Exploring Quantum Information Theory through Graphs and Networks

DISSERTATION

zur Erlangung des Grades eines Doktors
der Naturwissenschaften

vorgelegt von

Kiara HANSENNE

eingereicht bei der Naturwissenschaftlich-Technischen Fakultät
der Universität Siegen
Siegen 2024

Betreuer und erster Gutachter
Prof. Dr. Otfried Gühne
Universität Siegen

Zweite Gutachterin
Prof. Dr. Dagmar Bruß
Heinrich-Heine-Universität Düsseldorf

Tag der mündlichen Prüfung
01. Oktober 2024

Abstract

In this manuscript, we explore different aspects of quantum information using graph theory as a principal tool. The research presented in this thesis addresses fundamental questions in quantum information theory, such as uncertainty relations and quantum entanglement, as well as practical applications such as certification of quantum systems.

First, we define and analyse the anticommutativity graph associated with a set of observables. This approach allows us to relate the expectation values of these observables to the Lovász number of their anticommutativity graph, a well-known graph invariant. More specificity, the Lovász number provides an upper bound on the sum of the squares of the expectation values. This relationship enables us to derive uncertainty relations for any set of dichotomic observables. These can be transformed into witnesses to detect entanglement, including in PPT entangled states.

Second, we address the problem of measurement scheduling for marginal state tomography, i.e., finding measurement settings that allow for the reconstruction of marginal states of a quantum system. We demonstrate that, for Pauli tomography, this problem can be mapped to a specific instance of the graph-theoretical problem of edge clique covering. Using this mapping, we show for instance that, for two-body marginal tomography of planar qubit topologies, nine Pauli settings are necessary and sufficient, regardless of the numbers of qubits in the system. Furthermore, we establish that with general local projective measurements, 3^k measurement settings are sufficient to reconstruct all k-body marginal states of a multi-qubit system. We report an experimental demonstration of the applicability of the measurement settings derived in our work.

Lastly, we develop necessary criteria for network entanglement, revealing that many graph states, as well as permutationally symmetric states, cannot be prepared in network structures without the usage of classical communication. We then propose a certification protocol for the topology of quantum networks, which has later been implemented experimentally.

Zusammenfassung

In dieser Arbeit werden verschiedene Aspekte der Quanteninformation unter Verwendung der Graphentheorie als Hauptwerkzeug untersucht. Die vorliegende Studie befasst sich sowohl mit grundlegenden Fragen der Quanteninformationstheorie, wie Unschärferelationen und Quantenverschränkung, als auch mit praktischen Anwendungen, beispielsweise der Zertifizierung von Quantensystemen.

Erstens definieren und analysieren wir den Antikommutativitätsgraph, der mit einer Menge von Observablen verbunden ist. Dieser Ansatz ermöglicht es uns, die Erwartungswerte dieser Observablen mit der Lovász-Zahl des Graphen, einer bekannten Grapheninvariante, in Beziehung zu setzen. Die Lovász-Zahl liefert eine obere Schranke an die Summe der Quadrate der Erwartungswerte. Aus dieser Beziehung lassen sich Unschärferelationen für beliebige dichotome Observablen ableiten, die wiederum zum Nachweis verschränkter Zustände, einschließlich PPT-verschränkter Zustände, verwendet werden können.

Im zweiten Teil der Arbeit befassen wir uns mit der optimalen Messstrategie für Marginalzustands-Tomographie. Wir zeigen, dass dieses Problem im Fall der Pauli-Tomographie auf einen Spezialfall des graphentheoretischen Problems der Kanten-Cliquen-Abdeckung reduziert werden kann. Mit Hilfe dieser Methode demonstrieren wir zum Beispiel, dass für die Zweikörper-Marginal-Tomographie von planaren Qubit-Topologien neun Pauli-Einstellungen ausreichen, unabhängig von der Anzahl der Qubits im System. Zudem zeigen wir, dass bei allgemeinen lokalen projektiven Messungen 3^k Messeinstellungen genügen, um alle k-Körper-Marginalzustände eines Multiqubit-Systems zu rekonstruieren. Die Anwendbarkeit unserer Messeinstellungen wurde experimentell überprüft.

Zuletzt entwickeln wir notwendige Kriterien für Netzwerkverschränkung und zeigen, dass viele Graphenzustände sowie alle permutationssymmetrischen Zustände in Netzwerkstrukturen ohne klassische Kommunikation nicht erzeugt werden können. Anschließend schlagen wir ein Zertifizierungsprotokoll für die Topologie von Quantennetzwerken vor und präsentieren hiervon eine experimentelle Implementierung.

Acknowledgements

First and foremost, I want to thank Otfried Gühne for being an exceptional supervisor, both scientifically and personally. Otfried's supervision style evolved over the years, from sitting down with me and working through calculations in my early months, to listening and commenting on what I found interesting in the later years, always having insightful ideas whenever I was stuck. I am deeply grateful for his ability to provide what his students need and for the great group atmosphere he has achieved.

I also thank all past and current members of the TQO group for all the scientific and non-scientific discussions we had over the years. It would not have been the same without you. Special thanks go to Lina and Jan for being great office mates, door open or door closed. Thanks to Julia for being my first friend (and only option) when we arrived in Siegen in the midst of the pandemic, you have a home wherever I live.

I am grateful to all the non-scientific workers of the Emmy Noether Campus, without whom working at the university would not be possible. I especially thank Daniela, who, despite having so much to do, was always there to help with bureaucracy.

I thank all my coauthors for the joint work and all the people with whom I had the opportunity to discuss over the years. I am also grateful to Qiongyi He and her group for their warm welcome during my stay at Peking University.

I thank the House of Young Talents of the University of Siegen, in particular Marcus Niechciol and Christine Hrncal, for their financial and non-financial support.

I also thank Carlos, Jan, Konrad, Leo, Lina, Marta, Nicole, and Ties for proofreading parts of this thesis.

Very special thanks go to my family for the support throughout the years, especially to my mother and my sisters Dana and Nelle for chatting with me every single day.

Finally, I thank Carlos for making every aspect of my life better, from my coffee to my binary programs.

Contents

Acknowledgements iii

List of abbreviations viii

Preface 1

1 Preliminaries 3
- 1.1 Quantum states and measurements . . . 3
- 1.2 Uncertainty relations . . . 6
- 1.3 Quantum entanglement . . . 8
  - 1.3.1 Bipartite entanglement . . . 8
  - 1.3.2 Multipartite entanglement . . . 10
  - 1.3.3 Entanglement detection and quantification . . . 12
  - 1.3.4 Network entanglement . . . 14
- 1.4 Symmetric states . . . 19
  - 1.4.1 Stabiliser and graph states . . . 19
  - 1.4.2 Permutationally symmetric states . . . 22
- 1.5 Quantum state tomography . . . 25
- 1.6 Mathematical toolbox . . . 27
  - 1.6.1 Mathematical optimisation . . . 28
  - 1.6.2 Graph theory . . . 31

2 Uncertainty relations 36
- 2.1 Multi-observable uncertainty relations . . . 37
  - 2.1.1 Reformulation . . . 37
  - 2.1.2 Including commutation relations . . . 41
  - 2.1.3 Imprecise observables . . . 44
- 2.2 Application to entanglement detection . . . 45
  - 2.2.1 Entanglement witnesses . . . 45

2.2.2 Imprecise observables . . . 47
2.2.3 Schmidt number witnesses . . . 48
2.3 Discussion . . . 51

3 Marginal tomography **52**
3.1 Pauli tomography . . . 53
3.1.1 Two-body marginal tomography . . . 53
3.1.2 Marginal tomography of arbitrary strength . . . 57
3.1.3 Overlapping tomography of arbitrary strength . . . 58
3.1.4 Reduction for large number of qubits . . . 62
3.1.5 On the optimality of constructions for strength two . . . 67
3.2 Minimal settings for overlapping tomography . . . 70
3.2.1 Random measurement directions . . . 70
3.2.2 Numerically optimised measurement directions . . . 72
3.3 Discussion on the sample cost . . . 75
3.4 Discussion . . . 77

4 Entanglement in quantum networks **79**
4.1 Covariance matrices of network states . . . 80
4.1.1 Covariance matrices for tripartite states . . . 81
4.1.2 Basic triangle network . . . 81
4.1.3 Triangle network with local operations . . . 86
4.1.4 Covariance matrix criterion for triangle network states 89
4.1.5 NCDS networks . . . 90
4.2 Symmetric states in quantum networks . . . 93
4.2.1 Inflation technique . . . 94
4.2.2 GHZ state . . . 96
4.2.3 Cluster state . . . 97
4.2.4 Graph states . . . 99
4.2.5 Networks with tripartite sources . . . 101
4.2.6 Permutationally symmetric states . . . 103
4.3 Certification of network links . . . 105
4.4 Certification of network topology . . . 106
4.4.1 Statistical hypotheses test . . . 106
4.4.2 Simultaneous fidelity estimation . . . 108
4.4.3 Certification based on experimental data . . . 109
4.4.4 Device-independent approach . . . 112
4.5 Discussion . . . 114

Conclusion **116**

A Appendix to Chapter 3 **118**

B Appendix to Chapter 4 **121**

Publication list **129**

Bibliography **130**

List of abbreviations

BTN	basic triangle network
CA	covering array
CM	covariance matrix
CPTP	completely positive and trace preserving
CTN	channel triangle network
GHZ	Greenberger–Horne–Zeilinger
GME	genuine multipartite entanglement
LOCC	local operations and classical communication
LOSR	local operations and shared randomness
NCDS	no common double source
POVM	positive operator-valued measure
PPT	positive partial transpose
PSD	positive semidefinite
PVM	projection-valued measure
SDP	semidefinite programming
SLOCC	stochastic local operations and classical communication
SN	Schmidt number
UR	uncertainty relation
UTN	unitary triangle network

Preface

In the last decades, quantum information science has witnessed a remarkable development. Since the end of the 20th century, the field has transitioned from merely observing peculiar quantum phenomena to developing practical protocols. A prominent example is quantum key distribution, which allows for the distribution of cryptographic keys between distant parties and is theoretically provably secure [14, 47]. Today, we find ourselves in an era where experimental implementations of these protocols are feasible, at least at a proof-of-principle level. Examples include long-distance entanglement distribution [166, 149], quantum key distribution in networks [127, 119], and quantum metrology [32]. This rapid progress calls for more and more verification and certification techniques of quantum devices.

Despite the significant progress of the field, some of the earliest seeds of quantum information science remain incompletely characterised. Fundamental concepts such as uncertainty relations, discovered by Heisenberg as early as 1927 [72], and quantum entanglement, first discussed by Schrödinger in 1935 [129], still elude complete understanding. For instance, uncertainty relations are still a central topic in quantum information theory, yet the problem of determining the possible expectation values of a collection of quantum observables on a specific state remains generally unresolved. Additionally, emerging concepts like network entanglement [3, 94, 101, 111] require further exploration.

This thesis aims to contribute in two significant ways: It addresses foundational problems in quantum mechanics and proposes new techniques for characterising quantum systems. To do so, Chapter 1 introduces the essential concepts and mathematical tools necessary for understanding the results presented in the subsequent chapters.

In Chapter 2, we establish a novel connection between quantum observables and graph theory, which can be used to derive uncertainty relations for any set of dichotomic observables. Specifically, we obtain an upper bound

on the sum of the squares of their expectation values. This result and its extensions derived in [106, 163] not only advances our understanding of uncertainty relations but also finds practical application in entanglement detection, ground state energy estimation [4], and quantum state tomography [90].

Chapter 3 focuses on the certification of quantum devices through quantum state tomography. It is well-known that the number of samples required for quantum state tomography of a multi-qubit system grows exponentially with the number of qubits, making these protocols impractical for large systems. However, in practice, many natural and engineered systems are subject to only local interactions, or are highly symmetric, making their global properties largely contained in a few of their parts. For these cases, marginal tomography is more appropriate and scalable. Marginal tomography aims to reconstruct (low-dimensional) reduced density operators of multipartite quantum systems. This problem is closely related to concepts in combinatorial design theory. We present different measurement scheduling strategies, each optimal according to specific figures of merit, whose applicabilities are verified in a six-photon experiment.

Finally, in Chapter 4, we address open problems in network entanglement, which deals with characterising the set of states that can be generated when only some resources, such as bipartite entangled sources among nearby parties, are available. We develop new techniques to tackle this issue and apply them to derive necessary criteria for network-entangled states. Notably, we show that several classes of symmetric states cannot be prepared in network structures without classical communication. Additionally, we present two certification methods for network states and discuss an experimental demonstration.

In summary, this thesis seeks to advance both the foundational and applied aspects of quantum information theory, with the concepts of graphs and networks as a common thread. By exploring novel connections and developing efficient techniques for quantum state characterisation, we address critical challenges in the field. The contributions presented are intended to improve our understanding of quantum information theory and facilitate future research.

Chapter 1

Preliminaries

This first chapter covers the key concepts needed to understand the results in this thesis. We begin by introducing fundamental elements in quantum mechanics, namely quantum states and measurements, uncertainty relations, quantum entanglement, classes of symmetric states, and quantum state tomography. In the last section, we present basic notions of mathematical optimisation and graph theory.

1.1 Quantum states and measurements

In quantum mechanics, quantum systems are described by *pure states*, which are given by vectors belonging to a complex Hilbert space. If $d \in \mathbb{N}$ is the dimension of the quantum system considered, we associate to it the Hilbert space $\mathcal{H}^d \simeq \mathbb{C}^d$ and represent its state by a normalised *state vector* $|\psi\rangle \in \mathcal{H}^d$. When no superscript is present, i.e., $\mathcal{H}$, the dimension is understood as an arbitrary finite dimension d. We give a brief overview of these fundamental concepts, and refer to [152] for a detailed discussion. In this thesis, only finite-dimensional systems are considered.

In general, the state of the system may not be pure and could instead be in a a statistical mixture of pure states. In that case, the state is represented by a unit trace and positive semidefinite (PSD) operator acting on $\mathcal{H}^d$. These are called *density operators*, generally denoted by ϱ and can be decomposed according to the spectral decomposition

$$\varrho = \sum_{k=1}^{L} p_k \, |\psi_k\rangle\langle\psi_k| \, , \tag{1.1}$$

with $L = \text{rank}(\varrho)$ and where p_k are the non-zero eigenvalues of ϱ satisfying $p_k > 0$ and $\sum_{k=1}^{L} p_k = 1$, and $|\psi_k\rangle$ their corresponding normalised eigenvectors, for all $k \in [L]$. The notation $[L] = \{1, \ldots, L\}$ is used throughout this thesis. When the system can be described by a single vector $|\psi\rangle$, its density operator reduces to the projection operator (or *projector*) $\varrho = |\psi\rangle\langle\psi|$. We note that the decomposition into a convex combination of pure states is not unique [80], and that any operator that can be written as the convex combination of rank-one projectors is a valid density operator. The set of all density operators is called the *set of states* of $\mathcal{H}^d$ and denoted by $\mathcal{S}(\mathcal{H}^d)$ [152],

$$\mathcal{S}(\mathcal{H}^d) = \{\varrho \in \mathcal{L}(\mathcal{H}^d) \mid \varrho \succeq 0, \text{tr}(\varrho) = 1\}, \tag{1.2}$$

where $\mathcal{L}(\mathcal{H}^d)$ is space of linear operators acting on $\mathcal{H}^d$, and where $\varrho \succeq 0$ means that ϱ is a PSD operator. By abuse of language, we simply refer to elements of $\mathcal{S}(\mathcal{H}^d)$ as *states*.

Of particular interest in quantum information theory are two-level systems, called *qubits* [71]. Their states can be written with the help of two real parameters $\varphi \in [0, 2\pi[$ and $\theta \in [0, \pi]$ as

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|1\rangle, \tag{1.3}$$

where $|0\rangle = (1,0)^T$ and $|1\rangle = (0,1)^T$ form the two-dimensional computational basis[1], and where $\cdot^T$ stands for transposition.

Qubit states therefore have a convenient representation as unit vectors on a sphere, which is called the *Bloch sphere* [71] and presented in Figure 1.1. In order to show how mixed states also fit into this description, we introduce the *Pauli basis* of the real vector space of 2×2-dimensional Hermitian operators. The Pauli basis is composed of four elements (the *Pauli operators*) [118],

$$\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{1.4}$$

The operator σ_0 is simply the two-dimensional identity operator, $\mathbb{1}_2$.[2] Any

[1] The computational basis can trivially be extended to d-dimensional spaces, denoted by $\{|i\rangle\}_{i=0}^{d-1}$ with $|i\rangle$ being the d-dimensional unit vector in the ith direction.

[2] We denote the d-dimensional identity operator by $\mathbb{1}_d$, and drop the subscript when the situation is unambiguous.

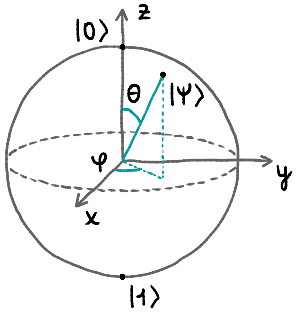

Figure 1.1: *Bloch sphere.* Each qubit state can be represented by a three-dimensional real vector with a norm of at most one. Pure states lie on the Bloch sphere such as $|\psi\rangle$, meaning their Bloch vectors have a unit norm. Mixed states lie inside the sphere.

state $\varrho \in \mathcal{S}(\mathcal{H}^2)$ can be written as

$$\varrho = \frac{1}{2}\left(\sigma_0 + a_x\sigma_x + a_y\sigma_y + a_z\sigma_z\right) \tag{1.5a}$$

$$= \frac{1}{2}\left(\mathbb{1}_2 + \mathbf{a}\cdot\boldsymbol{\sigma}\right) \tag{1.5b}$$

with $\mathbf{a} = (a_x, a_y, a_z)^T \in \mathbb{R}^3$, $\|\mathbf{a}\| \leq 1$, where $\|\mathbf{a}\| = \sqrt{\mathbf{a}^T\mathbf{a}}$ is the Euclidean norm [75]. We introduced in Eq. (1.5) the notation $\mathbf{a}\cdot\boldsymbol{\sigma} = a_x\sigma_x + a_y\sigma_y + a_z\sigma_z$, with $\boldsymbol{\sigma} = (\sigma_x, \sigma_y, \sigma_z)^T$. The vector $\mathbf{a}$ can be represented inside the Bloch sphere and is called the *Bloch vector* of ϱ [71]. The entries of $\mathbf{a}$ are given by $a_i = \mathrm{tr}(\sigma_i\varrho)$ for all $i = x, y, z$. Conversely, any three-dimensional real vector with a norm less or equal to one represents a state in $\mathcal{S}(\mathcal{H}^2)$ [28, 89]. We note that for systems with three or more dimensions, this description does not generalise trivially to higher-dimensional spheres (for details, see [89] or [48]).

In this thesis, the Pauli operators play a significant role. The three other Pauli operators are traceless and have eigenvalues $+1$ and -1, hence they all square to the identity operator. For readability, we often use the notation $\sigma_0 = \mathbb{1}$, $\sigma_x = X$, $\sigma_y = Y$ and $\sigma_z = Z$.

In order to have access to information about a d-dimensional quantum system, one has to perform a *quantum measurement* on the system. An important class of quantum measurements is the class of *projective measurements*, sometimes called *projection-valued measures* (PVMs) measurements. A projective measurement is described by an *observable* A, a Hermitian operator acting on the set of states $\mathcal{S}(\mathcal{H}^d)$ [114]. The possible outcomes of the measurement operation are given by the (real) eigenvalues of A, $\{a_i\}_{i=1}^{L}$.

When the system is in a state $\varrho \in \mathcal{S}(\mathcal{H}^d)$, the probability of obtaining the ith outcome a_i is given by the Born rule, $p_i = \mathrm{tr}(\Pi_i \varrho)$, where Π_i is the projector onto the eigenspace of A corresponding to the eigenvalue a_i, with $i \in [L]$. As the spectral decomposition of the observable A reads $A = \sum_{i=1}^{L} a_i \Pi_i$, it is clear that the expectation value of the observable A on the state ϱ is $\langle A \rangle_\varrho = \sum_{i=1}^{L} a_i p_i = \mathrm{tr}(A\varrho)$ [114].

Although most of the results in this thesis involving measurement concern projective measurements, we briefly present the concept of *positive operator-valued measures* (POVMs), the most general description of measurement operations on quantum systems. A POVM M is described by a set of PSD operators, $M = \{E_i\}_{i=1}^{L}$, obeying the normalisation constraint $\sum_{i=1}^{L} E_i = \mathbb{1}$ [152]. The PSD operators E_i, with $i \in [L]$, are called POVM elements. Without loss of generality, the set of measurement outcomes is $[L]$, and each operator E_i is associated with the outcome $i \in [L]$. When performing the POVM measurement M on a quantum system, probability of obtaining the measurement outcome $i \in [L]$ is given by $p_i = \mathrm{tr}(E_i \varrho)$, and the positivity of the elements of M together with the normalisation constraint ensure that the probabilities are positive and normalised. Clearly, projective measurements are a type of POVM measurements, where all POVM elements are projectors and verify an orthogonality relation [152].

1.2 Uncertainty relations

When the state vector $|\psi\rangle \in \mathcal{H}$ of a quantum system corresponds to an eigenvector of some observable $A \in \mathcal{L}(\mathcal{H})$, the system is said to be in an *eigenstate* of A. We denote by a the corresponding eigenvalue, such that $A|\psi\rangle = a|\psi\rangle$. In that case, performing the projective measurement associated to A on the quantum system always gives the same outcome a. The variance of A on the state $|\psi\rangle$, defined as $\Delta^2_\varrho(A) = \langle A^2 \rangle_\varrho - \langle A \rangle^2_\varrho$ with $\varrho = |\psi\rangle\langle\psi|$, is thus equal tor zero [71].

Now, consider a second observable, $B \in \mathcal{L}(\mathcal{H})$. If A and B share an eigenstate $|\psi\rangle$, the variances of both observables on that state are equal to zero. However, if no common eigenstate to A and B can be prepared, the variances cannot simultaneously vanish. We are thus interested in formalising the relation between the probability distributions that arise when measuring A and B on the same state ϱ: This is commonly expressed through fundamental bounds on functions of the observables' variances or entropies, referred to as *(preparation) uncertainty relations* (URs). In this thesis,

the focus is on inequalities involving expectation values of observables, thus only variance-based URs are discussed. While variance-based URs are typically taught in undergraduate quantum mechanics, entropic URs are sometimes considered more fundamental due to their independence from the label of possible measurement outcomes. For a thorough review of entropic URs, see [35].

One of the foundational variance-based URs is the Robertson UR [125] that asserts a non-trivial lower bound on the product of variances of A and B,

$$\Delta^2_\varrho(A)\Delta^2_\varrho(B) \geq \left|\frac{1}{2}\langle[A,B]\rangle_\varrho\right|^2 \quad \forall \varrho \in \mathcal{S}(\mathcal{H}). \tag{1.6}$$

Notably, for the position and momentum observables, a similar inequality was proposed as early as 1927 by Heisenberg and formulated by Kennard and Weyl [72, 85, 159].

Although URs such as Eq. (1.6) remarkably bound the variances of two observables on the same state, we notice that when evaluated on an eigenstate of either A or B, the lower bound becomes trivial. Various approaches, such as those by Huang [79] and by Maccone and Pati [102], have attempted to address this issue by introducing bounds on the sum of variances. A well known example of such an UR puts a bound on the sum of the variances of the Pauli observables X, Y, and Z for all states ϱ, namely [49]

$$\Delta^2_\varrho(X) + \Delta^2_\varrho(Y) + \Delta^2_\varrho(Z) \geq 2. \tag{1.7}$$

Unlike the Robertson UR, its lower bound does not depend on the state on which the variances are computed. Such relations, called *state independent* URs, can be evaluated even when no information on the state is known.

Exceptions aside, very few variance-based URs satisfy the properties of (i) being state-independent, (ii) providing a lower bound for the sum of variances, and (iii) applying to more than two observables. Chapter 2 proposes URs that fulfil these criteria, albeit limited to dichotomic observables. Similar preparation URs have been previously studied, for instance in [2, 130, 55, 139], but the results were mainly applicable to two or three observables and not to larger sets.

The message conveyed by preparation URs is that, given a set of observables, it is not always possible the prepare a quantum system in a sate that is arbitrarily close to eigenstates of all the observables considered. On the other hand, preparation URs do not reveal anything about the measurement

process in itself. This equally fundamental question is covered by *measurement uncertainty relations*, which aim to quantify the disturbance caused by one measurement onto another when they are performed simultaneously or sequentially. For a detailed discussion on the topic, we refer to [26] and to [27].

1.3 Quantum entanglement

Quantum entanglement was first described in 1935 by Schrödinger [129] and by Einstein, Podolsky, and Rosen [46], sparking many debates among physicists at the time. Years later, Bell proposed experimentally testable inequalities that could demonstrate a deviation from classical physics [12], now referred to as *Bell inequalities*. These inequalities have later been implemented experimentally [50, 6, 155], leading to the awarding of the 2022 Nobel Prize in physics to Aspect, Clauser, and Zeilinger "for experiments with entangled photons, establishing the violation of Bell inequalities and pioneering quantum information science". Although driven by interest for a fundamental understanding of the quantum theory, physicists have since realised that entanglement is not just a theoretical curiosity but can be a practical resource, with applications such as quantum teleportation [15] and quantum key distribution [47].

From a theoretical perspective, the structure of the set of entangled states is extremely rich, especially when going to more than two parties. In this section, we review basic concepts in entanglement theory that are relevant for the subsequent chapter. We first present in Section 1.3.1 the definitions of entanglement between two parties. We then discuss in Section 1.3.2 how these definitions behave when entanglement is shared between more than two parties, and present some of the main methods for entanglement detection in Section 1.3.3. Finally, we present in Section 1.3.4 the more recent concept of *network entanglement*, which is concerned with entanglement distribution in network structures.

1.3.1 Bipartite entanglement

When considering *composite systems*, that is, systems that are made up of several subsystems, tensor products of Hilbert spaces are required. Let us consider a quantum system made up of two subsystems A and B, each of dimension d without loss of generality. Its global Hilbert space is $\mathcal{H} = \mathcal{H}_A \otimes$

$\mathcal{H}_B$ [152]. Naturally, this space contains states of the form $|\Psi\rangle = |\phi\rangle \otimes |\chi\rangle$ where $|\phi\rangle \in \mathcal{H}_A$ and $|\chi\rangle \in \mathcal{H}_B$. However, not all elements of $\mathcal{H}$ can be decomposed in such a way. A evident four-dimensional example is the two-qubit state

$$\left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle), \tag{1.8}$$

which is one of the four *Bell states* [152]. Physically, bipartite systems in the state $|\Phi^+\rangle$ cannot be described separately by pure states. This motivates the definition of *separable* and *entangled pure states*.

Definition 1.1 (Separable (pure) state [60])**.** A pure state $|\Psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ is said to be *separable* if there exist two states $|\phi\rangle \in \mathcal{H}_A$ and $|\chi\rangle \in \mathcal{H}_B$ such that $|\Psi\rangle$ can be written as a tensor product, i.e., $|\Psi\rangle = |\phi\rangle \otimes |\chi\rangle$. Otherwise, the state $|\Psi\rangle$ is called *entangled*.

In the following, we omit the tensor product symbol, or directly write the states in the same vector when the situation is unambiguous, e.g., $|\phi\rangle \otimes |\chi\rangle = |\phi\rangle\,|\chi\rangle = |\phi\chi\rangle$. This is also applied to Pauli operators, e.g., $X \otimes X = XX$.

In order to decide whether a (pure) state $|\Psi\rangle$ is entangled, it suffices to look at its *Schmidt decomposition*. Indeed, for any state $|\Psi\rangle \in \mathcal{H}_A^d \otimes \mathcal{H}_B^d$, it is possible to find two local orthonormal bases $\{|\alpha_i\rangle \in \mathcal{H}_A\}_{i=1}^d$ and $\{|\beta_i\rangle \in \mathcal{H}_B\}_{i=1}^d$, and r coefficients $\varsigma_1 \geq \cdots \geq \varsigma_r > 0$, such that [152]

$$|\Psi\rangle = \sum_{i=1}^{r} \varsigma_i\,|\alpha_i\rangle\,|\beta_i\rangle\,. \tag{1.9}$$

The right hand side is called the Schimdt decomposition of $|\Psi\rangle$, and the number r of coefficients is called its *Schmidt rank* of $|\Psi\rangle$ [60]. Clearly, r is at most d, the local dimension. The uniqueness of the coefficients follows from a singular value decomposition [152], from which follows that $|\Psi\rangle$ is separable if and only if its Schmidt rank is equal to one. We note that this is not the only way to determine if a state is separable or entangled [52, 60, 77].

Unfortunately, such a necessary and sufficient criterion for separability does not exist for mixed states. When the state of the system is mixed, we say that it is separable if it can be written as a convex combination of pure separable states.

Definition 1.2 (Separable (mixed) state [60])**.** A mixed state $\varrho \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ is said to be *separable* if the exist two sets of L pure states $\{|\phi_k\rangle \in \mathcal{H}_A\}_{k=1}^L$

and $\{|\chi_k\rangle \in \mathcal{H}_B\}_{k=1}^L$, and convex weights $\{p_k\}_{k=1}^L$ such that ϱ can be written as a convex combination of pure separable states, i.e., $\varrho = \sum_{k=1}^L p_k |\phi_k\rangle\langle\phi_k| \otimes |\chi_k\rangle\langle\chi_k|$. Otherwise, the state ϱ is called *entangled*.

The set of separable states is convex. As a particular case, we define *product states*.

Definition 1.3 (Product state [60])**.** A *product state* $\varrho \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ is a state that can be written as a tensor product, i.e., $\varrho = \varrho_A \otimes \varrho_B$ with $\varrho_A \in \mathcal{S}(\mathcal{H}_A)$ and $\varrho_B \in \mathcal{S}(\mathcal{H}_B)$. In particular, all pure separable states are product states.

Deciding whether a general quantum state is entangled or not is a central question in quantum information theory.

Problem 1.1 (Separability problem)**.** *Given a bipartite state $\varrho \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$, determine whether it is separable or entangled.*

It has been shown that this problem is in general NP-hard [66]. As mentioned, it is fully solved for bipartite pure states, for instance through the Schimdt decomposition. For the general case, only partial results are known, mostly under the form of necessary or sufficient criteria (see e.g. [52, 60, 67, 77] for reviews on the topic).

In practical situations, it might not be possible or relevant to have access to the state of the global system. In this case, it may be interesting to describe only a single subsystem. This can be done via *marginal states* (or *reduced density operators*). A bipartite state $\varrho \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ has two marginal states, $\varrho^{(A)} = \mathrm{tr}_B(\varrho)$ and $\varrho^{(B)} = \mathrm{tr}_A(\varrho)$, which belong to $\mathcal{S}(\mathcal{H}_A)$ and to $\mathcal{S}(\mathcal{H}_B)$ respectively. Therein, the *partial trace* operation is used, which is the unique linear map $\mathrm{tr}_A : \mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_B) \to \mathcal{L}(\mathcal{H}_B)$ such that $\mathrm{tr}_A(X \otimes Y) = \mathrm{tr}(X)Y$ for all $X \in \mathcal{L}(\mathcal{H}_A)$ and all $Y \in \mathcal{L}(\mathcal{H}_B)$ [152]. This definition extends trivially to tr_B. As an example, the marginal states of $|\Psi^+\rangle$ defined in Eq. (1.8) are $\varrho^{(A)} = \varrho^{(B)} = \mathbb{1}/2$, i.e., the maximally mixed state[3].

1.3.2 Multipartite entanglement

The situation gets arguably more intricate for multipartite systems with more than two parties. Here, we only introduce concepts for tripartite systems ABC, as it generalises easily for more parties. Let us start with a few definitions.

[3]The d-dimensional mixed state $\mathbb{1}/d$ is called *maximally mixed*, as it is an equal-probability mixture of all basis states of $\mathcal{H}^d$.

Definition 1.4 (Separable pure state [60])**.** A tripartite pure state $|\Psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$ is *biseparable across the bipartition* $A \mid BC$ if there exist states $|\phi\rangle \in \mathcal{H}_A$ and $|\chi\rangle \in \mathcal{H}_B \otimes \mathcal{H}_C$ such that $|\Psi\rangle = |\phi\rangle \otimes |\chi\rangle$. The same holds for the bipartitions $B \mid CA$ and $C \mid AB$. If there exist states $|\phi\rangle \in \mathcal{H}_A$, $|\chi\rangle \in \mathcal{H}_B$ and $|\zeta\rangle \in \mathcal{H}_C$ such that $|\Psi\rangle = |\phi\rangle \otimes |\chi\rangle \otimes |\zeta\rangle$, the pure state $|\Psi\rangle$ is called *fully separable*.

These definitions extend naturally to mixed states.

Definition 1.5 (Separable state [60])**.** A tripartite state $\varrho \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C)$ is *biseparable* if it can be written as a convex combination of biseparable pure states. If it can be written as a convex combination of fully separable pure states, it is called *fully separable*.

An important note is that the pure states in the biseparable decomposition of $\varrho \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C)$ may be biseparable across different bipartitions, e.g., $\varrho = 1/2(|0\rangle\langle 0|_A \otimes |\Phi^+\rangle\langle\Phi^+|_{BC} + |\Phi^+\rangle\langle\Phi^+|_{AB} \otimes |0\rangle\langle 0|_C)$. The first term of its decomposition is biseparable across $A \mid BC$, whereas the second is biseparable across $AB \mid C$. For the sake of clarity, we added subscripts indicating to which subsystems the states refer. The definitions of full separability and biseparability naturally generalise to n-partite systems with $n > 3, n \in \mathbb{N}$.

Finally, we define the central concept of *genuine multipartite entanglement* (GME).

Definition 1.6 (Genuine multipartite entanglement [60])**.** An n-partite state $\varrho \in \mathcal{S}(\bigotimes_{i=1}^{n} \mathcal{H}_i)$ is said to be *genuine multipartite entangled* if it cannot be written as a convex combination of biseparable pure states, i.e., if it is not biseparable.

A famous example is the three-qubit *Greenberger–Horne–Zeilinger* (GHZ) *state*, [58]

$$|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle), \tag{1.10}$$

which can be extended to n-qubit systems, $|\mathrm{GHZ}_n\rangle = \frac{1}{\sqrt{2}}(|0\ldots0\rangle + |1\ldots1\rangle)$. Notice that $|\mathrm{GHZ}_2\rangle$ is equal to $|\Phi^+\rangle$, defined in Eq. (1.8). The so-called W state [44]

$$|W\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle) \tag{1.11}$$

is GME as well. Notably, if a tripartite quantum system is in a $|\mathrm{GHZ}\rangle$ state, it is not possible to transform it into a W state using local operations assisted

by classical communication (a set of transformations called LOCC), even if the transformation may only be achieved stochastically (we then talk about SLOCC transformations) [44]. Indeed, the GHZ state and the W state belong to distinct classes of three-qubit entangled states that are inequivalent under SLOCC operations, and form the homonymous *entanglement classes*. For three-qubit systems, these are the only inequivalent GME classes [60].

1.3.3 Entanglement detection and quantification

As entanglement is a central resource for many quantum information applications, it is of importance to certify that a given state is entangled (GME) or not. Moreover, one may be interested in quantifying the amount of entanglement in a state. In other words, answering whether some states can be in a sense "more entangled" than others. A vast literature exists on the subject, for which we refer the reader to [52, 60, 67, 77]. We introduced here some concepts that are necessary for the proper understanding of this thesis.

Entanglement witnesses

Probably the easiest-to-understand tool for entanglement detections is the concept of *entanglement witnesses*.

Definition 1.7 (Entanglement witness [60])**.** An *entanglement witness* is a Hermitian operator $W \in \mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_B)$ such that $\mathrm{tr}\big(W\varrho_{\mathrm{sep}}\big) \geq 0$ holds for all separable states $\varrho_{\mathrm{sep}} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ and such that there exists at least one entangled state $\varrho \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ for which $\mathrm{tr}(W\varrho) < 0$.

Clearly, any state ϱ that satisfies $\mathrm{tr}(W\varrho) < 0$ is detected to be entangled, which makes entanglement witnesses sufficient criteria for entanglement. It has been shown that every entangled state can be detected by a witness [76], but this only shifts the separability problem to finding the appropriate witness for a given state.

Since entanglement witnesses are Hermitian operators, they correspond to physical observables. They are thus considered experimentally friendly, as $\mathrm{tr}(W\varrho)$ corresponds to the expectation value of the observable W on the state ϱ. Nevertheless, measuring non-product observables remains experimentally challenging, and in practice witnesses are often decomposed in a sum of product operators that are in turn all individually measured [61, 21, 52].

To illustrate the concept of entanglement witnesses, we consider the class of *fidelity witnesses* that rely on the maximal *fidelity* to some entangled state. The fidelity F_ψ of a state $\varrho \in \mathcal{S}(\mathcal{H})$ to a pure state $|\psi\rangle$ quantifies the overlap between them in the following way

$$F_\psi(\varrho) = \langle\psi|\,\varrho\,|\psi\rangle\,. \tag{1.12}$$

From this, we construct a witnesses based on an entangled state $|\Psi\rangle$,

$$W_\Psi = \varsigma_1^2 \mathbb{1} - |\Psi\rangle\langle\Psi|\,, \tag{1.13}$$

where ς_1 is the largest Schimdt coefficient of $|\Psi\rangle$ (see Eq. (1.9)). The fact that operators of that form are proper entanglement witnesses follows from $\max_{\varrho_{\text{sep}}} F_\Psi(\varrho_{\text{sep}}) = \varsigma_1^2$ [21, 65, 42]. As an example, consider an n-qubit GHZ state as in Eq. (1.10). For any bipartition, its Schmidt decomposition is the same and $\varsigma_1^2 = 1/2$. Therefore, $W_{\text{GHZ}} = \mathbb{1}/2 - |\text{GHZ}_n\rangle\langle\text{GHZ}_n|$ is an entanglement witness for any bipartition of n qubits that detects states with a fidelity F_{GHZ_n} strictly lager than $1/2$ to be entangled.

Fidelity witnesses are easy to derive and an important class of witnesses, nevertheless, it has been shown that they are not sufficient, in the sense that not all entangled states can be detected by such witnesses [156, 65].

Covariance matrices

First introduced in the context of quantum information for continuous variable systems [54, 158], covariance matrices (CMs) have been used since the early 2000s to characterise bipartite and multipartite quantum entanglement [56, 63]. For a given multipartite state, they quantify the covariance between the expectation values of different observables. A CM Γ is constructed for a state ϱ and a set of observables $\{M_i\}_{i=1}^N$, and has the following matrix entries

$$[\Gamma(\{M_i\}, \varrho)]_{mn} = \langle M_m M_n\rangle_\varrho - \langle M_m\rangle_\varrho \langle M_n\rangle_\varrho \tag{1.14}$$

for all $m, n \in [N]$. These are particularly used in the context of the separability problem when only local observables can be measured. When $\{M_i\}_{i=1}^N = \{A_i \otimes \mathbb{1}, \mathbb{1} \otimes B_i\}_{i=1}^{d^2}$, the CM has a block structure

$$\Gamma(\{A_i \otimes \mathbb{1}, \mathbb{1} \otimes B_i\}_{i=1}^{d^2}, \varrho) = \begin{pmatrix} \Gamma_A & \gamma_E \\ \gamma_E^T & \Gamma_B \end{pmatrix}, \tag{1.15}$$

where the diagonal blocks are CMs for the marginal states $\varrho_A = \mathrm{tr}_B(\varrho)$ and $\varrho_B = \mathrm{tr}_A(\varrho)$, i.e., $\Gamma_A = \Gamma(\{A_i\}_{i=1}^{d^2}, \varrho_A)$ and $\Gamma_B = \Gamma(\{B_i\}_{i=1}^{d^2}, \varrho_B)$. The separability problem can be restated as a necessary and sufficient condition on the block CM [56]. When A_i, $i \in [d^2]$, are orthogonal observables that fulfil $\mathrm{tr}(A_i A_j) = d\delta_{ij}$, $i, j \in [d^2]$ (similarly for B_i, $i \in [d^2]$), it follows that if the state ϱ is separable, then $\|\gamma_E\|_{\mathrm{tr}}^2 \leq d^2(1 - \mathrm{tr}(\varrho_A^2))(1 - \mathrm{tr}(\varrho_B^2))$, which is a computable entanglement criteria [56]. The norm $\|\cdot\|_{\mathrm{tr}}$ is the trace norm, given by the sum of the singular values of its argument [75].

Schmidt number

The Schmidt rank of pure states is an entanglement measure and can be used to quantify the entanglement dimensionality [77]. The notion of Schmidt rank extends to mixed states $\varrho \in \mathcal{S}(\mathcal{H}_A^d \otimes \mathcal{H}_B^d)$ under the name of *Schmidt number* (SN) as follows [77],

$$\mathrm{SN}(\varrho) = \min_{\varrho = \sum_{k=1}^{L} p_k |\psi_k\rangle\langle\psi_k|} \max_{k \in [L]} r(\psi_k) \tag{1.16}$$

where by $r(\psi_k)$ we mean the Schmidt rank of the pure state $|\psi_k\rangle$. Therefore, $1 \leq \mathrm{SN}(\varrho) \leq d$ holds for all $\varrho \in \mathcal{S}(\mathcal{H}_A^d \otimes \mathcal{H}_B^d)$. The Schmidt number quantifies the amount of entanglement in a mixed state ϱ through the largest Schmidt rank-state that is at least needed to prepare ϱ. The set of states with Schmidt number smaller or equal to q is convex, and denoted S_q, $q \in [d]$. Clearly, we have $S_1 \subset S_2 \subset \cdots \subset S_d$ and S_1 is the set of separable states.

Similarly to entanglement witnesses, we can define Schmidt number witnesses as Hermitian operators W_q that verify $\mathrm{tr}(W_q \varrho_q) \geq 0$ for all $\varrho_q \in S_q$ and for which there exists at least one state ϱ with a Schmidt number strictly larger than q such that $\mathrm{tr}(W_q \varrho) < 0$. Obviously, when $q = 1$, we recover the definitions of entanglement witnesses. In Chapter 2, we propose a way of constructing such witnesses from uncertainty relations.

