $\epsilon_{i+1} \leq \epsilon'_i$ holds for all $i \in \{1, \ldots, n-m-1\}$. To prove the statement we will explicitly derive the local operations which perform the transformation. More precisely, we will construct an $(n-1) \times n$ matrix C which has rank $n-1$ such that $\mathcal{P}_\psi C^T$ is strictly equivalent to $\mathcal{P}_\psi C^T$ in Eq. (D.2), where the gray areas vanish. Then we will show that the rank of this matrix pencil, $\tilde{\mathcal{P}}$, is m. We will then explicitly construct $\tilde{B} \in M_m$ such that $\tilde{B}\mathcal{P}_\phi = \mathcal{P}_\psi C^T$. As the rank of $\mathcal{P}_\psi C^T$ is maximal (and coincides with the rank of the matrix pencil $\mathcal{P}_\phi$), $\tilde{B}$ must be invertible, which shows that there exist B and C such that $\mathbb{1} \otimes B \otimes C|\psi\rangle = |\phi\rangle$.

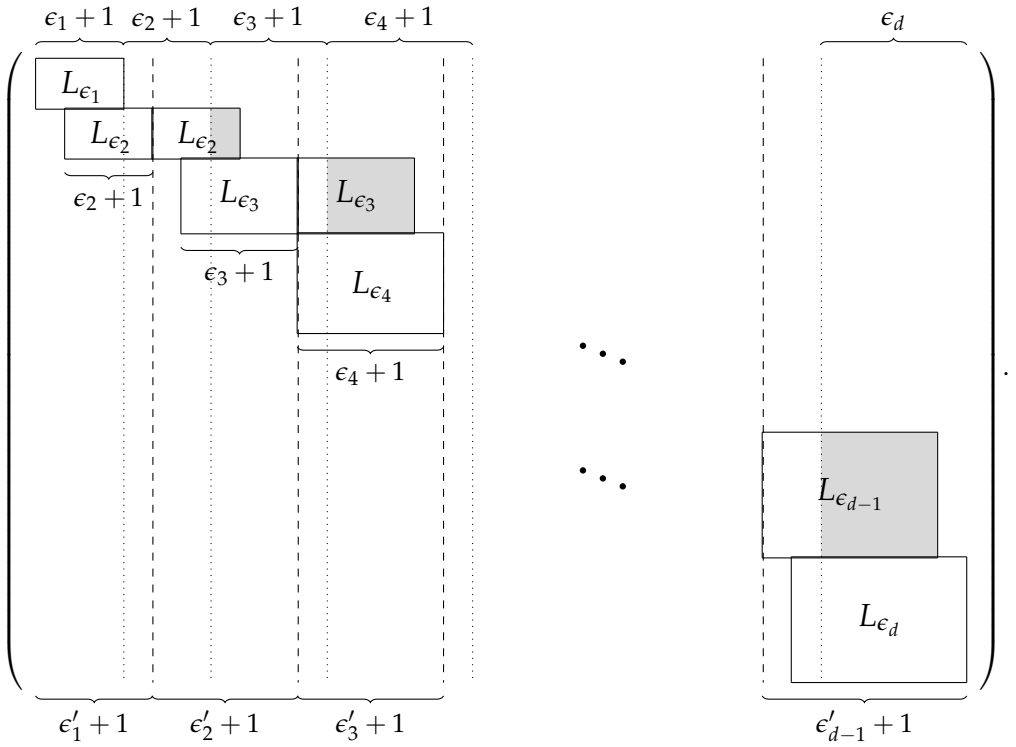
Let us write $d = n - m$, where $d \geq 2$ and let us assume that the matrix pencils $\mathcal{P}_\psi$ and $\mathcal{P}_\phi$ are in KCF and, furthermore, w.l.o.g. the blocks $L_{\epsilon_1}, \ldots, L_{\epsilon_d}$ present in $\mathcal{P}_\psi$ and $L_{\epsilon'_1}, \ldots, L_{\epsilon'_{d-1}}$ present in $\mathcal{P}_\phi$ are arranged in order of ascending size. Let us now consider an operation C by the third party given in terms of the $n \times (n-1)$ matrix

$$C^T = \sum_{i=1}^{d-1} \mathcal{I}_{p_i, p'_i}(\epsilon_i + 1) + \mathcal{I}_{p_{i+1}, p'_i + \epsilon'_i - \epsilon_{i+1}}(\epsilon_{i+1} + 1), \tag{D.1}$$

where $p_i = \sum_{j=1}^{i-1}(\epsilon_j + 1)$, $p'_i = \sum_{j=1}^{i-1}(\epsilon'_j + 1)$, and $\mathcal{I}_{k,l}(\epsilon)$ is an $(m+d) \times (m+d-1)$ matrix with all entries vanishing except an $\epsilon \times \epsilon$ identity submatrix with its upper left corner placed at the

coordinate (k, l). This operator transforms the pencil $\mathcal{P}_\psi$ to an $m \times (n-1)$ sized pencil $\mathcal{P}_\psi C^T$ given by

$$\mathcal{P}_\psi C^T =$$



(D.2)

In other words, the operator C^T copies the blocks L_{ϵ_i} and redistributes these copies to new columns as indicated in Eq. (D.2). Note that this transformation is achieved by column operations on the pencil solely. Hence, indeed only the third party has to apply some operation to perform the transformation. Let us look at the structure of the pencil $\mathcal{P}_\psi C^T$ in Eq. (D.2) in more detail. The columns of the pencil can be grouped into $d-1$ sectors of width $\epsilon'_i + 1$, respectively. In each of this sectors, two blocks, L_{ϵ_i} and $L_{\epsilon_{i+1}}$, occur. It is ensured that these blocks entirely fit into the sector, as due to the assumption $\epsilon_{i+1} \leq \epsilon'_i$ and thus also $\epsilon_i \leq \epsilon'_i$. Furthermore note, that the horizontal overlap of those two blocks is at least one column, as

$$\epsilon'_i = m - \sum_{j=1, j\neq i}^{d-1} \epsilon'_j = m - \sum_{j=1}^{i-1} \epsilon'_j - \sum_{j=i+1}^{d-1} \epsilon'_j \tag{D.3}$$

$$\leq m - \sum_{j=1}^{i-1} \epsilon_j - \sum_{j=i+1}^{d-1} \epsilon_{j+1} = m - \sum_{j=1, j\neq i, j\neq i+1}^{d} \epsilon_j = \epsilon_i + \epsilon_{i+1}, \tag{D.4}$$

where we used the assumption $\epsilon_{j+1} \leq \epsilon'_j$ to obtain the inequality. This shows that the transformation from $\mathcal{P}_\psi$ to $\mathcal{P}_\psi C^T$ as given in Eq. (D.2) is always possible. The grey shaded areas will be explained later on.