1.3.4 Network entanglement

Quantum networks are a central topic in the development of the concept of the *quantum internet*: A network of interconnected computers that should be able to send, receive and manipulate quantum systems [16, 88, 126, 134, 154]. Such structures should in the future answer a demand for operations such as remote quantum computations [24], distant frequency comparison [112] or multipartite quantum key agreement [110]. Building blocks including en-

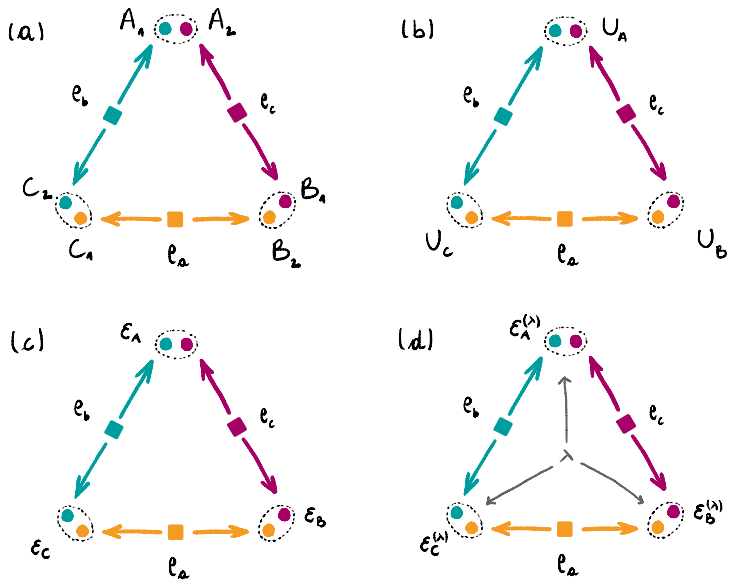

Figure 1.2: *The four different network state definitions.* (a) BTN: Three (entangled) source states ϱ_a, ϱ_b and ϱ_c distribute parties to the three nodes $A = A_1A_2$, $B = B_1B_2$ and $C = C_1C_2$. (b) UTN: The three parties A, B and C perform unitary operations U_A, U_B and U_C on their respective systems. (c) CTN: The operations are no longer restricted to unitary operation, but may be any CPTP maps $\mathcal{E}_A$, $\mathcal{E}_B$ and $\mathcal{E}_C$. (d) LOSR triangle network: The local operation may be coordinated by a shared random variable $\lambda \in [L]$.

tanglement generation and distribution [25, 82, 87, 137], quantum repeaters [8, 133] or quantum memories [91, 98] are currently being investigated both theoretically and experimentally.

In this context, we present the notion of *network entanglement*, which aims to answer the question whether a multipartite state can be prepared using several source states with lower numbers of parties that are distributed in a network structure, without classical communication (see e.g. [3, 11, 36, 94, 101, 103, 151, 162, 164] and [A, C]). This situation differs from the usual consideration of multipartite entanglement, where the parties have access to a multipartite state generated by a global source. In addition, the absence of classical communication prevents from executing protocols such as quantum teleportation or entanglement swapping [15, 20, 116, 167].

For the sake of clarity, we consider the smallest non-trivial example, viz. the triangle network (see Figure 1.2). It involves three parties, A, B and C, wanting to share a tripartite (entangled) state, while only having access to bipartite sources. The different parties of the network are sometimes referred to as the *nodes* of the network. Between them, three states (*sources*

states) are distributed following the three edges. Depending on the situation, the parties may perform local operation on their systems, either restricted to unitary operations or not, or even have access to shared randomness. We present in what follows four different definitions of *network states*: the basic triangle network (BTN), where bipartite sources are shared among the parties, the triangle network with local unitaries (referred to as UTN) where A, B and C are allowed to perform unitary operations on their local systems, the triangle network with local channels (referred to as CTN) where, as the name indicates, local channels are performed by the parties, and finally, LOSR networks where channels are applied and the nodes have access to shared randomness. All are illustrated in Figure 1.2.

In the BTN, three (entangled) bipartite source states ϱ_a, ϱ_b, and ϱ_c are prepared and each subsystem is sent to a node according to the distribution in Figure 1.2 (a), i.e., ϱ_a is distributed to B_2 and C_1, ϱ_b is distributed to C_2 and A_1, and ϱ_c is distributed to A_2 and B_1. Without loss of generality, we assume that the sources all send $d \times d$-dimensional states. The three nodes A, B, and C have access to the bipartite systems A_1A_2, B_1B_2, and C_1C_2 respectively, as shown in Figure 1.2 (a). We define BTN states as follows.

Definition 1.8 (BTN states)**.** Let $\varrho_a \in \mathcal{S}(\mathcal{H}_{B_2} \otimes \mathcal{H}_{C_1})$, $\varrho_b \in \mathcal{S}(\mathcal{H}_{C_2} \otimes \mathcal{H}_{A_1})$, and $\varrho_c \in \mathcal{S}(\mathcal{H}_{A_2} \otimes \mathcal{H}_{B_1})$ be $d \times d$-dimensional bipartite source states. The global *state of a basic triangle network* reads

$$\varrho_{\text{BTN}} = \varrho_b \otimes \varrho_c \otimes \varrho_a, \tag{1.17}$$

where $\varrho_{\text{BTN}} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C)$ is a $d^2 \times d^2 \times d^2$-dimensional state.

Notice that the order of the subsystems in Eq. (1.17) is ABC for the left-hand side, whereas the right-hand-side is organised following the order $C_2A_1A_2B_1B_2C_1$. This scenario has for instance been studied in the context of pair entangled network states in [36], where the authors show that GME in BTN with bipartite sources depends on both the level of noise and on the network topology.

When thinking about practical implementations of quantum networks, it is perfectly reasonable to assume that the parties have the ability to perform operations on their local systems. We distinguish two types of local operations: unitary operations and the more general completely positive and trace preserving (CPTP) operations [152].

Definition 1.9 (UTN states)**.** Let ϱ_{BTN} be a BTN state as in Definition 1.8 and let U_A, U_B and U_C be unitary operators in $\mathcal{L}(\mathcal{H}^{d^2})$. The global *state of a unitary triangle network* reads

$$\varrho_{\text{UTN}} = (U_A \otimes U_B \otimes U_C)\varrho_{\text{BTN}}(U_A^\dagger \otimes U_B^\dagger \otimes U_C^\dagger). \tag{1.18}$$

In this situation, the nodes no longer necessarily hold separable states. We note that here again, there is no tripartite interaction between the parties.

Second, we drop the unitary restriction on the local operations, meaning that the nodes may now perform channels on their local systems, represented by CPTP maps $\mathcal{E}_A$, $\mathcal{E}_B$ and $\mathcal{E}_C$.

Definition 1.10 (CTN states)**.** Let ϱ_{BTN} be a BTN state as in Definition 1.8 and let $\mathcal{E}_A$, $\mathcal{E}_B$ and $\mathcal{E}_C$ be CPTP maps transforming elements from $\mathcal{S}(\mathcal{H}^{d^2})$ to elements in $\mathcal{S}(\mathcal{H}^{d'})$. The global *state of a channel triangle network* reads

$$\varrho_{\text{CTN}} = \mathcal{E}_A \otimes \mathcal{E}_B \otimes \mathcal{E}_C(\varrho_{\text{BTN}}). \tag{1.19}$$

We note that the channels applied may reduce the dimension, e.g., the sources may be four-dimensional states and the channels reduce the dimension to qubits, $\mathcal{E}_X : \mathcal{S}(\mathcal{H}^4) \to \mathcal{S}(\mathcal{H}^2)$, with $X = A, B, C$. The preparations of UTN and CTN states are represented in Figures 1.2 (b) and (c) respectively.

Lastly, we allow the local operations to be coordinated by a global classical random variable $\lambda \in [L]$, as presented in Figure 1.2 (d). This corresponds physically to coordinating which CPTP maps are applied, i.e., access to *shared randomness*. Depending on the allowed local operations and on the presence or absence of shared randomness, the set of preparable states varies, it is therefore important to always explicitly mention which definition of network entanglement is considered.

Definition 1.11 (LOSR network states)**.** Let ϱ_{BTN} be a BTN state as in Definition 1.8 and let $\mathcal{E}_A^{(\lambda)}$, $\mathcal{E}_B^{(\lambda)}$ and $\mathcal{E}_C^{(\lambda)}$ be CPTP maps acting from $\mathcal{S}(\mathcal{H}^{d^2})$ to $\mathcal{S}(\mathcal{H}^{d'})$ that depend on a random variable $\lambda \in [L]$. Let p_λ, with $\lambda \in [L]$, be convex weights. The global state of a LOSR triangle network reads

$$\varrho_\Delta = \sum_{\lambda=1}^{L} p_\lambda \mathcal{E}_A^{(\lambda)} \otimes \mathcal{E}_B^{(\lambda)} \otimes \mathcal{E}_C^{(\lambda)}(\varrho_{\text{BTN}}). \tag{1.20}$$

The discerning reader may have noticed that in Eq. (1.20) the state ϱ_{BTN} does not depend on the shared random variable $\lambda \in [L]$. As pointed out in

[111], in the case of unbounded source dimensions, it suffices to consider that either the state or the parties have solely access to the global variable. Indeed, the dependency on the shared random variable in the source states can always be removed by enlarging the dimension. To see that, consider $\sum_{\lambda=1}^{L} p_\lambda \mathcal{E}_A^{(\lambda)} \otimes \mathcal{E}_B^{(\lambda)} \otimes \mathcal{E}_C^{(\lambda)}(\varrho_{\text{BTN}}^{(\lambda)})$, with $\varrho_{\text{BTN}}^{(\lambda)} = \varrho_b^{(\lambda)} \otimes \varrho_c^{(\lambda)} \otimes \varrho_a^{(\lambda)}$, $\lambda \in [L]$. It is possible to combine the set $\{\varrho_a^{(\lambda)}\}_{\lambda=1}^{L}$ to a single, higher dimensional ϱ_a and redefine the maps $\mathcal{E}_A^{(\lambda)}$ such that they act on the appropriate $\varrho_a^{(\lambda)}$, with $\lambda \in [L]$, and similarly for b and c. This results in a form where ϱ_{BTN} does not depend on λ any more, hence the state can be written as in Eq. (1.20).

Equivalently, the dependency of the map $\mathcal{E}_X$ on λ may be removed such that the shared randomness is solely carried by the source states, for all $X = A, B, C$. More explicitly, the source states may be redefined as $\varrho_c^{(\lambda)} \otimes |\lambda\rangle\langle\lambda|$ with orthogonal ancilla states $|\lambda\rangle$ being send to party B such that B can, by measuring $|\lambda\rangle$, decide which channel to apply, for all $\lambda \in [L]$. The sources $\varrho_a^{(\lambda)}$ and $\varrho_b^{(\lambda)}$ are refined similarly, sending their ancillas respectively to C and A. This measurement can then be seen as a global channel $\mathcal{E}_B$ that does not depend on λ. From the linearity of the maps, LOSR networks states may equivalently be defined as $\varrho_\Delta = \mathcal{E}_A \otimes \mathcal{E}_B \otimes \mathcal{E}_C(\sum_\lambda p_\lambda \varrho_{\text{BTN}}^{(\lambda)})$.

A direct observation is that, whereas Eqs. (1.17 – 1.19) lead to non-convex state sets [94], the set of LOSR network states is convex. Its extremal points are of the form $\mathcal{E}_A \otimes \mathcal{E}_B \otimes \mathcal{E}_C(|a\rangle\langle a| \otimes |b\rangle\langle b| \otimes |c\rangle\langle c|)$, with $|a\rangle, |b\rangle, |c\rangle \in \mathcal{H}^{d^2}$. For instance, pure biseparable tripartite states, such as $|\psi\rangle = |\phi\rangle_{AB} \otimes |\eta\rangle_C$ are extremal points. Nonetheless, some extreme points are mixed states, which can be seen as follows: It was shown in [101] that pure three-qubit states that are GME cannot be prepared in the triangle network. On the other hand, in [111], it was shown that there are LOSR network states having a GHZ fidelity of 0.5170[4], which implies that they are GME, as certified by the GHZ fidelity witness (see Section 1.3.3). So, the set of LOSR network states must have some extremal points that are GME mixed states. Finally, notice that pure GME states can exist in higher-dimensional triangle networks: For instance, the three-ququart state $|\phi^+\rangle_{A_2B_1} \otimes |\phi^+\rangle_{B_2C_1} \otimes |\phi^+\rangle_{C_2A_1}$ is GME for the partition $A_1A_2 \mid B_1B_2 \mid C_1C_2$, as pointed out in [36].

Figure 1.2 summarises the four aforementioned definitions. Each of them can directly be extend to more parties and to multipartite sources. We nevertheless require that no matter the definition, n-partite networks should involve source states that are at most $(n-1)$-partite. An example are the

[4] In a private communication, Nikolai Wyderka reported three-qubit LOSR network states with a fidelity of 0.548047 to the GHZ state.

no common double source (NCDS) networks, where any two parties can share subsystems from at most one common source. For instance, networks with only bipartite sources are NCDS networks.

Importantly, such constructions do not allow for classical communication between the parties, nor for non-local operations, which makes the set of network states a non-trivial subset of general states. A crucial example is that the GHZ state $|\mathrm{GHZ}\rangle = 1/\sqrt{2}(|000\rangle + |111\rangle)$ cannot be prepared in LOSR triangle networks [3, 94, 101, 111].

Analogously to the separability problem, we aim to find necessary and/or sufficient criteria that determine whether a tripartite state can or cannot be prepared in such a way. We address this question in Chapter 4.

1.4 Symmetric states

As discussed, multipartite entanglement is a crucial resource for many quantum information protocols, but characterising the set of GME states has proved to be challenging. Indeed, already for four-qubit systems, the number of inequivalent entanglement classes under SLOCC is infinite [96, 150]. The focus has thus been shifted to specific classes of states that are not only highly entangled, but also describable using simple formalisms. Among these, symmetric states stand out. In this context, we consider two types of symmetric states that are invariant under transformations of the form $\varrho \mapsto T\varrho T^\dagger = \varrho$, namely, *stabiliser states* and *permutationally symmetric states*.

1.4.1 Stabiliser and graph states

Among the large class of stabiliser states, *graph states* are multi-qubit entangled pure states that find numerous applications. It has long been established that they serve as essential resources for quantum error correction codes [57] and measurement-based quantum computation [23, 124]. Applications are still being developed today, such as their recent use in benchmarking quantum computers [19]. Furthermore, graph states are relevant in foundational topics, such as achieving maximal violation of Bell inequalities [62]. Graph states have a convenient graphical description where certain graphical operations directly correspond to physical operations on the states.

We begin by defining *stabiliser states*. A stabiliser state is an n-qubit pure state described by a *stabiliser* S, a set of 2^n pairwise commuting n-qubit Pauli

operators (up to a ± 1 factor). The stabiliser state $|\Psi\rangle$ associated to S is the unique common (normalised) $+1$-eigenstate of the elements in S, hence it satisfies

$$s\,|\Psi\rangle = |\Psi\rangle \quad \forall s \in S. \tag{1.21}$$

It thus directly follows that the projector onto $|\Psi\rangle$ reads

$$|\Psi\rangle\langle\Psi| = \frac{1}{2^n}\sum_{s\in S} s. \tag{1.22}$$

As an example, consider the Bell state $|\Phi^+\rangle = 1/\sqrt{2}(|00\rangle + |11\rangle)$ of Eq. (1.8). It is easy to verify that it is invariant under the action of XX, $-YY$, and ZZ. We say that $|\Phi^+\rangle$ is *stabilised* by these operators, and its stabiliser reads $S = \{\mathbb{1}_4, XX, -YY, ZZ\}$.

A stabiliser can alternatively be described by a set of n *generators*. The generators g_i, with $i \in [n]$, are n elements of S that are such that $S = \{\prod_{i=1}^n g_i^{k_i} \mid k_i = 0, 1, i \in [n]\}$, i.e., they *generate* the 2^n elements of S. In the case of $|\Phi^+\rangle$, the elements XX and ZZ generate its stabiliser. It is often more convenient to directly work with the set of generators of a stabiliser state then with the state itself.

Graph states are particular n-qubit stabiliser states that can be described by mathematical graphs. Each qubit is associated with a vertex of a graph $G = ([n], E)$, where $[n]$ is the vertex set and E the edge set (see the later Section 1.6.2 for graph theory definitions). The set of edges dictates how the generators behave. Let us denote the neighbourhood of the vertex i in G by $\mathcal{N}_i$, that is, the set of all vertices of G that share an edge with i. The generators of the graph state associated to G are given by

$$g_i = X_i \prod_{j\in\mathcal{N}_i} Z_j \quad \forall i \in [n]. \tag{1.23}$$

The indices on the Pauli operators refer to the qubits they act on. As an example, consider the six-vertex star graph G_* presented in Figure 1.3. Following the above equation, the graph state $|G_*\rangle$ is the $+1$-common eigenstate of

$$\begin{aligned} &g_1 = XZZZZZ, \quad g_2 = ZX\mathbb{1}\mathbb{1}\mathbb{1}\mathbb{1}, \quad g_3 = Z\mathbb{1}X\mathbb{1}\mathbb{1}\mathbb{1}, \\ &g_4 = Z\mathbb{1}\mathbb{1}X\mathbb{1}\mathbb{1}, \quad g_5 = Z\mathbb{1}\mathbb{1}\mathbb{1}X\mathbb{1}, \quad g_6 = Z\mathbb{1}\mathbb{1}\mathbb{1}\mathbb{1}X. \end{aligned} \tag{1.24}$$

From a more practical perspective, graph states can be generated using controlled Z operations, $CZ = \mathbb{1} - 2\,|11\rangle\langle 11|$ [70]. Preparing the graph state

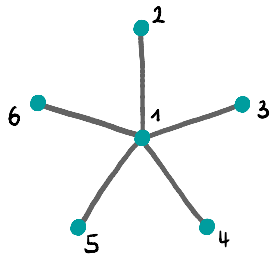

Figure 1.3: *Six-vertex star graph* G_*. The corresponding six-qubit graph state is the unique $+1$-common eigenstate of the six generators presented in Eq. (1.24).

$|G\rangle$ associated to the graph $G = ([n], E)$ goes as follows: All the n qubits are initialised in the state

$$|+\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + |1\rangle \right). \tag{1.25}$$

The global n-qubit state reads $|+\rangle^{\otimes n}$. Then, for each edge $\{i, j\} \in E$, the unitary operation CZ is applied on the qubits i and j. The resulting global state is the graph state

$$|G\rangle = \left(\prod_{\{i,j\} \in E} CZ_{ij} \right) |+\rangle^{\otimes n}, \tag{1.26}$$

where the indices ij specifies on which two qubits the CZ operation is applied. The state $|G_*\rangle$ associated to the graph G_* of Figure 1.3 thus reads

$$|G_*\rangle = CZ_{1,2}CZ_{1,3}CZ_{1,4}CZ_{1,5}CZ_{1,6} |+\rangle^{\otimes 6}. \tag{1.27}$$

As previously discussed, determining whether two multipartite entangled states are equivalent under SLOCC transformations is a question of significant importance, although hard to answer in general. Perhaps surprisingly, this equivalence for graph states reduces to equivalence under local unitary transformations [70]. In this context, we introduce a graphical formalism to determine whether two graph states are equivalent under a specific set of local unitary transformations, namely those within the local Clifford group[5].

We introduce a graph operation called *local complementation*. Consider a

[5]The local Clifford group is the set of transformations that preserve the Pauli group. For further details, we refer the reader to [69], as the relevant point here is that these operations exist and are local.

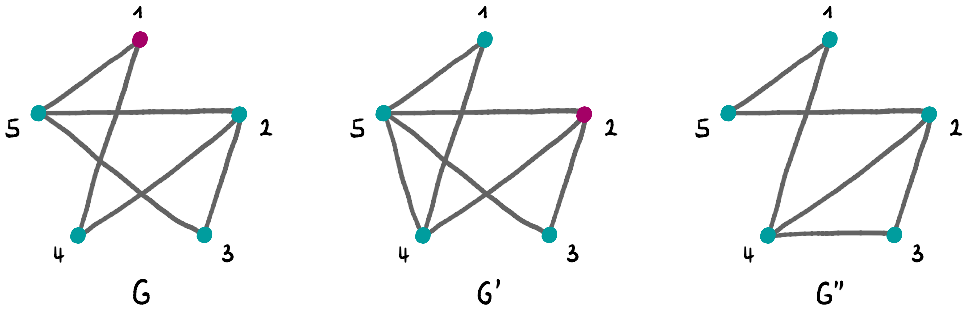

Figure 1.4: *Example of local complementation.* First, the local complementation is applied on vertex 1 of G. The neighbourhood of vertex 1 is $\{4,5\}$, which are not connected. The set E_1 is thus empty and $\bar{E}_1 = \{\{4,5\}\}$. The resulting graph is G', whose edge set is $E' = (E \setminus \emptyset) \cup \{\{4,5\}\}$. The local complementation is now applied to vertex 2 of G', whose neighbourhood is $\{3,4,5\}$. Therein, the vertices 3 and 5 are connected, as well as 4 and 5. The resulting graph is G'' with edge set $E'' = (E' \setminus \{\{3,5\},\{4,5\}\}) \cup \{\{3,4\}\}$. The three graph states $|G\rangle$, $|G'\rangle$, and $|G'\rangle$ are equivalent under local operations.

graph $G = ([n], E)$ and one of its vertices $x \in [n]$. Let us define

$$E_x = \{\{i,j\} \in E \mid i,j \in \mathcal{N}_x\}, \tag{1.28a}$$

$$\bar{E}_x = \{\{i,j\} \notin E \mid i,j \in \mathcal{N}_x\} \tag{1.28b}$$

where E_x is the set of edges of neighbourhood of x, and $\bar{E}_x$ is its complement. The local complementation of G on x renders a graph G' with the same vertex set, and as edge set $E' = (E \setminus E_x) \cup \bar{E}_x$. Figure 1.4 depicts an example. The two graph states $|G\rangle$ and $|G'\rangle$ are related by $|G'\rangle = U_x |G\rangle$ [69, 147], where

$$U_x = \sqrt{-iX_x} \prod_{y \in \mathcal{N}_x} \sqrt{iZ_y}. \tag{1.29}$$

The indices x and y indicate on which qubits the Pauli operators act. Whereas it is now clear that if two graphs are equivalent under local complementation, then the corresponding graph states are equivalent under local unitaries, the converse is not true, despite being conjectured for some time [83, 145, 148]. Interestingly, it has been shown that every stabiliser state is equivalent under local complementation to some graph state [147].

1.4.2 Permutationally symmetric states

We now define *permutationally symmetric states* and present some of their properties. An n-partite state $\varrho \in \mathcal{S}(\mathcal{H}^{\otimes n})$ is said to be permutationally

symmetric for the pair $\{i,j\}$, with $i,j \in [n]$, if it is contained in the permutationally symmetric subspace of parties i and j. Mathematically speaking, it satisfies

$$\Pi_{ij}\varrho\Pi_{ij} = \varrho, \tag{1.30}$$

where $\Pi_{ij} = 1/2(\mathbb{1} + F_{ij})$ is the projector onto the symmetric subspace for the pair $\{i,j\}$, with F_{ij} being the swap operator that exchanges parties i and j. The swap operator is a unitary operators that is defined through the action

$$F_{ij}\left(|\psi_1\rangle \ldots |\psi_i\rangle \ldots |\psi_j\rangle \ldots |\psi_n\rangle\right) = |\psi_1\rangle \ldots |\psi_j\rangle \ldots |\psi_i\rangle \ldots |\psi_n\rangle\,, \tag{1.31}$$

for all product states $|\psi_1\rangle \ldots |\psi_i\rangle \ldots |\psi_j\rangle \ldots |\psi_n\rangle \in \mathcal{H}^{\otimes n}$. For two qubits, it reads $F_{12} = |00\rangle\langle 00| + |01\rangle\langle 10| + |10\rangle\langle 01| + |11\rangle\langle 11|$.

This definition naturally extends to any permutation π in the symmetric group on n symbols, denoted $\mathrm{Symm}(n)$. The operator F_π, $\pi \in \mathrm{Symm}(n)$ is defined through the action

$$F_\pi\left(|\psi_1\rangle \ldots |\psi_n\rangle\right) = \left|\psi_{\pi^{-1}(1)}\right\rangle \ldots \left|\psi_{\pi^{-1}(n)}\right\rangle, \tag{1.32}$$

for all product states $|\psi_1\rangle \ldots |\psi_n\rangle \in \mathcal{H}^{\otimes n}$ [152]. We define the projector onto the symmetric subspace and the (totally) permutationally symmetric states.

Definition 1.12 (Symmetric subspace)**.** The *projector onto the symmetric subspace* of $\mathcal{S}\left((\mathcal{H}^d)^{\otimes n}\right)$ is given by

$$\Pi^+ = \frac{1}{n!}\sum_{\pi\in\mathrm{Symm}(n)} F_\pi. \tag{1.33}$$

The dimension of the symmetric subspace is $\binom{d+n-1}{n}$ [152].

Definition 1.13 (Totally permutationally symmetric states)**.** A state $\varrho \in \mathcal{S}\left((\mathcal{H}^d)^{\otimes n}\right)$ is *(totally) permutationally symmetric* if is satisfies

$$\Pi^+\varrho\Pi^+ = \varrho. \tag{1.34}$$

Since the permutations $\{i, i+1\}$ for $i \in [n-1]$ generate the symmetric group [128], a state $\varrho \in \mathcal{S}(\mathcal{H}^{\otimes n})$ that satisfies $\Pi_{i,i+1}\varrho\Pi_{i,i+1} = \varrho$ for all $i \in [n-1]$ is totally permutationally symmetric.

When considering mixed states, we note that some states may be *exchangeable*, i.e., satisfy $F_{ij}\varrho F_{ij} = \varrho$ for a pair $\{i,j\}$, $i,j \in [n]$, but not permutationally symmetric for that same pair. The simplest example of a

state verifying this is the two-qubit maximally mixed state $\mathbb{1}/4$, which is exchangeable, but not permutationally symmetric.

Similarly, we define the projector onto the antisymmetric subspace as $\Pi^- = 1/n! \sum_{\pi \in \mathrm{Symm}(n)} \mathrm{sign}(\pi) F_\pi$. A state $\varrho \in \mathcal{S}\left((\mathcal{H}^d)^{\otimes n}\right)$ that fulfils $\Pi^- \varrho \Pi^-$ is called *(totally) permutationally antisymmetric*. We note that totally antisymmetric states only exist when the local dimension d is at least equal to the number of parties n, as the dimension of the antisymmetric subspace is $\binom{d}{n}$ [152]. Examples of totally symmetric and totally antisymmetry states are respectively

$$|S\rangle = \frac{1}{\sqrt{3}} \left(|001\rangle + |010\rangle + |100\rangle\right), \tag{1.35a}$$

$$|A\rangle = \frac{1}{\sqrt{6}} \left(|012\rangle + |120\rangle + |201\rangle - |021\rangle - |102\rangle - |210\rangle\right), \tag{1.35b}$$

where $|S\rangle \in (\mathcal{H}^2)^{\otimes 3}$ and $|A\rangle \in (\mathcal{H}^3)^{\otimes 3}$.

In what follows, we present three selected results concerning symmetric states that are exploited in Chapter 4.

Proposition 1.1 ([45], [A]). *Let $\varrho = \sum_{k=1}^{L} p_k |\psi_k\rangle\langle\psi_k|$ be in $\mathcal{S}(\mathcal{H})$, and let Π be a projector on a subspace of $\mathcal{H}$. The state ϱ satisfies $\Pi\varrho\Pi = \varrho$ if and only if $\Pi |\psi_k\rangle = |\psi_k\rangle$, $\forall k \in [L]$.*

Proof. Let us show that if $\Pi\varrho\Pi = \varrho$, then $\Pi |\psi_k\rangle = |\psi_k\rangle$, $\forall k \in [L]$, since the converse is trivial. From $\mathrm{tr}(\Pi\varrho\Pi) = 1$, it directly follows that $\langle\psi_k| \Pi |\psi_k\rangle = 1$, $\forall k \in [L]$. Since Π is a projector, we conclude that $\Pi |\psi_k\rangle = |\psi_k\rangle$, $\forall k \in [L]$. □

This holds in particular for the projectors onto the symmetric and antisymmetric subspaces.

Proposition 1.2 ([45], [A]). *Let ϱ be the state of an n-partite system, $n \geq 3$, and let A and B be two of its subsystems. If the marginal state on AB is permutationally symmetric (respectively antisymmetric) under the exchange of parties A and B, then the global state also is.*

Proof. Let $\varrho = \sum_{k=1}^{L} p_k |\psi_k\rangle\langle\psi_k|$ be the state of a tripartite system ABC. By considering the Schmidt decompositions $|\psi_k\rangle = \sum_{i=1}^{r_k} \varsigma_{k,i} \left|\phi_{k,i}^{(AB)}\right\rangle \left|\chi_{k,i}^{(C)}\right\rangle$ with respect to the bipartition $AB \mid C$ for all $k \in [L]$, we obtain

$$\varrho = \sum_{k=1}^{L} p_k \sum_{i,j=1}^{r_k} \varsigma_{k,i} \varsigma_{k,j}^* \left|\phi_{k,i}^{(AB)}\right\rangle\!\left\langle\phi_{k,j}^{(AB)}\right| \otimes \left|\chi_{k,i}^{(C)}\right\rangle\!\left\langle\chi_{k,j}^{(C)}\right|. \tag{1.36}$$

From that, $\varrho^{(AB)} = \sum_{k=1}^{L} p_k \sum_{i=1}^{r_k} |s_{k,i}|^2 \left|\phi_{k,i}^{(AB)}\right\rangle \left\langle\phi_{k,i}^{(AB)}\right|$. So, if $\varrho^{(AB)}$ is permutationally symmetric (respectively antisymmetric), then from Proposition 1.1 all states in its decomposition also are. Clearly, if the states $\left|\phi_{k,i}^{(AB)}\right\rangle$, $i \in [r_k], k \in [L]$, are permutationally symmetric (respectively antisymmetric), then ϱ also is. □

We note that for this proposition, the converse is trivial.

Proposition 1.3 (Entanglement in symmetric states [A]). *1. All permutationally symmetric multipartite states are either* GME *or fully separable.*

2. All permutationally antisymmetric multipartite states are GME.

Proof. Due to Proposition 1.1, we only need to consider pure states. Let $|\Psi\rangle$ be an n-partite (anti)symmetric state that is separable across a certain bipartition. Without loss of generality, we assume that there exist $t \in [n]$ such that

$$|\Psi\rangle = |\varphi_{1,\ldots,t}\rangle \otimes |\phi_{t+1,\ldots,n}\rangle . \tag{1.37}$$

When tracing out the first t parties, the resulting marginal state is pure. The symmetry of $|\Psi\rangle$ thus implies that the marginal state is pure after tracing out any t parties. This can only be true if $|\Psi\rangle$ is fully separable.

Now, let $|\Psi\rangle$ be a permutationally antisymmetric product state, i.e., $|\Psi\rangle = \bigotimes_{i=1}^{n} |\psi_i\rangle$. Then, we have $|\psi_1\rangle |\psi_2\rangle \bigotimes_{i=3}^{n} |\psi_i\rangle = -|\psi_2\rangle |\psi_1\rangle \bigotimes_{i=3}^{n} |\psi_i\rangle$. It implies that $-1 = \langle\psi_1\psi_2 \prod_{i=3}^{n} \psi_i | \psi_2\psi_1 \prod_{i=3}^{n} \psi_i\rangle = |\langle\psi_1|\psi_2\rangle|^2 \geq 0$, hence we arrive at a contradiction. □

1.5 Quantum state tomography

The practical implementation of most quantum information processing protocols relies on the generation and manipulation of quantum systems, mathematically represented by quantum states. Thus, it is crucial to accurately determine the quantum state that best describes a source of physical quantum systems. When a full characterisation of the quantum state is required, a *quantum state tomography* protocol must be performed.

Quantum state tomography refers to a collection of techniques for estimating the quantum state prepared by a source (see for instance [140]). Generally, measurements are repeatedly performed on identical copies of the quantum systems prepared by the source. From the collected experimental data, a *state estimate* $\hat{\varrho}$ is constructed. Since the density operator of

a d-dimensional quantum system is composed of $d^2 - 1$ real parameters, the set of measurements is called *tomographically complete* if it allows for the estimation of these $d^2 - 1$ parameters.

A major challenge with quantum state tomography is that, for increasing dimension, it requires an exponentially increasing number of state preparations with respect to the number of qudits. To address to this, it can be valuable to incorporate constraints on the state, such as purity or symmetry [17, 39, 59, 109, 132]. Additionally, the technique known as *shadow tomography* [1, 78] offers an alternative approach when one only needs to estimate expectation values of local observables, thereby potentially reducing the complexity of the tomographic process.

Once the measurement data is acquired, it needs to be processed to obtain an estimate of the state. Various methods exist to reconstruct a density operator from measurement data. We present in the section how to obtain an estimate through linear inversion, though methods based on cost functions are also widespread in the literature [140].

It is convenient to describe the tomographic experiment by a single POVM $\{E_i\}_{i=1}^L$ performed on N independent copies of the state, resulting in a list of measurement outcomes $\{N_i\}_{i=1}^L$ such that $\sum_{i=1}^L N_i = N$. A vector $\mathbf{f}$ of frequencies is constructed with entries $f_i = {}^{N_i}/_N$ for all $i \in [L]$. For every POVM $\{E_i\}_{i=1}^L$, there exists a measurement map M that, once applied on a density operator ϱ, yields a vector of probabilities for each outcome $i \in [L]$ of the POVM. Formally, M is defined through

$$M : \mathbb{C}^{d\times d} \to \mathbb{R}^L : \varrho \mapsto M\varrho = \mathbf{p}, \tag{1.38}$$

where the ith entry of $\mathbf{p}$ is given by the probability of obtaining the measurement outcome i when measuring the POVM on ϱ, i.e., $\mathrm{tr}(E_i\varrho)$. If the measurement performed is tomographically complete, from the probabilities it is possible to obtain the corresponding state ϱ through $M^+\mathbf{p} = \varrho$, where M^+ is any left inverse of M, i.e., such that $M^+M\varrho = \varrho$ holds for all $\varrho \in \mathcal{S}(\mathcal{H}^d)$. Given a vector of frequencies $\mathbf{f}$ obtained from measurement data, we straightforwardly obtain an estimate for the state of the system,

$$\hat{\varrho} = M^+\mathbf{f}. \tag{1.39}$$

Since quantum mechanics is an inherently probabilistic theory, the state ϱ cannot be exactly reconstructed from finite data. It is thus important to give a guarantee of precision together with the estimate $\hat{\varrho}$, which in

the case of frequentist statistics is called *confidence regions*. A confidence region for state tomography is a region in the space of Hermitian operators, centred on $\hat{\varrho}$, that contains the state ϱ with a certain level of confidence [140]. For concreteness, let us consider the norm-based confidence region C_A developed in [41]. Therein, the authors show that with N samples of the state ϱ, the estimate $\hat{\varrho}$ satisfies

$$\Pr[\|\hat{\varrho} - \varrho\| < \varepsilon\sigma] \geq 1 - \delta, \tag{1.40}$$

where $1 - \delta \in [0, 1]$ is the confidence level which can be evaluated through $\varepsilon = 3\sqrt{u}(\sqrt{u} + \sqrt{u+1})$, with $u = {}^{2}/_{9N} \log(8/\delta)$, and where the norm is the Hilbert-Schmidt norm. The parameter σ is related to the variance in the measurements. When a vectorisation of ϱ is considered in Eq. (1.38), the measurement map can be represented by a $L \times d^2$ matrix, and in that case σ reads

$$\sigma = \max_{k \in [d^2]} \left\| M_k^+ \right\|, \tag{1.41}$$

where M_k^+ is the kth column vector of M^+ [41]. The resulting confidence region is a sphere of radius $\varepsilon\sigma$ centred in $\hat{\varrho} = M^+\mathbf{f}$ in the space of Hermitian operators,

$$C_A(\varepsilon, \mathbf{f}) = \left\{ \varrho \mid \left\| M^+\mathbf{f} - \varrho \right\| \leq \varepsilon\sigma \right\}. \tag{1.42}$$

The advantages of this confidence region are multiple. It is easy to describe and compute, and performs well when compared to other regions from the literature [41]. Furthermore, C_A depends on the measurement scheme considered, which makes it a good candidate to quantify the quality of a given measurement scheme. Indeed, the parameter σ in Eq. (1.40) only depends on the measurement map and is related to the variance of the measurement results. Clearly, a large σ would lead to a larger confidence region and σ can thus be used as a figure of merit for a particular measurement scheme. This line of thought is relevant for Chapter 3.

1.6 Mathematical toolbox

In this section, we present some key mathematical concepts that are useful throughout the thesis. We first discuss mathematical optimisation, then introduce basic notions in graph theory. These concepts are required for the proper understanding of Chapters 2 and 3.

1.6.1 Mathematical optimisation

In physics, we are often confronted to problems that can be expressed as finding a vector of parameters $\mathbf{x} \in \mathbb{R}^n$ that maximises an *objective function* $f : \mathbb{R}^n \to \mathbb{R}$ under constraints of the type $f_i(x) \leq b_i$, where $f_i : \mathbb{R}^n \to \mathbb{R}$ and $b_i \in \mathbb{R}$, with $i \in [m]$. Such a problem is called an *optimisation problem*, and the set of $\mathbf{x} \in \mathbb{R}^n$ that satisfy the constraints is called the *feasible region*. If the feasible region is empty, the problem is called *unfeasible*. While solving optimisation problems is in general quite hard, there are classes of problems that can be (efficiently) solved to global optimality. We introduce here three types of optimisation problems, namely *linear programming*, *semidefinite programming* (SDP), and *integer programming*.

Linear programming

When the objective function as well as the constraints are linear functions, the optimisation problem can be formulated as, given $A \in \mathbb{R}^{m \times n}$ and $\mathbf{b} \in \mathbb{R}^m$, solve

$$\max_{\mathbf{x} \in \mathbb{R}^n} \mathbf{c}^T \mathbf{x} \tag{1.43a}$$

$$\text{such that } A\mathbf{x} \leq \mathbf{b}, \tag{1.43b}$$

$$\mathbf{x} \geq 0, \tag{1.43c}$$

where the inequalities are to be understood as component-wise. Since all constraints are linear, the feasible region is a convex polytope in $\mathbb{R}^n$. The fundamental theorem of linear programming states that every feasible, bounded linear program has an optimal solution on a vertex of the feasible region. If two or more vertices lead to the optimal solution, any point lying on a face connecting them is also an optimal solution.

Semidefinite programming

Semidefinite programming is a class of programs that generalises linear programing. It is a type of optimisation where the objective function is linear and the constraints are matrix semidefinite positivity. As states and measurements are represented by PSD operators, SDP is one of the most widely used types of mathematical programming in quantum information (for a detailed presentation with a focus on quantum information theory, we refer to [135]). To name a few, SDPs have found applications to fundamental

problems such as quantum state discrimination [10], quantum steering [29], and causality hierarchies for network entanglement [97, 161]. Semidefinite programming is particularly relevant as SDPs can be efficiently solved to a global extremum [152]. Formally, given $\mathbf{c} \in \mathbb{C}^n$ and $F_0, \ldots, F_n \in \mathbb{C}^{m\times m}$, the standard form of an SDP reads

$$\max_{\mathbf{x}\in\mathbb{C}^n} \mathbf{c}^\dagger \mathbf{x} \tag{1.44a}$$

$$\text{such that } F_0 + \sum_{i=1}^{n} x_i F_i \succeq 0. \tag{1.44b}$$

Let us introduce an illustrative example. Consider an unknown two-qubit state $\varrho \in \mathcal{S}(\mathcal{H}^4)$ for which the expectation values $\mathrm{tr}(XX\varrho) = a$ and $\mathrm{tr}(ZZ\varrho) = b$ are known. We are interested in finding a lower bound on the fidelity of ϱ to the pure state $|\Phi^+\rangle \in \mathcal{H}^4$. This can be obtained by solving

$$\min_{\varrho\in\mathbb{C}^{4\times4}} \langle\Phi^+|\varrho|\Phi^+\rangle \tag{1.45a}$$

$$\begin{aligned} \text{such that} \quad & \varrho \succeq 0, && \text{(1.45b)}\\ & \mathrm{tr}(\varrho) = 1, && \text{(1.45c)}\\ & \mathrm{tr}(XX\varrho) = a, && \text{(1.45d)}\\ & \mathrm{tr}(ZZ\varrho) = b. && \text{(1.45e)} \end{aligned}$$

Although a bit tedious, this program can be written in the standard form of Eq. (1.44). We first define $\mathbf{x} = \mathbf{v}(\varrho)$ and $\mathbf{c} = -\mathbf{v}(|\Phi^+\rangle\langle\Phi^+|)$, where $\mathbf{v} : \mathbb{C}^{4\times4} \to \mathbb{C}^{16}$ is a vectorisation function. In order to enforce Eq. (1.45b), we define $F_0 = 0$ and $F_i = \mathbf{v}^{-1}(\mathbf{e}_i)$, where $\mathbf{e}_i$ is the ith element from the 16-dimensional standard basis, with $i \in [16]$. Equation (1.45b) is thus equivalent to $F_0 + \sum_{i=1}^{16} x_i F_i \succeq 0$. Further, Eq. (1.45c) is satisfied when both $\mathbb{1} - \sum_{i=1,5,9,13} x_i \mathbb{1} \succeq 0$ and $-\mathbb{1} + \sum_{i=1,5,9,13} x_i \mathbb{1} \succeq 0$ are satisfied. The remaining constraints can be converted analogously, and using direct sums, all those constraints can be integrated in a in a single matrix inequality of the type of Eq. (1.44b) with $m = 28$.

Thankfully, many modelling languages tailored to mathematical optimisation, such as JuMP for Julia, enable the user to write their program directly in the algebraic form such as in Eq. (1.45). The algebraic modelling language then translates the program to a standard form that is supported by the solver.

Integer programming

Integer programs aim to find an extremum of a linear function where, as the name indicates, the variables are restricted to integer numbers. In their standard form, integer programs read

$$\max_{\mathbf{x}\in\mathbb{Z}^n} \mathbf{c}^T\mathbf{x} \tag{1.46a}$$

$$\text{such that } A\mathbf{x} \leq \mathbf{b}, \tag{1.46b}$$

$$\mathbf{x} \geq 0, \tag{1.46c}$$

given $\mathbf{c} \in \mathbb{R}^n$, $\mathbf{b} \in \mathbb{R}^m$, and $A \in \mathbb{R}^{m\times n}$. Similarly to SDPs, modelling languages are used to avoid writing integer programs in the standard form. We note that if for some $i \in [n]$, the variables x_i are not in $\mathbb{Z}$, the optimisation is called *mixed integer programming* (MIP).

Integer programs are generally solved using *branch and bound* algorithms. In a nutshell, branch and bound algorithms work as follows. The program is first relaxed to a version where the variables are real numbers, i.e., the integrality restrictions are dropped. The resulting relaxation is thus a linear program, which we name P_0 and solve. Unless the optimal solution happens to be in $\mathbb{Z}^n$ (which would solve the original program), one of the variables whose optimal value in P_0 is not an integer is chosen as the branching variable. For the sake of clarity, let us consider an example. Say we aim to solve

$$\max_{\mathbf{x}\in\mathbb{Z}^2} x_1 + 2x_2 \tag{1.47a}$$

$$\text{such that} \quad x_1 + 15x_2 \leq 150, \tag{1.47b}$$

$$8x_1 + 5x_2 \leq 160, \tag{1.47c}$$

$$\mathbf{x} \geq 0. \tag{1.47d}$$

The feasible region is shown in Figure 1.5. Solving the relaxation gives a maximum of 32.4 at $\mathbf{x} = (14.3, 9.04)^T$. This directly yields an upper bound on the solution. We now chose the variable x_1 to branch over, and solve two linear programs: P_1 with the additional constraint that $x_1 \leq 14$ and P_2 with $x_1 \geq 15$. The former branch yields 32.1 at $\mathbf{x} = (14, 9.07)^T$, and the latter 31 at $\mathbf{x} = (15, 8)^T$. As the solution of P_2 is integer, we stop the branching there. Indeed, it is a feasible solution to Eq. (1.47), and is used as a lower bound on the optimal solution. On the other hand, we branch over P_1 by solving two

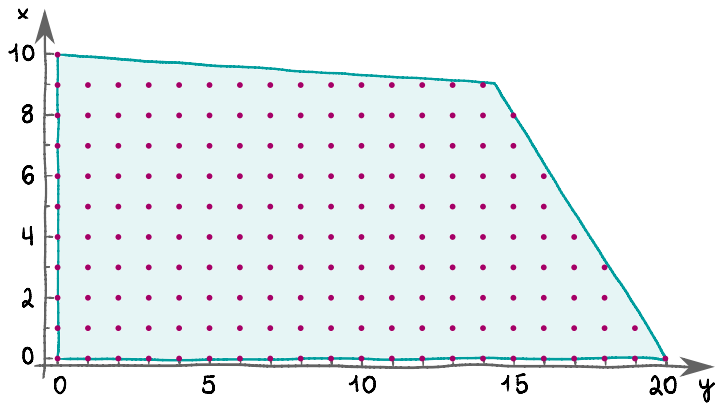

Figure 1.5: *Feasible region.* Purple: Discrete feasible region of in integer program described in Eq. (1.47) (179 points). Green: Feasible region of its relaxation to a linear program.

further linear programs, P_{11} and P_{12}, for which in addition to the constraints of P_1, we incorporate $x_2 \leq 9$ and $x_2 \geq 10$ respectively. The program P_{11} has a maximal value of 32 at $\mathbf{x} = (14, 9)^T$, and P_{12} of 20 at $\mathbf{x} = (0, 10)^T$. As all the different branches give integer solutions, we conclude that the solution to the integer program of Eq. (1.47) is 32, and is achieved by $\mathbf{x} = (14, 9)^T$.

Although in this example all branches are terminated by an integer solution, this is not necessary the case. Indeed, it also can happen that branches turn out to be unfeasible, or that the solution to a relaxation is smaller than the best feasible solution so far. The branches are then also terminated. We note that in the worst case, the branch and bound method has to go through all elements of the feasible region, so, they cannot be solved efficiently in general.

In addition to branch and bound algorithms, commercial solvers (such as Gurobi) implement all sorts of symmetry removal and heuristic algorithms to reduce the size of the problems. For a deeper introduction to the topic, see for instance [117].

1.6.2 Graph theory

As the name suggests, graph theory is a field in discrete mathematics that studies mathematical objects called *graphs*. Graphs can be used to represent relations between objects, and, due to this property, are of significant importance in Chapters 2 and 3 of this thesis. Formally, a graph G is an ordered pair (V, E), where V is the set of *vertices* and E the set of *edges*. Each

edge in E is a pair of vertices of V, that is, $E \subseteq \{\{i,j\} \in V^2 \mid i \neq j\}$, where $V^2 = \{\{i,j\} \mid i,j \in V\}$. The number of vertices in a graph is called its order and is equal to $|V|$. Useful is also the *graph complement* $\bar{G}$ of $G = (V,E)$, which has the same vertex set V, and an edge is in the edge set of $\bar{G}$ if and only if it is not in E. As an example, we introduce the n-vertex *complete graph* K_n, where any pair of vertices are connected by an edge. Its complement $\bar{K}_n$ is the n-vertex empty graph.

Except when explicitly mentioned, we consider that the vertex set of a graph of order n is $V = [n]$. By abuse of notation, we sometimes refer to the vertex i of V as $i \in G$, and to the edge $\{i,j\}$ of E as $\{i,j\} \in G$, with $i,j \in [n]$. We note that we only consider *undirected* graphs, i.e., graphs where the edges are unordered pairs of vertices.

Graph theory problems have long been studied and found numerous applications in everyday life. We present here few hand-picked results that play a role later in this thesis. Let us start with a few definitions, taken from [43].

Definition 1.14 (Neighbourhood)**.** The *neighbourhood* $\mathcal{N}_i$ of a vertex $i \in V$ from a graph $G = (V,E)$ is the set of vertices that are connected to i, i.e., $\mathcal{N}_i = \{j \in V \mid \{i,j\} \in E\}$. The cardinality of the neighbourhood $d_i = |\mathcal{N}_i|$ is called the *degree* of the vertex $i \in V$.

Definition 1.15 (Subgraph)**.** A graph $G' = (V',E')$ is a *subgraph* of $G = (V,E)$ if $V' \subseteq V$ and $E' \subseteq E$. The graph G' is an *induced subgraph* of G if $V' \subseteq V$ and $E' = \{\{i,j\} \in E \mid i,j \in V'\}$.

Definition 1.16 (Clique)**.** A *clique* of a graph $G = (V,E)$ is an induced subgraph of G in which every pair of vertices is connected by an edge. A *maximal clique* of G is a clique that is not part of a larger clique. The *clique number* $\omega(G)$ of G is the maximal order of its maximal cliques, i.e., the largest integer r such that K_r is an induced subgraph of G.

Following this, we introduce the *vertex colouring problem*, which we need to define the *chromatic number* of a graph.

Problem 1.2 (Vertex colouring problem)**.** *Given a graph G, find a way of colouring each vertex of G such that no adjacent vertices share the same colour, with the smallest number of colours.*

Definition 1.17 (Chromatic number)**.** The *chromatic number* $\chi(G)$ of a graph G is the number of colours needed to solve the vertex colouring problem.

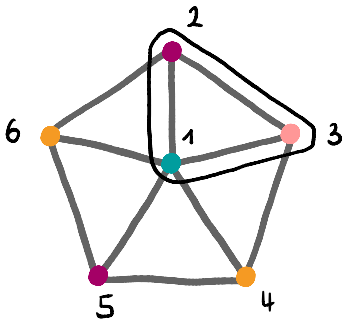

Figure 1.6: *Wheel graph* G_W. Its maximal cliques are triangles, leading to $\omega(G_W) = 3$, and its chromatic number is four, i.e., $\chi(G_W) = 4$.

It is trivial to see the chromatic number of a graph G cannot be less than its clique number. Indeed, colouring the vertices of a maximal clique of G already requires $\omega(G)$ colours, as all the vertices are connected. By considering the most trivial connected graph composed of two connected vertices, we can directly see that some graph achieve $\omega(G) = \chi(G)$. Now, the question arises as to whether $\chi(G)$ can be strictly larger than $\omega(G)$. To see that this question is answered positively, we consider the wheel graph G_W depicted in Figure 1.6. Maximal cliques are of order three, however, it is impossible to colour G_W with only three colours, at least four are needed. Therefore we conclude that $\omega(G) \leq \chi(G)$, and introduce the following definition.

Definition 1.18 (Perfect graph)**.** A *perfect graph* is a graph G for which the clique and chromatic numbers of all its induced subgraphs (including itself) are equal. When $\omega(G) = \chi(G)$ holds, but not necessarily for all induced subgraphs, G is called *weakly perfect*.

The long-conjectured strong perfect graph theorem states that a graph is perfect if and only if it neither has odd-length induced cycles of length at least five nor complements thereof [31]. Thus, the smallest imperfect graph is the five-vertex odd cycle, the pentagon. Both problems of finding whether a clique of a given size exists in a graph G and if G is colourable with a given number of colours are widely studied and known to be NP-complete [84].

Nevertheless, those two quantities can be estimated efficiently through the *Lovász number* of the complement graph. The Lovász number of a graph was first introduced to upper bound the Shannon capacity of a graph [100] and has multiple equivalent definitions [92]. We present here two that are relevant for Chapter 2, yet not the most common.

Definition 1.19 (Lovász number [92])**.** The *Lovász number* of a graph $G = ([n], E)$ is defined as

$$\vartheta(G) = \max_{B \in \mathbb{R}^{n \times n}} \Lambda(B) \tag{1.48a}$$

$$\text{such that} \quad B \succeq 0, \tag{1.48b}$$

$$B_{ii} = 1 \quad \forall i \in [n], \tag{1.48c}$$

$$B_{ij} = 0 \quad \forall \{i, j\} \in E, \tag{1.48d}$$

where $\Lambda(\cdot)$ stands for the largest eigenvalue.

A weighted version of the Lovász number for non-negative weights $\mathbf{w} = (w_1, \ldots, w_n)$ can be defined by setting B_{ii} of Eq. (1.48c) equal to w_i for all $i \in [n]$. Notably, the Lovász number can be formulated as an SPD [92],

$$\vartheta(G) = \max_{C \in \mathbb{R}^{n \times n}} \sum_{i,j=1}^{n} C_{ij} \tag{1.49a}$$

$$\text{such that} \quad C \succeq 0, \tag{1.49b}$$

$$\operatorname{tr}(C) = 1, \tag{1.49c}$$

$$C_{ij} = 0 \quad \forall \{i, j\} \in E. \tag{1.49d}$$

Proof. Let B fulfil Eqs. (1.48b-1.48d). There exists a set of n-dimensional real vectors $\{\mathbf{v}^{(i)} \mid ||\mathbf{v}^{(i)}|| = 1\}_{i=1}^{n}$ such that $B_{ij} = (\mathbf{v}^{(i)})^T \mathbf{v}^{(j)}$. The largest eigenvalue of B can be written as $\max_{\mathbf{x} \in \mathbb{R}^n, \|\mathbf{x}\|=1} \mathbf{x}^T B \mathbf{x}$, and by identifying C_{ij} with $(x_i \mathbf{v}^{(i)})^T (x_j \mathbf{v}^{(j)})$ for all $i, j \in [n]$, we recover Eq. (1.49). □

The Lovász number relates to the clique and chromatic numbers through the *sandwich theorem*, which states that for any graph G, the following inequality holds [92]

$$\omega(G) \leq \vartheta(\bar{G}) \leq \chi(G). \tag{1.50}$$

Naturally, equality holds for perfect graphs.

We finally present another well-studied graph theoretic problem, namely the *edge clique cover problem*.

Problem 1.3 (Edge clique cover problem)**.** *Given two graphs G_1 and G_2, find a set of cliques of G_2 that is minimal with respect to the number of elements such that every edge of G_1 appears in a least one clique of the set.*

We note that this problem is not feasible if the edge set of G_1 is not included in the edge set of G_2. From it follows the *edge clique cover number*.

Definition 1.20 (Edge clique cover number)**.** Given two graphs, the *edge clique cover number* is the cardinality of the set of cliques that solves their edge clique cover problem.

We note that this problem is usually considered for $G_1 = G_2$, and as an example, we consider again the wheel graph of Figure 1.6. Its edge clique cover number is equal to five, as all the triangles are needed to cover all its edges. Note that in this example, all cliques used for the covering are maximal. This is not the case in general.

Chapter 2

Uncertainty relations

Uncertainty relations are a fundamental topic in quantum information theory. As outlined in Section 1.2, deriving meaningful variance-based uncertainty relations (URs) is challenging, especially given that variances are zero when evaluated on eigenstates of the observables. The problem is closely related to the behaviour of the set of observables' expectation values on a given state, known as the *numerical range* of the observables [138]. For instance, the UR presented in Eq. (1.7) expresses a lower bound on the sum of the variances of the Pauli operators X, Y, and Z that directly translates to a bound on the sum of the expectation values for any state $\varrho \in \mathcal{S}(\mathcal{H})$,

$$\langle X\rangle_\varrho^2 + \langle Y\rangle_\varrho^2 + \langle Z\rangle_\varrho^2 \leq 1. \tag{2.1}$$

This relation is not only of fundamental interest but also finds applications in entanglement characterisation [74] and quantum cryptography [122]. Additionally, we explore its application to network entanglement criteria in Chapter 4. Consequently, this chapter addresses the generalisation of Eq. (2.1) to arbitrary sets of observables $\{A_i\}_{i=1}^L$, i.e., aims to bound the expression $\mathbb{E} = \sum_{i=1}^L \langle A_i\rangle_\varrho^2$.

This chapter is structured as follows. In Section 2.1, we derive a non-trivial upper bound on $\mathbb{E}$ for any set of observables by linking this problem to graph theory. This result gives rise to URs for dichotomic observables that (i) are state-independent, (ii) provide a lower bound for the sum of variances, and (iii) apply to more than two observables. We further analyse the case of observables that either commute or anticommute, such as multi-qubit Pauli observables. We also discuss the behaviour of the bound on $\mathbb{E}$ when the observables have a degree of imprecision, for instance due to their

experimental implementation. In Section 2.2, the bound on $\mathbb{E}$ is used to detect and quantify entanglement through the derivation of entanglement and Schmidt number witnesses. Most of the results are published in [B] and we closely follow the presentation of this publication.

2.1 Multi-observable uncertainty relations

We begin by reformulating the UR as an expectation value problem and prove our main result, which provides a bound on the sum of the squares of the expectation values of observables, based on their anticommutativity relations. We go on with discussing the tightness of our bound, particularly in the case of observables that either commute or anticommute. We later extend these results to observables for which the anticommutator is not exactly zero.

2.1.1 Reformulation

Given a set of dichotomic observables $\{A_i\}_{i=1}^{L}$, we aim to compute a lower bound on the sum of their variances, that is, find a positive constant $c \in \mathbb{R}$ such that

$$\sum_{i=1}^{L} \Delta_{\varrho}^2(A_i) \geq c \quad \forall \varrho \in \mathcal{S}(\mathcal{H}). \tag{2.2}$$

The constant c only depends on the observables, and not on ϱ, such that Eq. (2.2) is a state-independent UR. Without loss of generality, we consider that the spectrum of each observable is $\{+1, -1\}$. They thus square to the identity and we can write Eq. (2.2) as $L - \sum_{i=1}^{L} \langle A_i \rangle_{\varrho}^2 \geq c$. Finding a lower bound for Eq. (2.2) is equivalent to finding an upper bound on

$$\mathbb{E} = \sum_{i=1}^{L} \langle A_i \rangle_{\varrho}^2 \tag{2.3}$$

that holds for any state ϱ.

Naturally, such a question has been considered before, and answers for particular cases are known. First, when $\{A_i\}_{i=1}^{d^2}$ contains operators that span the space of Hermitian operators acting on $\mathcal{H}^d$ and that satisfy $\mathrm{tr}\{A_i A_j\} = d\delta_{ij}$ for all $i, j \in [d^2]$, then $\mathbb{E} \leq d$. This follows from the positivity of the density operator and can be interpreted as an upper bound on the length of its generalised Bloch vector [28, 89]. Second, when all observables pairwise commute (i.e., $[A_i, A_j] = A_i A_j - A_j A_i = 0$ for all $i, j \in [L]$) they share

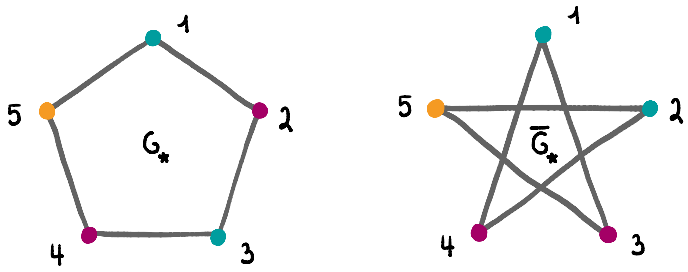

Figure 2.1: *Pentagon graph $G_\star$ and its complement $\bar{G}_\star$.* The vertices are coloured with the minimal number of colours such that no adjacent vertices share the same colour. Both graphs have a chromatic numbers equal to three, $\chi(G_\star) = \chi(\bar{G}_\star) = 3$. Note that these graphs are isomorphic (self-complementary), which is not the case in general. Figure adapted from [B].

eigenvectors and the trivial bound $\mathbb{E} \leq L$ is tight[1]. On the other hand, if all observables pairwise anticommute ($\{A_i, A_j\} = A_iA_j + A_jA_i = 0$ for all $i \neq j, i, j \in [L]$), then $\mathbb{E} \leq 1$ [144, 153]. This inequality led to the derivation of entropic URs for multiple observables [113, 153], Bell monogamy inequalities [95] and is used in Chapter 4 for quantum network state compatibility criteria, among others. If we consider a set of observables $\{A_i\}_{i=1}^L$ where only some pairs anticommute, an upper bound on $\mathbb{E}$ can be obtained by combining those facts, i.e., by partitioning the observables in subsets where all anticommute and counting the number of subsets.

This can conveniently be formulated using graphs. To any set $\{A_i\}_{i=1}^L$, we associate a graph G in the following fashion: L vertices represent the L observables, and the vertices i and j are connected when $\{A_i, A_j\} \neq 0$, with $i, j \in [L]$. As an example, consider a set of five three-qubit observables, $O_\star = \{X\mathbb{1}\mathbb{1}, \mathbb{1}X\mathbb{1}, Z\mathbb{1}X, ZZ\mathbb{1}, \mathbb{1}ZZ\}$. Its graph $G_\star$ is the five-vertex cycle graph depicted in Figure 2.1, i.e., the pentagon graph. We want to partition the observables (the vertices) in the smallest number of subsets where they all anticommute (where none are connected). As it turns out, this is exactly the vertex colouring problem (see Problem 1.2 and related definitions). Indeed, a vertex colouring of G guarantees that observables associated to vertices of the same colour all pairwise anticommute, therefore the sum of the square of their expectation values is upper bounded by one. This enables us to write

$$\sum_{i=1}^{L} \langle A_i \rangle_\varrho^2 \leq \chi(G) \quad \forall \varrho \in \mathcal{S}(\mathcal{H}), \tag{2.4}$$

[1] An inequality (or bound) $f(x) \leq c$, with $x \in A$ and $c \in B$, on a function $f : A \to B$ is said to be tight if there exists a $y \in A$ such that $f(y) = c$.

where $\chi(G)$ is the chromatic number of G. This fact has for instance been used in the context of Bell monogamy relations [95], albeit not formulated in a graph theoretical language. In the case of the pentagon observables of $O_\star$, the graph $G_\star$ has a chromatic number of three (see Figure 2.1), and we obtain $\mathbb{E} \leq 3$ for all $\varrho \in \mathcal{S}(\mathcal{H})$. The obvious question that follows is whether such a bound is tight, i.e., whether there exists a state ϱ for which equality holds.

This question is answered in the negative by the following proposition, where we introduce the *anticommutativity graph* $\bar{G}$ of a set of observables $\{A_i\}_{i=1}^L$. It is defined as the L-vertex graph whose edges connect i and j if A_i and A_j anticommute, $i, j \in [L]$, i.e., the complement of the graph G introduced previously.

Proposition 2.1 (Lovász number bound [B])**.** *Consider a set of observables $\{A_i\}_{i=1}^L$ where each element squares to the identity. The sum of their variances is lower bounded by the number of observables minus the Lovász number of their anticommutativity graph, i.e,*

$$\sum_{i=1}^{L} \Delta_\varrho^2(A_i) \geq L - \vartheta(\bar{G}) \quad \forall \varrho \in \mathcal{S}(\mathcal{H}). \tag{2.5}$$

Equivalently,

$$\sum_{i=1}^{L} \langle A_i \rangle_\varrho^2 \leq \vartheta(\bar{G}) \quad \forall \varrho \in \mathcal{S}(\mathcal{H}). \tag{2.6}$$

Proof. Consider a state $\varrho \in \mathcal{S}(\mathcal{H})$ and define $a_i = \langle A_i \rangle_\varrho$ for all $i \in [L]$ and $E_\varrho = \sum_{i=1}^L a_i A_i$. The variance of this operator on the same state ϱ is non-negative, hence $\langle E_\varrho^2 \rangle_\varrho \geq \langle E_\varrho \rangle_\varrho^2$. Here and in the following proofs, we omit the subscript ϱ on the expectation values for the sake of readability. The left hand side of this inequality can be expressed as

$$\sum_{i,j=1}^{L} a_i a_j \langle A_i A_j \rangle = \sum_{i,j=1}^{L} a_i a_j \Re(\langle A_i A_j \rangle), \tag{2.7}$$

where we used the fact that $\langle A_i A_j \rangle = \langle A_j A_i \rangle^*$. Using $\langle E_\varrho \rangle^2 = \|\mathbf{a}\|^2 \sum_{i=1}^L \langle A_i \rangle^2$, we obtain

$$\sum_{i=1}^{L} \langle A_i \rangle^2 \leq \frac{1}{\|\mathbf{a}\|^2} \sum_{i,j=1}^{L} a_i a_j \Re(\langle A_i A_j \rangle), \tag{2.8}$$

for $\mathbf{a} \neq 0$ (when this is not satisfied, $\mathbb{E} = 0$). The right hand side of Eq. (2.8) is upper bounded by $\Lambda(\mathcal{A})$, the largest eigenvalue of the $L \times L$ real matrix

with entries $\mathcal{A}_{ij} = \Re(\langle A_i A_j \rangle)$, $i, j \in [L]$. Clearly, the diagonal entries of $\mathcal{A}$ are equal to one. By noticing that $\langle A_i A_j \rangle$ is an imaginary number when $\{A_i, A_j\} = 0$, $i, j \in [L]$, we can finally write

$$\sum_{i=1}^{L} \langle A_i \rangle^2 \leq \max_{\mathcal{A} \in \mathbb{R}^{L \times L}} \Lambda(\mathcal{A}) \tag{2.9a}$$

$$\text{such that} \quad \mathcal{A} \succeq 0, \tag{2.9b}$$

$$\mathcal{A}_{ii} = 1 \quad \forall i \in [L], \tag{2.9c}$$

$$\mathcal{A}_{ij} = 0 \quad \forall \{i, j\} \in [L]^2 : \{A_i, A_j\} = 0, \tag{2.9d}$$

with $[L]^2 = \{\{i, j\} \mid i, j \in [L]\}$. The edge set of the L-vertex anticommutativity graph $\bar{G}$ of $\{A_i\}_{i=1}^{L}$ is exactly $\{\{i, j\} \mid \{A_i, A_j\} = 0, i, j \in [L]\}$, therefore Eq. (2.9) recovers Definition 1.19 of the Lovász number of $\bar{G}$. This proves the claim. □

From the sandwich theorem (see Eq. (1.50)), we know that $\vartheta(\bar{G}) \leq \chi(G)$, and that there are graphs for which the inequality is strict. Such graphs are for instance the anticommutativity graph $\bar{G}_\star$ of $O_\star$ and its complement $G_\star$, both presented in Figure 2.1. Indeed, $\vartheta(\bar{G}_\star) = \sqrt{5}$ and from Proposition 2.1 it follows that $\sum_{A \in O_\star} \langle A \rangle_\varrho^2 \leq \sqrt{5} \simeq 2.2361$, which is an improvement over the previously-known bound of Eq. (2.4), $\chi(G_\star) = 3$. Notably, this is also better than maximising $\mathbb{E}$ under the anticommutation relations given by $\bar{G}_\star$, i.e.,

$$\alpha(\bar{G}_\star) = \max_{(a_1, \ldots, a_5)^T \in \mathbb{R}^5} \sum_{i=1}^{5} a_i^2 \tag{2.10a}$$

$$\text{such that} \quad -1 \leq a_i \leq 1 \quad \forall i \in [5], \tag{2.10b}$$

$$a_i^2 + a_j^2 \leq 1 \quad \forall \{i, j\} \in \bar{G}_\star, \tag{2.10c}$$

where by $\{i, j\} \in \bar{G}_\star$, we mean that $\{i, j\}$ is an edge of $\bar{G}_\star$. Using a computer algebra system, Eq. (2.10) evaluates to $\alpha(\bar{G}_\star) = 5/2$.

When all the observables anticommute, the graph $\bar{G}$ is complete and since the Lovász number of complete graphs is one, we recover the previously known result. On the other hand, when none of the L observables anticommutes, $\bar{G}$ is empty and $\vartheta(\bar{G}) = L$. This recovers for instance the result that pairwise commuting observables share eigenvectors. Both cases directly follow from the definition of the Lovász number.

Also notably, there is a similar connection between linear expressions

on squares of the expectation values, $\mathbb{E}_{\mathbf{w}} = \sum_{i=1}^{L} w_i \langle A_i \rangle_\varrho^2$, where $\mathbf{w} = (w_1, \ldots, w_L)$, $w_i > 0$ for all $i \in [L]$, and the weighted Lovász number $\vartheta(\bar{G}, \mathbf{w})$ introduced in Section 1.6.2. Indeed, in [B] and in [40] it is shown that

$$\sum_{i=1}^{L} w_i \langle A_i \rangle_\varrho^2 \leq \vartheta(\bar{G}, \mathbf{w}) \quad \forall \varrho \in \mathcal{S}(\mathcal{H}), \tag{2.11}$$

and that by setting the weights to $\mathbf{w} = (\Lambda(A_1^2), \ldots, \Lambda(A_L^2))$, we obtain $\sum_{i=1}^{L} \langle A_i \rangle_\varrho^2 \leq \vartheta(\bar{G}, \mathbf{w})$ for all $\varrho \in \mathcal{S}(\mathcal{H})$. Computing $\vartheta(\bar{G}, \mathbf{w})$ is also a small instance of an SDP, thus the bound is easily computable [92].

Two remarks are in order here. First, we showed that the bound from Eq. (2.4) is in general not tight, and provided a tighter bound in Proposition 2.1. Moreover, Proposition 2.1 is stronger than maximising a sum of squares of real numbers under the pairwise anticommutativity conditions, as demonstrated by the fact that Eq. (2.10) evaluates to $5/2$. Second, we note that in contrast to finding the chromatic number of a graph (which is an NP-hard problem), the Lovász number of a graph is computable through SDP (see Eq. (1.49)). Hence, more than being tighter, the Lovász number bound is efficient to compute.

Finally, we recall that Eq. (2.1) completely characterises the set of states in the two-dimensional case, in the sense that any Bloch vector having a norm of at most one corresponds to a valid quantum state (see Eq. (1.5)). However, such there is no extension of this statement valid for higher dimensions. To construct an example, we start from the Pauli basis in dimension $d = 4$, given by $\{A_i\}_{i=1}^{16} = \{\mathbb{1}, X, Y, Z\}^{\otimes 2}$. In this case, $\vartheta(\bar{G}) = 4$, and from Eq. (2.6), $\sum_{i=1}^{16} \langle A_i \rangle_\varrho^2 \leq 4$, implying that the length of the Bloch vector of any ququart is bounded by four. Although this bound is tight, it is well-known that there are vectors of length four that do not represent quantum states [28, 89], therefore there must be higher-order constraints not encoded in Eq. (2.5). A possible approach would be to consider sums of powers higher than two, for instance considering $\sum_{i=1}^{L} \langle A_i \rangle_\varrho^4$ with observables that satisfy relations of the type $\sum_{\pi \in \mathrm{Symm}(4)} \mathrm{sign}(\pi) A_{\pi^{-1}(1)} A_{\pi^{-1}(2)} A_{\pi^{-1}(3)} A_{\pi^{-1}(4)} = 0$. Finding such relations is an interesting topic for further research.

2.1.2 Including commutation relations

A prominent application of the Lovász number bound is to multi-qubit Pauli operators. These operators either commute or anticommute, hence in this subsection, we analyse the Lovász number bound for observables that obey

this.

In that case, the equality $\sum_{i=1}^{L}\langle A_i\rangle_\varrho^2 = \omega(G)$ clearly holds for $\varrho = |\psi\rangle\langle\psi|$, where $|\psi\rangle$ is any common eigenstate of the largest pairwise commuting observable subset. So, when $\omega(G) = \vartheta(\bar{G})$, the bound in Eq. (2.6) is tight. This relation is satisfied for many graphs, including all perfect graphs. The smallest graph (in terms of number of vertices) for which it does not hold is the pentagon $G_\star$. Its clique number is $\omega(G_\star) = 2$ and $\vartheta(\bar{G}_\star) = \sqrt{5}$. However, we show in the next proposition that this bound is not tight.

Proposition 2.2 ([B]). *Let $O_\star$ be a set of five observables with a star anticommutativity graph such as in Figure 2.1. Then,*

$$\max_{\varrho\in\mathcal{S}(\mathcal{H})}\sum_{A\in O_\star}\langle A\rangle_\varrho^2 = \omega(G_\star) = 2. \tag{2.12}$$

Proof. Let $a_i = \langle A_i\rangle$ and $\mathbf{a} = (a_1,\ldots,a_5)^T$. From the proof of Proposition 2.1, we know that $\|\mathbf{a}\|^2\sum_{i=1}^5\langle A_i\rangle^2 \leq \sum_{i,j=1}^5 a_i a_j\langle A_iA_j\rangle$. The right hand side evaluates to $\|\mathbf{a}\|^2 + 2\sum_{i=1}^5 a_i a_{i+1}\langle A_iA_{i+1}\rangle$ using the commutation relations of the observables in $O_\star$, where the subscript $i+1$ is to be understood as $(i \bmod 5)+1$. We therefore obtain

$$\sum_{i=1}^5\langle A_i\rangle^2 \leq 1 + \frac{2}{\|\mathbf{a}\|^2}\sum_{i=1}^5 a_i a_{i+1}\langle A_iA_{i+1}\rangle. \tag{2.13}$$

In the right hand side, the sum can be interpreted as the scalar product between two vectors, and using the Cauchy–Schwarz inequality we obtain

$$\sum_{i=1}^5 a_i a_{i+1}\langle A_iA_{i+1}\rangle \leq \sqrt{\sum_{i=1}^5 a_i^2 a_{i+1}^2}\sqrt{\sum_{i=1}^5\langle A_iA_{i+1}\rangle^2}. \tag{2.14}$$

Using the fact that the set $\{A_iA_{i+1}\}_{i=1}^5$ has a complete anticommutativity graph, i.e., $\sum_{i=1}^5\langle A_iA_{i+1}\rangle^2 \leq 1$, we obtain

$$\sum_{i=1}^5\langle A_i\rangle^2 \leq 1 + \frac{2}{\|\mathbf{a}\|^2}\sqrt{\sum_{i=1}^5 a_i^2 a_{i+1}^2}. \tag{2.15}$$

Using a computer algebra system, we show that the right hand side is upper bounded by two. Since $\omega(G_\star) = 2$, $\sum_{i=1}^5\langle A_i\rangle^2 \leq 2$ is tight. □

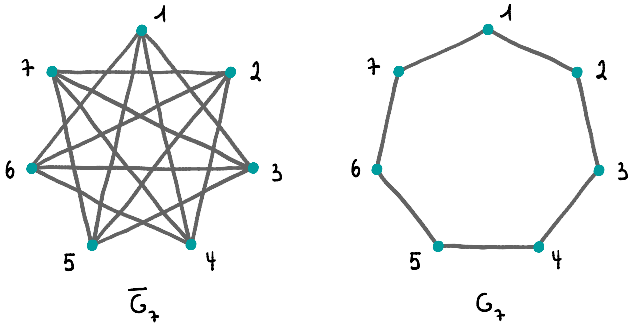

Figure 2.2: *Anticommutativity graph $\bar{G}_7$ and its complement, G_7.* For the corresponding observable set O_7, the quantity $\max_{\varrho\in\mathcal{S}(\mathcal{H})}\sum_{A\in O_7}\langle A\rangle_\varrho$ is equal to $1/7(9+4\sqrt{2}) \simeq 2.0938$ [106], which is strictly lager than the clique number of G_7, $\omega(G_7)=2$.

We summarise the bounds for the set of observables $O_\star$ through

$$\sum_{A\in O_\star}\langle A\rangle_\varrho^2 = \omega(G_\star) < \vartheta(\bar{G}_\star) < \alpha(\bar{G}_\star) < \chi(G_\star), \tag{2.16}$$

where $\omega(G_\star)=2$, $\vartheta(\bar{G}_\star)=\sqrt{5}\simeq 2.2361$, $\alpha(\bar{G}_\star)=2/5$, and $\chi(G_\star)=3$. Notice that none depend on the actual observables, only on their anticommutation relations (and commutation for Proposition 2.2).

This naturally raises the question whether the clique number of G could be the actual tight bound. To answer this, the authors of [163] analyse the set of three-qubit observables $O_7=\{ZZ\mathbb{1}, Z\mathbb{1}\mathbb{1}, \mathbb{1}X\mathbb{1}, X\mathbb{1}\mathbb{1}, XZX, YZZ, YYY\}$. We denote by $\bar{G}_7$ its anticommutativity graph and by G_7 the complement thereof, both depicted in Figure 2.2. Proposition 2.1 tells us that $\mathbb{E}=\sum_{A\in O_7}\langle A\rangle_\varrho^2$ is upper bounded by $\vartheta(\bar{G}_7)=1+(\cos(\pi/7))^{-1}\simeq 2.1099$, with $\varrho\in\mathcal{S}(\mathcal{H})$. The clique number of G_7 is equal to two, and any common eigenstate to two commuting observables of O_7 reaches $\mathbb{E}=2$. However, it is shown in [163] that by taking the state corresponding to the eigenvector of the most negative eigenvalue of $\sum_{A\in O_7}A$, we obtain $\mathbb{E}=1/7(9+4\sqrt{2})\simeq 2.0938$, which is clearly greater than two. In the same work, the authors define $\beta(\bar{G})=\sup_{\varrho\in\mathcal{S}(\mathcal{H})}\mathbb{E}$ as a new graph invariant, and investigate its properties. They leave as an open question how to obtain efficient upper bounds on this quantity.

In [106], the authors answer this question by providing a complete SDP hierarchy that converges to $\beta(\bar{G})$, whose first level recovers the Lovász number. Of course, if at any level of the hierarchy $\omega(G)$ is obtained, then $\beta(\bar{G})=\omega(G)$. They compute up to level seven of their hierarchy for all

seven-, eight- and nine-vertex graphs, reaching for instance $\beta(\bar{G}_7) \leq 2.0938$. This shows that, up to numerical precision, $\sum_{A\in O_7}\langle A\rangle_\varrho^2 \leq 1/7(9+4\sqrt{2})$ is a tight bound.

2.1.3 Imprecise observables

As noted above, if no pair of observables in a given set $\{A_i\}_{i=1}^L$ anticommutes, then $\vartheta(\bar{G}) = L$ is a trivial bound. Although the bound is tight when the observables share eigenstates, it is not always the case. This can be improved if we have access to more information regarding the observables. For example, one may wonder how the Lovász number bound scales in the presence of a perturbation such that some pairs of observables "almost" anticommute. More than an interesting theoretical consideration, this is also in line with approaches to devise entanglement tests which are robust against imprecisely calibrated devices [107, 108, 131].

Let us compute $\left\|\{A_i, A_j\}\right\| = \varepsilon_{ij}$, with $i, j \in [L]$, where $\|\cdot\|$ is any norm that satisfies $\Lambda(\cdot) \leq \|\cdot\|$ (for instance, the operator norm [75]), and define a critical $\varepsilon > 0$. We say that any pair of observables with ε_{ij} strictly less than ε *almost anticommute*, with $i, j \in [L]$. We are interested in how this affects the Lovász number bound, as it for now depends on vanishing anticommutators. For that purpose, we construct the $L \times L$ matrix $\mathcal{E}(\mathbf{w})$ with entries $\sqrt{w_i w_j}\varepsilon_{ij}$ if A_i and A_j almost anticommute and zero otherwise, with $i, j \in [L]$. Proposition 2.1 extends to this case as

$$\sum_{i=1}^{L} w_i \langle A_i\rangle_\varrho^2 \leq \vartheta(\bar{G}_\varepsilon, \mathbf{w}) + \frac{1}{2}\Lambda\left(\mathcal{E}(\mathbf{w})\right) \quad \forall \varrho \in \mathcal{S}(\mathcal{H}), \tag{2.17}$$

where two vertices in $\bar{G}_\varepsilon$ are connected if their corresponding observables almost anticommute. The graph $\bar{G}_\varepsilon$ is called the *almost anticommutativity graph* of $\{A_i\}_{i=1}^L$.

Proof. Following the proof of Proposition 2.1 and the notation therein, we can show that $\|\mathbf{a}\|^2 \sum_{i=1}^L w_i \langle A_i\rangle^2 \leq \sum_{i,j=1}^L a_i a_j \sqrt{w_i w_j}\langle A_i A_j\rangle$, with $a_i = \sqrt{w_i}\langle A_i\rangle$, $i \in [L]$. Then, by splitting the right hand side into a sum over the pairs that do not almost anticommute and a sum over the pair that do, we write

$$\|\mathbf{a}\|^2 \sum_{i=1}^{L} w_i \langle A_i\rangle^2 \leq \sum_{\{i,j\}\in G_\varepsilon} a_i a_j \sqrt{w_i w_j}\langle A_i A_j\rangle + \sum_{\{i,j\}\in \bar{G}_\varepsilon} a_i a_j \sqrt{w_i w_j}\langle A_i A_j\rangle. \tag{2.18}$$

The right hand side's first sum is upper bounded by $\|\mathbf{a}\|^2\vartheta(\bar{G}_\varepsilon,\mathbf{w})$ as previously, whereas the second sum is upper bounded by $\frac{\|\mathbf{a}\|^2}{2}\Lambda(\mathcal{E}(\mathbf{w}))$, which finished the proof. □

Equation (2.17) is surprisingly simple. Moreover, as is discussed later, the fact that it decouples the contributions of the idealised observables and the perturbation also greatly simplifies the design and analysis of entanglement tests under more realistic conditions.

2.2 Application to entanglement detection

Entanglement witnesses (see Section 1.3.3) are among the main tools for entanglement detection in practice. However, constructing experimentally friendly witnesses can be difficult, since obtaining the bounds frequently require them to have a particular structure that may not necessarily match what can be implemented in a laboratory. Furthermore, it has been noticed that even small imprecisions in the measurements can lead to false positives in entanglement and nonlocality detection [107, 108, 131], but this analysis could only be done for the simplest examples. Here, we demonstrate how Eq. (2.17) gives a straightforward solution to both these problems. Then, we show how the results can be adapted in order to construct Schmidt number witnesses.

2.2.1 Entanglement witnesses

Recall from Section 1.3.1 that a bipartite state $\varrho \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ is separable ($\varrho \in S_1$) if it can be written as a convex combination of product states. Now, let $\{A_i\}_{i=1}^L$ and $\{B_i\}_{i=1}^L$ be sets of observables acting on $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively. Clearly,

$$\max_{\varrho\in S_1} \sum_{i=1}^{L} \langle A_i \otimes B_i\rangle_\varrho = \max_{\substack{\varrho_A\in\mathcal{S}(\mathcal{H}_A)\\ \varrho_B\in\mathcal{S}(\mathcal{H}_B)}} \sum_{i=1}^{L} \langle A_i\rangle_{\varrho_A}\langle B_i\rangle_{\varrho_B}. \tag{2.19}$$

Rewriting Eq. (2.6) and making use of the the Cauchy–Schwarz inequality, we get

$$\max_{\varrho\in S_1} \sum_{i=1}^{L} \langle A_i \otimes B_i\rangle_\varrho \leq \sqrt{\vartheta(\bar{G}_A)\vartheta(\bar{G}_B)}, \tag{2.20}$$

where $\vartheta(\bar{G}_A)$ is the Lovász number of the anticommutativity graph of $\{A_i\}_{i=1}^L$ and similarly for $\vartheta(\bar{G}_B)$. For convenience, we define

$$\vartheta_{AB} = \sqrt{\vartheta(\bar{G}_A)\vartheta(\bar{G}_B)}.$$

We thus obtain a class of entanglement witnesses that we summarise in the following proposition.

Proposition 2.3 ([B]). *Let $\{A_i\}_{i=1}^L$, $\{B_i\}_{i=1}^L$ and ϑ_{AB} be such as above. The observable*

$$W_{\mathbb{E}} = \vartheta_{AB}\mathbb{1} - \sum_{i=1}^{L} A_i \otimes B_i \tag{2.21}$$

is an entanglement witness for states in $\mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$.

For cases where both involved Lovász number bounds are tight, $W_{\mathbb{E}}$ is a weakly optimal entanglement witness, i.e., there exists at least one separable state $\varrho_s \in \mathcal{S}(\mathcal{H})$ such that $\mathrm{tr}(W\varrho_s) = 0$ [60]. We note that the separability problem can be reformulated in terms of weakly optimal witnesses [9].

For concreteness, let us choose a two-ququart PPT entangled state,

$$\varrho_I = \frac{1}{6}\left(\varrho_{\mathbb{1}Y} + \varrho_{XX} + \varrho_{YZ} + \varrho_{ZX} + \varrho_{ZY} + \varrho_{ZZ}\right), \tag{2.22}$$

where ϱ_{AB} is the projector onto the pure state $|\psi_{AB}\rangle = {}^1/_2\left(\mathbb{1}\mathbb{1} AB \sum_{i=0}^3 |i\rangle\,|i\rangle\right)$, $A, B \in \{\mathbb{1}, X, Y, Z\}$ [13]. As sets of observables, we take the elements in the Bloch decomposition of ϱ_I which correspond to non-zero coefficients, that is,

$$\begin{aligned}\{A_i\}_{i=1}^{15} = \{&\mathbb{1}X, \mathbb{1}Y, \mathbb{1}Z, X\mathbb{1}, XX, XY, XZ, \\ &Y\mathbb{1}, YX, YY, YZ, Z\mathbb{1}, ZX, ZY, ZZ\},\end{aligned} \tag{2.23a}$$

$$\begin{aligned}\{B_i\}_{i=1}^{15} = \{&-\mathbb{1}X, \mathbb{1}Y, -\mathbb{1}Z, -X\mathbb{1}, XX, -XY, -XZ, \\ &Y\mathbb{1}, YX, YY, -YZ, Z\mathbb{1}, -ZX, -ZY, -ZZ\}.\end{aligned} \tag{2.23b}$$

These sets have the same anticommutativity graph $\bar{G}_I$ depicted in Figure 2.3, for which $\vartheta(\bar{G}_I) = \omega(G_I) = 3$. The witness based on these observables reads

$$W_I = 3 - \sum_{i=1}^{15} A_i \otimes B_i \tag{2.24}$$

and detects $\nu\varrho_I + (1-\nu)\mathbb{1}/16$, with $\nu \in [0,1]$ to be entangled for $\nu > {}^3/_5$, which is exactly the separability bound [108]. Notice that the chromatic

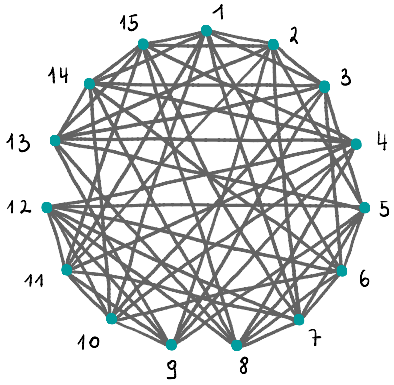

Figure 2.3: *Anticommutatvity graph* $\bar{G}_I$. Its clique number and the Lovász number of its complement are equal to three, $\omega(G_I) = \vartheta(\bar{G}_I) = 3$. The chromatic number of its complement is four, $\chi(G_I) = 4$.

number of G_I is equal to four. If the witness were constructed with this quantity instead of the Lovász number bound, it would only be able to detect entanglement for a visibility ν above $4/5$. This illustrates how considering the chromatic number as a bound on $\mathbb{E}$ can lead to worst results. We finally note that the witness W_I is not a fidelity witness, and that entanglement of PPT entangled states cannot be detected using fidelity witnesses [65].