In the following, we show that this pencil, $\mathcal{P}_\psi C^T$, is strictly equivalent to $\mathcal{P}_\phi$. To this end, we first show that $\mathcal{P}_\psi C^T$ is a full rank matrix pencil, and then we show that there exists some

invertible operation B such that $B\mathcal{P}_\psi C^T = \mathcal{P}_\phi$. To see that $\mathcal{P}_\psi C^T$ is of full rank, we consider the pencil $\mathcal{P}_\psi C^T$ and apply one more transformation by the third party, which is invertible, to obtain a strictly equivalent pencil $\tilde{\mathcal{P}}$ which is of lower block-triangular form. We then show that $\tilde{\mathcal{P}}$ has full rank. Note that $\mathcal{P}_\psi C^T$ has a form where the first ϵ_1 rows are zero for all except the first $\epsilon_1 + 1$ columns. We now give an iterative procedure transforming $\mathcal{P}_\psi C^T$ to the desired pencil $\tilde{\mathcal{P}}$ which has the property that for all i, the first q_{i+1} rows are zero on all except the first p_{i+1} columns, where $q_i = \sum_{j=1}^{i-1} \epsilon_j$ and the above definition for p_i is used. In particular, $\tilde{\mathcal{P}}$ is the same matrix pencil as the one given in Eq. (D.2), but now the entries on the grey shaded areas vanish. As observed above, $\mathcal{P}_\psi C^T$ has the required form for the first $q_2 = \epsilon_1$ rows.

Let us now assume that the pencil has the required form for the first q_i rows. We will show that the pencil can be transformed to a pencil of required form for the first q_{i+1} rows. To this end, we show that the columns $p_i + 1$ until p'_i can be used to cancel the entries in the rows $q_i + 1$ until q_{i+1} of columns $p_{i+1} + 1$ until $p'_i + \epsilon_i + 1$, which constitute one of the grey shaded areas in Eq. (D.2). To see this, note that the columns $p_i + 1$ until p'_i have no non-zero entries in the first q_i rows due to the assumption. On rows $q_i + 1$ until q_{i+1}, these columns have the same entries as the columns $p_{i+1} + 1$ until $p'_i + \epsilon_i + 1$, as these are entries of two copies of the block L_{ϵ_i} which are positioned suitably. Hence, we can subtract the columns $p_i + 1$ until p'_i from the columns $p_{i+1} + 1$ until $p'_i + \epsilon_i + 1$ in order to cancel those entries. The resulting pencil now has the required form for the first q_{i+1} rows. Moreover, the rest of the pencil remains unchanged under this operation, because the columns $p_i + 1$ until p'_i vanish on all rows after q_{i+1}, as the first entry on such a row appears in column $p'_{i+1} - (\epsilon_{i+1} + 1) + 1$ and we have that $(p'_{i+1} - (\epsilon_{i+1} + 1) + 1) > p'_i$ due to the assumption $\epsilon'_i \geq \epsilon_{i+1}$.

Let us now observe important properties of the pencil $\tilde{\mathcal{P}}$. This pencil has lower block triangular form, i.e., the pencil has rectangular blocks on its diagonal, all entries to the upper right of the blocks in the diagonal vanish, and entries in the lower left region are arbitrary.

The first $d - 1$ blocks are cyclic column permutations of the blocks L_{ϵ_i}, respectively. The last block is a $\epsilon_d \times \epsilon_d$ sized block given by the last ϵ_d columns of L_{ϵ_d}. Let us now show that the rank of $\tilde{\mathcal{P}}$ is maximal, i.e., $r = m$. To this end, let us delete $d - 1$ columns from the pencil, one from each of the first $d - 1$ rectangular blocks in the diagonal, in order to obtain a $m \times m$ matrix of lower block-triangular form whose determinant is one m-minor of $\tilde{\mathcal{P}}$. The determinant of a block-triangular matrix equals the product of the determinants of the blocks on the diagonal [117] and as all of these determinants are non-vanishing we obtain an non-vanishing m-minor, which proves that $\tilde{\mathcal{P}}$ is of full rank and hence also $\mathcal{P}_\psi C^T$ is.

We show now that there exists an $m \times m$ matrix $\tilde{B}$ such that $\tilde{B}\mathcal{P}_\phi = \mathcal{P}_\psi C^T$. To see this, note that rows of the pencil $\mathcal{P}_\phi$ can be easily redistributed in order to obtain the pencil $\mathcal{P}_\psi C^T$. In particular, the operator $\tilde{B}$ is given by

$$\tilde{B} = \sum_{i=1}^{d-1} \mathcal{I}_{q_i, q'_i}(\epsilon_i) + \mathcal{I}_{q_{i+1}, q'_i + \epsilon'_i - \epsilon_{i+1}}(\epsilon_{i+1}), \tag{D.5}$$

where $q'_i = \sum_{j=1}^{i-1} \epsilon'_j$. Here, $\mathcal{I}_{k,l}(\epsilon)$ is a $m \times m$ matrix which is defined analogous to before.

As we have proven that the matrix pencil $\mathcal{P}_\psi C^T$ is of full rank, it follows that $\tilde{B}$ is invertible as otherwise the rank of $\mathcal{P}_\psi C^T$ must be smaller than m. Defining $B = \tilde{B}^{-1}$ we have that $\mathcal{P}_\phi = B\mathcal{P}_\psi C^T$ and hence $|\phi\rangle = \mathbb{1} \otimes B \otimes C|\psi\rangle$, which completes the proof. □

Let us prove the following Lemma about minimal indices.