2.2.2 Imprecise observables

Let us now consider a more realistic scenario and analyse how imprecisions in the measurements affect the entanglement detection threshold. To this end, let $\{A_i\}_{i=1}^{15}$ be the target observables of Eq. (2.23) and let us model the implemented observables by $\{\tilde{A}_i\}_{i=1}^{15}$. A similar notation holds for $\{B_i\}_{i=1}^{15}$. We choose an imprecision bound ε such that the almost anticommutativity graph $\bar{G}_\varepsilon$ is the same as $\bar{G}$, and for simplicity we consider that $\varepsilon_{ij} = \varepsilon$ for all $\{i,j\} \in \bar{G}_\varepsilon$. Equation (2.17) then comes in handy, as it enables us to construct the witness $\tilde{W}_I = (3+4\varepsilon)\,\mathbb{1} - \sum_i \tilde{A}_i \otimes \tilde{B}_i$, which can detect entangled states as long as $\varepsilon < 1/2$. For the PPT entangled state ϱ_I, the witness can certify that $\nu\varrho_I + (1-\nu)\mathbb{1}/16$ is entangled for $\nu > (3+4\varepsilon)/5$. This exemplifies that, although Eq. (2.21) is a witness, if it is implemented by measuring imprecisely the observables of Eq. (2.23), a negative expectation value can no longer be taken as a certification that the state is entangled. Indeed, it may be the case that although $\mathrm{tr}(W_I\varrho)$ is negative, when the imprecision on the measurement is taken into account $\mathrm{tr}\big(\tilde{W}_I\varrho\big)$ is larger than zero, and thus the presence of entanglement is wrongly detected.

Naturally, this discussion is only relevant when measured observables are $\tilde{A}_i \otimes \tilde{B}_i$, $i \in [L]$, and not the witness directly. This is especially relevant considering that most experimental implementation of observables require *product* observables, as discussed in [21, 52, 61].

2.2.3 Schmidt number witnesses

The following proposition shows how the Lovász bound can also be used to derive Schmidt number witnesses. We recall from Section 1.3.3 that an Hermitian operator W_q is a q-Schmidt number witness if $\mathrm{tr}(W_q \varrho_q) \geq 0$ for all $\varrho_q \in S_q$ and if there exists at least one state $\varrho \notin S_q$ such that $\mathrm{tr}(W_q \varrho) < 0$.

Proposition 2.4. *Let $\{A_i\}_{i=1}^L$ and $\{B_i\}_{i=1}^L$ be sets of observables that either commute or anticommute, and denote their anticommutativity graphs by $\bar{G}_A$ and $\bar{G}_B$ respectively. Let $\{\sigma_\alpha\}_{\alpha=1}^{4^m}$ be the set of m-qubit Pauli operators and denote its anticommutativity graph by $\bar{G}_m$. Then,*

$$\max_{\varrho \in S_{2^m}} \sum_{i=1}^{L} \langle A_i \otimes B_i \rangle_\varrho \leq \sqrt{\vartheta(\bar{G}_A \oplus \bar{G}_m)\, \vartheta(\bar{G}_B \oplus \bar{G}_m)}, \tag{2.25}$$

where $\oplus$ stands for the XOR *graph product*[2].

In other words,

$$\sqrt{\vartheta(\bar{G}_A \oplus \bar{G}_m)\, \vartheta(\bar{G}_B \oplus \bar{G}_m)}\, \mathbb{1} - \sum_{i=1}^{L} A_i \otimes B_i \tag{2.26}$$

is a 2^m-Schmidt number witness.

Proof. To prove this result, we first briefly introduce the *lifting technique* proposed by Hulpke and coauthors in [81] that maps q-Schmidt number witnesses W_q in $\mathcal{L}(\mathcal{H}_A^d \otimes \mathcal{H}_B^d)$ to entanglement witnesses in $\mathcal{L}(\mathcal{H}_A^d \otimes \mathcal{H}_{A'}^q \otimes \mathcal{H}_B^d \otimes \mathcal{H}_{B'}^q)$, with $q \in [d]$.

Let $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ be a $d \times d$-dimensional state with Schimdt decomposition $|\psi\rangle = \sum_{i=1}^q \varsigma_i |\alpha_i\rangle |\beta_i\rangle$ (see Eq. (1.9)). We associate $|\psi\rangle$ with a higher-dimensional separable state $|\Psi_q\rangle$. To do that, let us add auxiliary systems

[2] If G_1 and G_2 are n_1- and n_2-vertex graphs respectively, their XOR graph product is the $n_1 n_2$-vertex graph $G_1 \oplus G_2$ whose vertices $v(i_1, i_2)$ and $v(j_1, j_2)$ are connect if either i_1 and j_1 are connected in G_1 or i_2 and j_2 are connected in G_2, but not if both edges exist in G_1 and G_2 respectively.

A' and B', each of dimension q, and set

$$|\psi\rangle \mapsto \left|\Psi_q\right\rangle = \left(\sum_{i=1}^{q} \varsigma_i \left|\alpha_i\right\rangle_A \left|i\right\rangle_{A'}\right) \otimes \left(\frac{1}{\sqrt{q}} \sum_{i=1}^{q} \left|\beta_i\right\rangle_B \left|i\right\rangle_{B'}\right). \tag{2.27}$$

Clearly, $\left|\Psi_q\right\rangle$ is separable across the bipartition $AA' \mid BB'$. Let T be an operator acting on $\mathcal{H}_A \otimes \mathcal{H}_B$ and analogously lift it to

$$\mathbb{T}_q = T \otimes q \sum_{i,j=1}^{q} |ii\rangle\langle jj|_{A'B'} \tag{2.28a}$$

$$= T \otimes \sum_{\alpha=1}^{q^2} \mu_\alpha \otimes \mu_\alpha^T \tag{2.28b}$$

where $\{\mu_\alpha\}_{\alpha=1}^{q^2}$ is an orthogonal basis of $\mathcal{L}(\mathcal{H}^q)$ fulfilling $\mathrm{tr}(\mu_\alpha \mu_{\alpha'}) = q\delta_{\alpha,\alpha'}$, $\alpha, \alpha' \in [q^2]$ such as for instance the Pauli basis. The subscript $\cdot^T$ stands for transposition. Then we obtain

$$\langle\psi|T|\psi\rangle = \left\langle\Psi_q\right|\mathbb{T}_q\left|\Psi_q\right\rangle, \tag{2.29}$$

which is Eq. (9) of [81], up to different normalisations of $\left|\Psi_q\right\rangle$ and $\mathbb{T}_q$. Notice that by abuse of notation, different subsystem ordering are used for $\left|\Psi_q\right\rangle$ and $\mathbb{T}_q$. From the convexity of S_q, it follows that

$$\max_{\varrho \in S_q} \langle T\rangle_\varrho \leq \max_{\rho \in S_1(AA'|BB')} \langle \mathbb{T}_q\rangle_\rho, \tag{2.30}$$

where $S_1(AA' \mid BB')$ specifies that separability across the bipartition $AA' \mid BB'$ is considered.

We are now ready to prove the proposition. We set $T = \sum_{i=1}^{L} A_i \otimes B_i$, and consider the Schmidt number $q = 2^m$, with $m \in \mathbb{N}$. The lifted operator reads $\mathbb{T}_{2^m} = \sum_{i=1}^{L} \sum_{\alpha=1}^{4^m} A_i \otimes \sigma_\alpha \otimes B_i \otimes \sigma_\alpha^T$, where $\{\sigma_\alpha\}_{\alpha=1}^{4^m}$ is the set of m-qubit Pauli operators. Using Eq. (2.20),

$$\max_{\rho \in S_1(AA'|BB')} \langle \mathbb{T}_{2^m}\rangle_\rho \leq \sqrt{\vartheta(\bar{G}_\mathcal{A})\vartheta(\bar{G}_\mathcal{B})}, \tag{2.31}$$

where $\bar{G}_\mathcal{A}$ and $\bar{G}_\mathcal{B}$ are the anticommutativity graphs of $\{A_i \otimes \sigma_\alpha \mid i \in [L], \alpha \in [4^m]\}$ and of $\{B_i \otimes \sigma_\alpha^T \mid i \in [L], \alpha \in [4^m]\}$ respectively.

The observables $A_i \otimes \sigma_\alpha$ and $A_j \otimes \sigma_\beta$ anticommute only if either $\{A_i, A_j\} = 0$ or $\{\sigma_\alpha, \sigma_\beta\} = 0$, but not if both are equal to zero, with $i, j \in [L]$, $\alpha, \beta \in [4^m]$.

Hence it is easy to see that that $\bar{G}_{\mathcal{A}}$ is the XOR graph product of the anticommutativity graphs of $\{A_i\}_{i=1}^{L}$ and of $\{\sigma_\alpha\}_{\alpha=1}^{4^m}$. Since transposing the Pauli operators does not affect their commutation relations, an analogous statement holds for $\bar{G}_{\mathcal{B}}$. Combining this with Eqs. (2.29–2.31), we finally obtain

$$\max_{\varrho \in S_{2^m}} \sum_{i=1}^{L} \langle A_i \otimes B_i \rangle_\varrho \leq \sqrt{\vartheta(\bar{G}_A \oplus \bar{G}_m)\vartheta(\bar{G}_B \oplus \bar{G}_m)}, \tag{2.32}$$

which finishes the proof.

□

As an example, consider a $2n$-qubit system, and take $T_n = \sum_{i=1}^{4^n} \sigma_i \otimes \sigma_i^T$ with $\{\sigma_i\}_{i=1}^{4^n}$ being the set of n-qubit Pauli operators. From Proposition 2.4, we obtain

$$\max_{\varrho \in S_{2^m}} \sum_{i=1}^{4^n} \langle \sigma_i \otimes \sigma_i^T \rangle_\varrho \leq \vartheta(\bar{G}_n \oplus \bar{G}_m). \tag{2.33}$$

For $n = 4$, we computed the Lovász numbers of $\bar{G}_n \oplus \bar{G}_m$, with $m \leq n$. The results translate to the following inequality that holds for all $\varrho \in \mathcal{S}(\mathcal{H}^{2^4} \otimes \mathcal{H}^{2^4})$, up to numerical precision

$$\langle T_4 \rangle_\varrho \underset{\mathrm{SN}(\varrho)\leq 1}{\leq} 16.0 \underset{\mathrm{SN}(\varrho)\leq 2}{\leq} 32.0 \underset{\mathrm{SN}(\varrho)\leq 4}{\leq} 64.0 \underset{\mathrm{SN}(\varrho)\leq 8}{\leq} 128.0 \underset{\mathrm{SN}(\varrho)\leq 16}{\leq} 256.0, \tag{2.34}$$

where the subscripts below the inequality signs indicates that the inequality is valid for states with a Schmidt number below a certain value. Clearly, the last bound is trivial, as it expresses the number of terms present in T_4. This series of bounds can be applied to the isotropic state $\varrho_v = v\,|\psi_{16}\rangle\langle\psi_{16}| + (1-v)\mathbb{1}/256$, with $v \in [0,1]$ and where $|\psi_{16}\rangle = 1/4 \sum_{i=0}^{15} |ii\rangle$. We find that

$$v > \frac{1}{17} \quad \Rightarrow \quad \mathrm{SN}(\varrho_v) > 1, \tag{2.35a}$$

$$v > \frac{31}{255} \quad \Rightarrow \quad \mathrm{SN}(\varrho_v) > 2, \tag{2.35b}$$

$$v > \frac{21}{85} \quad \Rightarrow \quad \mathrm{SN}(\varrho_v) > 4, \tag{2.35c}$$

$$v > \frac{127}{255} \quad \Rightarrow \quad \mathrm{SN}(\varrho_v) > 8, \tag{2.35d}$$

$$v > 1 \quad \Rightarrow \quad \mathrm{SN}(\varrho_v) > 16, \tag{2.35e}$$

which recovers the results of [141].

2.3 Discussion

In this chapter, we have established a connection between quantum observables and graph theory, specifically by showing that the sum of squares of expectation values of any set of observables is bounded by the Lovász number of their anticommutativity graph. This is a significant improvement to the previous bound based on the chromatic number. Nevertheless, as discussed, there exist cases of imperfect graphs for which Proposition 2.1 does not lead to a tight bound. The follow-up works [163] and [106] took steps toward characterising the cases where Proposition 2.1 is tight, nevertheless some questions remain open: Does $\max_{\varrho\in\mathcal{S}(\mathcal{H})}\mathbb{E}$ correspond to a known graph invariant of its associated anticommutativity graph? Are there instances where $\max_{\varrho\in\mathcal{S}(\mathcal{H})}\mathbb{E}=\vartheta(\bar{G})$ while $\vartheta(\bar{G})$ differs from $\omega(G)$? Does including higher order terms lead to a better characterisation of the set of quantum states, in the sense of Eq. (2.1)?

The implications of our results extend beyond foundational considerations. Specifically, they have practical applications in the characterisation of entanglement. We have developed entanglement witnesses that are robust to imprecise measurements of observables, an essential feature for practical quantum information processing. Additionally, by integrating our results with the lifting technique introduced in [81], we have constructed Schmidt number witnesses. So far, the applications of Proposition 2.4 are merely simple examples, and future work will determine whether it can lead to new Schmidt number detections.

Finally, we note that our results can be formulated in the language of entropic uncertainty relations. These can in turn be used to construct *quantum steering detection criteria* [37, 146], as is shown in [B] and [40].

Chapter 3

Marginal tomography

The process of determining the state of a quantum system from measured data, known as quantum state tomography, is essential in quantum information theory. However, as the number of qubits in a system increases, performing full state tomography becomes impractical due to the exponential growth in the number of required measurement settings. In this chapter, we focus on a more feasible approach: obtaining k-qubit marginal states from an n-qubit quantum system. Specifically, we aim to develop efficient measurement scheduling strategies that minimise the number of required measurement settings. As introduced in [38], we refer to the problem of obtaining all k-qubit marginal states of an n-qubit system as *k-body overlapping tomography*. This falls under the broader topic of marginal tomography, which aims to reconstruct some marginal states of a multipartite quantum system.

To address this question, we investigate two general measurement schemes. The first scheme, discussed in Section 3.1, is restricted to Pauli settings. We show that constructing the minimal number of Pauli settings for marginal tomography can be mapped to an edge clique cover problem in graph theory, and present a few examples. Notably, we show that two-body marginal tomography of nearest neighbours in planar topologies only requires nine Pauli settings. The second scheme, covered in Section 3.2, allows for any projective measurement setting. We demonstrate that in this case, k-body overlapping tomography can be performed with only 3^k settings, independently of the number of qubits in the system. In Section 3.4, we compare these schemes in terms of the number of samples required to achieve the same confidence level in the reconstructed states. This comparison highlights the trade-offs between the different measurement strategies.

The results will appear in [E].

3.1 Pauli tomography

First, we analyse the problem as it was introduced in [38], [18], and [53], i.e., when the measurement settings are restricted to Pauli settings. In [38] and [18], the authors demonstrate that in order to obtain all k-qubit marginal states of an n-qubit state, the number of Pauli settings whose expectation values have to be estimated scales logarithmically in the number of qubits n. More specifically, García-Pérez and coauthors show in [53] that it is sufficient to consider $6\lceil \log_3(n) \rceil + 3$ Pauli settings on n qubits in order to recover all two-qubit marginals (i.e., $k = 2$.). In [5], the authors aim to reconstruct *some* k-qubit marginal states dictated by the physical structure of the considered system, referred to as *local overlapping tomography*. They propose different methods depending on the topology of the problem to obtain Pauli measurement settings.

In this section, we contribute to the effort by characterising the optimal Pauli settings, i.e., minimal with respect to the number of settings, that are necessary to obtain k-qubit marginal states of n-qubit states. Throughout this chapter, n always refers to the number of qubits of the global state, while k denotes the number of qubits in the desired marginals, which we refer to as the *strength*. In Section 3.1.1, we look at the particular case of strength two, i.e., $k = 2$, for which we give methods for obtaining optimal Pauli settings that allow the reconstruction of specific two-qubit marginal states. We then extend the results to higher strengths in Section 3.1.2. These methods recover the particular case of the overlapping tomography problem, which we discuss in details in Section 3.1.3. We proceed in Section 3.1.4 to reduce the size of the problem for large number of qubits, and finally discuss the optimality of known constructions in Section 3.1.5.

3.1.1 Two-body marginal tomography

In marginal tomography, which of the marginals of an n-qubit state ϱ must be obtained is dictated by the physical problem that is considered: In some cases, we might want all of the $n(n-1)/2$ two-qubit marginals, whereas in other cases only a subset of those may be relevant, such as nearest neighbours in many-body systems. In this section, we show how the problem of finding Pauli settings that are tomographically complete for some pairs of

qubits can be mapped to a graph theory problem, namely the edge clique covering problem (see Problem 1.3 in Chapter 1).

In the case of strength two, the information about which marginals are to be reconstructed can be encoded in a graph G with n vertices.

Definition 3.1 (Connectivity graph [E])**.** An n-vertex graph G with vertex set $[n]$ and edge set E is the *connectivity graph* of an n-qubit system in a state ϱ for which the marginal states $\varrho^{(e)}$ for all $e \in E$ are desired.

Further, we define *(minimal) Pauli sets*.

Definition 3.2 (Pauli set [E])**.** A set of n-qubit Pauli operators that is tomographically complete for all qubit subsets $e \in E$ for some graph $G = ([n], E)$ is called a *Pauli set* for the graph G. If the cardinality of the Pauli set is minimal, it is called a *minimal Pauli set* for G. The cardinality of a minimal Pauli set is denoted by $\phi_2(G)$.

Notice that Pauli sets are not unique: A relabelling of the Pauli operators X, Y, and Z also leads to a valid Pauli set. Moreover, if two vertices have the same neighbouring in G, their local settings may be exchanged still form a Pauli set for G.

For concreteness, let us first focus on the case of a three-qubit state ϱ for which we want to reconstruct the marginal states $\varrho^{(1,2)}$ and $\varrho^{(2,3)}$. The corresponding connectivity graph is a three-vertex line graph, depicted in Figure 3.1 (a). We are thus looking for a set of three-qubit Pauli operators that are tomographically complete for the qubit pairs $\{1,2\}$ and $\{2,3\}$, i.e., a minimal Pauli set that covers the nine two-body Pauli operators

$$XX, XY, XZ, YX, YY, YZ, ZX, ZY, ZZ \tag{3.1}$$

for both qubit pairs.[1]

How to obtain such a Pauli set can be described with the help of two additional graphs. First, we construct a graph where the edges represent the two-qubit operators required for reconstructing the marginals. So, in this case, the 18 two-body Pauli operators for the pairs of qubits $\{1,2\}$ and $\{2,3\}$, i.e.,

$$X_1X_2, X_1Y_2, X_1Z_2, Y_1X_2, Y_1Y_2, Y_1Z_2, Z_1X_2, Z_1Y_2, Z_1Z_2, \tag{3.2a}$$

$$X_2X_3, X_2Y_3, X_2Z_3, Y_2X_3, Y_2Y_3, Y_2Z_3, Z_2X_3, Z_2Y_3, Z_2Z_3, \tag{3.2b}$$

[1] In this chapter, the term "pair" is used as in "pair set".

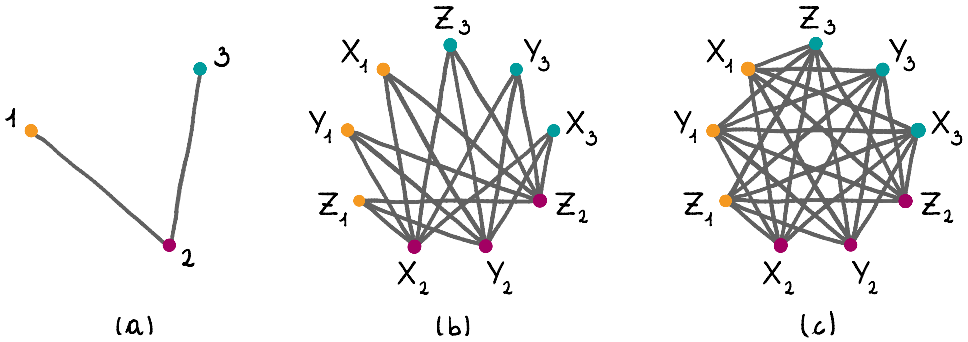

Figure 3.1: (a) *Connectivity graph L of three qubits.* The set of edges $\{\{1,2\},\{2,3\}\}$ represents the two-qubit marginals that are desired. (b) *Covering graph $L^{\times 3}$ of L.* Each edge represents a two-body Pauli operator that is needed to recover the two-qubit marginal states. For instance, the expectation value of X_1Y_2 is required and thus corresponds to an edge of $L^{\times 3}$. On the other hand, Y_1 and Z_3 are not connected, as the marginal $\varrho^{(1,3)}$ does not need to be reconstructed. (c) *Measurement graph $K_{3,3}$.* Each triangle represent a possible three-qubit Pauli setting. Figures taken from [E].

where the indices indicate on which qubits the Pauli operators act. To do that, we instantiate three vertices per qubit (each of them representing a Pauli operator), and connect the vertices corresponding to the required Pauli operators of Eq. (3.2), as in Figure 3.1 (b). It is called the *covering graph* and denoted by $L^{\times 3}$.

The last graph, called *measurement graph*, represents all possible three-qubit Pauli settings. It has the same set of vertices as $L^{\times 3}$, and two vertices are connected if and only if they represent single Pauli operators corresponding to different qubits, resulting in the complete tripartite graph with three vertices per party, $K_{3,3}$.[2] Therein, a global Pauli setting is represented by the triangle on the vertices corresponding to the Pauli setting, and all the triangles represent physical three-qubit Pauli settings. For instance, the global Pauli setting $Y_1X_2Z_3$ is represented by the triangle with vertices Y_1, X_2 and Z_3 in the measurement graph (Figure 3.1 (c)). Note that each of the triangles of $K_{3,3}$ covers three two-body Pauli settings, which in this case are Y_1X_2, Y_1Z_3, and X_2Z_3.

This formulation can easily be extended to n parties and arbitrary connectivity graphs G: First, we let the edges of $G^{\times 3}$ represent all the two-body Pauli operators whose expectation values need to be known. Mathematically speaking, the vertex set of $G^{\times 3}$ is given by $\cup_{i=1}^{n}\{X_i, Y_i, Z_i\}$, and its edge

[2] The complete n-partite graph with v vertices per party $K_{n,v}$ is the graph whose nv vertices can be partitioned into n sets of v unconnected vertices, and such that vertices belonging to different sets are connected [43].

set by $\{\{A_i, B_j\} \mid A, B \in \{X, Y, Z\}, \{i, j\} \in G\}$. The measurement graph is the n-partite complete graph with three vertices per party, $K_{n,3}$. Its vertices are the same than $G^{\times 3}$, and its edge set is $\{\{A_i, B_j\} \mid A, B \in \{X, Y, Z\}, i \neq j, i, j \in [n]\}$. Then, the maximal cliques[3] of $K_{n,3}$ represent all the possible n-qubit Pauli settings. We notice that each clique is part of a maximal clique, and that the orders of the maximal cliques are all equal to n. Finding a minimal Pauli set for the connectivity graph G is thus equivalent to finding the minimal number of maximal cliques of $K_{n,3}$ that are needed to cover all the edges of $G^{\times 3}$, i.e., solving the edge clique cover problem for $G^{\times 3}$ and $K_{n,3}$ as defined in Problem 1.3.

Inspired by this construction, it is shown in [E] and [40] how finding minimal Pauli sets can be formulated as a binary program and solved exactly.

Proposition 3.1 (Binary program for marginal tomography [E], [40])**.** *Let G be a connectivity graph for two-body marignal tomography of an n-qubit system. A minimal Pauli set for G can be obtained by solving the following binary program*

$$\phi_2(n) = \min_{\{z_c\}_{c\in C} \in \{0,1\}^{3^n}} \sum_{c \in C} z_c \tag{3.3a}$$

$$\text{such that} \quad z_c \in \{0, 1\} \quad \forall c \in C \tag{3.3b}$$

$$\sum_{c \in C} z_c e_c \geq 1 \quad \forall e \in E, \tag{3.3c}$$

where C denotes the set of cliques and edges of $K_{n,3}$, E denotes the set of edges of $G^{\times 3}$, and where $e_c = 1$ if $e \in c$, and 0 otherwise. The e_c are constants of the problem.

For the three-qubit example with the line connectivity graph L, a solution to the edge clique cover and the corresponding Pauli set are given in Figure 3.2, using Proposition 3.1. Obtaining the expectation values of the nine Pauli settings of Figure 3.2 (b) is therefore sufficient in order to reconstruct the marginals $\varrho^{(1,2)}$ and $\varrho^{(2,3)}$. Although this particular example may seem trivial, it is clear that the general problem is not.

We note that the number of variables in Eq. (3.3) is equal to 3^n, therefore large instances may become too expensive to compute. However, we show in Section 3.1.4 that for many physically motivated connectivities, finding a minimal Pauli set can be reduced to a small instance of the program, and

[3] We recall that a clique is a complete subgraph, as defined in Definition 1.16.

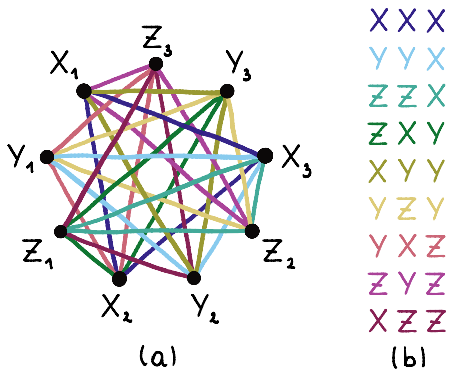

Figure 3.2: (a) *Cover of the edges of* $L^{\times 3}$ *by the cliques of* $K_{3,3}$. Each clique used in the covering is highlighted in a different colour. (b) *The corresponding minimal Pauli set.* The three-qubit Pauli settings form a minimal Pauli set for the connectivity graph L is presented in Figure 3.1. Each three-qubit Pauli setting is associated to the triangle of the same colour in (a). Figures adapted from [E].

we discuss in Section 3.1.5 how minimal Pauli sets for a few parties can be extended to larger cases.

3.1.2 Marginal tomography of arbitrary strength

Although most previous methods focused on two-body partial tomography [18, 38, 53], some physical problems may require k-body marginals of higher strength. We show how the graph formulation for two-body partial tomography can be generalised to arbitrary strength $k \leq n$ by using hypergraphs.

To do that, we begin by encoding the desired marginals in a connectivity hypergraph H, where each hyperedge connects k vertices representing the qubits from the desired marginal sates. As an example, Figure 3.3 depicts the hypergraph H_7 representing seven qubits in a ring configuration where, for each qubit $i \in [7]$, we want to have access to the three-qubit marginal of the triplet $\{i-1, i, i+1\}$, i.e., $k = 3$. Definition 3.2 of Pauli sets extends straightforwardly, and we denote the cardinality of minimal Pauli set of H as $\phi_k(H)$.

The covering hypergraph $H^{\times 3}$ follows the same idea than in the case of strength two: Each hyperedge represents a k-body Pauli operator whose expectation value is required to reconstruct the marginals dictated by the connectivity hypergraph H. The measurement hypergraph $K^k_{n,3}$ is such that its hyperedges represent all possible k-body Pauli settings. Similarly to the

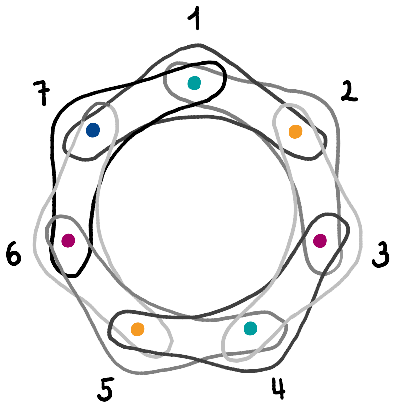

Figure 3.3: *Connectivity hypergraph H_7 of seven qubits in a ring.* The marginals of each consecutive triplet of qubits are to be reconstructed, i.e., $\varrho^{(1,2,3)}$, $\varrho^{(2,3,4)}$, $\varrho^{(3,4,5)}$, $\varrho^{(4,5,6)}$, $\varrho^{(5,6,7)}$, $\varrho^{(6,7,1)}$, and $\varrho^{(7,1,2)}$. The vertices are coloured such that vertices belonging to a same edge have distinct colours. The grey scale of the edges are for better readability. Figure taken from [E].

case of strength two, a global Pauli setting is a maximal clique[4] in $K^k_{n,3}$. Both hypergraphs $H^{\times 3}$ and $K^k_{n,3}$ have $3n$ vertices, one for each single-qubit Pauli setting.

Finding a minimal Pauli set for the k-body marginal tomography of H is equivalent to finding a minimal hyperedge covering of $H^{\times 3}$ with cliques of $K^k_{n,3}$. Whereas hypergraphs quickly become cumbersome to draw on paper, it is shown in [E] that the hypergraph covering can also be formulated as a binary program and solved exactly, leading to a direct extension of Proposition 3.1. The number of variable used in the binary program quickly exceeds what is manageable by standard computers, and only a few cases could be computed. For instance, a minimal Pauli set for H_7 is computed in [E] and presented in Figure 3.4.

3.1.3 Overlapping tomography of arbitrary strength

In this section, we consider the overlapping tomography problem as introduced in [38], [18], and [53], i.e., how to find Pauli settings that allow for the reconstruction of all k-body marginals of an n-qubit quantum state. In that case, the Pauli set must be tomographically complete for all k-sets of qubits. The connectivity hypergraph thus is the complete hypergraph K^k_n, and the covering graph is $K^k_{n,3}$, as all k-body Pauli operators are needed: The

[4]Given a hypergraph H, its cliques are its induced subgraphs where any distinct k vertices are connected by a hyperedge.

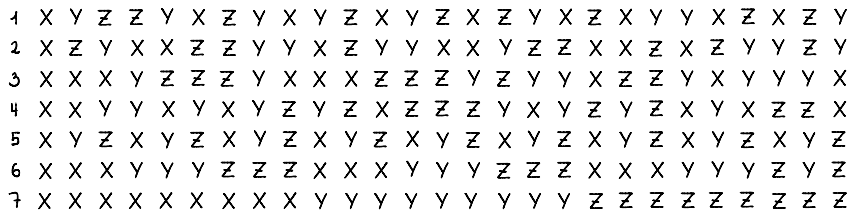

Figure 3.4: *A minimal Pauli set for the connectivity hypergraph H_7.* Each column corresponds to one seven-qubit Pauli setting, and the number of settings is $\phi_3(H_7) = 27$. These 27 Pauli settings grantee that, for every triplet $\{i-1, i, i+1\}$ of qubits, with $i \in [7]$, the corresponding rows cover each of the $3^3 = 27$ combinations of X, Y, and Z (at least) once.

covering graph is the same as the measurement graph. For conciseness, we define $\phi_k(n) = \phi_k(K_n^k)$. We note that in this case, any Pauli set for n qubits leads to Pauli sets for n' qubits, with $n' < n$, by omitting the measurement settings on the additional qubits.

In other words, we are looking for an array with n columns, such that for every k-sets of columns, all 3^k possible combinations of X, Y, and Z appear. Incidentally, the same problem is central in the combinatorial designs literature, where it appears under the name of *covering arrays* (CAs).

Definition 3.3 (Covering array [34])**.** A *covering array* $\mathrm{CA}(L; n, k, v)$ is an $L \times n$ array such that the rows of any $L \times n$ subarray cover all the k^v possible combinations of v symbols. A minimal covering array is a covering array for which L is minimal. The covering array number $\mathrm{CAN}(n, k, v)$ is the number L of rows of a minimal $\mathrm{CA}(L; n, k, v)$.

For reviews of the topic, see [34, 143]. Clearly, finding a minimal Pauli set is equivalent to finding a minimal CA with three symbols (i.e., $v = 3$). Therefore, it follows that $\mathrm{CAN}(n, k, 3) = \phi_k(n)$, the minimal number of Pauli settings needed to reconstruct all k-qubit marginal states of an n-qubit system. Similarly to Pauli settings, from a $\mathrm{CA}(L; n, k, 3)$, it is possible to obtain $\mathrm{CA}(L; n', k, 3)$, with $n' < n$, by deleting $n - n'$ columns. Several facts about the minimal Pauli sets can thus be immediately borrowed, such as bounds on $\phi_k(n)$ and explicit constructions. As examples, it is known [34, 143] that

$$\phi_k(k+1) = 3^k, \tag{3.4}$$

and that

$$\phi_k(n) \leq \frac{k-1}{\log\left(\frac{3^k}{3^k-1}\right)} \log(n)(1 + o(1)), \tag{3.5}$$

n	4	5	6	5	9	10	20
$\phi_2(n)$	9	11	12	12	13	14	15
$\phi_3(n)$	27	33	33				

Table 3.1: *Covering array numbers* for CAs of strength two and three and with three symbols [93]. For integers $n' \in [20]$ that are not displayed, $\phi_k(n') = \phi_k(n)$, where n is the closest larger integer to n' displayed.

confirming the logarithmical scaling of the number of settings for overlapping tomography [38, 18]. However, minimal covering arrays are notoriously hard to construct: To this day, strength-two covering arrays[5] with three symbols are only known up to $n = 20$ parties [93]. The known values of $\phi_2(n)$ and $\phi_3(n)$, with $n \in [20]$, are given in Table 3.1.

On the other hand, when considering strength two, the particular case of two symbols has been shown to have an efficient method for computing a CA. Although not of use in the case of quantum state tomography, this could turn out to be relevant in a multi-qubit Mermin inequality setting, as it only requires the expectation values of tensor products of two binary observables. We leave the discussion for Section 4.4.4 of Chapter 4.

Minimal Pauli sets were obtained through the use of the binary program described in Proposition 3.1 for $k = 2$ up to $n = 8$, and for the case $k = 3$, it rendered $\phi_3(4) = 27$ and $\phi_3(5) = \phi_3(6) = 33$. As an example, Figure 3.5 depicts a minimal Pauli set for two-body overlapping tomography of six-qubit systems. We note that to the best of our knowledge, the fact that $\mathrm{CAN}(5, 3, 3) = \phi_3(5) = 33$ had not been shown previously.

Inspired by the field of combinatorial designs, we notice that there exist (non-minimal) Pauli set on n-qubits such that, for every k-sets of qubits, each combination of k Pauli operators appears exactly t times. These Pauli sets are called *uniform Pauli sets*, and called minimal uniform Pauli sets when the number of settings, given by $3^k t$, is minimal. We recall that in general, Pauli sets only require that each combination of k Pauli operators appears at least once. Uniform Pauli sets correspond to *orthogonal arrays* with three symbols, see [68] for an introduction to the topic and see [136] for tables of orthogonal arrays.

Naturally, when the number of repetitions t is fixed, given n and k, it is not always possible to find a uniform Pauli set. The simple example is to consider $t = 1$, then if $k = 2$, uniform Pauli sets only exist for $n = 2, 3, 4$, as for $n = 5$, minimal Pauli sets are of composed of 11 elements, which

[5] The strength of a $\mathrm{CA}(L; n, k, v)$ is given by k.

1	X	Y	Y	Z	Y	Z	X	Z	X	Z	Y	X
2	X	Y	Z	X	X	Z	Z	Y	Y	X	Y	Z
3	X	Z	Y	Y	Z	X	Y	Z	Y	X	X	Z
4	X	Z	Y	Z	Y	Z	X	X	Y	Y	X	Z
5	X	Y	Z	Z	X	X	Y	Z	X	Y	Z	Z
6	X	X	X	X	Y	Y	Y	Y	Z	Z	Z	Z

Figure 3.5: Minimal Pauli set for two-body overlapping tomography of a six-qubit system computed using Proposition 3.1. Each column corresponds to a six-qubit Pauli setting, and there are 12 settings in total. The settings ensure that, for any pair of qubits, the corresponding rows cover the nine two-body Pauli operators. Note that comparing to Definition 3.3 of covering arrays, the table is transposed.

implies the repetitions of some two-body Pauli terms for all pairs of qubits. Nevertheless, for given n and k, it is always possible to find a number t such that a uniform Pauli set exists. For instance, the set of all n-qubit Pauli operators is a uniform Pauli set for any strength k, with repetition $t = 3^{n-k}$.

Uniform Pauli sets have the advantage that all k-qubit Pauli settings are in the end measured the same amount of times. Therefore, using uniform Pauli sets with the smallest number of repetitions possible combines having a smaller number of settings together with a uniform distribution of the number of samples of each k-body Pauli operator. However, contrarily to minimal Pauli sets, the number of settings does not scale logarithmically with the number of qubits n. The most general lower bound on the number of settings $3^k t$ is given by the Rao bound [68, 123], and reads

$$3^k t \geq \begin{cases} 1 + \sum_{i=1}^{k/2} \binom{n}{i} (k-1)^i & \text{if } k \text{ is even} \\ 1 + \sum_{i=1}^{k-1/2} \binom{n}{i} (k-1)^i + \binom{n-1}{k-1/2} (n-1)^{k+1/2} & \text{if } k \text{ is odd.} \end{cases} \tag{3.6}$$

It can be shown that there are infinitely many orthogonal arrays for which this bound is tight, nevertheless, it is a difficult problem to determine for which parameters equality occurs [68]. Figure 3.6 shows how this lower bound behaves for $k = 2, 3, 4$.

It is for instance known that for seven qubits, minimal uniform Pauli sets for retrieving all two-qubit marginal states have 18 elements, i.e., each two-qubit Pauli term appears exactly twice for each pair of qubits [68]. The Pauli set is given in Figure 3.7. For systems with eight to 13 qubits, minimal uniform Pauli sets of strength two have 27 elements, i.e., with three repetitions [68].

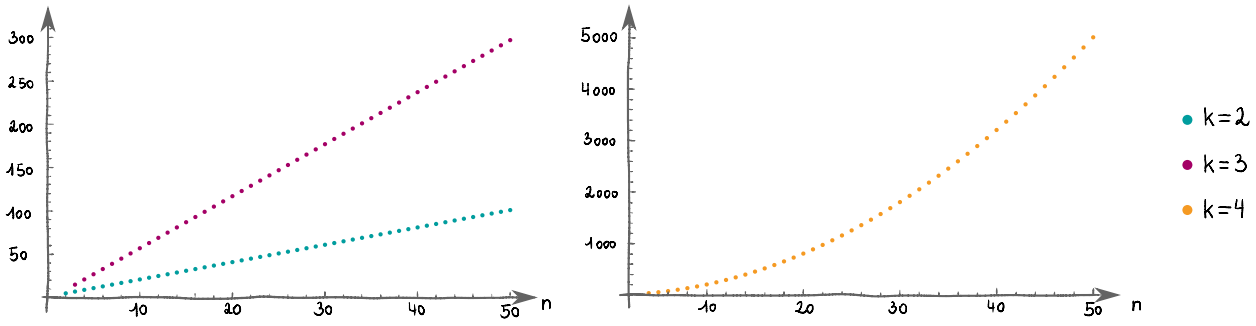

Figure 3.6: *Value of the Rao bound* for different strengths ($k = 2, 3, 4$) as a function of the number of qubits n.

3.1.4 Reduction for large number of qubits

Measurement scheduling for marginal tomography can be mapped to a graph covering problem, which can in turn be formulated as a binary program and therefore solved exactly. However, for large connectivity graphs, those techniques can quickly reach their limits regarding what can actually be solved by standard computers. Fortunately, for many physically motivated classes of connectivity graphs, we show in this section how finding minimal Pauli sets can be mapped to small instances of Eq. (3.3) and optimally computed. We start by presenting an example for the sake of clarity, and move on to the general case at the end of the section.

Consider 16 qubits in a square lattice configuration, where we aim to reconstruct the two-body marginals of each pair of first and second neighbours, such that its connectivity graph G_{16} is the one depicted in Figure 3.8. For 16 qubits, the binary program of Eq. (3.3) is not solvable with standard computers (see [E] for details). Regardless, we directly notice that maximal cliques of G_{16} put a lower bound on $\phi_2(G_{16})$. Indeed, for the qubits 1, 2, 5, and 6, we need to reconstruct the marginals of all six pairs of qubits, therefore at least nine global Pauli settings are needed, and we formalise

$$\phi_2(4) \leq \phi_2(G_{16}). \tag{3.7}$$

We proceed by taking a minimal Pauli set for recovering all two-body marginals of a four-qubit system. We associate one colour to each qubit, as shown in Figure 3.9 (a). Each party has nine single-qubit Pauli settings of one colour. Then, using the same four colours, we colour the 16 vertices of the connectivity graph G_{16} in such a way that no adjacent vertices (qubits) have the same colour. A possible way of doing that is presented in Figure

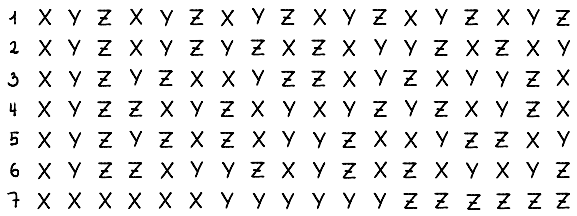

Figure 3.7: *A minimal uniform Pauli set* for two-body overlapping tomography of seven qubits [136]. Each column corresponds to a seven-qubit Pauli setting, and there are 18 settings in total. These settings ensure that, for every pair of qubits, the corresponding rows cover exactly twice each of the nine two-body Pauli operators presented in Eq. (3.1).

3.8. We construct a Pauli set in the following way: To each qubit $i \in [16]$, we associate the colour given by the graph colouring of G_{16}, and later the single-qubit Pauli settings of the same colour given by the four-qubit minimal Pauli set of Figure 3.9 (a). The resulting Pauli set is given in Figure 3.9 (b) and we obtain $\phi_2(G_{16}) = 9$. We can easily check that the Pauli settings form a minimal Pauli set for G_{16}: Any two connected qubits in G_{16} have a different colours, and any two single-qubit Pauli settings of different colour recover all the two-body Pauli operators, as ensured by the minimal Pauli set of Figure 3.9 (a). Moreover, from Eq. (3.7) we know that a Pauli set of cardinality nine must be minimal.

However, there exist connectivity graphs for which such a construction is not possible. Indeed, in graph theory, it is widely known that for any graph G, its clique number $\omega(G)$ is always smaller or equal to the chromatic number $\chi(G)$. Recall that the clique number is given by the number of vertices in a maximal clique of G, and the chromatic number is the smallest numbers of colours needed to colour adjacent vertices with different colours, as defined in Section 1.6.2. A graph G that fulfils $\omega(G) = \chi(G)$, such as G_{16} of Figure 3.8, is called weakly perfect (see Definition 1.18). For arbitrary connectivity graphs G, we thus have to consider a minimal Pauli set for $\chi(G)$ qubits, associate a distinct colour to each qubit, and then proceed as described above. This results is a Pauli set, as each pair of connected qubits in G have two-qubit Pauli settings that allow for the reconstruction of all the two-body Pauli expectation values.

Unfortunately, this construction does not ensure minimality of the number of Pauli settings when $\omega(G) < \chi(G)$. Indeed, there might be a more efficient covering of $G^{\times 3}$ than the one suggested by the above construction and thus a different Pauli set that solves the partial tomography of G

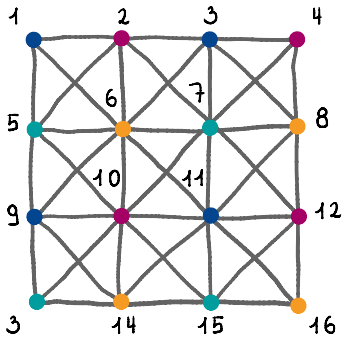

Figure 3.8: *Connectivity graph G_{16} of 16 qubits in a square lattice.* The two-body marginals of the first and second neighbours are to be reconstructed. The vertices are coloured with the minimal number of colours such that no adjacent vertices have the same colour, hence $\chi(G_{16}) = 4$. Figure taken from [E].

with less settings. We summarise this statement in the following sandwich equation,

$$\phi_2(\omega(G)) \leq \phi_2(G) \leq \phi_2(\chi(G)). \tag{3.8}$$

It is unclear whether $\phi_2(G)$ can be strictly smaller than $\phi_2(\chi(G))$. Trying to answer this question, we considered a somewhat artificial connectivity graph with seven vertices (qubits) and edges as shown in Figure 3.10. It is the only connected graph with seven vertices whose clique number is four, whereas its chromatic number is five, which leads to $9 \leq \phi_2(G_{26}) \leq 11$. By running the binary program of Eq. (3.3), we obtain $\phi_2(G_{26}) = 11$, certifying that minimal Pauli sets of G_{26} have 11 settings. Similarly, we ran Eq. (3.3) for all 26 non-isomorphic, connected, not weakly perfect graphs with eight vertices, and did not find an instance where the colouring construction did not give a minimal Pauli set. In other words, there are no connectivity graphs with at most eight vertices for which $\phi_2(G) \neq \phi_2(\chi(G))$. It thus remains an open question whether there are connectivity graphs for which the colouring construction does not lead to a minimal Pauli set, and any counterexample would be for at least nine qubits.

Moreover, since equality between the clique and chromatic numbers results in an optimal solution for the partial tomography problem, the colouring construction leads to minimal Pauli sets for many physically motivated classes of connectivity graphs. It is worth noting that the colouring construction is also optimal for graphs for which $\phi_2(\omega(G)) = \phi_2(\chi(G))$ despite the clique and chromatic numbers being distinct. For example, for $n = 2, 3, 4$, $\phi_2(n) = 9$, and for $n = 11, \ldots, 20$, $\phi_2(n) = 15$, therefore the

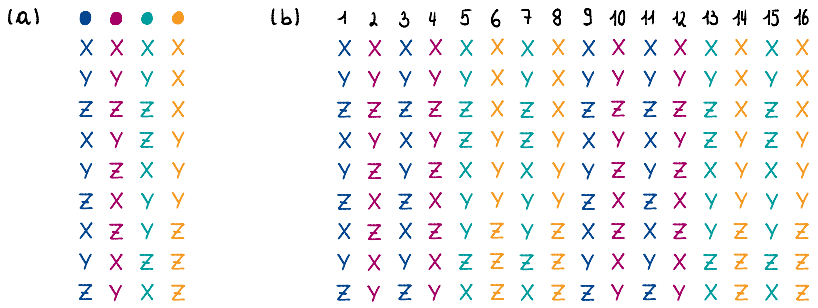

Figure 3.9: (a) *A minimal Pauli set* for four qubits where all the two-body marginals are required. (b) *A minimal Pauli set* for G of Figure 3.8. The colour of each column corresponds to the graph colouring of G_{16} in Figure 3.8, and the Pauli settings are taken from (a). Figures taken from [E].

colouring construction for any connectivity graph G with e.g. $\omega(G) = 11$ and $\chi(G) = 12$ leads to a minimal Pauli set. This allows us to construct minimal Pauli sets for many different classes of connectivity graphs.

Proposition 3.2 (Minimal Pauli sets for $\chi(G) \leq 4$ [E])**.** *Let G be the connectivity graph of an n-qubit system. If $\chi(G) \leq 4$, then $\phi_2(G) = 9$.*

For instance, the grid example of Figure 3.8 can be extended to an arbitrary large number of qubits, and the cardinality of the minimal Pauli set remains equal to nine. Notably, it has been shown that planar graphs[6] have chromatic numbers of at most four [43], therefore it follows from Proposition 3.2 that two-body marginal tomography for planar connectivity graphs can always be performed with nine Pauli settings.

The colouring construction can be generalised to larger strengths, that is, to $k > 2$. Given a hypergraph H, a lower bound on $\phi_k(H)$ is directly set by $\phi_k(\omega(H))$, where $\omega(H)$ is the number of vertices in the largest complete subgraph of H [22]. The natural extension of strength two suggests to colour the vertices of H such that vertices contained in the same edge have different colours. This is known as a strong colouring of H, and the smallest number of colours is the chromatic number of H, $\chi(H)$ [22]. Pauli sets are then constructed analogously to strength two graphs: One considers a minimal Pauli set for $\chi(H)$ qubits where all the k-body marginals are desired, and associates a distinct colour to each qubit. Then, the Pauli set for partial tomography of H is constructed by taking the single-qubit Pauli settings of the minimal Pauli set for $\chi(H)$ following a strong colouring of

[6] Planar graphs are graphs that can be drawn in the Euclidean plane in such a way that no edges cross each other.

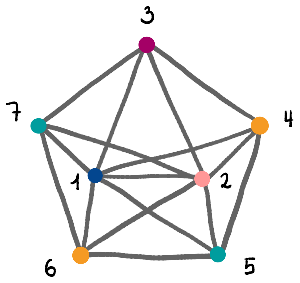

Figure 3.10: *Connectivity graph G_{26} for seven qubits.* Its clique number is equal to four, whereas its chromatic number is equal to five. The colouring construction gives a Pauli set with 11 elements, which turns out to be equal to the number of settings in the minimal Pauli set according to Proposition 3.1. Figure taken from [E].

H, exactly as in the case of two-body partial tomography. Similarly, when $\phi_k(\omega(H)) = \phi_k(\chi(H))$, the Pauli set is minimal. If we look at the ring hypergraph H_7 of Figure 3.3, we have $\omega(H_7) = 3$ and $\chi(H_7) = 4$, and since $\phi_3(3) = \phi_3(4) = 27$, we recover that the partial tomography of H_7 can be performed with a minimal number of 27 global Pauli settings.

We note that the authors of [51] already realised that for line connectivities, marginal tomography can always be realised with 3^k settings, as in that case, $\chi(H) = k$. The case of ring connectivites is thus less trivial, as the chromatic number depends on n and k, as discussed in the next paragraph.

The colouring construction generalises and unifies the results of Araújo and coauthors in [5] concerning qubits. First, a general construction is proposed for connectivity hypergraphs where the vertices are ordered in a lattice, and where the hyperedges have a periodic structure. However, because of the generality of the construction, it is argued that the number of Pauli settings is rather wasteful, and one should look at specific cases and try to reduce the number of Pauli settings. Then, a similar idea to the graph colouring is introduced, however, not connected it to smaller instances. Concerning strength two, a construction is presented that leads to the costly number of settings of $3^{\chi(G)}$, given a connectivity graph G. They further look at a few cases where hypergraphs can be coloured using only k colours (the size of the hyperedges) that is, $\chi(H) = k$. This is recovered by our colouring construction, and we add that k-body overlapping tomography of a connectivity hypergraph H can be done with 3^k Pauli settings if $\chi(H) \leq k+1$. This comes from the fact that minimal Pauli sets for k-body overlapping tomography of $k+1$ qubits have 3^k elements, as stated in Eq. (3.4). Finally, they turn their attention to cyclic topologies such as cycles and toruses. There

again, the number of Pauli settings can be improved using the colouring construction. For instance, it is know that cycle hypergraphs with hyperedge size k have a chromatic number equal to $k + \lceil r/q \rceil$ where q is the quotient and r the remainder of n divided by k (see Theorem 3.1 of [115]). So, when $r \leq q$ (which is in particular satisfied when $n \geq k^2 - 1$), the chromatic number is at most $k + 1$ and thus minimal Pauli sets have 3^k elements, for which the method described in [5] needs twice as many settings. The case of H_7 is again recovered, as its chromatic number is four, which is equal to $k + 1$. The strong colouring of H_7 is shown in Figure 3.3.

3.1.5 On the optimality of constructions for strength two

Unfortunately, in the case of complete connectivity graphs, the colouring construction does not reduce the size of the problem. In this case, it can be convenient to resolve to explicit constructions, which might come at the cost of optimality. In [53], the authors propose a method to construct Pauli sets for two-body overlapping tomography that translates to an upper bound on $\phi_2(n)$,

$$\phi_2(n) \leq 6\lceil \log_3(n) \rceil + 3. \tag{3.9}$$

Alternatively, a well-known recursive construction for covering arrays shows that, from two Pauli sets for n_1 and n_2 qubits, it is possible to build a Pauli set for $n_1 n_2$ qubits [34, 143]. We present here a slightly modified version that requires one less setting, and show that the recursive construction also leads to an upper bound on ϕ_2.

The recursive construction is exemplified in Figure 3.11 goes as follows. First, assume we know (not necessarily minimal) Pauli sets for n_1 and n_2 qubits, with cardinalities $m_1 \geq \phi_2(n_1)$ and $m_2 \geq \phi_2(n_2)$ respectively. Write them as $\mathcal{M}_1 = \{M_\alpha^1\}_{\alpha=1}^{m_1}$ and $\mathcal{M}_2 = \{M_\alpha^2\}_{\alpha=1}^{m_2}$. Therein, M_α^ℓ is an n_ℓ-qubit Pauli operator for $\ell = 1, 2$, with $\alpha \in [m_\ell]$. Without loss of generality, assume that $X^{\otimes n_\ell}$ is part of both Pauli sets, with $\ell = 1, 2$. Then, take the Pauli settings $\{(M_\alpha^1)^{\otimes n_2}\}_{\alpha=1}^{m_1}$, which amounts to m_1 Pauli settings acting on $n_1 n_2$ qubits. A moment's thought shows that all the two-body marginals can be obtained for all pairs of qubits, except for the pairs $(xn_1 + z, yn_1 + z)$ for $x, y = 0, \ldots, n_2 - 1$, provided $x < y$, and $z \in [n_1]$. To amend this, we complete the set of Pauli settings with m_2 additional operators of the form

$$(M_\alpha^2)_{1,n_1+1,2n_1+1,\ldots} \otimes (M_\alpha^2)_{2,n_1+2,2n_1+2,\ldots} \quad \otimes \ldots \otimes (M_\alpha^2)_{n_1,2n_1,3n_1,\ldots}, \tag{3.10}$$

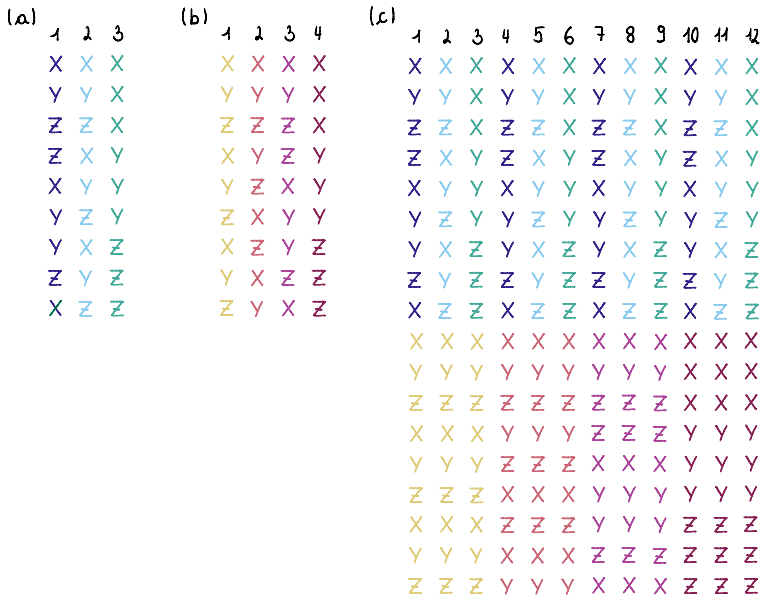

Figure 3.11: *Example of the recursive construction with* $n_1 = 3$ *and* $n_2 = 4$. (a) Minimal Pauli set for $n_1 = 3$ qubits (see also Figure 3.2). Each row corresponds to a three-qubit Pauli operator. (b) Minimal Pauli set for $n_2 = 4$ qubits (see Figure 3.9 (a)). Each row corresponds to a four-qubit Pauli operator. (c) Pauli set for two-body overlapping tomography of 12 qubits, where the colours correspond to the ones of (a) and (b). From the first nine measurements, all two-body marginals can be obtained except for pairs which have the same colour, such as for instance the qubit pair $\{1,4\}$. Similarly, the marginal of the qubit pair $\{1,2\}$ cannot be reconstructed from the last nine measurements alone, as the settings only cover XX, YY, and ZZ. However, when considering all 18 Pauli settings, any qubit pair is covered by the nine two-body Pauli operators. Notice that the setting $X^{\otimes 12}$ is represented twice, hence the cardinality of the Pauli set is $9 + 9 - 1 = 17$. As a comparison, the construction from [53] renders a Pauli set with 21 settings. We note that none of these constructions is optimal, as $\phi_2(12) = 15$. Figures taken from [E].

with $\alpha \in [m_2]$, and where the indices indicate on which qubits the Pauli operators in each M_α^2 should act. Recall that $X^{\otimes n_\ell}$, with $\ell = 1, 2$, appears in $\mathcal{M}_1$ and $\mathcal{M}_2$ respectively, thus twice in the Pauli set for $n_1 n_2$ qubits. We end up with a Pauli set $\mathcal{M}_{1\times 2}$ for $n_1 n_2$ qubits containing $m_1 + m_2 - 1$ measurement settings. Clearly, $\phi_2(n_1 n_2) \leq m_1 + m_2 - 1$. This holds in particular when $\mathcal{M}_1$ and $\mathcal{M}_2$ are minimal Pauli sets, and we obtain

$$\phi_2(n_1 n_2) \leq \phi_2(n_1) + \phi_2(n_2) - 1. \tag{3.11}$$

Remarkably, the construction leads to an upper bound on $\phi_2(n)$, for all $n \in \mathbb{N}$.

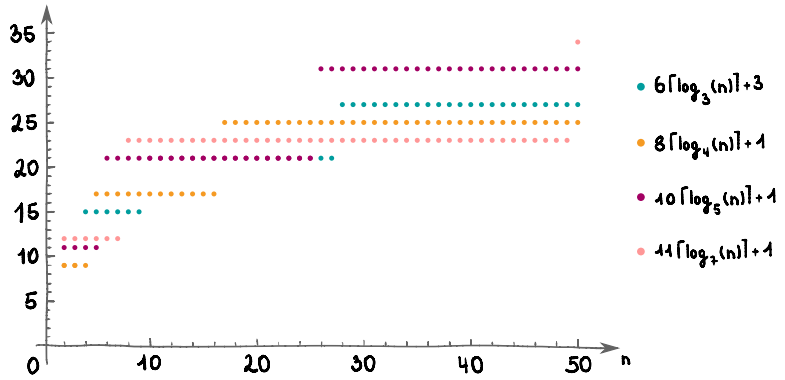

Figure 3.12: *Different upper bounds on the number of Pauli settings for two-body overlapping tomography on an n-qubit system as a function of n.* Green: upper bound from [53]. Orange: upper bound from the recursive construction with $\alpha = 4$. Purple: upper bound from the recursive construction with $\alpha = 5$. Pink: upper bound from the recursive construction with $\alpha = 7$. Figure taken from [E].

Proposition 3.3 (Scaling from covering array construction [E])**.** *The minimal number of Pauli settings $\phi_2(n)$ to perform two-body overlapping tomography of an n-qubit system satisfies*

$$\phi_2(n) \leq (\phi_2(\alpha) - 1)\,\lceil \log_\alpha(n) \rceil + 1, \tag{3.12}$$

for any $\alpha \in \mathbb{N}$ and $\alpha \geq 2$.

Proof. By fixing $n_1 = \alpha$ and setting $n_2 = n$, we can rewrite Eq. (3.11) as $\phi_2(\alpha n) \leq \phi_2(\alpha) + \phi_2(n) - 1$. Next, we define k such that $n = \alpha^k$, and introduce $\xi(k) = \phi_2(\alpha^k)$. The inequality thus reads $\xi(k+1) \leq \phi_2(\alpha) + \xi(k) - 1$. By recurrence and using the fact that $\xi(1) = \phi_2(\alpha)$, we obtain $\xi(k) \leq (k-1)\,(\phi_2(\alpha) - 1) + \phi_2(\alpha)$, which holds for $k \in \mathbb{N}^+$. Rearranging the terms we get $\phi_2(\alpha^k) \leq k(\phi_2(\alpha) - 1) + 1$, and ultimately $\phi_2(n) \leq \log_\alpha(n)(\phi_2(\alpha) - 1) + 1$, for all n such that $\log_\alpha(n) \in \mathbb{N}^+$. Since ϕ_2 is monotonically increasing, Eq. (3.12) is proved for all $n \geq 2$. □

In Figure 3.12, we compare this scaling for different values of α for which we know $\phi_2(\alpha)$, to the scaling of [53] given in Eq. (3.9).

Similar recursive constructions exist for $k > 2$, for instance, it can be shown that [34, 143]

$$\phi_3(2n) \leq \phi_3(n) + 2\phi_2(n). \tag{3.13}$$

For the explicit construction and for larger strengths, we refer the reader to

the reviews [34, 143] and to the references therein.

Lastly, we note that significant effort has been deployed by the combinatorial designs community to obtain small covering arrays, which directly translates to Pauli sets. For readers interested by the smallest Pauli sets known up to date for a given number of qubits and a given strength, we refer to the online tables [33, 142] and the references therein.

3.2 Minimal settings for overlapping tomography

The previous section aimed to obtain sets of Pauli operators that, once repeatedly measured on independent copies of an n-qubit state ϱ, enable the reconstruction of its marginals. Although Pauli settings are an obvious choice to perform multi-qubit tomography, in most photonic experimental implementations, linear combinations of Pauli measurement are just as easy to perform. In the context of minimising the number of settings, this point is highly relevant. Indeed, we have shown that partial tomography of strength k with Pauli settings cannot in general be performed with the minimal number of projective measurement settings of 3^k. In this section, we show that allowing general (product) projective measurements on qubits reduces the number of settings needed to perform the same task. We first rigorously state the problem and give keys to solve it in Section 3.2.1, then consider the particular case of two-body tomography of a six-qubit state for which we numerically optimise measurement directions in Section 3.2.2.

3.2.1 Random measurement directions

Let us start with a few definitions. We aim to minimise the number L of measurement settings $\mathcal{M}_\alpha$, with $\alpha \in [L]$, defined as

$$\mathcal{M}_\alpha = \bigotimes_{i=1}^{n} \mathbf{v}_\alpha^{(i)} \cdot (X, Y, Z), \tag{3.14}$$

where $\{\mathbf{v}_\alpha^{(i)} \in \mathbb{R}^3 \mid \alpha \in [L], i \in [n]\}$ are three-dimensional real vectors, and where we used the notation $\mathbf{v} \cdot (X, Y, Z) = v_1 X + v_2 Y + v_3 Z$, with $\mathbf{v} = (v_1, v_2, v_3)^T$. The settings $\mathcal{M}_\alpha$, with $\alpha \in [L]$, are physical n-qubit observables, thus they correspond to projective measurements (see Section 1.1). We call $\otimes_{i=1}^n \mathbf{v}_\alpha^{(i)}$ the measurement direction of the setting α, and $\mathbf{v}_\alpha^{(i)}$ the measurement direction of the setting α on the ith qubit, with $\alpha \in [L]$ and

$i \in [n]$. Without loss of generality, the measurement directions are assumed to be normalised. Notice that taking the measurement directions to be from the standard basis renders the Pauli operators as measurement settings.

For the set $\{\mathcal{M}_\alpha\}_{\alpha=1}^{L}$ to be tomographically complete for a given k-set of qubits $\mathcal{S}$, it is necessary and sufficient that the measurement directions on those k qubits form a (possibly overcomplete) basis of $\mathbb{R}^{3^k}$, i.e.,

$$\operatorname{span}\left(\left\{\bigotimes_{i\in\mathcal{S}} \mathbf{v}_\alpha^{(i)}\right\}_{\alpha=1}^{L}\right) = \mathbb{R}^{3^k}. \tag{3.15}$$

Remarkably, by choosing the measurement directions for each setting $\mathcal{M}_\alpha$ randomly, with $\alpha \in [L]$, it is sufficient to consider $L = 3^k$ measurement settings to perform k-body overlapping tomography of any n-qubit system, independently of its size. In order to show this, we first introduce the following lemma, whose proof is given in [E] and in [157].

Lemma 3.1 (Linear independence of tensor products [E], [157])**.** *Given $k, r \in \mathbb{N}^+$, let $\mathbf{v}_\alpha^{(i)} \in \mathbb{R}^r$ for all $i \in [k]$ and $\alpha \in [r^k]$ be independently and identically distributed (i.i.d.) vectors with respect to the uniform distribution on the unit sphere in $\mathbb{R}^r$. Then, it holds almost surely that*

$$\operatorname{span}\left(\left\{\bigotimes_{i=1}^{k} \mathbf{v}_\alpha^{(i)}\right\}_{\alpha=1}^{r^k}\right) = \mathbb{R}^{r^k}, \tag{3.16}$$

i.e., the products of these vectors are linearly independent and thus form a basis of $\mathbb{R}^{r^k}$.

Intuitively this makes sense: Randomly chosen vectors should be linearly independent, even if tensor products. The connection with Eq. (3.15) is direct, hence the following proposition holds trivially.

Proposition 3.4 (Measurement directions for partial tomography [E], [157])**.** *Let*

$$\mathcal{M}_\alpha = \bigotimes_{i=1}^{n} \mathbf{v}_\alpha^{(i)} \cdot (X, Y, Z) \quad \forall \alpha \in [3^k] \tag{3.17}$$

be n-qubit measurement settings with i.i.d. measurement directions $\mathbf{v}_\alpha^{(i)} \in \mathbb{R}^3$ for all $i \in [k]$ and $\alpha \in [3^k]$ with respect to the uniform distribution on the unit sphere in $\mathbb{R}^3$. Then $\{\mathcal{M}_\alpha\}_{\alpha=1}^{3^k}$ is tomographically complete for all k-sets of qubits.

We note that the proof of Lemma 3.1 does not depend on local dimen-

sions and thus shows that k-body overlapping tomography of qudit systems of arbitrary local dimension d can be performed with $(d^2-1)^k$ settings.

3.2.2 Numerically optimised measurement directions

Nevertheless, it is reasonable to expect that all sets of measurement directions do not perform equally good with respect to confidence regions for a fixed number of samples. In what follows, we aim to find measurement directions for two-body overlapping tomography of a six-qubit state, i.e., $9 \times 6 = 54$ local measurement directions that lead to small confidence regions for each pair of qubits $\mathcal{S} \subset [6]$ with $|\mathcal{S}| = 2$. Specifically, we analyse the confidence region C_A of [41], which we have introduced in Section 1.5. We thus use the linear inversion state estimate $\hat{\varrho}$ of the true state ϱ, which we recall from Section 1.5 satisfies

$$\Pr[\|\hat{\varrho} - \varrho\| \leq \varepsilon\sigma] \geq 1 - \delta, \tag{3.18}$$

where $1-\delta \in [0,1]$ is the confidence level, $\varepsilon = 3\sqrt{u}(\sqrt{u} + \sqrt{u+1})$, with $u = {}^2\!/_{9N} \log(8/\delta)$ and where the norm $\|\cdot\|$ is the Hilbert-Schmidt norm. The quantity σ is given by

$$\sigma = \max_{k \in [d^2]} \left\| M_k^+ \right\|, \tag{3.19}$$

where M_k^+ is the kth column vector of M^+, the pseudo-inverse of the measurement map M (see Section 1.5, and in particular Eq. (1.41)).

In the context of overlapping tomography, each k-set of qubits $\mathcal{S} \subset [n]$ with $|\mathcal{S}| = k$ corresponds one estimate $\hat{\varrho}_{\mathcal{S}}$, hence leading to $\binom{n}{k}$ confidence regions, with corresponding $\sigma_{\mathcal{S}}$. We focus our attention on $\max_{\mathcal{S}} \sigma_{\mathcal{S}} = \sigma_{\max}$, such that we can phrase Eq. (3.18) as

$$\Pr[\|\hat{\varrho}_{\mathcal{S}} - \varrho_{\mathcal{S}}\| \leq \varepsilon\sigma_{\max}] \geq 1 - \delta \tag{3.20}$$

for all pairs of qubits $\mathcal{S}$.

Intuitively, we would expect measurement directions that are spread out in $\mathbb{R}^9$ to lead to smaller confidence regions. Indeed, in Appendix A, we show how $\sigma_{\mathcal{S}}$ is related to the volume spanned by the measurement directions $\{\mathbf{v}_\alpha^{(i)} \otimes \mathbf{v}_\alpha^{(j)}\}_{\alpha=1}^9$, for each pair of qubits $\mathcal{S} = \{i, j\}$. Formally, the volume $\mathcal{V}_{\mathcal{S}}$ spanned by the vectors is given by $|\det(Z_{\mathcal{S}})|$, where $Z_{\mathcal{S}}$ is the 9×9-dimensional matrix whose columns are $\mathbf{v}_\alpha^{(i)} \otimes \mathbf{v}_\alpha^{(j)}$ for all $\alpha \in [9]$. We

use $\mathcal{V}_\mathcal{S}$ as a figure of merit.

Taking a (product) orthonormal basis as measurement directions for the pair $\mathcal{S} = \{i, j\}$ directly leads to the maximum of $\mathcal{V}_\mathcal{S} = 1$. One obvious choice is to take the standard basis, resulting in $Z_\mathcal{S}$ to be the nine-dimensional identity matrix. We recall that this corresponds to Pauli measurements (see Eq. (3.14)). However, since the number of Pauli settings needed for two-body overlapping tomography of a six-qubit system is given by $\phi_2(6) = 12 > 9$, it is not possible to find 54 local measurement directions $\mathbf{v}_\alpha^{(i)}$, with $\alpha \in [9]$ and $i \in [6]$, such that for every pair of qubits $\mathcal{S} = \{i, j\}$, the nine vectors $\mathbf{v}_\alpha^{(i)} \otimes \mathbf{v}_\alpha^{(j)}$, with $\alpha \in [9]$, form the standard basis. As a consequence, our goal is to find 54 local measurement directions $\mathbf{v}_\alpha^{(i)}$, with $\alpha \in [9]$ and $i \in [6]$, such that for each of the 15 pairs of qubits $\mathcal{S}$, the volume $\mathcal{V}_\mathcal{S}$ is large. As a direct maximisation $\min_\mathcal{S} \mathcal{V}_\mathcal{S}$ is not easy, we introduce the objective function

$$f\left(\{\mathbf{v}_\alpha^{(i)} \in \mathbb{R}^3 \mid \alpha \in [9], i \in [6]\}\right) = w_1 \sum_\mathcal{S} \mathcal{V}_\mathcal{S} - w_2 \sum_\mathcal{S} \mathcal{V}_\mathcal{S}^2 \tag{3.21}$$

with weights $w_1, w_2 \geq 0$ and $w_1^2 + w_2^2 = 1$, and where the sums run over all pairs of numbers in $[6]$. This is inspired by modern portfolio theory, or mean-variance analysis, which is a framework for assembling a collection of investments such that the expected return is maximised for a given level of risk in finance [104]. The theory has initially been introduced by Markowitz in 1952, for which he was eventually awarded the Nobel Memorial Prize in Economic Sciences in 1990. Using the Broyden-Fletcher-Goldfarb-Shanno (BFGS) algorithm, we maximised the objective function Eq. (3.21) for different weights, and found that for $w_2 \lesssim \cos(\pi/5)$, the achieved $\mathcal{V}_\mathcal{S}$ are equal for all pairs of qubits $\mathcal{S}$ (see Figure 3.13). Using this approach, we were able to find 54 measurement directions with $\sigma_{\max} \simeq 7.65$. We discuss in the next section how this reflects on the number of samples.

To further refine our measurements, we arranged the local directions to form three orthonormal bases. Specifically, for each qubit $i \in [6]$, we partitioned the nine vectors $\mathbf{v}_\alpha^{(i)}$, for all $\alpha \in [9]$, into three orthonormal bases. This approach allowed us to achieve measurement directions with $\sigma_{\max} \simeq 7.78$. These measurement directions and their orthonormal partitioning are provided in Table A.1 of Appendix A.

The measurement directions obtained through numerical optimisation were subsequently used in a six-photon experiment to perform two-body overlapping tomography of the six-photon system [E]. The minimal Pauli set with 12 settings (see Figure 3.5) has been implemented as well. The

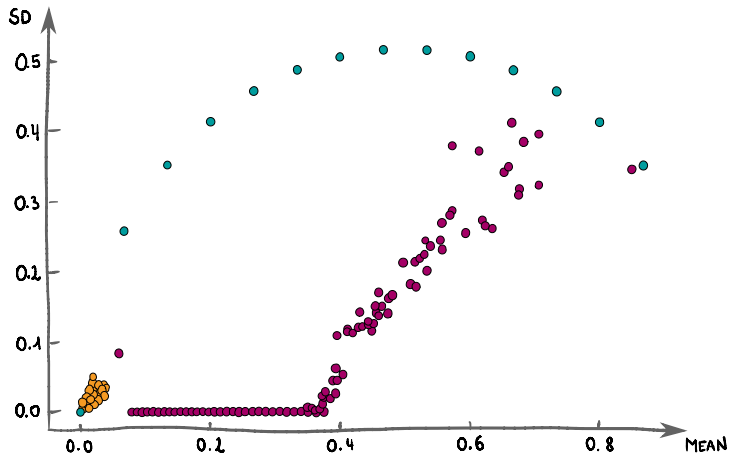

Figure 3.13: *Mean and standard deviation of the volumes.* Each point corresponds to one set of measurement directions, with its x-coordinate being the mean of all 15 volumes, and its y-coordinate being the standard deviation. The orange points correspond to randomly-chosen measurement directions as in Proposition 3.4, the purple points correspond to optimised directions with different weights (see Eq. (3.21)), and the green points correspond to cases where the vectors all are from the standard basis (i.e., the volumes are either zero or one and correspond to Pauli settings). Figure taken from [E].

setup of the experiment is presented in Figure 3.14, and we refer to [E] for a detailed explanation. In a nutshell, ultraviolet pulses (390nm wavelength, 80MHz repetition rate, 300mW power) are directed onto a special type of crystal (β-barium borate) using a lens to produce three pairs of photons through spontaneous parametric down-conversion. The photons are then recollimated using additional lenses, filtered to ensure the desired spectral and spatial properties, and combined into a single path using a polarising beam splitter, producing a six photon Dicke state $|D_{6,2,3}\rangle = 1/2\sqrt{5}\sum_{\pi}|\pi\rangle$, where the sum runs over all permutations of $(0,0,0,1,1,1)$.

Next, the six indistinguishable photons are randomly distributed into six different paths using a series of beam splitters. This arrangement gives a maximum success rate of $5/324$ for detecting one photon in each measurement part. Finally, the polarisation of the photons in each path is analysed using a setup consisting of wave plates and single-photon detectors (the measurement part), as shown in Figure 3.14. In the measurement part, the 12 Pauli settings of Figure 3.5 are implemented, as well as the nine optimised measurement directions (see Table A.1 of Appendix A). Each setting was measured for two hours, with a rate of 7.0 per minute [E].

Using the data of each measurement scheme, all two-qubit marginals

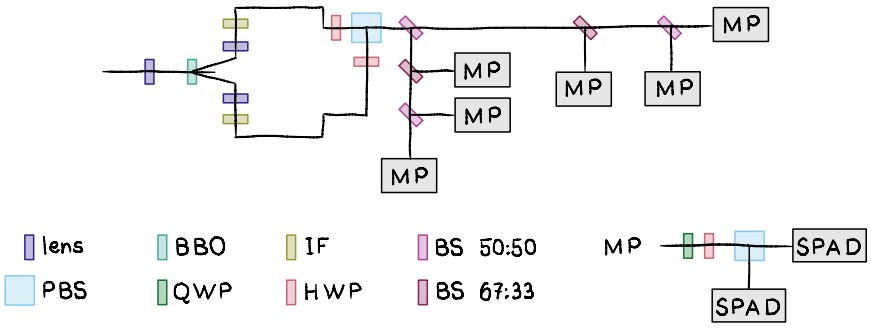

Figure 3.14: *Experimental setup for two-body overlapping tomography of a six-photon system.* A six-photon state is generated, and each photon is detected in a measurement part (MP) by a single-photon avalanche detector (SPAD). PBS: polarising beam splitter. BBO: β-barium borate crystal. QWP: quarter wave plate. HWP: half wave plate. IF: interference filter. BS: beam splitter. Figure adapted from [E].

can be reconstructed. As $|D_{6,2,3}\rangle$ is a symmetric state, all its marginal states of a given dimension are equal. The reconstructed marginals and their corresponding confidence regions are presented in [40], using the confidence region C_A developed in [41]. For alternative estimates based on maximum likelihood estimation, see [E]. For completeness, we present in Figure 3.15 the different mixed state fidelities[7] of the reconstructed states to the two-qubit marginal states of the Dicke state $|D_{6,2,3}\rangle$ [E]. However, we emphasise that the goal of quantum state tomography is to reconstruct the complete density operator of a quantum system, not merely to estimate a fidelity.

3.3 Discussion on the sample cost

Throughout this chapter, we have given several methods to construct measurement settings for performing k-body overlapping tomography of n-qubit systems, with $k < n$. In this section, we compare the different measurement schemes in terms of the number of samples of the n-qubit state to achieve the same radius $\varepsilon\sigma = 0.1$ in the confidence region. We specifically look at the case of $n = 6$ qubits and $k = 2$. For each measurement scheme, we compute $\sigma_{\max} = \max_{\mathcal{S}} \sigma_{\mathcal{S}}$, which we recall only depends on the measurement settings.

When quantum state tomography of a two-qubit state is performed with the nine two-body Pauli settings, the unique σ is equal to five [41]. Therefore,

[7] Given two density operators ϱ and τ, their mixed state fidelity is $F(\varrho, \tau) = \mathrm{tr}\left(\sqrt{\sqrt{\tau}\varrho\sqrt{\tau}}\right)$ [152].

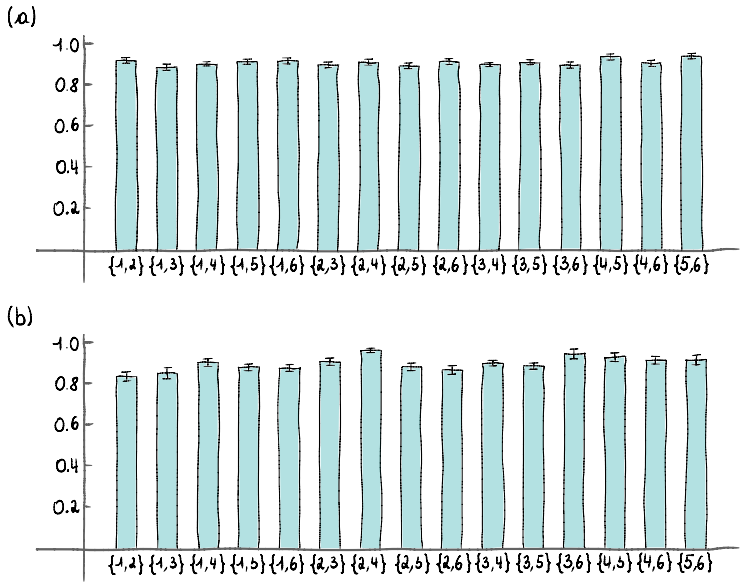

Figure 3.15: *Mixed state fidelity* of each reconstructed state through maximum likelihood estimation compared to the two-quit marginal state of the six-qubit Dicke state $|D_{6,2,3}\rangle$. (a) The measurement settings are from the minimal Pauli set of Figure 3.5. (b) The measurement settings are obtained through the numerical optimisation presented in this section, and explicitly given in Table A.1 of Appendix A. Figures adapted from [E].

uniform Pauli sets have $\sigma_{\max} = 5 = \sigma_{\text{Pauli}}$. A minimal uniform Pauli set for two-body overlapping tomography of a six-qubit system is for instance give by the first six rows of Figure 3.7, and are made of 18 settings. The 12 minimal Pauli settings obtained through Proposition 3.1 (see Figure 3.5) lead to $\sigma_{\max} = 6.52 = \sigma_{\text{bin. prog.}}$. The measurement settings optimised in the previous section achieve $\sigma_{\max} = 7.65 = \sigma_{\text{opti.}}$ and $\sigma_{\max} = 7.78 = \sigma_{\text{orth. opti.}}$ in the case of unrestricted optimisation and orthonormal basis optimisation respectively. Finally, we want to compare with the 15 settings from [53] and the 21 settings from [38], [18], and [165], which respectively have $\sigma_{\max} = 7.81 = \sigma_{15}$ and $\sigma_{\max} = 10.7 = \sigma_{21}$.

We fix the radius $\varepsilon\sigma_{\max}$ to 0.1, and report in Table 3.2 how many more samples are needed when comparing a scheme with a larger $\sigma_{\max}$ to one with a smaller $\sigma_{\max}$. First, we directly notice that the construction from [38, 18] that was experimentally implemented in [165] has the worst performance: Comparing to minimal Pauli sets, it needs 168% more samples to achieve the same confidence level. Second, the minimal uniform Pauli set clearly requires less samples than any other scheme. It comes the closest to the

	σ_{Pauli}	$\sigma_{\text{bin. prog.}}$	$\sigma_{\text{opti.}}$	$\sigma_{\text{orth. opti.}}$	σ_{15}	σ_{21}
σ_{Pauli}	·	69.5%	133%	141%	143%	355%
$\sigma_{\text{bin. prog.}}$	69.5%	·	37.5%	42.2%	43.2%	168%
$\sigma_{\text{opti.}}$	133%	37.5%	·	3.41%	4.21%	95.1%
$\sigma_{\text{orth. opti.}}$	141%	42.2%	3.41%	·	0.769%	88.7%
σ_{15}	143%	43.2%	4.21%	0.769%	·	87.3%
σ_{21}	355%	168%	95.1%	88.7%	87.3%	·

Minimal uniform Pauli set, σ_{Pauli}	18
Minimal Pauli set, $\sigma_{\text{bin. prog.}}$	12
Optimised directions, $\sigma_{\text{opti.}}$	9
Optimised directions (OTB), $\sigma_{\text{orth. opti.}}$	9
Scheme from [53], σ_{15}	15
Scheme from [38, 18], σ_{21}	21

Table 3.2: Comparison of the different measurement schemes. For example, the optimised directions with orthogonal bases (OTB) with $\sigma_{\text{orth. opti.}} = 7.78$ requires 141% more samples than when using a minimal uniform Pauli set with $\sigma_{\text{Pauli}} = 5$ to achieve the same radius $\varepsilon\sigma_{\max} = 0.1$. Below the table, we recall the number of settings for each scheme (OTB stands for orthogonal bases).

minimal Pauli set that (only) requires 69.5% more samples but six settings less, and the strongest difference is with the scheme from [38, 18], which requires 355% more samples and three more settings. Table 3.2 also shows that there is little difference between the unrestricted optimised settings and the settings partitioned in three orthonormal basis per qubit (3.4% more for the settings partitioned in basis). Interestingly, the construction by García-Pérez and coauthors [53] has a very similar performance to the optimised settings, with only 4.21% and 0.769% more sample needing comparing to the unrestricted and orthonormal bases optimisation respectively. Finally, the analysis shows that requiring the minimal number of measurement settings (i.e., nine) for two-body overlapping tomography of six qubits comes at a cost of more measurement samples (of the order of 40% more) to reach the same confidence level than the optimal Pauli settings (which require 12 measurement settings).

3.4 Discussion

In this chapter, we presented several methods for the measurement scheduling for marginal tomography of multi-qubit systems. We began by focusing on Pauli tomography, providing numerical methods and constructions to obtain minimal Pauli sets. Notably, we proved that for systems having

a connectivity graph with a chromatic number of at most four, two-body marginal tomography can always be performed with nine Pauli settings, regardless of the number of qubits. We further explored the specific case of overlapping tomography, demonstrating its equivalence to the problem of finding covering arrays in combinatorial designs, and derived an upper bound on the number of settings for strength two, which we compared to previous results.

Next, we demonstrated that when measurement settings are not restricted to Pauli settings, k-body overlapping tomography can always be performed with 3^k projective measurement settings, irrespective of the size of the multi-qubit system. Additionally, we optimised measurement directions for the specific case of six qubits and strength two, which were experimentally implemented in [E], alongside the minimal Pauli set.

Finally, in Section 3.4, we compared the different measurement schemes based on the number of samples needed to achieve the same level of confidence in the reconstructed states.

Although we addressed a fundamental problem for overlapping tomography by finding minimal Pauli sets, several questions remain open. While we proved that 3^k measurement directions can be chosen randomly, this does not result in a satisfactory sample cost. Better constructions could be obtained through numerical optimisation, but ideally, an analytical construction should be found. Moreover, the optimality of the colouring construction described in Section 3.1.4 is still unresolved: A counterexample or a proof of optimality would be valuable. Since we have tested every graph with up to eight vertices, any counterexample would need to involve at least nine parties.

We conclude this chapter by saying that deciding which measurement scheme to use depends on the practical implementation of the protocol. If the implementation is highly sensitive to setting changes, we recommend using the 3^k minimal settings. On the other hand, if the number of settings is less critical than the number of state samples, minimal uniform Pauli sets are preferable. As a compromise, minimal Pauli sets offer a small number of settings (scaling logarithmically with the number of qubits) and appear to require fewer samples than the minimal settings. Further research into the sample cost analysis and generalisation to arbitrary strengths and numbers of qubits would be highly relevant.

Chapter 4

Entanglement in quantum networks

Network entanglement is an emerging area of research within multipartite entanglement theory, explored in works such as [111], [101], and [94]. Substantial efforts have been dedicated to characterising the states that can be prepared in quantum networks without the usage of classical communication. As discussed in Section 1.3.4, the absence of classical communication prevents the execution of crucial protocols, such as quantum teleportation or entanglement swapping, which are typically employed to generate global states shared by distant parties (see e.g. [7]). Despite classical communication being considered an inexpensive resource in quantum communication protocols, it introduces practical challenges. The transmission of classical information between network nodes introduces time delays, which can be particularly undesirable given the current limitations of quantum memories.

Moreover, with the rapid development in the implementation of quantum networks [30, 121], there is a growing demand for verification techniques for network structures. Indeed, to perform tasks across a quantum network, such as a quantum key distribution protocol, the network parties need reliable information about the network they share.