Lemma D.1. *Given a list of p linearly independent (in the sense introduced in the preliminaries) homogenous polynomial vectors in μ and λ $(\vec{y}_1, \vec{y}_2, \ldots, \vec{y}_p)$ of ascending degrees and given a matrix pencil $\mathcal{P}$ such that $\mathcal{P}\vec{y}_l = 0 \; \forall \; 1 \leq l \leq p$. Let $\epsilon_1 \leq \epsilon_2 \leq \ldots \leq \epsilon_p$ be the first p minimal indices of $\mathcal{P}$. Then it holds that $\epsilon_l \leq \deg(\vec{y}_l) \; \forall \; 1 \leq l \leq p$, where $\deg(\vec{y}_l)$ denotes the degree of $\vec{y}_l$.*

Proof. W.l.o.g. we assume that the matrix pencil $\mathcal{P}$ is in KCF. Note that the J block and the $L_{v_i}^T$ blocks do not have any vector in the right null-space. The vectors $\vec{y}_l$ can hence only be non-vanishing for the first $\sum_{j=1}^{a}(\epsilon_j + 1)$ entries, where a denotes the number of right null-space blocks in $\mathcal{P}$. Moreover, for each L_ϵ there exists exactly one (linearly independent) vector in the nullspace. Note that the smallest possible degree of such a vector is ϵ. Let us now write the vectors $\vec{y}_l$ as $\vec{y}_l = (\vec{y}_l^1, \ldots, \vec{y}_l^a, 0, \ldots)^T$, where the dimension of $\vec{y}_l^k$ is $\epsilon_k + 1$. Given the block diagonal form of $\mathcal{P}$ (in KCF) we have that $\mathcal{P}\vec{y}_l = \mathcal{P}(\vec{y}_l^1, \ldots, \vec{y}_l^a, 0, \ldots)^T = (L_{\epsilon_1}\vec{y}_l^1, \ldots, L_{\epsilon_a}\vec{y}_l^a, 0, \ldots)^T$. The fact that each L_{ϵ_i} has only one vector in the null-space implies that for any set of k linearly independent vectors $\{\vec{y}_l\}$ one needs to have at least k different $\vec{y}_l^k \neq 0$. As mentioned before, for any $\vec{y}_l^k$ for which $L_{\epsilon_k}\vec{y}_l^k = 0$ it must hold that $\deg(\vec{y}_l^k) \geq \epsilon_k$ and therefore $\deg(\vec{y}_l) \geq \epsilon_k$. As the vectors $(\vec{y}_l)$ are sorted in order of increasing degree, the assertion $\deg(\vec{y}_l) \geq \epsilon_l$ for all l follows. □

Bibliography

[1] A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?," *Physical review*, vol. 47, no. 10, p. 777, 1935.

[2] E. Schrödinger, "Die gegenwärtige situation in der quantenmechanik," *Naturwissenschaften*, vol. 23, no. 49, pp. 823–828, 1935.

[3] J. S. Bell, "On the Einstein-Podolsky-Rosen paradox," *Physics Physique Fizika*, vol. 1, pp. 195–200, 1964.

[4] S. J. Freedman and J. F. Clauser, "Experimental test of local hidden-variable theories," *Physical Review Letters*, vol. 28, no. 14, p. 938, 1972.

[5] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, "Proposed experiment to test local hidden-variable theories," *Phys. Rev. Lett.*, vol. 23, pp. 880–884, Oct 1969.

[6] E. S. Fry and R. C. Thompson, "Experimental test of local hidden-variable theories," *Physical Review Letters*, vol. 37, no. 8, p. 465, 1976.

[7] A. Aspect, P. Grangier, and G. Roger, "Experimental tests of realistic local theories via bell's theorem," *Physical review letters*, vol. 47, no. 7, p. 460, 1981.

[8] A. Aspect, P. Grangier, and G. Roger, "Experimental realization of einstein-podolsky-rosen-bohm gedankenexperiment: a new violation of bell's inequalities," *Physical review letters*, vol. 49, no. 2, p. 91, 1982.

[9] A. Aspect, J. Dalibard, and G. Roger, "Experimental test of bell's inequalities using time-varying analyzers," *Physical review letters*, vol. 49, no. 25, p. 1804, 1982.

[10] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. Vermeulen, R. N. Schouten, C. Abellán, *et al.*, "Loophole-free bell inequality violation using electron spins separated by 1.3 kilometres," *Nature*, vol. 526, no. 7575, p. 682, 2015.

[11] M. Giustina, M. A. M. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J.-A. Larsson, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, J. Beyer, T. Gerrits, A. E. Lita, L. K. Shalm, S. W. Nam, T. Scheidl, R. Ursin, B. Wittmann, and A. Zeilinger, "Significant-loophole-free test of bell's theorem with entangled photons," *Phys. Rev. Lett.*, vol. 115, p. 250401, Dec 2015.

[12] L. K. Shalm, E. Meyer-Scott, B. G. Christensen, P. Bierhorst, M. A. Wayne, M. J. Stevens, T. Gerrits, S. Glancy, D. R. Hamel, M. S. Allman, K. J. Coakley, S. D. Dyer, C. Hodge, A. E. Lita, V. B. Verma, C. Lambrocco, E. Tortorici, A. L. Migdall, Y. Zhang, D. R. Kumor, W. H. Farr, F. Marsili, M. D. Shaw, J. A. Stern, C. Abellán, W. Amaya, V. Pruneri, T. Jennewein, M. W. Mitchell, P. G. Kwiat, J. C. Bienfang, R. P. Mirin, E. Knill, and S. W. Nam, "Strong loophole-free test of local realism," *Phys. Rev. Lett.*, vol. 115, p. 250402, Dec 2015.

[13] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels," *Physical review letters*, vol. 70, no. 13, p. 1895, 1993.

[14] C. H. Bennett and S. J. Wiesner, "Communication via one-and two-particle operators on einstein-podolsky-rosen states," *Physical review letters*, vol. 69, no. 20, p. 2881, 1992.

[15] A. K. Ekert, "Quantum cryptography based on bell's theorem," *Physical review letters*, vol. 67, no. 6, p. 661, 1991.

[16] R. Raussendorf and H. J. Briegel, "A one-way quantum computer," *Physical Review Letters*, vol. 86, no. 22, p. 5188, 2001.

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

[18] A. Higuchi and A. Sudbery, "How entangled can two couples get?," *Physics Letters A*, vol. 273, no. 4, pp. 213–217, 2000.

[19] S. L. Braunstein, C. M. Caves, R. Jozsa, N. Linden, S. Popescu, and R. Schack, "Separability of very noisy mixed states and implications for nmr quantum computing," *Physical Review Letters*, vol. 83, no. 5, p. 1054, 1999.

[20] R. Jozsa and N. Linden, "On the role of entanglement in quantum-computational speed-up," *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, vol. 459, no. 2036, pp. 2011–2032, 2003.

[21] H. J. Kimble, "The quantum internet," *Nature*, vol. 453, no. 7198, p. 1023, 2008.

[22] V. Giovannetti, S. Lloyd, and L. Maccone, "Quantum-enhanced measurements: beating the standard quantum limit," *Science*, vol. 306, no. 5700, pp. 1330–1336, 2004.

[23] P. Hayden, D. W. Leung, and A. Winter, "Aspects of generic entanglement," *Communications in Mathematical Physics*, vol. 265, pp. 95–117, Jul 2006.

[24] D. Gross, S. T. Flammia, and J. Eisert, "Most quantum states are too entangled to be useful as computational resources," *Phys. Rev. Lett.*, vol. 102, p. 190501, May 2009.

[25] M. J. Bremner, C. Mora, and A. Winter, "Are random pure states useful for quantum computation?," *Phys. Rev. Lett.*, vol. 102, p. 190502, May 2009.

[26] T. Morimae, "Finding resource states of measurement-based quantum computing is harder than quantum computing," *Physical Review A*, vol. 96, no. 5, p. 052308, 2017.

[27] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. Van den Nest, and H. J. Briegel, "Entanglement in graph states and its applications," *Quantum Computers, Algorithms and Chaos, (IOS Press, Amsterdam, 2006), quant-ph/0602096.*, vol. 162, 2006.

[28] D. Gottesman, "Stabilizer codes and quantum error correction," *arXiv preprint quant-ph/9705052*, 1997.

[29] N. D. Mermin, "Extreme quantum entanglement in a superposition of macroscopically distinct states," *Physical Review Letters*, vol. 65, no. 15, p. 1838, 1990.

[30] M. Gachechiladze, C. Budroni, and O. Gühne, "Extreme violation of local realism in quantum hypergraph states," *Physical review letters*, vol. 116, no. 7, p. 070401, 2016.

[31] M. Van den Nest, J. Dehaene, and B. De Moor, "Local equivalence of stabilizer states," in *Proceedings of the 16th international symposium on mathematical theory of networks and systems (MTNS). KU Leuven, Belgium*, 2004.

[32] M. Gachechiladze, N. Tsimakuridze, and O. Gühne, "Graphical description of unitary transformations on hypergraph states," *Journal of Physics A: Mathematical and Theoretical*, vol. 50, no. 19, p. 19LT01, 2017.

[33] M. Gachechiladze, O. Gühne, and A. Miyake, "Changing the circuit-depth complexity of measurement-based quantum computation with hypergraph states," *Physical Review A*, vol. 99, no. 5, p. 052304, 2019.

[34] G. Nebe, E. M. Rains, and N. J. A. Sloane, *Self-dual codes and invariant theory*, vol. 17. Springer, 2006.

[35] A. R. Calderbank, E. M. Rains, P. Shor, and N. J. Sloane, "Quantum error correction via codes over gf (4)," *IEEE Transactions on Information Theory*, vol. 44, no. 4, pp. 1369–1387, 1998.

[36] M. Hebenstreit, M. Gachechiladze, O. Gühne, and B. Kraus, "Coarse graining of entanglement classes in 2× m× n systems," *Physical Review A*, vol. 97, no. 3, p. 032330, 2018.

[37] M. Gachechiladze, N. Wyderka, and O. Gühne, "The structure of ultrafine entanglement witnesses," *Journal of Physics A: Mathematical and Theoretical*, vol. 51, no. 36, p. 365307, 2018.

[38] S. Popescu and D. Rohrlich, "Generic quantum nonlocality," *Physics Letters A*, vol. 166, no. 5-6, pp. 293–297, 1992.

[39] N. Gisin and A. Peres, "Maximal violation of bell's inequality for arbitrarily large spin," *Physics Letters A*, vol. 162, no. 1, pp. 15–17, 1992.

[40] M. Gachechiladze and O. Gühne, "Completing the proof of "generic quantum nonlocality"," *Physics Letters A*, vol. 381, no. 15, pp. 1281–1285, 2017.

[41] A. Peres, "Separability criterion for density matrices," *Phys. Rev. Lett.*, vol. 77, pp. 1413–1415, Aug 1996.

[42] M. Horodecki, P. Horodecki, and R. Horodecki, "Separability of mixed states: necessary and sufficient conditions," *Physics Letters A*, vol. 223, pp. 1–8, Feb 1996.

[43] P. Horodecki, "Separability criterion and inseparable mixed states with positive partial transposition," *Physics Letters A*, vol. 232, pp. 333–339, Feb 1997.

[44] K. Chen and L.-A. Wu, "A matrix realignment method for recognizing entanglement," *arXiv e-prints*, pp. quant–ph/0205017, May 2002.

[45] G. Svetlichny, "Distinguishing three-body from two-body nonseparability by a bell-type inequality," *Phys. Rev. D*, vol. 35, pp. 3066–3069, May 1987.

[46] D. M. Greenberger, M. A. Horne, and A. Zeilinger, "Going Beyond Bell's Theorem," *arXiv e-prints*, p. arXiv:0712.0921, Dec 2007.

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

[48] F. Verstraete, J. Dehaene, B. De Moor, and H. Verschelde, "Four qubits can be entangled in nine different ways," *Physical Review A*, vol. 65, no. 5, p. 052112, 2002.

[49] J. Cirac, W. Dür, B. Kraus, and M. Lewenstein, "Entangling operations and their implementation using a small amount of entanglement," *Physical Review Letters*, vol. 86, no. 3, p. 544, 2001.

[50] S. Virmani, S. F. Huelga, and M. B. Plenio, "Classical simulability, entanglement breaking, and quantum computation thresholds," *Physical Review A*, vol. 71, no. 4, p. 042328, 2005.