In this chapter, we contribute to the topic of network entanglement and certification through several key investigations. We begin by conducting a thorough analysis of the covariance matrices (CMs) of network states in Section 4.1, by presenting alternative proofs for their block decomposition [3]. These results provide insights into the structural constraints imposed on the CM by the network states. Next, we focus on states with symmetric properties, where we demonstrate in Section 4.2 that large classes of

symmetric states cannot be prepared within quantum networks. Finally, we turn our attention to certification techniques of network elements by considering two different aspects: First, we derive in Section 4.3 simple testable inequalities that allow to verify that a certain link in the network is properly working, i.e., distributing entanglement. Second, in Section 4.4 we aim to certify the topology of the whole network by deriving rigorous hypotheses tests based on fidelities to the source states. This protocol has been experimentally implemented, and the hypotheses are tested based on the experimental data.

4.1 Covariance matrices of network states

As a first tool for the investigation of network states, we consider covariance matrices (see Section 1.3.3 for definitions) and restrict our attention to networks without shared randomness. The results of this section are published in [C] and we closely follow the presentation in the article. Covariance matrices have already been used to derive necessary criteria for network entanglement without shared randomness in [3, 94, 162, 11]. In [3], the authors formulate a necessary condition for a probability distribution to arise from measurements performed on a quantum network state. The condition expresses that the covariance matrix of the probability distribution can be decomposed into a sum of PSD block matrices,[1] and can be formulated as an SDP. This result was applied in [94] to derive practical analytical criteria for networks with dichotomic measurements and for networks with bipartite sources. More recently, similar SDPs were developed in [162] for the case of LOSR networks, with extra assumptions on rank and purity. Finally, striking generality, the authors of [11] showed that in the case of NCDS networks, the block decomposition criterion holds for all generalised probabilistic theories [120].

In this section, we propose an alternative proof to the block decomposition of the CM of triangle network state derived in [3]. From it, we obtain an analytical, computable necessary criterion for a state to arise from a triangle network. We later show how this result can be extended to NCDS networks. Although the results presented in this chapter are valid only in the context of finite-dimensional Hilbert spaces, as mentioned in Section 1.3.3 CMs are also well suited for continuous variable systems. Thus, a potential future

[1] We call this decomposition into a sum of PSD block matrices the *block decomposition of a covariance matrix*.

research direction is to investigate how these results can be extended to the infinite-dimensional case since.

4.1.1 Covariance matrices for tripartite states

Since in network scenarios the parties can only access their local systems, it is sensible to choose observables that only act on one party at a time. Explicitly, we choose N observables per party, $A_i \otimes \mathbb{1}_B \otimes \mathbb{1}_C$, $\mathbb{1}_A \otimes B_i \otimes \mathbb{1}_C$, and $\mathbb{1}_A \otimes \mathbb{1}_B \otimes C_i$, with $i \in [N]$, and we use the notation $\{A_i, B_i, C_i\}_{i=1}^N = \{A_i \otimes \mathbb{1}_B \otimes \mathbb{1}_C\}_{i=1}^N \cup \{\mathbb{1}_A \otimes B_i \otimes \mathbb{1}_C\}_{i=1}^N \cup \{\mathbb{1}_A \otimes \mathbb{1}_B \otimes C_i\}_{i=1}^N$. Similarly to Eq. (1.15), the CM of a tripartite state ϱ has the following block structure,

$$\Gamma(\{A_i, B_i, C_i\}_{i=1}^N, \varrho) = \begin{pmatrix} \Gamma_A & \gamma_E & \gamma_F \\ \gamma_E^T & \Gamma_B & \gamma_G \\ \gamma_F^T & \gamma_G^T & \Gamma_C \end{pmatrix} \tag{4.1}$$

where $\Gamma_A = \Gamma(\{A_i\}_{i=1}^N, \varrho^{(A)})$ is a CM of the marginal $\varrho^{(A)}$. The matrices Γ_B and Γ_C have analogous expressions. The entries of the off-diagonal block γ_E are given by the real numbers

$$[\gamma_E]_{mn} = \langle A_m \otimes B_n \rangle_\varrho - \langle A_m \rangle_\varrho \langle B_n \rangle_\varrho \quad \forall m, n \in [N], \tag{4.2}$$

with identity operators padded where needed. Notice that Eq. (4.2) can be defined equivalently by taking the expectation values on $\varrho^{(AB)}$. Again, the matrices γ_F and γ_G are defined in a similar way.

4.1.2 Basic triangle network

In this section, we derive the explicit structure of CMs of BTN states. Given three source states $\varrho_a \in \mathcal{S}(\mathcal{H}_{B_2} \otimes \mathcal{H}_{C_1})$, $\varrho_b \in \mathcal{S}(\mathcal{H}_{C_2} \otimes \mathcal{H}_{A_1})$, and $\varrho_c \in \mathcal{S}(\mathcal{H}_{A_2} \otimes \mathcal{H}_{B_1})$, we recall that the BTN state reads

$$\varrho_{\text{BTN}} = \varrho_b \otimes \varrho_c \otimes \varrho_a, \tag{4.3}$$

as defined in Definition 1.8. This network is represented in Figure 4.1 (a). Let us first define what we call the reduced observable $A_i^{(2)}$ of A_i, with $i \in [N]$, which describes an effective observable on the system A_2. It is given by

$$A_i^{(2)} = \text{tr}_{A_1}\left(A_i(\varrho_{\text{BTN}}^{(A_1)} \otimes \mathbb{1}_{A_2})\right) \quad \forall i \in [N]. \tag{4.4}$$

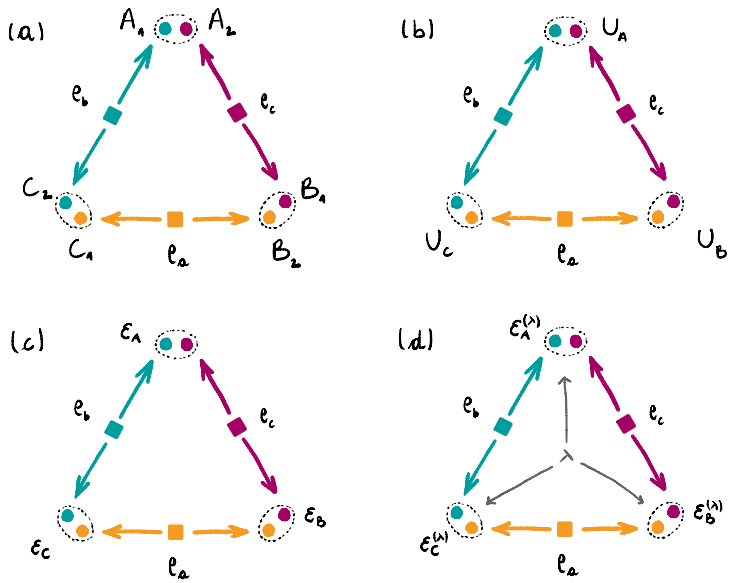

Figure 4.1: *Illustration of the four definitions of triangle network states.* (a) BTN: Three potentially entangled source states ϱ_a, ϱ_b and ϱ_c are distributed to three nodes $A = A_1A_2$, $B = B_1B_2$ and $C = C_1C_2$. (b) UTN: The three parties A, B and C perform unitary operations U_A, U_B and U_C on their respective systems. (c) CTN: The operations are no longer restricted to unitary operation, but may be any CPTP maps $\mathcal{E}_A$, $\mathcal{E}_B$ and $\mathcal{E}_C$. (d) LOSR triangle network: The local operation may be coordinated by a shared random variable $\lambda \in [L]$.

We note that A_i acts both on system A_1 and on system A_2, so $A_i^{(2)}$ is an operator acting on states of A_2, where the effect of $\varrho_b = \varrho_{\text{BTN}}^{(A_1C_2)}$ has been taken into account, with $i \in [N]$. We define $B_i^{(1)}$ for all $i \in [N]$ similarly and use the notation $\{A_i^{(2)}, B_i^{(1)}\}_{i=1}^N = \{A_i^{(2)} \otimes \mathbb{1}_{B_1}\}_{i=1}^N \cup \{\mathbb{1}_{A_2} \otimes B_i^{(1)}\}_{i=1}^N$. The off-diagonal blocks of Eq. (4.1) can be expressed using the reduced observables, that is,

$$[\gamma_E]_{mn} = \langle A_m^{(2)} \otimes B_n^{(1)} \rangle_{\varrho_{\text{BTN}}^{(A_2B_1)}} - \langle A_m^{(2)} \rangle_{\varrho_{\text{BTN}}^{(A_2B_1)}} \langle B_n^{(1)} \rangle_{\varrho_{\text{BTN}}^{(A_2B_1)}} \quad \forall m, n \in [N]. \tag{4.5}$$

To see this, notice that the reduces state $\varrho_{\text{BTN}}^{(AB)}$ is a product state with respect to the partition $A_1 \mid A_2B_1 \mid B_2$ and use a local basis decomposition of the observables A_m and B_n, for all $m, n \in [N]$ (see Appendix B). All expectation values in Eq. (4.5) are taken with respect to the state $\varrho_{\text{BTN}}^{(A_2B_1)}$, which is nothing but ϱ_c.

This representation shows that γ_E can be computed using only the reduced observables on the state $\varrho_{\text{BTN}}^{(A_2B_1)}$, which is ultimately crucial for the

block decomposition of CMs of BTN states. This is a direct consequence of the fact that the marginal states on A, B and C are product states. Let us now introduce our first proposition.

Proposition 4.1 (Block decomposition for CMs of BTN states [C])**.** *The* CM *of a* BTN *state with local observables* $\{A_i, B_i, C_i\}_{i=1}^N$ *can be decomposed as*

$$\begin{aligned}\Gamma_{\text{BTN}} &= \Gamma(\{A_i, B_i, C_i\}_{i=1}^N, \varrho_{\text{BTN}}) \\ &= \underbrace{\begin{pmatrix} \Gamma_{A_2} & \gamma_E & 0 \\ \gamma_E^T & \Gamma_{B_1} & 0 \\ 0 & 0 & 0 \end{pmatrix}}_{T_c} + \underbrace{\begin{pmatrix} \Gamma_{A_1} & 0 & \gamma_F \\ 0 & 0 & 0 \\ \gamma_F^T & 0 & \Gamma_{C_2} \end{pmatrix}}_{T_b} + \underbrace{\begin{pmatrix} 0 & 0 & 0 \\ 0 & \Gamma_{B_2} & \gamma_G \\ 0 & \gamma_G^T & \Gamma_{C_1} \end{pmatrix}}_{T_a} + \underbrace{\begin{pmatrix} R_A & 0 & 0 \\ 0 & R_B & 0 \\ 0 & 0 & R_C \end{pmatrix}}_{R}\end{aligned} \tag{4.6}$$

where the matrices T_a, T_b and T_c are CMs *for the state-dependent reduced observables, i.e.,*

$$T_c = \Gamma(\{A_i^{(2)}, B_i^{(1)}\}_{i=1}^N, \varrho_{\text{BTN}}^{(A_2B_1)}). \tag{4.7}$$

and analogously for T_b and T_a. The matrix R is PSD*.*

Using Eq. (4.5), it is only left to show that $R_A = \Gamma_A - \Gamma_{A_1} - \Gamma_{A_2}$ is PSD, as well as R_B and R_C. To do this, we show that $\mathbf{x}^\dagger R_A \mathbf{x}$ can be written as the trace of a product of PSD matrices for all $\mathbf{x} \in \mathbb{C}^N$. The proof is given in Appendix B.

Armed with this, we can now derive the structure of the CM of a BTN state in the case of the observables being full sets of local orthogonal observables. More precisely, we take $\{A_i\}_{i=1}^{d^4} = \{\sigma_\alpha^{(A_1)} \otimes \sigma_\beta^{(A_2)}\}_{\alpha,\beta=1}^{d^2}$, where $\{\sigma_\alpha^{(A_k)}\}_{\alpha=1}^{d^2}$ is a set of orthogonal observables acting on states of the system A_k such that $\text{tr}\left(\sigma_\alpha^{(A_k)} \sigma_{\alpha'}^{(A_k)}\right) = d\delta_{\alpha\alpha'}$, with $\alpha, \alpha' \in [d^2]$ and $k = 1, 2$. This is done in a similar way for the systems B and C. When the situation is explicit enough, we drop the superscripts. For qubit systems, the Pauli operators together with the identity operator are an obvious choice. With such sets of observables, a direct computation (see Appendix B) shows that

$$\begin{aligned} R_X =& \Gamma_X - \Gamma_{X_1} - \Gamma_{X_2} \\ =& \Gamma\left(\{\sigma_\alpha\}_{\alpha=1}^{d^2}, \varrho_{\text{BTN}}^{(X_1)}\right) \otimes \Gamma\left(\{\sigma_\alpha\}_{\alpha=1}^{d^2}, \varrho_{\text{BTN}}^{(X_2)}\right), \quad \forall X = A, B, C \end{aligned} \tag{4.8}$$

and since CMs are PSD matrices, Proposition 4.1 is trivially satisfied. The structure of the matrices T_a, T_b and T_c can also be further explored. First, let

us compute the reduced observables

$$A^{(2)}_{(\alpha-1)d^2+\beta} = \mathrm{tr}\left(\sigma_\alpha \varrho^{(A_1)}_{\mathrm{BTN}}\right)\sigma_\beta = a^{(1)}_\alpha \sigma_\beta \tag{4.9}$$

where the coefficients $a^{(1)}_\alpha = \mathrm{tr}\left(\sigma_\alpha \varrho^{(A_1)}_{\mathrm{BTN}}\right)$ are nothing but the (real) Bloch coefficients of the marginals, with $\alpha, \beta \in [d^2]$. A direct calculation shows that [C]

$$\Gamma_{A_2} = \mathbf{a}^{(1)}(\mathbf{a}^{(1)})^T \otimes \Gamma(\{\sigma_\alpha\}_{\alpha=1}^{d^2}, \varrho^{(A_2)}_{\mathrm{BTN}}) \tag{4.10}$$

and that

$$\gamma_E = \mathbf{a}^{(1)}(\mathbf{b}^{(2)})^T \otimes \gamma(\{\mathbb{1}\otimes\sigma_\alpha, \sigma_\alpha\otimes\mathbb{1}\}_{\alpha=1}^{d^2}, \varrho^{(A_2B_1)}_{\mathrm{BTN}}) \tag{4.11}$$

with $\mathbf{a}^{(1)} = (a^{(1)}_1, \ldots, a^{(1)}_{d^2})^T \in \mathbb{R}^{d^2}$ and similarly for $\mathbf{b}^{(2)}$. The matrix $\gamma(\{\mathbb{1}\otimes\sigma_\alpha, \sigma_\alpha\otimes\mathbb{1}\}_{\alpha=1}^{d^2}, \varrho^{(A_2B_1)}_{\mathrm{BTN}})$ is the off-diagonal block of the CM with the same observables and state. Finally, we can write

$$T_c = \left[(\mathbf{a}^{(1)} \oplus \mathbf{b}^{(2)})(\mathbf{a}^{(1)} \oplus \mathbf{b}^{(2)})^T\right] \star \Gamma\left(\varrho^{(A_2B_1)}_{\mathrm{BTN}}\right), \tag{4.12}$$

where we omitted the observables $\{\mathbb{1}\otimes\sigma_\alpha, \sigma_\alpha\otimes\mathbb{1}\}_{\alpha=1}^{d^2}$ of the CM, and where $\star$ is the block-wise Kronecker product, the Khatri-Rao product [86, 99]. If A and B are $N \times N$ block matrices, the i,j-th block of their Khatri-Rao product $(A \star B)_{i,j}$ is the Kronecker product of the i,j-th block of A and B, $A_{i,j} \otimes B_{i,j}$, with $i, j \in [N]$. For instance, if A and B are 2×2 block matrices,

$$A = \begin{pmatrix} A_{0,0} & A_{0,1} \\ A_{1,0} & A_{1,1} \end{pmatrix}, \quad B = \begin{pmatrix} B_{0,0} & B_{0,1} \\ B_{1,0} & B_{1,1} \end{pmatrix}, \tag{4.13}$$

we obtain

$$A \star B = \begin{pmatrix} A_{0,0}\otimes B_{0,0} & A_{0,1}\otimes B_{0,1} \\ A_{1,0}\otimes B_{1,0} & A_{1,1}\otimes B_{1,1} \end{pmatrix}. \tag{4.14}$$

Putting the results together, we obtain the following proposition.

Proposition 4.2 (CMs of BTN states with orthogonal observables [C])**.** *Using complete sets of orthogonal observables acting locally, the* CM *of a* BTN *state can be*

decomposed as

$$\begin{aligned}\Gamma_{\text{BTN}} = &\left[(\mathbf{a}^{(1)} \oplus \mathbf{b}^{(2)}) \cdot (\mathbf{a}^{(1)} \oplus \mathbf{b}^{(2)})^T\right] \star \Gamma\left(\varrho_{\text{BTN}}^{(A_2B_1)}\right) \\ &+ \left[(\mathbf{b}^{(1)} \oplus \mathbf{c}^{(2)}) \cdot (\mathbf{b}^{(1)} \oplus \mathbf{c}^{(2)})^T\right] \star \Gamma\left(\varrho_{\text{BTN}}^{(B_2C_1)}\right) \\ &+ \left[(\mathbf{c}^{(1)} \oplus \mathbf{a}^{(2)}) \cdot (\mathbf{c}^{(1)} \oplus \mathbf{a}^{(2)})^T\right] \star \Gamma\left(\varrho_{\text{BTN}}^{(C_2A_1)}\right) \\ &+ \text{diag}\left(\left\{\Gamma\left(\varrho_{\text{BTN}}^{(X_1)}\right) \otimes \Gamma\left(\varrho_{\text{BTN}}^{(X_2)}\right)\right\}_{X\in\{A,B,C\}}\right).\end{aligned} \tag{4.15}$$

Therefore, in order to test compatibility with the BTN scenario for a given state, one can check if its CM can be written like the right-hand side of the above equation. While this may be cumbersome to test, we notice that the matrix $\Gamma_{\text{BTN}} - R$ is also PSD, which can also be used to check compatibility in the following way.

Proposition 4.3 (Positivity condition [C])**.** *The matrix*

$$\begin{aligned}\Xi(\varrho_{\text{BTN}}) = &\Gamma\left(\{\sigma_\alpha^{A_1} \otimes \sigma_\beta^{A_2}, \sigma_\alpha^{B_1} \otimes \sigma_\beta^{B_2}, \sigma_\alpha^{C_1} \otimes \sigma_\beta^{C_2}\}_{\alpha,\beta=1}^{d^2}, \varrho_{\text{BTN}}\right) \\ &- \text{diag}\left(\left\{\Gamma\left(\{\sigma_\alpha^{X_1}\}_{\alpha=1}^{d^2}, \varrho_{\text{BTN}}^{(X_1)}\right) \otimes \Gamma\left(\{\sigma_\alpha^{X_2}\}_{\alpha=1}^{d^2}, \varrho_{\text{BTN}}^{(X_2)}\right)\right\}_{X\in\{A,B,C\}}\right)\end{aligned} \tag{4.16}$$

is PSD.

We note that neither term of the right-hand side of Eq. (4.16) contains the reduced observables, which makes Ξ easy to compute.

An advised reader might point out that in order to verify if a given state is compatible with the BTN scenario, it suffices to test whether ϱ_{BTN} is equal to $\varrho_{\text{BTN}}^{(A_2B_1)} \otimes \varrho_{\text{BTN}}^{(B_2C_1)} \otimes \varrho_{\text{BTN}}^{(C_2A_1)}$, up to reordering of the subsystems. We stress that although this simple equation does answer the question, it requires the knowledge of the full density operator, whereas CM-based criteria only need expectation values of some chosen observables in order to be evaluated.

To close the section on BTN states, we present a few examples. First, we note that the lowest dimensional achievable states are 64-dimensional states (six qubits, or three ququarts[2]) and that the local dimensions cannot be prime numbers. We start with the three-ququart GHZ state

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |333\rangle), \tag{4.17}$$

[2]A ququart (sometimes ququad) is a four-dimensional quantum system.

to which we apply a depolarising channel such that the resulting state reads

$$\varrho(v) = v\,|\psi\rangle\langle\psi| + (1-v)\frac{\mathbb{1}_{64}}{64}, \tag{4.18}$$

where $v \in [0,1]$ is called the visibility. The corresponding Ξ matrix is PSD only for $v = 0$, meaning that the GHZ state cannot be prepared in a BTN network even with a very high amount of noise. The same result is obtained when applied to the state $1/2(|000\rangle + |111\rangle + |222\rangle + |333\rangle)$.

Proposition 4.3 may also be applied to three-ququart Dicke states, which are defined by

$$|D_{3,4,k}\rangle = \mathcal{N} \sum_{i_1,i_2,i_3=1}^{3} \delta_{i_1+i_2+i_3,k}\,|i_1 i_2 i_3\rangle \quad \forall k \in [8], \tag{4.19}$$

with $\mathcal{N}$ being a normalisation factor. For $k = 1$, the preparation of the Dicke state after a depolarising channel in the BTN scenario is ruled out for $v \neq 0$ and $v \neq 1$. For $k = 2,\ldots,7$, the preparation of the Dicke states after a depolarising channel are excluded from the BTN scenario for $v \neq 0$.

More generally, by directly applying the result of Proposition 4.2, we can check whether the CM of a BTN state can be written like the right-hand side of Eq. (4.15). By doing that for $|D_{3,4,1}\rangle$, whose preparation could not be ruled out by the positivity condition, we conclude that this state cannot be generated in the BTN scenario. On the other hand, the CM of the maximally mixed state $\mathbb{1}/64$ has such a decomposition.

4.1.3 Triangle network with local operations

Let us now consider the situation where the parties can perform unitary operations on their respective systems. Following Definition 1.9, the global state now reads

$$\varrho_{\text{UTN}} = (U_A \otimes U_B \otimes U_C)\varrho_{\text{BTN}}(U_A^\dagger \otimes U_B^\dagger \otimes U_C^\dagger). \tag{4.20}$$

The generation of this state is illustrated in Figure 4.1 (b). First, we note that in general, for any observable set $\{M_i\}_{i=1}^N$, any unitary $U \in \mathcal{L}(\mathcal{H})$ and any state $\varrho \in \mathcal{S}(\mathcal{H})$, there exists an orthogonal matrix $O \in \mathcal{L}(\mathcal{H})$ such that [56]

$$\Gamma(\{M_i\}_{i=1}^N, U\varrho U^\dagger) = \Gamma(\{U^\dagger M_i U\}_{i=1}^N, \varrho) = O^T\Gamma(\{M_i\}_{i=1}^N, \varrho)O. \tag{4.21}$$

Not all orthogonal transformations of CMs correspond to a physical unitary transformation on the system [56]. From that we obtain to the following proposition.

Proposition 4.4 (CMs of UTN states [C]). *Consider the* CM *of a* UTN *state with observables* $\{A_i, B_i, C_i\}_{i=1}^N$. *There exist an orthogonal matrix* $O = O_A \oplus O_B \oplus O_C$ *and a* BTN *state* ϱ_{BTN} *such that the* CM *of* ϱ_{UTN} *can be written as*

$$\Gamma_{\text{UTN}} = \Gamma(\{A_i, B_i, C_i\}_{i=1}^N, \varrho_{\text{UTN}}) = O^T \Gamma_{\text{BTN}} O, \tag{4.22}$$

with Γ_{BTN} *as in Eq.* (4.6).

Thus, the CM of ϱ_{UTN} can always be decomposed as a sum of PSD matrices with the following block decomposition

$$\Gamma_{\text{UTN}} = \underbrace{\begin{pmatrix} \blacksquare & \blacksquare & 0 \\ \blacksquare & \blacksquare & 0 \\ 0 & 0 & 0 \end{pmatrix}}_{O^T T_c O} + \underbrace{\begin{pmatrix} \blacksquare & 0 & \blacksquare \\ 0 & 0 & 0 \\ \blacksquare & 0 & \blacksquare \end{pmatrix}}_{O^T T_b O} + \underbrace{\begin{pmatrix} 0 & 0 & 0 \\ 0 & \blacksquare & \blacksquare \\ 0 & \blacksquare & \blacksquare \end{pmatrix}}_{O^T T_a O} + \underbrace{\begin{pmatrix} \blacksquare & 0 & 0 \\ 0 & \blacksquare & 0 \\ 0 & 0 & \blacksquare \end{pmatrix}}_{O^T R O}, \tag{4.23}$$

where T_c, T_b, T_a, and R are such as in Eq. (4.6). We may also look at this situation by noticing that the CMs of UTN states can be written as

$$\begin{aligned} \Gamma_{\text{UTN}} &= \Gamma(\{U_A^\dagger A_i U_A, U_B^\dagger B_i U_B, U_C^\dagger C_i U_C\}_{i=1}^N, \varrho_{\text{BTN}}) \\ &= T_c^U + T_b^U + T_a^U + R^U, \end{aligned} \tag{4.24}$$

with T_c^U being the CMs of $\varrho_{\text{BTN}}^{(A_2 B_1)}$ with the following reduced observables

$$\begin{aligned} A_{U,i}^{(2)} &= (U_A^\dagger A_i U_A)^{(2)} \\ &= \sum_{\alpha,\beta=1}^{d^2} \text{tr}\Big(U_A^\dagger A_i U_A \, \sigma_\alpha \otimes \sigma_\beta\Big) \, \text{tr}(\sigma_\alpha \varrho_{A_1}) \sigma_\beta \quad \forall i \in [N] \end{aligned} \tag{4.25}$$

and $B_{U,i}^{(1)}$, with $i \in [N]$, build in a similar manner. The matrices T_b^U and T_a^U are defined analogously. The matrix R_A^U is equal to $A^U - E_A^U - F_A^U$. The issue with this formulation is that the unitaries U_A, U_B and U_C and the state ϱ_{BTN} corresponding to the decomposition of ϱ_{UTN} are in general not known, thus there is no way to explicitly know the reduced observables and use Eq. (4.24) to test whether a given state is compatible with the UTN scenario.

We now move to triangle networks where the local operations can be any quantum channel as presented in Definition 1.10 and Figure 4.1 (c), i.e.,

not longer restricted to unitary operations. By making use of the Stinespring dilation theorem [71], we can show that CTN states also lead to CMs that possess a block decomposition. As a matter of fact, any quantum channel can be implemented by performing a unitary transformation on the system together with an ancilla, and then tracing out the ancilla. The CM of any state ϱ after applying a channel $\mathcal{E}$ with observables $\{M_i\}_{i=1}^N$ therefore has the same expression as taking the CM of the state together with an ancilla ϱ_{ancilla} and applying the corresponding unitary U, that is, $U(\varrho \otimes \varrho_{\text{ancilla}})U^\dagger$, with observables $\{M_i \otimes \mathbb{1}_{\text{ancilla}}\}_{i=1}^N$. We can also see this by noticing that the CM of a marginal state is just a principal submatrix of the CM of the global state. Applying this to each node of the triangle network, we obtain the following proposition.

Proposition 4.5 (Block decomposition for CMs of CTN states [C])**.** *Let Γ_{CTN} be the covariance matrix of $\varrho_{\text{CTN}} = \mathcal{E}_A \otimes \mathcal{E}_B \otimes \mathcal{E}_C(\varrho_{\text{BTN}})$ with observables $\{A_i, B_i, C_i\}_{i=1}^N$ as in Eq. (4.1). There exist matrices Y_i^X, with $X = A, B, C$ and $i = 1, 2$, such that*

$$\Gamma_{\text{CTN}} = \underbrace{\begin{pmatrix} \mathrm{Y}_2^A & \gamma_E & 0 \\ \gamma_E^T & \mathrm{Y}_1^B & 0 \\ 0 & 0 & 0 \end{pmatrix}}_{\succeq 0} + \underbrace{\begin{pmatrix} \mathrm{Y}_1^A & 0 & \gamma_F \\ 0 & 0 & 0 \\ \gamma_F^T & 0 & \mathrm{Y}_2^C \end{pmatrix}}_{\succeq 0} + \underbrace{\begin{pmatrix} 0 & 0 & 0 \\ 0 & \mathrm{Y}_2^B & \gamma_G \\ 0 & \gamma_G^T & \mathrm{Y}_1^C \end{pmatrix}}_{\succeq 0}. \tag{4.26}$$

Comparing to Eq. (4.23), we consider that we distributed the diagonal blocks of $O^T R O$ to the first three matrices. Although the proof techniques differ notably, the block decomposition has already been presented in a previous work on CMs of network states [3]. As demonstrated in that same work, Proposition 4.5 can be evaluated as an SDP. However, we are seeking practical analytical methods and criteria to determine if a state cannot be prepared in a network setting: In the next section, we present such a criterion that follows from Proposition 4.5.

Let us here briefly comment on how this proposition behaves for LOSR triangle network states ϱ_Δ defined in Eq. (1.20) and illustrated in Figure 4.1 (d). We recall that in this set up, the sources and the local operations may be coordinated by a classical random variable $\lambda \in [L]$. From the concavity property in [56], we know that

$$\Gamma(\{M_i\}_{i=1}^N, \varrho_\Delta) - \sum_{\lambda=1}^{L} p_\lambda \Gamma\left(\{M_i\}_{i=1}^N, \mathcal{E}_A^{(\lambda)} \otimes \mathcal{E}_B^{(\lambda)} \otimes \mathcal{E}_C^{(\lambda)}(\varrho_{\text{BTN}})\right) \succeq 0. \tag{4.27}$$

Using Proposition 4.5, we directly obtain that there exist block matrices such

that

$$\Gamma(\varrho_\Delta) \succeq \underbrace{\begin{pmatrix} \blacksquare & \blacksquare & 0 \\ \blacksquare & \blacksquare & 0 \\ 0 & 0 & 0 \end{pmatrix}}_{\succeq 0} + \underbrace{\begin{pmatrix} \blacksquare & 0 & \blacksquare \\ 0 & 0 & 0 \\ \blacksquare & 0 & \blacksquare \end{pmatrix}}_{\succeq 0} + \underbrace{\begin{pmatrix} 0 & 0 & 0 \\ 0 & \blacksquare & \blacksquare \\ 0 & \blacksquare & \blacksquare \end{pmatrix}}_{\succeq 0}. \tag{4.28}$$

While a similar trick can lead to powerful necessary criteria for separability in the case of entanglement [56], it is not the case here. This is because the extreme points in the case of LOSR triangle network states are not well characterised, as already discussed in Section 1.3.4. Nevertheless, when additional properties of the states are known, such as the purity or the rank, SDP-based criteria for LOSR networks can be obtained, as shown in [162].

4.1.4 Covariance matrix criterion for triangle network states

As seen in the previous section, CMs of CTN states with observables $\{A_i, B_i, C_i\}_{i=1}^N$ possess a block decomposition. From Proposition 4.5, we obtain inequalities valid for any unitarily invariant norm $\|\cdot\|$, $2\|\gamma_E\| \leq \|A_2\| + \|B_1\|$ [75], for which we can take the trace norm and obtain

$$2\|\gamma_E\|_{\mathrm{tr}} + 2\|\gamma_F\|_{\mathrm{tr}} + 2\|\gamma_G\|_{\mathrm{tr}} \leq \mathrm{tr}(A_1 + A_2 + B_1 + B_2 + C_1 + C_2). \tag{4.29}$$

This gives us a direct necessary criterion for triangle network states.

Proposition 4.6 (CMs and trace norm criterion for triangle network states [C]). *Let Γ be the CM of a triangle network state $\varrho_{\mathrm{CTN}} = \mathcal{E}_A \otimes \mathcal{E}_B \otimes \mathcal{E}_C(\varrho_{\mathrm{BTN}})$ with local observables $\{A_i, B_i, C_i\}_{i=1}^N$. Then*

$$\mathrm{tr}(\Gamma) \geq 2\|\gamma_E\|_{\mathrm{tr}} + 2\|\gamma_F\|_{\mathrm{tr}} + 2\|\gamma_G\|_{\mathrm{tr}} \tag{4.30}$$

has to hold, with γ_E, γ_F and γ_G as in Eq. (4.1).

Let us now consider a few examples. First, we notice that contrarily to BTN states, three-qubit states can be generated in the CTN scenario. Therefore, we consider the three-qubit GHZ state after a depolarising channel, i.e.,

$$\varrho(v) = v\,|\mathrm{GHZ}\rangle\langle\mathrm{GHZ}| + (1-v)\frac{\mathbb{1}_8}{8}, \tag{4.31}$$

with $v \in [0,1]$. By taking the three-qubit observable set $\{Z\mathbb{1}\mathbb{1}, \mathbb{1}Z\mathbb{1}, \mathbb{1}\mathbb{1}Z\}$, the CM and trace norm criterion prevents $\varrho(v)$ to be generated in a CTN for

$v > 1/2$. Proposition 4.6 with observables $\{X\mathbb{1}\mathbb{1}, Y\mathbb{1}\mathbb{1}, \mathbb{1}X\mathbb{1}, \mathbb{1}Y\mathbb{1}, \mathbb{1}\mathbb{1}X, \mathbb{1}\mathbb{1}Y\}$ is also not satisfied by the state $|W\rangle = 1/\sqrt{3}(|100\rangle + |010\rangle + |001\rangle)$ after a depolarising channel for $v > 3/4$.

4.1.5 NCDS networks

In this section, we show that the block decomposition of CMs of network states can also hold for larger networks. Indeed, if we consider networks where two network nodes share parties from at most one common source (NCDS networks), the triangle network results can be extended. Although this may seem like a strong restriction on the network structure, we note that the condition is fulfilled by networks with only bipartite sources, which are the easiest to implement physically.

More explicitly, consider an n-node NCDS network with a set of sources $\mathbb{S}$. The number of sources is given by $|\mathbb{S}|$, and each source $s \in \mathbb{S}$ is the set of nodes the source connects. Let Γ_{NCDS} be the CM of a global state of such a network with observables $\{A_{x|i} \mid x \in [n]\}_{i=1}^{N}$, where $A_{x|i}$ is the ith observables that only acts on the node x, with $i \in [N]$ and $x \in [n]$. Then Γ_{NCDS} has a block form analogous to Eq. (4.1), where the diagonal blocks are labelled Γ_x and the off-diagonal block are $\gamma_{xy} = \gamma_{yx}^T$, with $x \neq y$ and $x, y \in [n]$.

Proposition 4.7 (Block decomposition for CMs of NCDS network states [C])**.** *There exist matrices Υ_x^s for all $s \in \mathbb{S}$ and $x \in s$ such that Γ_{NCDS} can be decomposed as a sum of $|\mathbb{S}|$ PSD block matrices T_s, where the off-diagonal blocks of each T_s are γ_{xy} for $\{x, y\} \subset s$ and 0 for $\{x, y\} \not\subset s$, and where the diagonal blocks are Υ_x^s, with $s \in \mathbb{S}$, $x \neq y$ and $x, y \in [n]$.*

For a technical proof, see Appendix B. Therein, we prove that in the case of basic (i.e., without local operations) networks with no common double source, the proposition holds. Following a similar line of reasoning to the proofs for triangle networks, the proposition naturally extends to NCDS networks with local operations.

Let us consider an easy example for the sake of clarity. Figure 4.2 shows a five-partite network consisting of two tripartite sources ϱ_a and ϱ_b, and one bipartite ϱ_c. The set of sources is given by $\mathbb{S} = \{a, b, c\} = \{\{1, 2, 3\}, \{3, 4, 5\}, \{1, 5\}\}$. Following the notation of Proposition 4.7, there must exist eight matrices Υ_1^a, Υ_2^a, Υ_3^a, Υ_3^b, Υ_4^b, Υ_5^b, Υ_1^c, and Υ_5^c such that the CM

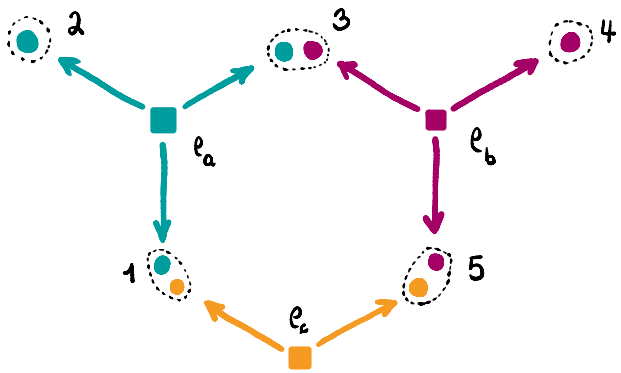

Figure 4.2: *Five-partite network.* The two sources ϱ_a and ϱ_b are tripartite, and the source ϱ_c is bipartite. The parties 1, 2, 3, 4 and 4 may perform a local channel $\mathcal{E}_i$ on their corresponding system i, with $i \in [5]$. Figure adapted from [C].

of the global network state

$$\varrho_{\text{NCDS}} = \mathcal{E}_1 \otimes \mathcal{E}_2 \otimes \mathcal{E}_3 \otimes \mathcal{E}_4 \otimes \mathcal{E}_5(\varrho_a \otimes \varrho_b \otimes \varrho_c) \tag{4.32}$$

may be decomposed as

$$\Gamma_{\text{NCDS}} = \underbrace{\begin{pmatrix} Y_1^a & \blacksquare & \blacksquare & 0 & 0 \\ \blacksquare & Y_2^a & \blacksquare & 0 & 0 \\ \blacksquare & \blacksquare & Y_3^a & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}}_{T_a} + \underbrace{\begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & Y_3^b & \blacksquare & \blacksquare \\ 0 & 0 & \blacksquare & Y_4^b & \blacksquare \\ 0 & 0 & \blacksquare & \blacksquare & Y_5^b \end{pmatrix}}_{T_b} + \underbrace{\begin{pmatrix} Y_1^c & 0 & 0 & 0 & \blacksquare \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ \blacksquare & 0 & 0 & 0 & Y_5^c \end{pmatrix}}_{T_c}, \tag{4.33}$$

where the off-diagonal blocks are simply the ones from Γ_{NCDS}. We see that we can extend Proposition 4.6.

Proposition 4.8 (CMs and trace norm criterion for NCDS network states [C])**.** *Let* Γ_{NCDS} *be as above. Then*

$$\operatorname{tr}(\Gamma_{\text{NCDS}}) \geq 2 \sum_{x>y=1}^{N} \|\gamma_{xy}\|_{\text{tr}} \tag{4.34}$$

holds.

We note that this criterion does not take network topology into account:

It treats a network with a single $(N-1)$-partite source the same way it treats a line network with $N-1$ bipartite sources. This is interesting because if a state does not satisfy Proposition 4.8, its preparation in *any* network structure is ruled out. However, we also expect this proposition to be weaker than criteria designed for specific network topologies. On top of that, Proposition 4.8 only takes into account that the principal submatrices of each matrix T_s are PSD, not that the matrices themselves are PSD.

As an example, let us consider an n-qubit GHZ state $|\mathrm{GHZ}_n\rangle = 1/\sqrt{2}(|0\ldots0\rangle + |1\ldots1\rangle)$ on which we apply a depolarising channel,

$$\varrho(v) = v\,|\mathrm{GHZ}_n\rangle\langle\mathrm{GHZ}_n| + (1-v)\frac{\mathbb{1}}{2^n}, \quad v \in [0,1]. \tag{4.35}$$

As observables, we take the Pauli observable Z_x on each qubit $x \in [n]$, where the index specifies on which qubit the observable act, i.e., $\{Z_1, \ldots, Z_n\}$. The resulting CM has diagonal entries equal to one, whereas the off-diagonal entries are equal to v. Applying the previous proposition, we show that n-partite depolarised GHZ states cannot be prepared in NCDS networks for

$$v > \frac{1}{n-1}. \tag{4.36}$$

With $n = 3$, we recover the result of the example for the triangle network.

Nevertheless, we are forced to observe that the criterion only considers two-body correlation, therefore cannot fully capture the entanglement in the target states. To see this, let us consider the four-qubit cluster state

$$|C_4\rangle = \frac{1}{2}(|{+}0{+}0\rangle + |{+}0{-}1\rangle + |{-}1{-}0\rangle + |{-}1{+}1\rangle), \tag{4.37}$$

with $|\pm\rangle = 1/\sqrt{2}(|0\rangle \pm |1\rangle)$ as defined in Eq. (1.25). The four-qubit cluster state is a stabiliser state, and its generators are $XZ\mathbb{1}\mathbb{1}$, $ZXZ\mathbb{1}$, $\mathbb{1}ZXZ$ and $\mathbb{1}\mathbb{1}ZX$, where the only two-body correlators in its stabiliser are given by $XZ\mathbb{1}\mathbb{1}$ and $\mathbb{1}\mathbb{1}ZX$ (see Section 1.4.1). A possible set of observables is $O = \{X\mathbb{1}\mathbb{1}\mathbb{1}, \mathbb{1}Z\mathbb{1}\mathbb{1}, \mathbb{1}\mathbb{1}Z\mathbb{1}, \mathbb{1}\mathbb{1}\mathbb{1}X\}$, and we obtain

$$\Gamma(O, |C_4\rangle) = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}. \tag{4.38}$$

The trace criterion is satisfied and thus we cannot rule out the preparation of

$|C_4\rangle$ in NCDS network scenarios by means of Proposition 4.8. Moreover, we directly see that the matrix has a block decomposition, namely $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \oplus \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$, which a priori could arise from a network with two bipartite sources. However, we show in the next section that the four-qubit cluster state cannot be generated in networks with only bipartite sources.

4.2 Symmetric states in quantum networks

As discussed in Section 1.3.3, CMs are powerful tools to characterise network entanglement, but reach their limits when it comes to more than two-body correlations and to LOSR networks. In this section, we aim to derive exclusion criteria that hold for LOSR network states (see Figure 4.1 (d)), which we recall from Definition 1.11 are of the form

$$\varrho_\Delta = \sum_{\lambda=1}^{L} p_\lambda \mathcal{E}_A^{(\lambda)} \otimes \mathcal{E}_B^{(\lambda)} \otimes \mathcal{E}_C^{(\lambda)}(\varrho_{\text{BTN}}). \tag{4.39}$$

The results of this section are presented in [A], and we closely follow the structure of the article.

We first turn our attention to GHZ states, then to graph states and finally consider permutationally symmetric states. These three classes contain states that are invariant under some transformations, as detailed in Section 1.4, and we show that these strong characteristics make them impossible to be prepared in LOSR network scenarios.