[51] K. Audenaert, M. Plenio, and J. Eisert, "The entanglement cost under operations preserving the positivity of partial transpose," *arXiv preprint quant-ph/0207146*, 2002.

[52] F. G. Brandão and M. B. Plenio, "A reversible theory of entanglement and its relation to the second law," *Communications in Mathematical Physics*, vol. 295, no. 3, pp. 829–851, 2010.

[53] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, "Quantum entanglement," *Reviews of Modern Physics*, vol. 81, pp. 865–942, Apr 2009.

[54] M. B. Plbnio and S. Virmani, "An introduction to entanglement measures," *Quantum Info. Comput.*, vol. 7, pp. 1–51, Jan. 2007.

[55] T.-C. Wei and P. M. Goldbart, "Geometric measure of entanglement and applications to bipartite and multipartite quantum states," *Phys. Rev. A*, vol. 68, p. 042307, Oct 2003.

[56] A. Schimony, "Degree of entanglementa," *Annals of the New York Academy of Sciences*, vol. 755, no. 1, pp. 675–679, 1995.

[57] L. Tamaryan, H. Kim, E. Jung, M.-R. Hwang, D. Park, and S. Tamaryan, "Toward an understanding of entanglement for generalizedn-qubit w-states," *Journal of Physics A: Mathematical and Theoretical*, vol. 42, p. 475303, nov 2009.

[58] D. Markham, A. Miyake, and S. Virmani, "Entanglement and local information access for graph states," *New Journal of Physics*, vol. 9, pp. 194–194, jun 2007.

[59] M. Hajdušek and M. Murao, "Direct evaluation of pure graph state entanglement," *New Journal of Physics*, vol. 15, p. 013039, jan 2013.

[60] L. E. Buchholz, T. Moroder, and O. Gühne, "Evaluating the geometric measure of multiparticle entanglement," *Annalen der Physik*, vol. 528, no. 3-4, pp. 278–287, 2016.

[61] L. Qi, G. Zhang, and G. Ni, "How entangled can a multi-party system possibly be?," *Physics Letters A*, vol. 382, no. 22, pp. 1465 – 1471, 2018.

[62] R. Hübener, M. Kleinmann, T.-C. Wei, C. González-Guillén, and O. Gühne, "Geometric measure of entanglement for symmetric states," *Physical Review A*, vol. 80, no. 3, p. 032324, 2009.

[63] B. M. Terhal, "Bell inequalities and the separability criterion," *Physics Letters A*, vol. 271, no. 5-6, pp. 319–326, 2000.

[64] O. Gühne and G. Tóth, "Entanglement detection," *Physics Reports*, vol. 474, no. 1, pp. 1 – 75, 2009.

[65] A. Peres, "All the bell inequalities," *Foundations of Physics*, vol. 29, pp. 589–614, Apr 1999.

[66] J. F. Clauser and M. A. Horne, "Experimental consequences of objective local theories," *Phys. Rev. D*, vol. 10, pp. 526–535, Jul 1974.

[67] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, "Proposed experiment to test local hidden variable theories.," *Phys. Rev. Lett.*, vol. 24, pp. 549–549, Mar 1970.

[68] S. L. Braunstein, A. Mann, and M. Revzen, "Maximal violation of bell inequalities for mixed states," *Phys. Rev. Lett.*, vol. 68, pp. 3259–3261, Jun 1992.

[69] B. S. Cirel'son, "Quantum generalizations of bell's inequality," *Letters in Mathematical Physics*, vol. 4, pp. 93–100, Mar 1980.

[70] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson, "Loophole-free bell inequality violation using electron spins separated by 1.3 kilometres," *Nature*, vol. 526, pp. 682 EP –, Oct 2015.

[71] B. Hensen, N. Kalb, M. S. Blok, A. E. Dréau, A. Reiserer, R. F. L. Vermeulen, R. N. Schouten, M. Markham, D. J. Twitchen, K. Goodenough, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson, "Loophole-free bell test using electron spins in diamond: second experiment and additional analysis," *Scientific Reports*, vol. 6, pp. 30289 EP –, Aug 2016. Article.

[72] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, "Bell nonlocality," *Reviews of Modern Physics*, vol. 86, no. 2, p. 419, 2014.

[73] L. Hardy, "Nonlocality for two particles without inequalities for almost all entangled states," *Phys. Rev. Lett.*, vol. 71, pp. 1665–1668, Sep 1993.

[74] S. Abramsky, C. M. Constantin, and S. Ying, "Hardy is (almost) everywhere: nonlocality without inequalities for almost all entangled multipartite states," *Information and Computation*, vol. 250, pp. 3–14, 2016.

[75] P. O. Boykin, T. Mor, M. Pulver, V. Roychowdhury, and F. Vatan, "A new universal and fault-tolerant quantum basis," *Information Processing Letters*, vol. 75, no. 3, pp. 101–107, 2000.

[76] Y. Shi, "Both toffoli and controlled-not need little help to do universal quantum computation," *arXiv preprint quant-ph/0205115*, 2002.

[77] E. Knill and R. Laflamme, "Theory of quantum error-correcting codes," *Physical Review A*, vol. 55, no. 2, p. 900, 1997.

[78] E. M. Rains, "Nonbinary quantum codes," *IEEE Transactions on Information Theory*, vol. 45, no. 6, pp. 1827–1832, 1999.

[79] E. M. Rains, "Quantum weight enumerators," *IEEE Transactions on Information Theory*, vol. 44, no. 4, pp. 1388–1394, 1998.

[80] A. Scott, "Multipartite entanglement, quantum-error-correcting codes, and entangling power of quantum evolutions," *Physical Review A*, vol. 69, no. 5, p. 052330, 2004.

[81] E. M. Rains, "Shadow bounds for self-dual codes," *IEEE Transactions on Information Theory*, vol. 44, no. 1, pp. 134–139, 1998.

[82] E. Rains and N. Sloane, "Self-dual codes, in the handbook of coding theory, vs pless and wc huffman, eds," 1998.

[83] A. Ekert and C. Macchiavello, "Error correction in quantum communication," *arXiv preprint quant-ph/9602022*, 1996.

[84] P. Sarvepalli and A. Klappenecker, "Degenerate quantum codes and the quantum hamming bound," *Physical Review A*, vol. 81, no. 3, p. 032318, 2010.

[85] M. Grassl, "Bounds on the minimum distance of linear codes and quantum codes." Online available at `http://www.codetables.de`, 2007. Accessed on 2019-05-19.

[86] F. Huber, O. Gühne, and J. Siewert, "Absolutely maximally entangled states of seven qubits do not exist," *Physical review letters*, vol. 118, no. 20, p. 200502, 2017.

[87] M. Van den Nest, J. Dehaene, and B. De Moor, "Local unitary versus local clifford equivalence of stabilizer states," *Phys. Rev. A*, vol. 71, p. 062323, Jun 2005.

[88] Z. Ji, J. Chen, Z. Wei, and M. Ying, "The lu-lc conjecture is false," *arXiv preprint arXiv:0709.1266*, 2007.

[89] N. Tsimakuridze and O. Gühne, "Graph states and local unitary transformations beyond local clifford operations," *Journal of Physics A: Mathematical and Theoretical*, vol. 50, no. 19, p. 195302, 2017.

[90] O. Gühne, G. Tóth, P. Hyllus, and H. J. Briegel, "Bell inequalities for graph states," *Physical review letters*, vol. 95, no. 12, p. 120405, 2005.

[91] G. Tóth, O. Gühne, and H. J. Briegel, "Two-setting bell inequalities for graph states," *Physical Review A*, vol. 73, no. 2, p. 022303, 2006.

[92] O. Gühne and A. Cabello, "Generalized ardehali-bell inequalities for graph states," *Physical Review A*, vol. 77, no. 3, p. 032108, 2008.

[93] S. Roy, "Multipartiteseparability inequalities exponentially stronger than local reality inequalities," *Physical review letters*, vol. 94, no. 1, p. 010402, 2005.

[94] R. Raussendorf, D. E. Browne, and H. J. Briegel, "Measurement-based quantum computation on cluster states," *Physical review A*, vol. 68, no. 2, p. 022312, 2003.

[95] M. Van den Nest, A. Miyake, W. Dür, and H. J. Briegel, "Universal resources for measurement-based quantum computation," *Physical review letters*, vol. 97, no. 15, p. 150504, 2006.

[96] D. Gross and J. Eisert, "Quantum computational webs," *Physical Review A*, vol. 82, no. 4, p. 040303, 2010.

[97] J. Miller and A. Miyake, "Hierarchy of universal entanglement in 2d measurement-based quantum computation," *npj Quantum Information*, vol. 2, p. 16036, 2016.

[98] A. Kissinger and J. van de Wetering, "Universal MBQC with generalised parity-phase interactions and Pauli measurements," *arXiv e-prints*, p. arXiv:1704.06504, Apr 2017.

[99] M. Amy, D. Maslov, M. Mosca, and M. Roetteler, "A meet-in-the-middle algorithm for fast synthesis of depth-optimal quantum circuits," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 32, no. 6, pp. 818–830, 2013.

[100] M. A. Nielsen and I. Chuang, "Quantum computation and quantum information," 2002.

[101] D. Maslov, "Advantages of using relative-phase toffoli gates with an application to multiple control toffoli optimization," *Physical Review A*, vol. 93, no. 2, p. 022311, 2016.

[102] F. Motzoi, M. Kaicher, and F. Wilhelm, "Linear and logarithmic time compositions of quantum many-body operators," *Physical review letters*, vol. 119, no. 16, p. 160503, 2017.

[103] P. Selinger, "Quantum circuits of t-depth one," *Physical Review A*, vol. 87, no. 4, p. 042302, 2013.

[104] C. Kruszynska and B. Kraus, "Local entanglability and multipartite entanglement," *Physical Review A*, vol. 79, no. 5, p. 052304, 2009.

[105] R. Qu, J. Wang, Z.-s. Li, and Y.-r. Bao, "Encoding hypergraphs into quantum states," *Physical Review A*, vol. 87, no. 2, p. 022311, 2013.

[106] M. Rossi, M. Huber, D. Bruß, and C. Macchiavello, "Quantum hypergraph states," *New Journal of Physics*, vol. 15, no. 11, p. 113022, 2013.

[107] M. Rossi, D. Bruß, and C. Macchiavello, "Hypergraph states in grover's quantum search algorithm," *Physica Scripta*, vol. 2014, no. T160, p. 014036, 2014.

[108] H. Buhrman, R. Cleve, J. Watrous, and R. De Wolf, "Quantum fingerprinting," *Physical Review Letters*, vol. 87, no. 16, p. 167902, 2001.

[109] C. E. Mora, H. J. Briegel, and B. Kraus, "Quantum kolmogorov complexity and its applications," *International Journal of Quantum Information*, vol. 5, no. 05, pp. 729–750, 2007.

[110] Y. Takeuchi and T. Morimae, "Verification of many-qubit states," *Physical Review X*, vol. 8, no. 2, p. 021060, 2018.

[111] T. Morimae, Y. Takeuchi, and M. Hayashi, "Verification of hypergraph states," *Physical Review A*, vol. 96, no. 6, p. 062321, 2017.

[112] H. Zhu and M. Hayashi, "Efficient verification of hypergraph states," *arXiv preprint arXiv:1806.05565*, 2018.

[113] O. Gühne, M. Cuquet, F. E. Steinhoff, T. Moroder, M. Rossi, D. Bruß, B. Kraus, and C. Macchiavello, "Entanglement and nonclassical properties of hypergraph states," *Journal of Physics A: Mathematical and Theoretical*, vol. 47, no. 33, p. 335303, 2014.

[114] E. Chitambar, C. A. Miller, and Y. Shi, "Matrix pencils and entanglement classification," *Journal of Mathematical Physics*, vol. 51, no. 7, p. 072205, 2010.

[115] F. Gantmacher, "The theory of matrices chelsea publishing company," *New York*, vol. 1, pp. 125–131, 1959.

[116] E. Chitambar, C. A. Miller, and Y. Shi, "Comment on" matrix pencils and entanglement classification"," *arXiv preprint arXiv:0911.4058*, 2009.

[117] R. A. Horn and C. R. Johnson, *Matrix analysis*. Cambridge university press, 2012.

[118] R. F. Werner and M. M. Wolf, "All-multipartite bell-correlation inequalities for two dichotomic observables per site," *Physical Review A*, vol. 64, no. 3, p. 032112, 2001.