Our method is based on the inflation technique [160, 161]. This technique has been developed in the context of classical causal inference, which aims to answer the question whether a given probability distribution can arise from a certain causal structure. The classical inflation technique can be formulated as a hierarchy of SDPs and, remarkably, is complete (i.e., if a distribution is not compatible with the structure considered, it is detected at some level of the hierarchy) [160]. A version that is valid for probability distributions arising from measurement on quantum systems has been proposed shortly after, albeit not complete [161]. In [97], the authors propose a different hierarchy for the quantum case (where they introduce extra parameters) that they prove to be complete. The derivation and analysis of the different inflation techniques are a topic of research in themselves, and we solely

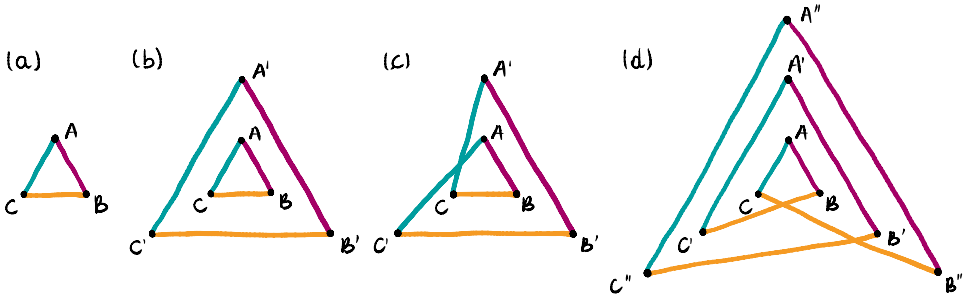

Figure 4.3: *Triangle network and three of its inflations.* (a) Schematic representation of the triangle network (see Figure 1.2). (b), (c) Respectively the τ- and γ-inflation of the triangle network. (d) An example of a higher order inflation. Edges with the same colour correspond to sources in the same state. Figures adapted from [A].

present here the results that are needed for the derivation of our results.

4.2.1 Inflation technique

In a nutshell, the inflation technique puts restrictions on correlations arising from network structures by considering 'inflated networks'. We describe here how it applies to the triangle network.

Consider the triangle network as depicted in Figure 1.2 (d). If a tripartite state $\varrho \in \mathcal{S}(\mathcal{H}^{d^3})$ can be prepared in the LOSR triangle network, then it should be possible to prepare a state $\tau \in \mathcal{S}(\mathcal{H}^{d^3} \otimes \mathcal{H}^{d^3})$ using two copies of the sources and channels used to prepare the state ϱ. This is presented in a schematic way in Figure 4.3 (b). Therein, the state τ is the state of a six-partite system $ABCA'B'C'$, where edges between parties represent a shared source state and the colour indicates which source of ϱ is used, conformably to the colours in Figures 1.2 (d) and Figure 4.3 (a). In other words, the source ϱ_b is distributed both between AC and between $A'C'$ (analogously for ϱ_a and ϱ_c, following Figure 4.3 (b)). Then, the channels are performed according to the random parameter $\lambda \in [L]$. Both on primed and non-primed A nodes, the same channel $\mathcal{E}_A^{(\lambda)}$ is applied and similarly for B and C.

Alternatively, by 'rewiring' the sources following Figure 4.3 (c), a third state $\gamma \in \mathcal{S}(\mathcal{H}^{d^3} \otimes \mathcal{H}^{d^3})$ can be prepared following the same idea. This leaves us with two network states, τ and γ. Those operators are physical states, i.e., they have a unit trace and are PSD. Formally, they can be written

as

$$\tau = \sum_{\lambda=1}^{L} p_\lambda \left[\mathcal{E}_A^{(\lambda)} \otimes \mathcal{E}_B^{(\lambda)} \otimes \mathcal{E}_C^{(\lambda)}\left(\varrho_{ABC}\right)\right] \otimes \left[\mathcal{E}_{A'}^{(\lambda)} \otimes \mathcal{E}_{B'}^{(\lambda)} \otimes \mathcal{E}_{C'}^{(\lambda)}\left(\varrho_{A'B'C'}\right)\right] \tag{4.40}$$

and

$$\gamma = \sum_{\lambda=1}^{L} p_\lambda \mathcal{E}_A^{(\lambda)} \otimes \mathcal{E}_B^{(\lambda)} \otimes \mathcal{E}_C^{(\lambda)} \otimes \mathcal{E}_{A'}^{(\lambda)} \otimes \mathcal{E}_{B'}^{(\lambda)} \otimes \mathcal{E}_{C'}^{(\lambda)}\left(\varrho_{ABCA'B'C'}\right), \tag{4.41}$$

where $\varrho_{ABC} = \varrho_{A'B'C'} = \varrho_c \otimes \varrho_b \otimes \varrho_a$ and $\varrho_{ABCA'B'C'} = \varrho_c \otimes \varrho_b \otimes \varrho_a \otimes \varrho_c \otimes \varrho_b \otimes \varrho_a$, with the ordering of parties being different on both sides. Here, one needs to carefully pay attention to which channel acts on which party (this is depicted in Figure 4.3). Clearly, given only the knowledge of ϱ, the precise form of τ and γ is not known. Still, due to the way they are constructed, some of their marginals have to be equal, e.g.,

$$\tau^{(ABC)} = \tau^{(A'B'C')} = \varrho, \tag{4.42a}$$

$$\gamma^{(ABC)} = \gamma^{(A'B'C')}, \tag{4.42b}$$

$$\mathrm{tr}_{XX'}(\tau) = \mathrm{tr}_{XX'}(\gamma) \quad \forall X = A, B, C. \tag{4.42c}$$

Furthermore, from Eq. (4.40) it is clear that τ and γ are permutationally symmetric under the exchange of all non primed and primed vertices and that τ is separable with respect to the partition $ABC \mid A'B'C'$. If, for some given state ϱ, it is not possible to find states τ and γ that satisfy those conditions, then ϱ cannot be generated in the considered network.

A notable point is that the question for the existence of τ and γ with the desired properties can be directly formulated as an SDP [111]. This can be used to prove that such inflations do not exist, and the corresponding dual program can deliver an witness-like construction that can be used to rule out the preparation of a state in the network. Still, these approaches are memory intensive. For instance, as the authors of [111] acknowledge, it is difficult to derive tests for tripartite qutrit states in a standard computer. The strength of the approach present in the next subsection hence lies in the fact that the constraints of inflation technique are applied analytically.

Finally, let us note that other triangle inflations may be considered, for instance inflations with $3n$ nodes, $n = 3, 4, \ldots$, and wired differently than τ and γ. Figure 4.3 (d) depicts such an example.

4.2.2 GHZ state

Let us start with the usual GHZ state of three qubits, $|\text{GHZ}\rangle = 1/\sqrt{2}(|000\rangle + |111\rangle)$. It is a stabiliser state, for which we can choose the following three generators

$$g_1 = XXX, \quad g_2 = \mathbb{1}ZZ, \quad g_3 = ZZ\mathbb{1}. \tag{4.43}$$

We recall that a stabiliser is composed of the products of the generators, in this case $S = \{\mathbb{1}, g_1, g_2, g_3, g_1g_2, g_1g_3, g_2g_3, g_1g_2g_3\}$ (see Section 1.4.1 for more details). In what follows, we omit the identity operator and specify with a subscript on which qubit the Pauli operators act, e.g., for g_2 we write Z_BZ_C.

We first consider the expectation value of Z_AZ_B and of Z_BZ_C on ϱ_Δ, a LOSR triangle state, and on its τ- and γ-inflations. The values are equal in all three states, which is one of the constraints imposed by the inflation technique, i.e.,

$$\langle Z_AZ_B\rangle_{\varrho_\Delta} = \langle Z_AZ_B\rangle_\tau = \langle Z_AZ_B\rangle_\gamma, \tag{4.44a}$$
$$\langle Z_BZ_C\rangle_{\varrho_\Delta} = \langle Z_BZ_C\rangle_\tau = \langle Z_BZ_C\rangle_\gamma. \tag{4.44b}$$

Note that these should be large if ϱ_Δ is close to a GHZ state, as $g_2 = \mathbb{1}ZZ$ and $g_3 = Z_AZ_B$ are elements of the stabiliser. Using the general relation

$$\langle Z_AZ_B\rangle_\rho + \langle Z_BZ_C\rangle_\rho - 1 \leq \langle Z_AZ_C\rangle_\rho \tag{4.45}$$

that holds for all states $\rho \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C)$ [111], we can estimate $\langle Z_AZ_C\rangle_\gamma$. The key observation is that the observables $X_AX_BX_C$ and $Z_{A'}Z_C$ anticommute. We know from Chapter 2 that for such observables, the sum of the squares of their expectation values is upper bounded by one, and in particular on the state τ we have

$$\langle X_AX_BX_C\rangle_\tau^2 + \langle Z_{A'}Z_C\rangle_\tau^2 \leq 1. \tag{4.46}$$

From the inflation technique's marginal relations, we know that $\langle X_AX_BX_C\rangle_\tau^2 = \langle X_AX_BX_C\rangle_{\varrho_\Delta}^2$ and $\langle Z_{A'}Z_C\rangle_\tau = \langle Z_AZ_C\rangle_\gamma$ have to hold. Applying Eq. (4.45) to the state γ and using the marginal relations of Eq. (4.44), we have proved the following proposition.

Proposition 4.9 (Network inequality [A]). *If ϱ_Δ is a* LOSR *triangle state as in*

Eq. (4.39), *then*

$$\langle X_A X_B X_C\rangle^2_{\varrho_\Delta} + (\langle Z_A Z_B\rangle_{\varrho_\Delta} + \langle Z_B Z_C\rangle_{\varrho_\Delta} - 1)^2 \leq 1 \tag{4.47}$$

has to hold.

This is clearly not satisfied by the GHZ state, as the operators involved belong to its stabiliser. In fact, applying Proposition 4.9 to a depolarised GHZ state $v\,|\mathrm{GHZ}\rangle\langle\mathrm{GHZ}| + (1-v)\mathbb{1}/8$ rules out its preparation in the LOSR triangle for $v \in]4/5, 1]$. Note that using the other observables of the stabiliser and permutations of the parties, other conditions such as $\langle Y_A Y_B X_C\rangle^2_\varrho + (\langle Z_A Z_B\rangle_\varrho + \langle Z_A Z_C\rangle_\varrho - 1)^2 \leq 1$ can be derived.

Remarkably, Proposition 4.9 can also be used to bound the fidelity of LOSR triangle states to the GHZ state, which we recall to be $F_{\mathrm{GHZ}}(\varrho) = \langle\mathrm{GHZ}|\,\varrho\,|\mathrm{GHZ}\rangle$ (see Eq. (1.12)).

Proposition 4.10 (Network fidelity to the GHZ state [A])**.** *If ϱ_Δ is a* LOSR *triangle state as in Eq.* (4.39)*, then its fidelity to the* GHZ *state satisfies*

$$F_{\mathrm{GHZ}}(\varrho_\Delta) \leq \frac{1}{16}\left(5 + \sqrt{73}\right) \simeq 0.8465. \tag{4.48}$$

Proof. The fidelity of any three-qubit state ϱ to the GHZ state is given by $F_{\mathrm{GHZ}}(\varrho) = 1/8 \sum_{s\in S}\langle s\rangle_\varrho$, where S is the stabiliser of the GHZ state. The symmetry of GHZ implies that one can assume that the LOSR triangle state ϱ_Δ that maximises the fidelity satisfies $\langle Z_A Z_B\rangle_{\varrho_\Delta} = \langle Z_B Z_C\rangle_{\varrho_\Delta} = \langle Z_A Z_C\rangle_{\varrho_\Delta}$ and $\langle X_A Y_B Y_C\rangle_{\varrho_\Delta} = \langle Y_A X_B Y_C\rangle_{\varrho_\Delta} = \langle Y_A Y_B X_C\rangle_{\varrho_\Delta}$. Hence it follows that

$$\begin{aligned} F_{\mathrm{GHZ}}(\varrho_\Delta) \leq \max_{a,b,c} \frac{1}{8}(1 + a + 3b + 3c) & && \text{(4.49a)}\\ \text{such that} \quad a, b, c \in [-1, 1], & && \text{(4.49b)}\\ a^2 + (2b-1)^2 \leq 1, & && \text{(4.49c)}\\ c^2 + (2b-1)^2 \leq 1. & && \text{(4.49d)} \end{aligned}$$

Using a computer algebra system, the right hand side evaluates to $1/16(5 + \sqrt{73})$. □

4.2.3 Cluster state

We now consider the four-qubit cluster state $|C_4\rangle$ (see Eq. (4.37)), and wonder whether it can be prepared in a LOSR square network depicted in Figure

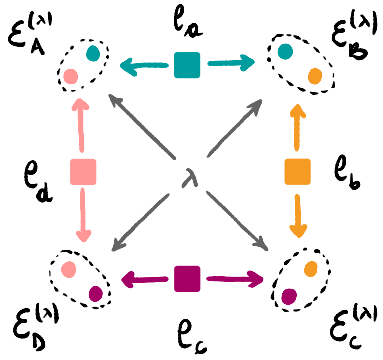

Figure 4.4: *Square network.* Four bipartite source states ϱ_a, ϱ_b, ϱ_c, and ϱ_d are distributed to the four nodes of the network, A, B, C, and D. The parties apply on their respective subsystems local channels $\mathcal{E}_A^{(\lambda)}$, $\mathcal{E}_B^{(\lambda)}$, $\mathcal{E}_C^{(\lambda)}$, and $\mathcal{E}_D^{(\lambda)}$ that are coordinated by a random variable $\lambda \in [L]$.

4.4. The four-qubit cluster states is the graph state associated to the square graph (see Section 1.4.1 for details on graph states), whose generators are

$$g_1 = XZ\mathbb{1}Z, \quad g_2 = ZXZ\mathbb{1}, \quad g_3 = \mathbb{1}ZXZ, \quad g_4 = Z\mathbb{1}ZX. \tag{4.50}$$

We again employ the inflation technique, and notice that if a four-qubit state $\varrho_\square$ can be prepared in the square network, then there must exist eight-qubit and 12-qubit states preparable following Figure 4.5 (b) and (c) respectively. In the ξ-inflation (Figure 4.5 (c)), the observables $X_{B''}X_D$, $Z_{B'}X_CZ_D$ and $X_AY_BY_D$ all pairwise anticommute. Moreover, their expectation values satisfy $\langle X_{B''}X_D\rangle_\xi = \langle X_BX_D\rangle_{\varrho_\square}$, $\langle Z_{B'}X_CZ_D\rangle_\xi = \langle Z_BX_CZ_D\rangle_{\varrho_\square}$ and $\langle X_AY_BY_D\rangle_\xi = \langle X_AY_BY_D\rangle_{\varrho_\square}$. Thus, for any LOSR square state $\varrho_\square$, the following must hold

$$\langle X_BX_D\rangle^2_{\varrho_\square} + \langle Z_BX_CZ_D\rangle^2_{\varrho_\square} + \langle X_AY_BY_D\rangle^2_{\varrho_\square} \leq 1, \tag{4.51}$$

and similar strategy in the τ-inflation leads to

$$\langle X_BX_D\rangle^2_{\varrho_\square} + \langle Y_AY_BZ_CZ_D\rangle^2_{\varrho_\square} \leq 1. \tag{4.52}$$

Together, these inequalities can be used to prove the following proposition.

Proposition 4.11 (Network fidelity to the four-qubit cluster state [A])**.** *If $\varrho_\square$ is a* LOSR *square network state as in a generalisation of Eq. 4.39 following Figure*

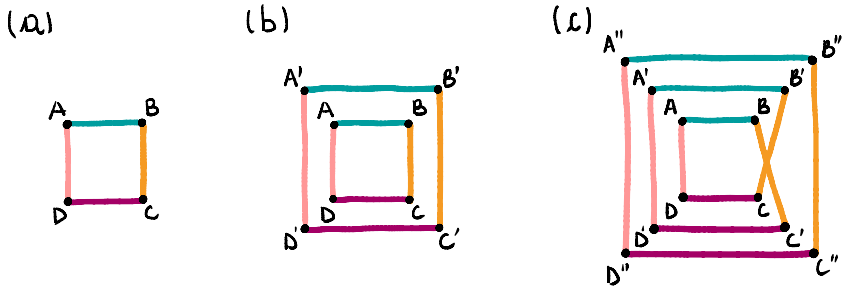

Figure 4.5: *Square network and two of its inflations.* (a) Square network. (b) τ-inflation of the square network. (c) ξ-inflation of the square network. Figures adapted from [A].

4.4, then its fidelity to the four-qubit cluster state satisfies

$$F_{C_4}(\varrho_\square) \leq \frac{1}{8}\left(1+\sqrt{13+8\sqrt{2}}\right) \simeq 0.7414. \tag{4.53}$$

Proof. The proof follows the same logic as the proof of Proposition 4.10. The stabiliser elements of $|C_4\rangle$ are presented in Table 4.1. The symmetries of $|C_4\rangle$ allow us to consider that the expectation values of elements of the same column on $\varrho_\square$ are equal. Using Eqs. (4.51–4.52), we can write

$$F_{C_4}(\varrho_\square) \leq \max_{a,b,c,d,e} \frac{1}{16}(1+4a+4b+2c+4d+e) \tag{4.54a}$$

$$\text{such that} \quad a,b,c,d,e \in [-1,1], \tag{4.54b}$$

$$c^2+d^2+a^2 \leq 1, \tag{4.54c}$$

$$c^2+b^2 \leq 1. \tag{4.54d}$$

We evaluate the right hand side with a computer algebra system and obtain $1/8\left(1+\sqrt{13+8\sqrt{2}}\right)$. □

Remarkably, both propositions are analytical results, facilitating a generalisation to higher-dimensional systems.

4.2.4 Graph states

The method presented in the previous section mostly relies on properties of stabiliser states, and can thus directly be generalised to more parties and more intricate networks. In [A], we prove several theorems that state that, if a graph fulfils certain graph-theoretic properties, its corresponding graph

Stabiliser elements of $\vert C_4\rangle$				
$s_1 = X\mathbb{1}Z\mathbb{1}$	$s_5 = YYZZ$	$s_9 = X\mathbb{1}X\mathbb{1}$	$s_{11} = -YXY\mathbb{1}$	$s_{15} = XXXX$
$s_2 = ZXZ\mathbb{1}$	$s_6 = YZZY$	$s_{10} = \mathbb{1}X\mathbb{1}X$	$s_{12} = -\mathbb{1}YXY$	
$s_3 = \mathbb{1}ZXZ$	$s_7 = ZYYZ$		$s_{13} = -Y\mathbb{1}YX$	
$s_4 = Z\mathbb{1}ZX$	$s_8 = ZZYY$		$s_{14} = -XY\mathbb{1}Y$	
$\langle\cdot\rangle_{\varrho_\square} = a$	$\langle\cdot\rangle_{\varrho_\square} = b$	$\langle\cdot\rangle_{\varrho_\square} = c$	$\langle\cdot\rangle_{\varrho_\square} = d$	$\langle\cdot\rangle_{\varrho_\square} = e$

Table 4.1: Elements of the stabiliser of the four-qubit cluster states. The qubit indices A, B, C, D are suppressed and the tensor product symbol omitted.

state cannot be prepared in LOSR networks. The results can be summarised in the following proposition.

Proposition 4.12 (Graph states in networks [A])**.** *1. If an n-vertex graph contains a vertex with degree strictly less than four, then its corresponding graph state cannot be prepared in an n-partite* LOSR *network with only bipartite sources.*

2. *The n-qubit two- and three-dimensional cluster states cannot be prepared in n-partite* LOSR *networks with only bipartite sources.*

3. *For $n \leq 12$, n-qubit graph states cannot be prepared in an n-partite* LOSR *network with only bipartite sources.*

For the proofs and more technical results, we refer the interested reader to the original reference, [A]. Although highly technical, the proofs are based on the ideas introduced in the previous sections: If a graph contains a triangle, then under simple and weak conditions a statement similar to Proposition 4.9 holds. This then rules out the preparation of noisy graph states from any network with only bipartite sources. At first sight, the identification of a specific triangle in the graph may seem a weak condition, but here the entanglement theory of graph states helps. By applying local complementations on the considered graph, which corresponds to local operations on the nodes of the network (see Section 1.4.1), triangles may appear. This is for instance doable for graphs with $n \leq 12$ vertices, as reflected by the third point of the above proposition.

In the same work, we conjectured that the third point of Proposition 4.12 holds for all numbers of qubits $n \in \mathbb{N}$. In [103, 151], this was later shown to be true. Specifically, the authors of [103] consider qudit graph states. They show that, when the local dimension is prime, if a n-vertex graph with $n \geq 3$ has at least one vertex that is connected to at least two

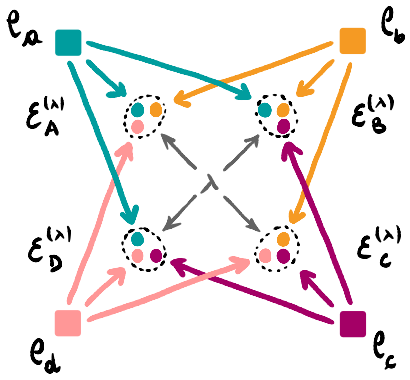

Figure 4.6: *Square network with four tripartite sources.* The tripartite sources distribute their parties to the nodes of the network as shown in the figure. The nodes apply on their respective subsystems local channels that are coordinated by a classical variable $\lambda \in [L]$. Figure adapted from [A].

other vertices, then the corresponding qudit graph state cannot be prepared in a LOSR network with only bipartite sources. This excludes form the set of LOSR network states all qubit graphs states whose graphs are connected. In [151], the authors show that if a state has a fidelity higher than $9/10$ to *any* qubit graph state, than it cannot be prepared in a LOSR network with only bipartite sources. Both works also present upper bounds on fidelities to qudit graph states for particular local dimensions and/or particular graph properties.

4.2.5 Networks with tripartite sources

So far, the results for LOSR networks concerned networks with only bipartite sources. We may wonder whether the proof techniques introduced above could be used to derive inequalities holding for networks where the source are of higher order. We therefore discuss here an example of a network with tripartite sources. Consider the fully connected four-partite graph state ϱ_*, whose generators are

$$g_1 = XZZZ, \quad g_2 = ZXZZ, \quad g_3 = ZZXZ, \quad g_4 = ZZZX. \tag{4.55}$$

It is locally equivalent to the four-partite GHZ state, and let us show that it cannot be prepared in the four partite network with four tripartite sources, illustrated in Figure 4.6. Let ϱ be a LOSR network state prepared in the network of Figure 4.6, and let us introduce the τ- and ν-inflations of that network, depicted in Figure 4.7, following a similar construction to what

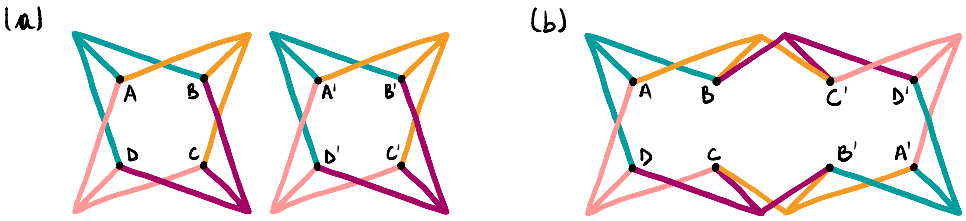

Figure 4.7: *Two inflations of the square network with tripartite sources.* (a), (b) Respectively the τ- and ν-inflations of the square network with tripartite sources. Figures adapted from [A].

was done for the triangle network. Any n-qubit state $\rho \in \mathcal{S}(\mathcal{H}^{\otimes n})$ verifies $\langle Y_i Y_k \rangle_\rho \geq \langle Y_i Y_j \rangle_\rho + \langle Y_j Y_k \rangle_\rho - 1$, for all distinct $i, j, k \in [n]$. In particular, by combining the inequalities on the state ν for $\{i, j, k\} = \{A, A', B\}$, $\{i, j, k\} = \{B, A', C'\}$, and $\{i, j, k\} = \{C', A', D'\}$ we obtain $\langle Y_A Y_{A'} \rangle_\nu \geq \langle Y_A Y_B \rangle_\nu + \langle Y_B Y_{C'} \rangle_\nu + \langle Y_{C'} Y_{D'} \rangle_\nu + \langle Y_{D'} Y_{A'} \rangle_\nu - 3$. Then, using the marginal relations between ν, τ, and ϱ,

$$\langle Y_A Y_{A'} \rangle_\tau \geq \langle Y_A Y_B \rangle_\varrho + \langle Y_B Y_C \rangle_\varrho + \langle Y_C Y_D \rangle_\varrho + \langle Y_D Y_A \rangle_\varrho - 3 \tag{4.56}$$

has to hold.

On the other hand, the observables $Y_A Y_{A'}$ and $X_A Z_B Z_C Z_D$ anticommute, thus the sum of the squares of their expectation values is upper bounded by one, in particular evaluated on the state τ. Using the fact that $\tau^{(ABCD)} = \varrho$, we obtain

$$\langle Y_A Y_{A'} \rangle_\tau^2 + \langle X_A Z_B Z_C Z_D \rangle_\varrho^2 \leq 1. \tag{4.57}$$

Combining this equation with Eq. (4.56) and making use of the symmetries of the fully connected graph state ϱ_*, for any state ϱ preparable in the network of Figure 4.6, we obtain an upper bound on its fidelity to ϱ_*

$$F_{\varrho_*}(\varrho) \leq \max_{a,b,x} \frac{1}{16}(4a + 4b + 8) \tag{4.58a}$$

$$\text{such that} \quad a, b, x \in [-1, 1], \tag{4.58b}$$

$$x \geq 4a - 3, \tag{4.58c}$$

$$x^2 + b^2 \leq 1, \tag{4.58d}$$

whose right hand side evaluates to $1/16(\sqrt{17} + 11) \simeq 0.9452$, using a computer algebra system. Thus, we certify that a fidelity higher than 0.9452 to the the fully connected graph state cannot be achieved by the four-partite network state of Figure 4.6.

From this example, we see that the anticommutation relation method also works for networks with more than bipartite sources. However, it remains an open question whether it leads to general results similar to those of Proposition 4.12.

4.2.6 Permutationally symmetric states

We now consider permutationally symmetric states, which were introduced in Section 1.4.2. Again, we first present our method with a three-qubit example, and present the general results later on.

Consider a tripartite permutationally symmetric ϱ_Δ state that can be prepared in a LOSR triangle network, and its inflated states γ and τ from Figure 4.3. First, we notice that τ is permutationally symmetric for the pairs $\{A, B\}$, $\{B, C\}$, $\{A, C\}$, $\{A', B'\}$, $\{B', C'\}$ and $\{A', C'\}$. This comes from the fact that the marginals of τ on those pairs are equal to the corresponding ones of ϱ, and that a state is permutationally invariant for a given pair if and only if its marginal on that pair also is (see Proposition 1.2).

Concerning the state γ, using a similar reasoning, we know that it is permutationally symmetric for the pairs $\{A, B\}$ and $\{B, C\}$. Since $F_{AB}F_{BC}F_{AB} = F_{AC}$, it follows that $\gamma^{(AC)}$ also is permutationally symmetric. Moreover, from the marginal conditions we know that $\gamma^{(AC)} = \tau^{(A'C)}$, hence τ is permutationally symmetric for the pair $\{A', C\}$.

Since permutations of the pairs $\{A, B\}$, $\{B, C\}$, $\{C, A'\}$, $\{A', B'\}$ and $\{B', C'\}$ generate the full permutation group [128], we conclude that τ is totally permutationally symmetric. However, τ is separable with respect to the bipartition $ABC \mid A'B'C'$, so τ and hence $\varrho_\Delta = \tau^{(ABC)}$ must be fully separable.

The same argument can easily be extended to more complex networks (e.g., not restricted to use bipartite sources) and holds for states of arbitrary local dimension.

Proposition 4.13 (Permutationally symmetric states in networks [A])**.**

1. *Unless they are fully separable, permutationally symmetric states of n parties cannot be prepared in* LOSR *networks with $(n-1)$-partite sources.*

2. *Permutationally antisymmetric states of n parties cannot be prepared in* LOSR *networks with $(n-1)$-partite sources.*

Proof. Let ϱ be an n-partite permutationally (anti-)symmetric state, and let us assume that it can be generated in an n-node network with at most

$(n-1)$-partite sources. Any state that can be produced in a network with n nodes and no n-partite sources can also be created in a network of n nodes using n different $(n-1)$-partite sources. The sources used to prepare ϱ are denoted ς_i and they distribute parties to all nodes except the ith one, for all $i \in [n]$.

We construct an inflated network of $2n$ nodes $\cup_{i=1}^{n}\{A_i, A_i'\}$ and $2n$ sources $\cup_{k=1}^{n}\{\zeta_k, \zeta_k'\}$ that distribute parties to

$$\zeta_k \to A_1 \dots A_{k-1} A_{k+1}' \dots A_N', \tag{4.59a}$$
$$\zeta_k' \to A_1' \dots A_{k-1}' A_{k+1} \dots A_N, \tag{4.59b}$$

where $\zeta_k = \zeta_k' = \varsigma_k$ for all $k \in [n]$. Following the inflation formalism, the global state η of this inflation is built with the same sources and the same channels on the nodes than ϱ. So, the marginals must satisfy

$$\eta_{A_i A_{i+1}} = \eta_{A_i' A_{i+1}'} = \varrho_{A_i A_{i+1}} \quad \forall i \in [n-1], \tag{4.60a}$$
$$\eta_{A_1 A_n'} = \eta_{A_1' A_n} = \varrho_{A_1 A_n}. \tag{4.60b}$$

Since the state ϱ is totally (anti-)symmetric, Proposition 1.2 and Eq. (4.60) imply that the state η is also totally (anti-)symmetric.

Now, we consider the inflated state τ, whose sources $\cup_{k=1}^{n}\{\omega_k, \omega_k'\}$ distribute states to

$$\begin{aligned} \omega_k &\to A_1 A_2 A_3 \dots A_{k-1} A_{k+1} \dots A_n \\ \omega_k' &\to A_1' A_2' A_3' \dots A_{k-1}' A_{k+1}' \dots A_n'. \end{aligned} \tag{4.61}$$

This is the generalisation of the two-copy inflation considered in Figure 4.3 (b) and Figure 4.5 (b), and it follows that

$$\tau_{A_1 \dots A_n} = \tau_{A_1' \dots A_n'} = \varrho. \tag{4.62}$$

Moreover,

$$\tau_{A_i A_i'} = \eta_{A_i A_i'}, \tag{4.63}$$

hence τ is totally permutationally (anti-)symmetric. Since τ is separable with respect to the bipartition $A_1 \dots A_n \mid A_1' \dots A_n'$, it is fully separable. Therefore ϱ is also fully separable. If ϱ is permutationally symmetric, the proof is concluded. In the case of anti-symmetric ϱ, we reach a contradiction, which also finishes the proof. □

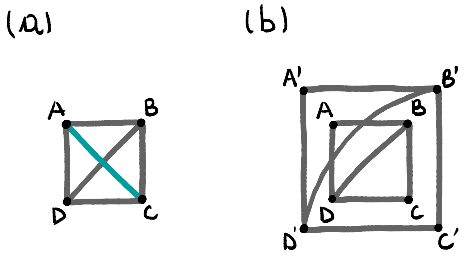

Figure 4.8: *Illustration of the link certification method.* (a) Four-partite network in the case of a broken AC link. (b) Its τ-inflation.

Finally, we note that states invariant under cyclic permutations may be prepared in LOSR networks, as already pointed out in [101]. As an example, we consider three Bell pairs $|\Phi^+\rangle$ as sources in the LOSR triangle network, and no channels applied on the nodes. The global (3×4)-partite state reads $|\Psi\rangle_{ABC} = |\Phi^+\rangle_{A_2B_1} |\Phi^+\rangle_{B_2C_1} |\Phi^+\rangle_{C_2A_1}$. With the appropriate reordering of the parties and by mapping $|ij\rangle_X \mapsto |2i + j\rangle_X$, for all $X = A, B, C$ and $i, j = 0, 1$, we obtain

$$\begin{aligned} |\Psi\rangle_{ABC} = \frac{1}{\sqrt{8}}\big(&|000\rangle + |012\rangle + |120\rangle + |201\rangle \\ &+ |132\rangle + |321\rangle + |213\rangle + |333\rangle \big), \end{aligned} \tag{4.64}$$

which is invariant under cyclic permutations of (A, B, C).

4.3 Certification of network links

For the experimental implementation of quantum networks, it is important to have access to methods that certify that the different network components are working properly. Here, we propose a method that detects if network links (to be understood as entanglement distribution) work properly. Consider a network where the link between two parties is absent or simply not working properly. For definiteness, we may consider the four-partite network in Figure 4.8 (a) and want to test whether the AC source distributed its parties to A and C correctly. We thus consider the LOSR network without the edge between A and C. In two-copy inflation (see Figure 4.8 (b)), the observables $Y_A Y_C$ and $Z_{A'} Z_C$ anticommute. Moreover, the state τ of this inflation verifies $\tau^{(AC)} = \tau^{(A'C)} = \varrho^{(AC)}$, so we have

$$\langle Y_A Y_C \rangle_\varrho^2 + \langle Z_A Z_C \rangle_\varrho^2 \leq 1, \tag{4.65}$$

for LOSR network states ϱ such as in Figure 4.8 (a), without the link AC. Using higher-order inflations, this reasoning can be extended and formulated for general networks.

Proposition 4.14 (Network link certification [A]). *If an n-qubit state ϱ verifies*

$$\langle X_A X_C P_{R_1}\rangle_\varrho^2 + \langle Y_A Y_C P_{R_2}\rangle_\varrho^2 + \langle Z_A Z_C P_{R_3}\rangle_\varrho^2 > 1, \tag{4.66}$$

then it cannot have been prepared in an n-partite LOSR *network with bipartite sources and a missing link AC. Therein, P_{R_1}, P_{R_2}, and P_{R_3}, are arbitrary observables on disjoint subsets of qubits (except qubits A and C), i.e., observables on subsets $R_i \not\supseteq \{A, C\}$ such that $R_i \cap R_j = \emptyset$ for all $i \neq j$, $i, j \in [3]$.*

For a detailed proof of this statement, see [A]. Finally, we give a simple example where this criterion can detect the functionality of a link. Consider the four-qubit target state

$$\varrho(v) = \left(v\left|\Phi^+\right\rangle\!\left\langle\Phi^+\right| + \frac{1-v}{4}\mathbb{1}\right)_{AC} \otimes |00\rangle\langle 00|_{BD}\,, \quad v \in [0,1]. \tag{4.67}$$

We want to check whether the link AC works or not, i.e., check that the entanglement between A and C was properly distributed. It is easy to verify that

$$-\langle Y_A Y_C Z_D\rangle_\varrho = \langle Z_A Z_C\rangle_\varrho = v. \tag{4.68}$$

Equation (4.65) thus certifies that $\varrho(v)$ cannot have been prepared in a network with a broken link when $v \in]1/\sqrt{2}, 1]$.

4.4 Certification of network topology

In this final section, we aim to certify the whole topology of a quantum network. Specifically, we analyse networks where n distant parties share an n-qubit basic network state, i.e., each of the parties holds a qubit from a single source and no operations are performed on the nodes. We note that the case of multiple qubits per node can be considered by treating each qubit as an individual node. The results in this section are published in [D].

4.4.1 Statistical hypotheses test

In order to be able to make rigorous claims about the topology of a basic network, we formulate our protocol in the language of hypothesis testing.

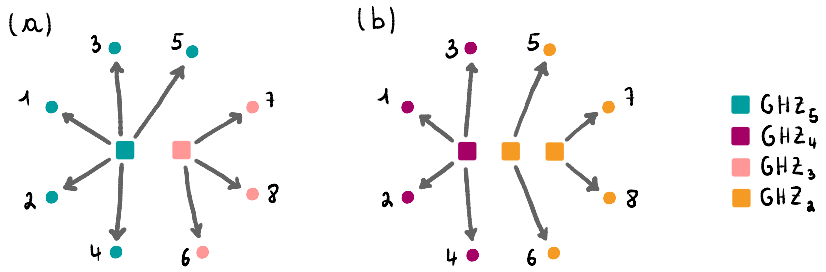

Figure 4.9: *Two possible topologies for an eight-partite network.* (a) Parties 1, 2, 3, 4 and 5 share a $|\mathrm{GHZ}_5\rangle$ state (in green) and parties 6, 7 and 8 share a $|\mathrm{GHZ}_3\rangle$ state (in pink). (b) Parties 1, 2, 3 and 4 share a $|\mathrm{GHZ}_4\rangle$ state (in purple) and parties 5 and 6, and 7 and 8 both share $|\mathrm{GHZ}_2\rangle$ states (in orange). Figures adapted from [D].

This goes as follows: The n parties sharing a basic network state identify the possible network topologies they may share, and to each possible topology, they associate a hypothesis based on the fidelities to the possible source states. The hypotheses should be mutually exclusive and the general protocol should tolerate a certain amount of noise in the source states, should require few state samples, and should be implementable with product measurements.

The protocol derived in [D] is best explained by example: Consider eight parties who each receive a qubit. They want to distinguish for instance between two possible topologies, which are represented in Figure 4.9. We label the networks by the partitioning of the parties following the source distribution, i.e., $T_a = \{\{1,2,3,4,5\},\{6,7,8\}\}$ corresponds to the topology of Figure 4.9 (a), and $T_b = \{\{1,2,3,4\},\{5,6\},\{7,8\}\}$ to Figure 4.9 (b). Clearly, other eight-qubit network topologies are possible, but omitted in this example for simplicity. Here and in the following, we aim to certify that the sources distribute (possibly noisy) multi-qubit GHZ states. As already mentioned, GHZ states are highly relevant states in quantum information theory, as they are key elements of many important applications, such as quantum key distribution [110].

We construct the hypotheses associated to the topologies under consideration based on the fidelities to the possible source states, i.e.,

$$F_s = \left\langle \mathrm{GHZ}_{|s|} \right| \varrho^{(s)} \left| \mathrm{GHZ}_{|s|} \right\rangle \quad \forall s \in T_a \cup T_b, \tag{4.69}$$

where we recall that $|s|$ is the cardinality of the set s, and $\varrho^{(s)}$ stands for the marginal of the global eight-qubit state $\varrho \in \mathcal{S}((\mathcal{H}^2)^{\otimes 8})$ on the qubits in s, with $s \in T_a \cup T_b$.

From a physical point of view, it is important to certify that a working source s produces GHZ states with a fidelity $F_s > 1/2$, as GHZ fidelity witnesses then guarantee the presence of GME (see Section 1.3.3). On the other hand, if F_s is close to one, the fidelity to any m-qubit GHZ state with $m < |s|$ is close to one half, due to the common entries on the diagonals of the density operators. Therefore, since we want the different hypotheses to be mutually exclusive, requiring that the fidelities to source states of a given topology are larger than one half may not be sufficient.

These considerations motivate the following strategy to formulate exclusive hypotheses for the L different topologies T_i, with $i \in [L]$. Any topology T_i is characterised by a set of fidelities to the sources of T_i, $\{F_s\}_{s\in T_i}$. We thus construct the hypothesis H_i corresponding to the network topology T_i as

$$H_i = \left\{ F_s - \max\left\{ F_{s'} \mid s' \supset s, s' \in \cup_{i=1}^{L} T_i \right\} > \frac{1}{2} \right\}_{s\in T} \quad \forall i \in [L], \tag{4.70}$$

and we note that s' must be a strict superset of s. For convenience, we define

$$D_s = F_s - \max\left\{ F_{s'} \mid s' \supset s, s' \in \cup_{i=1}^{L} T_i \right\} \quad \forall s \in \cup_{i=1}^{L} T_i. \tag{4.71}$$

In the example of Figure 4.9, the two hypotheses are

$$H_a = \begin{cases} F_{\{1,2,3,4,5\}} > 1/2 \quad \text{and} \\ F_{\{6,7,8\}} > 1/2, \end{cases} \tag{4.72a}$$

$$H_b = \begin{cases} F_{\{1,2,3,4\}} - F_{\{1,2,3,4,5\}} > 1/2, \\ F_{\{5,6\}} > 1/2 \quad \text{and} \\ F_{\{7,8\}} - F_{\{6,7,8\}} > 1/2. \end{cases} \tag{4.72b}$$

Additionally, we consider the null hypothesis H_0, which can account for instance for cases where states different from GHZ states have been distributes.

4.4.2 Simultaneous fidelity estimation

It remains to be shown how to compute the values of the fidelities to the possible source states efficiently. We recall that the fidelity of an arbitrary n-qubit state $\varrho \in \mathcal{S}((\mathcal{H}^2)^{\otimes n})$ to the n-qubit GHZ state can be obtained as

follows: $|\mathrm{GHZ}_n\rangle$ can be decomposed as

$$|\mathrm{GHZ}_n\rangle\langle\mathrm{GHZ}_n| = \frac{1}{2}\left(\underbrace{|0\rangle\langle 0|^{\otimes n} + |1\rangle\langle 1|^{\otimes n}}_{\mathcal{D}_n} + \underbrace{|0\rangle\langle 1|^{\otimes n} + |1\rangle\langle 0|^{\otimes n}}_{\mathcal{A}_n}\right), \quad (4.73)$$

where $\mathcal{D}_n$ and $\mathcal{A}_n$ correspond to the diagonal and antidiagonal terms respectively. The GHZ fidelity $F_{[n]}$ of ϱ is thus equal to $1/2(\mathrm{tr}(\mathcal{D}_n\varrho) + \mathrm{tr}(\mathcal{A}_n\varrho))$. The first term can be evaluated from the data of measuring $Z^{\otimes n}$, as $|0\rangle^{\otimes n}$ and $|1\rangle^{\otimes n}$ are part of its eigenstates. The antidiagonal term can be evaluated from the data of n further settings. Indeed, notice that it can be written as a linear combination of the Pauli observables X and Y [64],

$$\mathcal{A}_n = \frac{1}{n}\sum_{i=1}^{n}(-1)^{i-1}\mathcal{M}_i^{\otimes n}, \quad (4.74)$$

where

$$\mathcal{M}_i = \cos\left(\frac{(i-1)\pi}{n}\right)X + \sin\left(\frac{(i-1)\pi}{n}\right)Y, \quad \forall i \in [n]. \quad (4.75)$$

Using the expectation values $\mathcal{M}_i^{\otimes n}$ for all $i \in [n]$ and $Z^{\otimes n}$, the fidelity $F_{[n]}$ can thus be estimated with $n+1$ product measurement settings.

Remarkably, the data of those $n+1$ measurement settings is sufficient to compute the fidelity of the marginal states of ϱ to any m-qubit GHZ state, for $m \leq n$. This follows from the fact that the decomposition of $\mathcal{A}_n$ is not unique, thus other sets of measurements that are linear combination of X and Y also allow us to determine $\mathcal{A}_n$ [64]. This paves the way for the simultaneous estimation of several GHZ fidelities: The expectation values $\langle\mathcal{M}_k^{\otimes|s|}\rangle_{\varrho^{(s)}}$, for the sources $s \in \cup_{i=1}^{L} T_i$ of all topologies under consideration can be obtained from the same data set, which allows for the computation of the fidelity F_s for all sources s appearing in the topologies T_i, $i \in [L]$. For technical details and explicit formulas, see [D]. We emphasise that the protocol requires only $n+1$ measurement settings, independently of the number of topologies under consideration.