[119] M. Żukowski and Č. Brukner, "Bell's theorem for general n-qubit states," *Physical review letters*, vol. 88, no. 21, p. 210401, 2002.

[120] Č. Brukner, M. Żukowski, J.-W. Pan, and A. Zeilinger, "Bell's inequalities and quantum communication complexity," *Physical review letters*, vol. 92, no. 12, p. 127901, 2004.

[121] S. Abramsky and C. Constantin, "A classification of multipartite states by degree of non-locality," *arXiv preprint arXiv:1412.5213*, 2014.

[122] Z. Wang, D. Markham, *et al.*, "Nonlocality of symmetric states," *Physical review letters*, vol. 108, no. 21, p. 210407, 2012.

[123] D. Collins, N. Gisin, S. Popescu, D. Roberts, and V. Scarani, "Bell-type inequalities to detect true n-body nonseparability," *Physical review letters*, vol. 88, no. 17, p. 170405, 2002.

[124] W.-B. Gao, C.-Y. Lu, X.-C. Yao, P. Xu, O. Gühne, A. Goebel, Y.-A. Chen, C.-Z. Peng, Z.-B. Chen, and J.-W. Pan, "Experimental demonstration of a hyper-entangled ten-qubit schrödinger cat state," *Nature physics*, vol. 6, no. 5, p. 331, 2010.

[125] M. J. Hoban, E. T. Campbell, K. Loukopoulos, and D. E. Browne, "Non-adaptive measurement-based quantum computation and multi-party bell inequalities," *New Journal of Physics*, vol. 13, no. 2, p. 023014, 2011.

[126] T. Toffoli, "Reversible computing," in *International Colloquium on Automata, Languages, and Programming*, pp. 632–644, Springer, 1980.

[127] S. Xu, "Reversible logic synthesis with minimal usage of ancilla bits," *arXiv preprint arXiv:1506.03777*, 2015.

[128] G. Tóth and O. Gühne, "Entanglement detection in the stabilizer formalism," *Physical Review A*, vol. 72, no. 2, p. 022340, 2005.

[129] V. Scarani, A. Acín, E. Schenck, and M. Aspelmeyer, "Nonlocality of cluster states of qubits," *Physical Review A*, vol. 71, no. 4, p. 042325, 2005.

[130] A. Cabello and P. Moreno, "Bipartite all-versus-nothing proofs of bell's theorem with single-qubit measurements," *Physical review letters*, vol. 99, no. 22, p. 220402, 2007.

[131] D. W. Lyons, N. P. Gibbons, M. A. Peters, D. J. Upchurch, S. N. Walck, and E. W. Wertz, "Local pauli stabilizers of symmetric hypergraph states," *Journal of Physics A: Mathematical and Theoretical*, vol. 50, no. 24, p. 245303, 2017.

[132] G. Tóth and O. Gühne, "Detecting genuine multipartite entanglement with two local measurements," *Physical review letters*, vol. 94, no. 6, p. 060501, 2005.

[133] M. Ghio, D. Malpetti, M. Rossi, D. Bruß, and C. Macchiavello, "Multipartite entanglement detection for hypergraph states," *Journal of Physics A: Mathematical and Theoretical*, vol. 51, no. 4, p. 045302, 2017.

[134] Y. Shi, "Quantum and classical tradeoffs," *Theoretical computer science*, vol. 344, no. 2-3, pp. 335–345, 2005.

[135] M. Amy, "Towards large-scale functional verification of universal quantum circuits," *arXiv preprint arXiv:1805.06908*, 2018.

[136] D. J. Shepherd, "On the role of hadamard gates in quantum circuits," *Quantum Information Processing*, vol. 5, no. 3, pp. 161–177, 2006.

[137] D. J. Shepherd, "Quantum complexity: restrictions on algorithms and architectures," *arXiv preprint arXiv:1005.1425*, 2010.

[138] A. Montanaro, "Quantum circuits and low-degree polynomials over," *Journal of Physics A: Mathematical and Theoretical*, vol. 50, no. 8, p. 084002, 2017.

[139] A. Paetznick and B. W. Reichardt, "Universal fault-tolerant quantum computation with only transversal gates and error correction," *Physical review letters*, vol. 111, no. 9, p. 090505, 2013.

[140] B. Yoshida, "Topological phases with generalized global symmetries," *Physical Review B*, vol. 93, no. 15, p. 155131, 2016.

[141] T. J. Yoder, "Universal fault-tolerant quantum computation with bacon-shor codes," *arXiv preprint arXiv:1705.01686*, 2017.

[142] M. Vasmer and D. E. Browne, "Universal quantum computing with 3d surface codes," *arXiv preprint arXiv:1801.04255*, 2018.

[143] D. Gross and J. Eisert, "Novel schemes for measurement-based quantum computation," *Physical review letters*, vol. 98, no. 22, p. 220503, 2007.

[144] D. Gross, J. Eisert, N. Schuch, and D. Perez-Garcia, "Measurement-based quantum computation beyond the one-way model," *Physical Review A*, vol. 76, no. 5, p. 052315, 2007.

[145] J. Miller and A. Miyake, "Latent computational complexity of symmetry-protected topological order with fractional symmetry," *Physical review letters*, vol. 120, no. 17, p. 170503, 2018.

[146] X. Chen, Z.-C. Gu, Z.-X. Liu, and X.-G. Wen, "Symmetry protected topological orders and the group cohomology of their symmetry group," *Physical Review B*, vol. 87, no. 15, p. 155114, 2013.

[147] T. Monz, K. Kim, W. Hänsel, M. Riebe, A. Villar, P. Schindler, M. Chwalla, M. Hennrich, and R. Blatt, "Realization of the quantum toffoli gate with trapped ions," *Physical review letters*, vol. 102, no. 4, p. 040501, 2009.

[148] B. P. Lanyon, M. Barbieri, M. P. Almeida, T. Jennewein, T. C. Ralph, K. J. Resch, G. J. Pryde, J. L. O'brien, A. Gilchrist, and A. G. White, "Simplifying quantum logic using higher-dimensional hilbert spaces," *Nature Physics*, vol. 5, no. 2, p. 134, 2009.

[149] A. Fedorov, L. Steffen, M. Baur, M. P. da Silva, and A. Wallraff, "Implementation of a toffoli gate with superconducting circuits," *Nature*, vol. 481, no. 7380, p. 170, 2012.

[150] K. Mølmer, L. Isenhower, and M. Saffman, "Efficient grover search with rydberg blockade," *Journal of Physics B: Atomic, Molecular and Optical Physics*, vol. 44, no. 18, p. 184016, 2011.

[151] C. Moore and M. Nilsson, "Parallel quantum computation and quantum codes," *SIAM Journal on Computing*, vol. 31, no. 3, pp. 799–815, 2001.

[152] B. M. Terhal and D. P. DiVincenzo, "Adaptive quantum computation, constant depth quantum circuits and arthur-merlin games," *arXiv preprint quant-ph/0205133*, 2002.

[153] Y. Chen, A. Prakash, and T.-C. Wei, "Universal quantum computing using $(\mathbb{Z}_d)^3$ symmetry-protected topologically ordered states," *Phys. Rev. A*, vol. 97, p. 022305, Feb 2018.

[154] E. M. Rains, "Quantum codes of minimum distance two," *IEEE Transactions on Information theory*, vol. 45, no. 1, pp. 266–271, 1999.

[155] M. B. Plenio and S. S. Virmani, "An introduction to entanglement theory," in *Quantum Information and Coherence*, pp. 173–209, Springer, 2014.

[156] C. Eltschka and J. Siewert, "Quantifying entanglement resources," *Journal of Physics A: Mathematical and Theoretical*, vol. 47, no. 42, p. 424005, 2014.

[157] I. Bengtsson and K. Życzkowski, *Geometry of quantum states: an introduction to quantum entanglement*. Cambridge university press, 2017.

[158] M. A. Nielsen, "Conditions for a class of entanglement transformations," *Physical Review Letters*, vol. 83, no. 2, p. 436, 1999.

[159] J. I. de Vicente, C. Spee, and B. Kraus, "Maximally entangled set of multipartite quantum states," *Physical review letters*, vol. 111, no. 11, p. 110502, 2013.

[160] C. Spee, J. de Vicente, and B. Kraus, "The maximally entangled set of 4-qubit states," *Journal of Mathematical Physics*, vol. 57, no. 5, p. 052201, 2016.

[161] M. Hebenstreit, C. Spee, and B. Kraus, "Maximally entangled set of tripartite qutrit states and pure state separable transformations which are not possible via local operations and classical communication," *Physical Review A*, vol. 93, no. 1, p. 012339, 2016.

[162] G. Gour, B. Kraus, and N. R. Wallach, "Almost all multipartite qubit quantum states have trivial stabilizer," *Journal of Mathematical Physics*, vol. 58, no. 9, p. 092204, 2017.

[163] D. Sauerwein, N. R. Wallach, G. Gour, and B. Kraus, "Transformations among pure multipartite entangled states via local operations are almost never possible," *Physical Review X*, vol. 8, no. 3, p. 031020, 2018.

[164] R. Duan and Y. Shi, "When is there a multipartite maximum entangled state?," *arXiv preprint arXiv:0911.0879*, 2009.

[165] J. W. Demmel and A. Edelman, "The dimension of matrices (matrix pencils) with given jordan (kronecker) canonical forms," *Linear algebra and its applications*, vol. 230, pp. 61–87, 1995.

[166] S. Johansson, "Reviewing the closure hierarchy of orbits and bundles of system pencils and their canonical forms," 2009.

[167] S. Bandyopadhyay, S. Halder, and M. Nathanson, "Entanglement as a resource for local state discrimination in multipartite systems," *Physical Review A*, vol. 94, no. 2, p. 022311, 2016.

[168] C. Ritz, C. Spee, and O. Gühne, "Characterizing multipartite entanglement classes via higher-dimensional embeddings," *arXiv preprint arXiv:1901.08847*, 2019.

[169] G. Gour and N. R. Wallach, "Classification of multipartite entanglement of all finite dimensionality," *Physical review letters*, vol. 111, no. 6, p. 060502, 2013.

[170] A. Osterloh and J. Siewert, "Invariant-based entanglement monotones as expectation values and their experimental detection," *Physical Review A*, vol. 86, no. 4, p. 042302, 2012.

[171] F. Shahandeh, M. Ringbauer, J. C. Loredo, and T. C. Ralph, "Ultrafine entanglement witnessing," *Physical review letters*, vol. 118, no. 11, p. 110502, 2017.

[172] F. Shahandeh, M. Ringbauer, J. C. Loredo, and T. C. Ralph, "Erratum: Ultrafine entanglement witnessing [phys. rev. lett. 118, 110502 (2017)]," *Physical review letters*, vol. 119, no. 26, p. 269901, 2017.

[173] S.-Q. Shen, T.-R. Xu, S.-M. Fei, X. Li-Jost, and M. Li, "Optimization of ultrafine entanglement witnesses," *Physical Review A*, vol. 97, no. 3, p. 032343, 2018.

[174] O. Gühne, M. Reimpell, and R. F. Werner, "Estimating entanglement measures in experiments," *Physical review letters*, vol. 98, no. 11, p. 110502, 2007.

[175] J. Eisert, F. G. Brandao, and K. M. Audenaert, "Quantitative entanglement witnesses," *New Journal of Physics*, vol. 9, no. 3, p. 46, 2007.

[176] M. Zwerger, W. Dür, J.-D. Bancal, and P. Sekatski, "Device-independent detection of genuine multipartite entanglement for all pure states," *Physical review letters*, vol. 122, no. 6, p. 060502, 2019.

[177] S. Aaronson, "The ten most annoying questions in quantum computing. blog," *August 15 2006*, 2006.

[178] A. Montanaro and D. Shepherd, "Hadamard gates and amplitudes of computational basis states," 2006.

[179] M. Backens, "A new holant dichotomy inspired by quantum computation," *arXiv preprint arXiv:1702.00767*, 2017.

[180] M. Backens, "A complete dichotomy for complex-valued holantˆ c," *arXiv preprint arXiv:1704.05798*, 2017.

[181] M. Hajdušek and M. Murao, "Direct evaluation of pure graph state entanglement," *New Journal of Physics*, vol. 15, no. 1, p. 013039, 2013.