4.4.3 Certification based on experimental data

In the following, we demonstrate our protocol for six-partite photonic network states. The topologies under consideration are presented in Figure 4.10, still with the aim to certify GHZ sources. These four topologies are

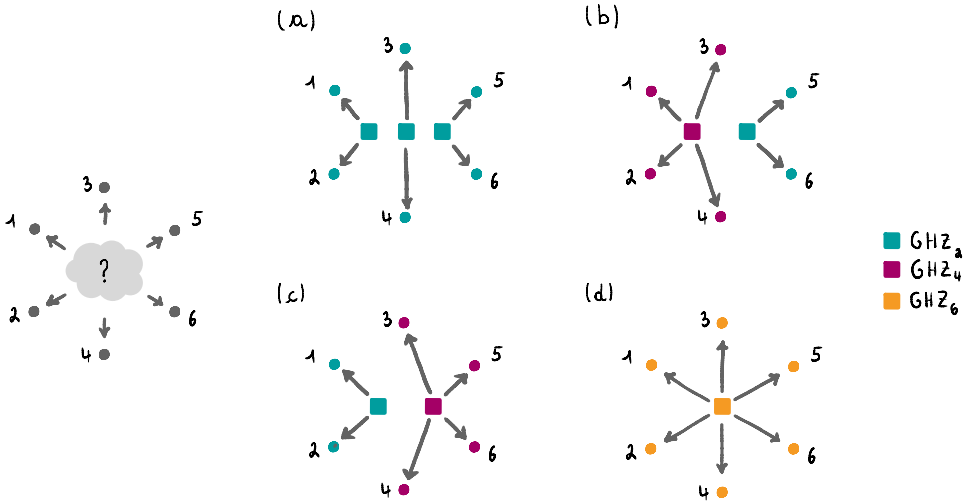

Figure 4.10: *Four possible topologies for a six-partite network.* Six parties share a basic network state with GHZ sources, but are unsure about its topology. (a), (b) (c), (d) Network topologies T_a, T_b, T_c, and T_d respectively.

identified on the basis of the experimental set up: By different programming of the same experiment, four different global states can be generated, namely $|\text{GHZ}_2\rangle \otimes |\text{GHZ}_2\rangle \otimes |\text{GHZ}_2\rangle$, $|\text{GHZ}_4\rangle \otimes |\text{GHZ}_2\rangle$, $|\text{GHZ}_2\rangle \otimes |\text{GHZ}_4\rangle$, and $|\text{GHZ}_6\rangle$. These are associated to the topologies T_a, T_b, T_c, and T_d of Figure 4.10 respectively. The hypothesis formulated on this basis are given by

$$H_a = \begin{cases} F_{\{1,2\}} - \max\{F_{\{1,2,3,4\}}, F_{\{1,2,3,4,5,6\}}\} > 1/2, \\ F_{\{3,4\}} - \max\{F_{\{1,2,3,4\}}, F_{\{3,4,5,6\}}, F_{\{1,2,3,4,5,6\}}\} > 1/2 \quad \text{and} \\ F_{\{5,6\}} - \max\{F_{\{3,4,5,6\}}, F_{\{1,2,3,4,5,6\}}\} > 1/2, \end{cases} \tag{4.76a}$$

$$H_b = \begin{cases} F_{\{1,2,3,4\}} - F_{\{1,2,3,4,5,6\}} > 1/2, \quad \text{and} \\ F_{\{5,6\}} - \max\{F_{\{3,4,5,6\}}, F_{\{1,2,3,4,5,6\}}\} > 1/2, \end{cases} \tag{4.76b}$$

$$H_c = \begin{cases} F_{\{1,2\}} - \max\{F_{\{1,2,3,4\}}, F_{\{1,2,3,4,5,6\}}\} > 1/2, \quad \text{and} \\ F_{\{3,4,5,6\}} - F_{\{1,2,3,4,5,6\}} > 1/2, \end{cases} \tag{4.76c}$$

$$H_d = \begin{cases} F_{\{1,2,3,4,5,6\}} > 1/2. \end{cases} \tag{4.76d}$$

We briefly explain how the experiment is implemented, and refer to [D] for a detailed description. As shown in Figure 4.11, a source first generates polarisation entangled photons in a GHZ state. Then, one of the two photons is detected, while its partner is stored in a quantum memory. It is then either

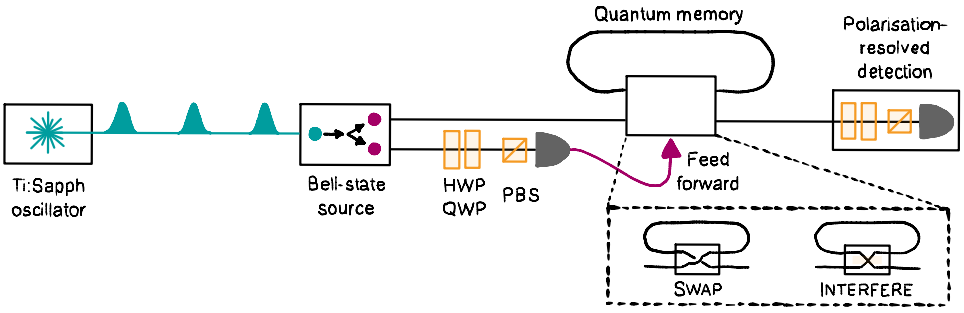

Figure 4.11: *Experimental setup for the certification of six-partite network topologies.* Three Bell pairs are successively produced by a probabilistic dispersion-engineered integrated source. One of the photons of the pair is detected, generating a feed-forward signal to the quantum memory. Following this, photons from different pairs are either swapped or interfered, producing one of the four states $|\mathrm{GHZ}_2\rangle \otimes |\mathrm{GHZ}_2\rangle \otimes |\mathrm{GHZ}_2\rangle$, $|\mathrm{GHZ}_4\rangle \otimes |\mathrm{GHZ}_2\rangle$, $|\mathrm{GHZ}_2\rangle \otimes |\mathrm{GHZ}_4\rangle$, or $|\mathrm{GHZ}_6\rangle$. HWP: half-wave plate. QWP: quarter-wave plate. PBS: polarising beam splitter. Figure adapted from [D].

swapped or interfered with a photon from a successive Bell pair, respectively leading to the generation of $|\mathrm{GHZ}_2\rangle \otimes |\mathrm{GHZ}_2\rangle$ or of $|\mathrm{GHZ}_4\rangle$. A third Bell pair is used similarly, such that in the end, one of the four states depicted in Figure 4.10 is produced. We note that in the setup, the four-photon GHZ state has a phase of $\left|\mathrm{GHZ}_4^-\right\rangle = 1/\sqrt{2}(|0000\rangle - |1111\rangle)$, we thus formulate the hypotheses for this four-photon state. By abuse of notation, we still refer to this four-qubit GHZ state by $|\mathrm{GHZ}_4\rangle$.

For each of the four possible states, the six observables $\mathcal{M}_i^{\otimes 6}$, for all $i \in [6]$, and the observable $Z^{\otimes 6}$ are measured around a thousand times to estimate their expectation values [D]. From this data, the fidelities to the six possible sources are computed and reported in green in Figure 4.12 [D]. The values of D_s, defined in Eq. (4.71), are plotted in purple in Figure 4.12 as well. Using Hoeffding's inequality [73], upper bounds on the p-values associated to each of the hypotheses are computed in [D], which we report in Table 4.2. We recall that the p-value of a hypothesis H describes the probability of observing the experimental data given that the hypothesis H is true. For the details concerning the evaluation of the upper bounds, see [D].

We note that on top of certifying the topology of the network, for each data set the parties characterised the quality of their sources through the fidelity to the different GHZ states.

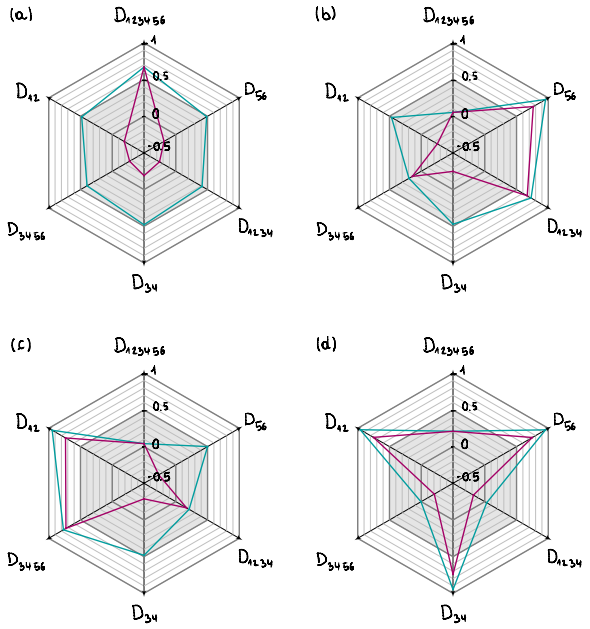

Figure 4.12: *Graphical depiction of the fidelities* F_s (green curves) and the differences of the fidelities D_s (purple curves) considered in the hypotheses for the four different experimental data sets, with $s \in \cup_{i=a,b,c,d} T_i$. Recall that the hypothesis H_i requires that D_s is strictly larger than one half for all the sources s of the topology T_i, with $i = a, b, c, d$. Figures adapted from [D].

4.4.4 Device-independent approach

An important point of the certification method introduced is that the measurement performed on the physical systems are assumed to be fully characterised. However, this is in general not the case. To remedy this situation, we briefly discuss how such a method could be implemented in a device-independent manner.

We consider the Bell operator $\mathcal{B}_n$ from the n-partite Mermin inequality [105], which contains products of two dichotomic observables that we label by A and B and reads

$$\mathcal{B}_n = \frac{1}{2}\left[(A + iB)^{\otimes n} + (A - iB)^{\otimes n}\right]. \tag{4.77}$$

Notably, the expectation value $\langle \mathcal{B}_n \rangle_\varrho$ can be used to bound the fidelity of the state ϱ to the n-qubit GHZ state, in the sense that if $\langle \mathcal{B}_n \rangle_\varrho$ is close to 2^{n-1}, the fidelity to $|\mathrm{GHZ}_n\rangle$ (up to local operations) must be high. For the detailed computations, we refer to [D].

The n parties involved in the certification protocol would have to obtain

	H_a	H_b
Data set 1	1	2.3724×10^{-139}
Data set 2	8.3274×10^{-92}	1
Data set 3	6.1789×10^{-93}	6.8294×10^{-259}
Data set 4	1.1810×10^{-32}	3.7960×10^{-174}

H_c	H_d	H_0
9.2153×10^{-146}	3.0256×10^{-116}	9.4765×10^{-8}
1.6231×10^{-258}	1.6231×10^{-258}	1.4347×10^{-13}
1	8.8629×10^{-272}	1.3010×10^{-23}
4.9169×10^{-188}	1	2.3295×10^{-22}

Table 4.2: Upper bound on the p-value of the different hypotheses for the four different data sets. Each data set corresponds to one of the four possible combinations of operations "swap" and "interfere". The hypotheses H_a, H_b, H_c, and H_d are explicitly given by Eq. (4.76), and H_0 is the null hypothesis.

the expectation values of all 2^n combinations of A and B, which they could then use to evaluate the expectation values of $\langle \mathcal{B}_m \rangle_\varrho^{(s)}$ for all $s \in \cup_{i=1}^{L} T_i$, where T_i with $i \in [L]$ are the L different topologies under consideration. As the number of settings scales exponentially with the number of qubits, such a protocol is in practice not feasible for large systems. Nevertheless, if we can reasonably assume that the GHZ sources are made up of at most m qubits with $m < n$, not all 2^n combinations of A and B have to be measured, but rather all 2^m combinations of A and B on all subsets of m parties. Settings that fulfil this are nothing but covering arrays $\mathrm{CA}(n, m, 2)$ with symbols A and B, for which it has been shown that [34]

$$\mathrm{CAN}(n, m, 2) \leq 2^n n^{\mathrm{O}_{\log(n)}} \log(m). \tag{4.78}$$

When all the sources of the network are bipartite, i.e., when $m = 2$, it is known that $\mathrm{CAN}(n, 2, 2)$ is the smallest natural number x such that [143]

$$n \leq \binom{x-1}{\lceil x/2 \rceil} \tag{4.79}$$

holds. Moreover, there exists an algorithm which, for a given numbers n and x, constructs a $\mathrm{CA}(x; n, 2, 2)$ in polynomial time [143]. Therefore, settings based on covering arrays are a potential candidate for the device independent implementation of the network topology certification protocol.

4.5 Discussion

This chapter dealt with states preparable in quantum network structures with no access to classical communication. We presented four distinct approaches to characterise network states.

First, we investigated how such network states impose strong conditions on the structure of their covariance matrices. We presented alternative proofs for the block decomposition of covariance matrices and derived analytical and computable necessary criteria for network states without shared randomness.

Second, we turned our attention to states with symmetric properties, demonstrating that large classes of states, such as noisy graph states with up to 12 qubits and permutationally symmetric states, cannot be prepared in quantum networks with shared randomness. We presented analytical techniques to derive upper bounds on the fidelity of LOSR network states to some target GME states, notably showing that state with a fidelity to the GHZ state higher than $1/16(5+\sqrt{73}) \simeq 0.8465$ cannot have been prepared in the LOSR triangle network. Beyond excluding the preparation of certain states in network scenarios, the proof techniques employed, analytically combining the inflation technique with general expectation value bounds, are valuable in their own right. The techniques can be used on different target states, and have since been used in the works [103] and [151].

Finally, we introduced methods for the certification of network links as well as network topology. Notably, the latter only requires $n+1$ measurement settings, regardless of the number of topologies under consideration, with n being the number of qubits in the network. The topology certification protocol was experimentally performed for six-qubit networks using entangled photon pairs.

As the field of network entanglement and its potential applications in quantum information theory continues to grow, it is valuable to investigate additional avenues for identifying compatible network states. Specifically, finding sufficient criteria for network states, as current results provide only necessary criteria, represents a crucial area of future research. Developing such criteria will lead to a better understanding of states that can be generated in networks without classical communication and their potential applications, such as in quantum conference key agreement. In this context, it is interesting to also consider noisy networks: This would translate to imposing additional conditions on the sources states, e.g., by making them

travel through depolarisation channels or by constraining their purity.

Conclusion

In this thesis, we aimed to contribute to the vast field of quantum information theory in two main ways: We both addressed foundational problems and developed innovative certification methods for quantum systems. All the problems addressed in this thesis were, in a sense, connected to notions in graph theory. These connections helped us to gain insight into physical problems, which we summarise here.

First, we focused our attention on the problem of bounding sums of squares of expectation values. The first connection to graph theory arises here, as we have shown that this function of expectation values is upper bounded by the Lovász number of their anticommutativity graph. Although this problem may seem highly specific at first glance, we have demonstrated that it has broader implications, particularly in the context of entanglement detection. Specifically, we illustrated that this bound can be used to derive entanglement and Schmidt number witnesses, and other authors later found applications in ground state energy estimation [4] and quantum state tomography [90]. Even after the follow-up works [163] and [106], several fundamental questions remain open that we hope will be answered in the upcoming years.

Moving towards the certification of quantum devices, we discussed the topic of marginal tomography. Quantum state tomography is essential for characterising quantum systems, but traditional methods become impractical for large systems. We presented different measurement scheduling schemes for marginal tomography of multi-qubit systems that are all optimal according to different figures of merit. In the case of Pauli tomography, we translated the problem of finding the minimal number of settings for the reconstruction of marginals to a graph covering problem. This allowed us to compute minimal Pauli sets for specific examples, and to discuss the optimality of previous construction. We also briefly discussed its connection to the concepts of covering and orthogonal arrays in combinatorial design

theory. Notably, we showed that the minimum of 3^k projective measurement settings is tomographically complete for any subset of k qubits when chosen randomly (according to the uniform distribution on the unit sphere). An analytical construction of measurement settings for any number of qubits n and any k is still left to be found. This presents a significant challenge and opportunity for future research. An experimental demonstration of two-body marginal tomography of a six-qubit system using measurement scheduling introduced in this thesis is presented in [E].

The last and largest chapter of this thesis was devoted to quantum networks. First, we were interested in the concept of network entanglement and derived necessary criteria for network entangled states that allowed us to rule out the preparation of well-known states in network scenarios. As discussed, there are two main definitions of network entanglement, with the difference of access or not to shared randomness. Criteria for networks without shared randomness were derived using covariance matrices, and using a combination of the inflation technique and expectation value bounds we proved propositions for network entanglement with shared randomness. Notably, for the latter, we showed that large classes of symmetric states cannot be prepared in network scenarios. This insight is crucial for understanding the limitations and potentials of quantum networks. Afterwards, we used these results to devise certification methods for network links, and finally tackled the certification of the whole topology of the network with few measurement settings. The topology certification protocol stands out as it is based on fidelity estimation, thus can certify that entanglement is indeed present in the shared network, distinguishing it from classical correlations. This protocol thus represents a significant advancement in the practical benchmarking of quantum networks.

In each chapter, many open problems remain. We also hope that the results and techniques developed in this thesis will be of use to others in the future.

Appendix A

Appendix to Chapter 3

In this appendix, we present the connection between $\sigma_{\mathcal{S}}$ and the volume spanned by the measurement directions of a given measurement map $M_{\mathcal{S}}$. We first adapt the measurement map of Eq. (1.38) and define the matrix $M_{\mathcal{S}} \in \mathbb{C}^{L\times d^2}$ such that

$$M_{\mathcal{S}}\mathbf{v}(\varrho_{\mathcal{S}}) = \mathbf{p}, \tag{A.1}$$

where $\mathbf{v} : \mathbb{C}^{d\times d} \to \mathbb{C}^{d^2}$ is a vectorisation satisfying $\mathbf{v}(A)\cdot\mathbf{v}(B) = \mathrm{tr}\big(A^\dagger B\big)$. Since we are interested in measurement direction for two-body tomography of a six-qubit system, $d = 4$ and $L = 36$. We further decompose $M_{\mathcal{S}}$ as $M_{\mathcal{S}} = A_{\mathcal{S}}B$, where the matrix B is such that its ith row is given by the vectorisation of the ith Pauli operator ordered as

$$(\mathbb{1}\mathbb{1}, X\mathbb{1}, Y\mathbb{1}, Z\mathbb{1}, \mathbb{1}X, \mathbb{1}Y, \mathbb{1}Z, XX, XY, XZ, YX, YY, YZ, ZX, ZY, ZZ), \tag{A.2}$$

for all $i \in [16]$. The matrix $A_{\mathcal{S}}$ is given by the 36×16 real matrix

$$A_{\mathcal{S}} = \frac{1}{36}\begin{pmatrix} 1 & \mathbf{v}_1^{(i)} & \mathbf{v}_1^{(j)} & \mathbf{v}_1^{(i)}\otimes\mathbf{v}_1^{(j)} \\ 1 & \mathbf{v}_1^{(i)} & -\mathbf{v}_1^{(j)} & -\mathbf{v}_1^{(i)}\otimes\mathbf{v}_1^{(j)} \\ 1 & -\mathbf{v}_1^{(i)} & \mathbf{v}_1^{(j)} & -\mathbf{v}_1^{(i)}\otimes\mathbf{v}_1^{(j)} \\ 1 & -\mathbf{v}_1^{(i)} & -\mathbf{v}_1^{(j)} & \mathbf{v}_1^{(i)}\otimes\mathbf{v}_1^{(j)} \\ 1 & \mathbf{v}_2^{(i)} & \mathbf{v}_2^{(j)} & \mathbf{v}_2^{(i)}\otimes\mathbf{v}_2^{(j)} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & -\mathbf{v}_9^{(i)} & -\mathbf{v}_9^{(j)} & \mathbf{v}_9^{(i)}\otimes\mathbf{v}_9^{(j)} \end{pmatrix}. \tag{A.3}$$

We define the 16×16 matrix $X_{\mathcal{S}} = M_{\mathcal{S}}^{\dagger} M_{\mathcal{S}} = B^{\dagger} A_{\mathcal{S}}^{T} A_{\mathcal{S}} B$ and compute

$$A_{\mathcal{S}}^{T} A_{\mathcal{S}} = \frac{4}{36^2} \begin{pmatrix} 9 & 0 & 0 & 0 \\ 0 & \sum_{\alpha=1}^{9} \mathbf{v}_{\alpha}^{(i)} (\mathbf{v}_{\alpha}^{(i)})^T & 0 & 0 \\ 0 & 0 & \sum_{\alpha=1}^{9} \mathbf{v}_{\alpha}^{(j)} (\mathbf{v}_{\alpha}^{(j)})^T & 0 \\ 0 & 0 & 0 & \sum_{\alpha=1}^{9} (\mathbf{v}_{\alpha}^{(i)} \otimes \mathbf{v}_{\alpha}^{(j)})(\mathbf{v}_{\alpha}^{(i)} \otimes \mathbf{v}_{\alpha}^{(j)})^T \end{pmatrix}. \tag{A.4}$$

On the other hand, we can express $\sigma_{\mathcal{S}}$ as

$$\sigma_{\mathcal{S}} = \max_{\mathbf{e}} \left\| M_{\mathcal{S}}^{+} \mathbf{e} \right\| = \max_{\mathbf{e}} \sqrt{\mathbf{e}^T (M_{\mathcal{S}}^{+})^{\dagger} M_{\mathcal{S}}^{+} \mathbf{e}}, \tag{A.5}$$

where the maximum is taken over vectors $\mathbf{e}$ from the standard basis, and where the norm is the Euclidean norm [41]. The pseudoinverse is chosen to be the Moore-Penrose inverse, and from the singular value decomposition of the measurement map $M_{\mathcal{S}} = \sum_{i=1}^{16} \mu_i \mathbf{u}_i \mathbf{w}_i^{\dagger}$, we can write $M_{\mathcal{S}}^{+} = \sum_{i=1}^{16} 1/\mu_i \mathbf{w}_i \mathbf{u}_i^{\dagger}$, such that

$$\sigma_{\mathcal{S}} \leq \sqrt{\sum_{i=1}^{16} \frac{1}{\mu_i^2}} = \sqrt{\sum_{i=1}^{16} \frac{1}{\nu_i}}, \tag{A.6}$$

where ν_i, $i \in [16]$ are the eigenvalues of $X_{\mathcal{S}}$. We denote the last 9×9 block of $A_{\mathcal{S}}^{T} A_{\mathcal{S}}$ by $Y_{\mathcal{S}}$, that is,

$$Y_{\mathcal{S}} = \sum_{\alpha=1}^{9} (\mathbf{v}_{\alpha}^{(i)} \otimes \mathbf{v}_{\alpha}^{(j)})(\mathbf{v}_{\alpha}^{(i)} \otimes \mathbf{v}_{\alpha}^{(j)})^T, \tag{A.7}$$

and its eigenvalues are non-negative numbers λ_i, $i \in [9]$. The matrix

$$Z_{\mathcal{S}} = (v_1^{(i)} \otimes v_1^{(j)}, v_2^{(i)} \otimes v_2^{(j)}, \ldots, v_9^{(i)} \otimes v_9^{(j)}) \tag{A.8}$$

is such that $Y_{\mathcal{S}} = Z_{\mathcal{S}} Z_{\mathcal{S}}^T$, and therefore $Z_{\mathcal{S}}$ has singular values $\sqrt{\lambda_i}$, $i \in [9]$. Finally, we can write the determinant of $Z_{\mathcal{S}}$ as $|\det(Z_{\mathcal{S}})| = \prod_{i=1}^{9} \sqrt{\lambda_i}$. By denoting the second and third block of $A_{\mathcal{S}}$ by Y_i and Y_j respectively, we can write $\det(X_{\mathcal{S}}) = 1/36 \det(BB^{\dagger}) \det(Y_i Y_j) \det(Z_{\mathcal{S}})^2$. Due to Eq. (A.6), we can expect that large $|\det(Z_{\mathcal{S}})|$ lead to small $\sigma_{\mathcal{S}}$.

The measurement directions obtained through the numerical optimisation of all volumes as described in Chapter 3 are presented in Table A.1. The

α	Qubit 1	Qubit 2	Qubit 3
1	$[1.34851, -1.7187]$	$[0.74451, 1.85896]$	$[2.81234, -1.66384]$
2	$[1.62452, -0.16006]$	$[0.83181, -1.13389]$	$[1.24291, -1.56911]$
3	$[0.2289, 1.17782]$	$[0.83405, -0.17509]$	$[2.33714, 0.27682]$
4	$[0.88628, 0.06155]$	$[0.98653, -2.38924]$	$[2.63105, -1.5318]$
5	$[0.9695, 2.22663]$	$[1.64509, 0.36903]$	$[1.06042, -1.5596]$
6	$[1.01301, -2.04348]$	$[1.83028, 0.04163]$	$[2.21489, 2.65553]$
7	$[2.70374, 0.28677]$	$[2.08781, -1.20394]$	$[1.16136, 1.41667]$
8	$[1.69042, -1.54368]$	$[1.55645, -1.52536]$	$[1.54184, 3.13342]$
9	$[1.9898, 3.11515]$	$[2.88169, -3.04215]$	$[1.58265, -3.12376]$

Qubit 4	Qubit 5	Qubit 6
$[1.22444, -2.24737]$	$[2.62025, -1.56922]$	$[1.61654, 2.41608]$
$[1.86266, 1.89939]$	$[0.78386, 2.4564]$	$[0.32988, 0.14995]$
$[0.74332, -0.27308]$	$[2.61964, -1.73379]$	$[1.32478, -1.55164]$
$[0.94539, 2.20137]$	$[1.04552, 0.26519]$	$[1.65486, 1.47209]$
$[1.70326, -2.5176]$	$[1.60308, 3.08691]$	$[2.42079, -0.27072]$
$[2.12737, 2.11179]$	$[1.05058, -1.644]$	$[1.56836, -2.29642]$
$[2.56575, -0.74011]$	$[2.09094, 1.49761]$	$[0.04581, 2.36286]$
$[2.56242, -2.33567]$	$[1.532, 3.04614]$	$[0.91042, 0.21545]$
$[1.08649, -2.97173]$	$[2.09094, 1.49761]$	$[1.2526, 3.01513]$

Table A.1: *Measurement directions used for the 6-qubit experimental implementation.* Each entry is a pair of Bloch vector angles $[\theta, \phi]$ in radians. Each row (continued on both tables) corresponds to one 6-qubit measurement setting $\mathcal{M}_\alpha$ as defined in Eq. (3.14), with $\alpha \in [9]$.

single-qubit $i \in [6]$ directions are partitioned in orthonormal bases following

$$\begin{array}{lll} \{\{1,2,3\}, & \{4,5,6\}, & \{7,8,9\}\}, \\ \{\{1,2,5\}, & \{3,4,7\}, & \{6,8,9\}\}, \\ \{\{1,2,8\}, & \{3,6,7\}, & \{4,5,9\}\}, \\ \{\{1,3,4\}, & \{2,8,9\}, & \{5,6,7\}\}, \\ \{\{1,5,9\}, & \{2,4,7\}, & \{3,6,8\}\}, \quad \text{and} \\ \{\{1,6,7\}, & \{2,4,9\}, & \{3,5,8\}\} \end{array} \tag{A.9}$$

respectively.

Appendix B

Appendix to Chapter 4

In this appendix, we prove the technical results from Chapter 4.

B.1 Off-diagonal blocks in terms of reduced observables

Here we prove that the off-diagonal blocks of the CM of a BTN state can be expressed using the reduced observables, that is,

$$[\gamma_E]_{mn} = \langle A_m^{(2)} \otimes B_n^{(1)} \rangle_{\varrho_{\mathrm{BTN}}^{(A_2B_1)}} - \langle A_m^{(2)} \rangle_{\varrho_{\mathrm{BTN}}^{(A_2B_1)}} \langle B_n^{(1)} \rangle_{\varrho_{\mathrm{BTN}}^{(A_2B_1)}} \quad \forall m, n \in [N]. \tag{B.1}$$

with

$$A_i^{(2)} = \mathrm{tr}_{A_1}\left(A_i (\varrho_{\mathrm{BTN}}^{(A_1)} \otimes \mathbb{1}_{A_2}) \right) \quad \forall i \in [N] \tag{B.2}$$

and similarly for $B_i^{(1)}$, $i \in [N]$.

Proof of Eq. (4.5). Let us decompose A_m and B_n respectively in orthogonal bases $\{\sigma_\alpha^{(A_1)} \otimes \sigma_\beta^{(A_2)}\}_{\alpha,\beta=1}^{d^2}$ and $\{\sigma_\gamma^{(B_1)} \otimes \sigma_\delta^{(B_2)}\}_{\gamma,\delta=1}^{d^2}$ as (we drop the superscripts)

$$A_m = \frac{1}{d^2} \sum_{\alpha,\beta=1}^{d^2} \mathrm{tr}\big(\sigma_\alpha \otimes \sigma_\beta A_m\big) \sigma_\alpha \otimes \sigma_\beta \tag{B.3}$$

and

$$B_n = \frac{1}{d^2} \sum_{\gamma,\delta=1}^{d^2} \mathrm{tr}(\sigma_\gamma \otimes \sigma_\delta B_n) \sigma_\gamma \otimes \sigma_\delta, \tag{B.4}$$

and notice that the reduced states of ϱ_{BTN} are product states,

$$\varrho_{\text{BTN}}^{(AB)} = \varrho_{\text{BTN}}^{(A_1)} \otimes \varrho_{\text{BTN}}^{(A_2B_1)} \otimes \varrho_{\text{BTN}}^{(B_2)}, \tag{B.5}$$

$$\varrho_{\text{BTN}}^{(A)} = \varrho_{\text{BTN}}^{(A_1)} \otimes \varrho_{\text{BTN}}^{(A_2)}, \tag{B.6}$$

$$\varrho_{\text{BTN}}^{(B)} = \varrho_{\text{BTN}}^{(B_1)} \otimes \varrho_{\text{BTN}}^{(B_2)}. \tag{B.7}$$

Combining this, $[\gamma_E]_{mn}$ straightforwardly decomposes as

$$\langle A_m^{(2)} \otimes B_n^{(1)} \rangle_{\varrho_{\text{BTN}}^{(A_2B_1)}} - \langle A_m^{(2)} \rangle_{\varrho_{\text{BTN}}^{(A_2)}} \langle B_n^{(1)} \rangle_{\varrho_{\text{BTN}}^{(B_1)}} \tag{B.8}$$

for all $m, n \in [N]$, and the proof is complete. □

B.2 Block decomposition for CMs of BTN states

We prove here one of our central results, Proposition 4.1, which states that the CM of a BTN state can be decomposed into the sum of CMs with reduced observables.

Proof of Proposition 4.1. Following Eq. (4.6), the matrix R_A is given by

$$R_A = \Gamma_A - \Gamma_{A_1} - \Gamma_{A_2}, \tag{B.9}$$

where the entries of Γ_{A_2} are

$$[\Gamma_{A_2}]_{mn} = \langle A_m^{(2)} A_n^{(2)} \rangle_{\varrho_{\text{BTN}}^{(A_2)}} - \langle A_m^{(2)} \rangle_{\varrho_{\text{BTN}}^{(A_2)}} \langle A_n^{(2)} \rangle_{\varrho_{\text{BTN}}^{(A_2)}} \quad \forall m, n \in [N], \tag{B.10}$$

which is a CM for the reduced observables, evaluated on the state $\varrho_{\text{BTN}}^{(A_2)}$ only. Let us now show that such a matrix R_A is PSD by showing that $\mathbf{x}^\dagger R_A \mathbf{x} \geq 0$ for all $\mathbf{x} \in \mathbb{C}^N$. Using the definition

$$M = \sum_{i=1}^{N} x_i A_i \tag{B.11}$$

and the fact that

$$M^{(1)} = \sum_{i=1}^{N} x_i A_i^{(1)} \quad \text{and} \quad M^{(2)} = \sum_{i=1}^{N} x_i A_i^{(2)}, \tag{B.12}$$

we have that

$$\begin{aligned}\mathbf{x}^\dagger R_A \mathbf{x} =& \Big(\langle M^\dagger M\rangle - \langle M^\dagger\rangle\langle M\rangle\Big) - \Big(\langle (M^{(1)})^\dagger M^{(1)}\rangle - \langle M^\dagger\rangle\langle M\rangle\Big) \\ &- \Big(\langle (M^{(2)})^\dagger M^{(2)}\rangle - \langle M^\dagger\rangle\langle M\rangle\Big) \\ =& \langle M^\dagger M\rangle + \langle M^\dagger\rangle\langle M\rangle - \langle (M^{(1)})^\dagger M^{(1)}\rangle - \langle (M^{(2)})^\dagger M^{(2)}\rangle,\end{aligned} \tag{B.13}$$

where the expectation values are taken on $\varrho_{\mathrm{BTN}}^{(A_1A_2)}$. Since M acts on A_1A_2, we can use a Schmidt-like decomposition for the bipartition $A_1 \mid A_2$,

$$M = \sum_{i=1}^{N} P_i \otimes Q_i \tag{B.14}$$

and use the fact that $\varrho_{\mathrm{BTN}}^{(A_1A_2)}$ is a product state. We then obtain

$$\begin{aligned}\mathbf{x}^\dagger R_A \mathbf{x} =& \sum_{i,j=1}^{N} \Big(\langle P_i^\dagger P_j\rangle\langle Q_i^\dagger Q_j\rangle + \langle P_i^\dagger\rangle\langle P_j\rangle\langle Q_i^\dagger\rangle\langle Q_j\rangle \\ &- \langle P_i^\dagger P_j\rangle\langle Q_i^\dagger\rangle\langle Q_j\rangle - \langle P_i^\dagger\rangle\langle P_j\rangle\langle Q_i^\dagger Q_j\rangle\Big) \\ =& \operatorname{tr}\Big(\big(\Gamma(P)\big)^T \Gamma(Q)\Big),\end{aligned} \tag{B.15}$$

where

$$[\Gamma(P)]_{ij} = \langle P_i^\dagger P_j\rangle_{\varrho_{\mathrm{BTN}}^{A_1}} - \langle P_i^\dagger\rangle_{\varrho_{\mathrm{BTN}}^{A_1}} \langle P_j\rangle_{\varrho_{\mathrm{BTN}}^{A_1}} \quad \forall i,j \in [N] \tag{B.16}$$

and similarly $\Gamma(Q)$ are CMs of the observables $\{P_i\}_{i=1}^N$ and $\{Q_i\}_{i=1}^N$ in the state $\varrho_{\mathrm{BTN}}^{A_1}$ and $\varrho_{\mathrm{BTN}}^{A_2}$, respectively. These matrices are PSD, so we have $\operatorname{tr}\Big(\big(\Gamma(P)\big)^T\Gamma(Q)\Big) \geq 0$, which finishes the proof. □

B.3 Matrix entries of R

In the main text, Eq. (4.8) reads

$$\begin{aligned}R_X =& \Gamma_X - \Gamma_{X_1} - \Gamma_{X_2} \\ =& \Gamma\left(\{\sigma_\alpha\}_{\alpha=1}^{d^2}, \varrho_{\mathrm{BTN}}^{(X_1)}\right) \otimes \Gamma\left(\{\sigma_\alpha\}_{\alpha=1}^{d^2}, \varrho_{\mathrm{BTN}}^{(X_2)}\right), \quad \forall X = A, B, C.\end{aligned} \tag{B.17}$$

A proof is given by direct calculation.

Proof of Eq. (4.8). We show the statement for $X = A$. The matrices Γ_A, Γ_{A_1}

and Γ_{A_2} have respectively the following matrix entries

$$[\Gamma_A]_{\alpha\beta|\alpha'\beta'} = \langle(\sigma_\alpha \otimes \sigma_\beta)(\sigma_{\alpha'} \otimes \sigma_{\beta'})\rangle - \langle\sigma_\alpha \otimes \sigma_\beta\rangle\langle\sigma_{\alpha'} \otimes \sigma_{\beta'}\rangle, \tag{B.18}$$

$$[\Gamma_{A_1}]_{\alpha\beta|\alpha'\beta'} = \langle\sigma_\alpha\sigma_{\alpha'}\rangle\langle\sigma_\beta\rangle\langle\sigma_{\beta'}\rangle - \langle\sigma_\alpha\rangle\langle\sigma_{\alpha'}\rangle\langle\sigma_\beta\rangle\langle\sigma_{\beta'}\rangle, \tag{B.19}$$

$$[\Gamma_{A_2}]_{\alpha\beta|\alpha'\beta'} = \langle\sigma_\alpha\rangle\langle\sigma_{\alpha'}\rangle\langle\sigma_\beta\sigma_{\beta'}\rangle - \langle\sigma_\alpha\rangle\langle\sigma_{\alpha'}\rangle\langle\sigma_\beta\rangle\langle\sigma_{\beta'}\rangle, \tag{B.20}$$

for all $\alpha, \beta, \alpha', \beta' \in [d^2]$ and where the expectation values are taken on the state $\varrho_{\mathrm{BTN}}^{(A)}$, with identity operators padded where needed. So, the matrix entries of R_A are

$$\begin{aligned}
[R_A]_{\alpha\beta|\alpha'\beta'} =& \langle(\sigma_\alpha \otimes \sigma_\beta)(\sigma_{\alpha'} \otimes \sigma_{\beta'})\rangle - \langle\sigma_\alpha\sigma_{\alpha'}\rangle\langle\sigma_\beta\rangle\langle\sigma_{\beta'}\rangle - \langle\sigma_\alpha\rangle\langle\sigma_{\alpha'}\rangle\langle\sigma_\beta\sigma_{\beta'}\rangle \\
&+ \langle\sigma_\alpha\rangle\langle\sigma_{\alpha'}\rangle\langle\sigma_\beta\rangle\langle\sigma_{\beta'}\rangle \\
=& (\langle\sigma_\alpha\sigma_{\alpha'}\rangle - \langle\sigma_\alpha\rangle\langle\sigma_{\alpha'}\rangle)(\langle\sigma_\beta\sigma_{\beta'}\rangle - \langle\sigma_\beta\rangle\langle\sigma_{\beta'}\rangle) \\
=& [\Gamma(\{\sigma_\alpha\}, \varrho_{\mathrm{BTN}}^{(A_1)}]_{\alpha\alpha'}[\Gamma(\{\sigma_\beta\}, \varrho_{\mathrm{BTN}}^{(A_2)}]_{\beta\beta'} \\
=& [\Gamma(\{\sigma_\alpha\}, \varrho_{\mathrm{BTN}}^{(A_1)}) \otimes \Gamma(\{\sigma_\beta\}, \varrho_{\mathrm{BTN}}^{(A_2)})]_{\alpha\beta|\alpha'\beta'}
\end{aligned} \tag{B.21}$$

for all $\alpha, \beta, \alpha', \beta' \in [d^2]$, and therefore

$$R_A = \Gamma(\{\sigma_\alpha\}, \varrho_{\mathrm{BTN}}^{(A_1)}) \otimes \Gamma(\{\sigma_\beta\}, \varrho_{\mathrm{BTN}}^{(A_2)}). \tag{B.22}$$

□

We note that in general, for a product state $\varrho = \varrho_1 \otimes \varrho_2$ and product observables $\{A_k \otimes B_l\}_{k,l=1}^N$, it holds that

$$\begin{aligned}
\Gamma(\{A_k \otimes B_l\}_{k,l=1}^N, \varrho) =& \mathbf{a}\mathbf{a}^T \otimes \Gamma(\{B_l\}_{l=1}^N, \varrho_2) + \Gamma(\{A_k\}_{k=1}^N, \varrho_1) \otimes \mathbf{b}\mathbf{b}^T \\
&+ \Gamma(\{A_k\}_{k=1}^N, \varrho_1) \otimes \Gamma(\{B_l\}_{l=1}^N, \varrho_2),
\end{aligned} \tag{B.23}$$

where $\mathbf{a}$ and $\mathbf{b}$ are the vector with entries $\langle A_k\rangle_{\varrho_1}$ and $\langle B_l\rangle_{\varrho_2}$ respectively, $k, l \in [N]$. In the case of complete sets of orthogonal observables, $\mathbf{a}$ and $\mathbf{b}$ are the Bloch vectors of ϱ_1 and ϱ_2 respectively.

B.4 Block decomposition for CMs of NCDS network states

In this appendix, we give the proof of Proposition 4.7. Let us first recall

notations from the main text. We have an N-node NCDS network with a set of sources $\mathbb{S}$. The number of sources is given by $|\mathbb{S}|$, and each source $s \in \mathbb{S}$ is the set of nodes the source connects where the nodes themselves are labelled by $x \in [n]$. The sources states are denotes ϱ_s, with $s \in \mathbb{S}$. Each party x receives n_x qudits from n_x different sources, with $x \in [n]$, and any two distinct parties share at most one source.

Let Γ_{NCDS} be the CM of a global state of such a network with observables $\{A_{x|i} \mid x \in [n]\}_{i=1}^{N}$, where $A_{x|i}$ is the ith observables that only acts on the node x, with $i \in [N]$ and $x \in [n]$. As mentioned in the main text, we first prove the proposition for basic networks with no common double source (BNCDS networks). The extension to NCDS networks without local operations follows using similar techniques to the triangle network scenario.

To do so, we extend Eq. (B.23) to n parties, which can be verified through direct calculation (see [C]).

Lemma B.1 ([C]). *Let $\varrho = \varrho_1 \otimes \cdots \otimes \varrho_n$ be a product state and $\{A_{i_1}^{(1)} \otimes \cdots \otimes A_{i_n}^{(n)}\}_{i_1,\ldots,i_n=1}^{n}$ be a set of product observables. The covariance matrix of these observables reads*

$$\Gamma(\varrho) = \bigotimes_{x=1}^{n} \left(\mathbf{a}_x \mathbf{a}_x^T + \Gamma(\{A_{i_x}^{(x)}\}_{i_x=1}^{N}, \varrho_x) \right) - \bigotimes_{x=1}^{n} \mathbf{a}_x \mathbf{a}_x^T, \tag{B.24}$$

where $\mathbf{a}_x$ is the vector with entries $\langle A_{i_x}^{(x)} \rangle_{\varrho_x}$, $i_x \in [N]$, $x \in [n]$.

We are now ready to prove the block decomposition of a CM of a BNCDS state with product observables, that is, we furthermore require that the observables are of the form $A_{x|i} = A_{x^1|i} \otimes \cdots \otimes A_{x^{n_x}|i}$, with $A_{x^1|i}$ acting on the first qudit of the party x, labelled x^1, and similarly for the others, with $x \in [n]$ and $i \in [N]$.

Lemma B.2 ([C]). *Let ϱ be a* BNCDS *network state. Then*

$$\Gamma\left(\{A_{x|i} \mid x \in [n]\}_{i=1}^{N}, \varrho\right) = \sum_{s \in \mathbb{S}} \Gamma\left(\{A_{x^\alpha|i}^{\text{RED}} \mid x^\alpha \in s\}_{i=1}^{N}, \varrho_s\right) + \bigoplus_{x=1}^{n} R_x, \tag{B.25}$$

where R_x are PSD *matrices and*

$$A_{x^\alpha|i_\alpha}^{\text{RED}} = \left(\prod_{\beta \neq \alpha, \beta=1}^{n_x} \langle A_{x^\beta|i_\beta} \rangle_{\varrho^{(x^\beta)}} \right) A_{x^\alpha|i_\alpha}. \tag{B.26}$$

We note that the matrices $\Gamma\left(\{A_{x^\alpha|i}^{\text{RED}} : x^\alpha \in s\}_{i=1}^{N}, \varrho_s\right)$ are padded with blocks of

zeros where needed, such that they are partitioned in $N \times N$ blocks with the xth diagonal block corresponding to the xth party.

Proof. From the fact that each subset of observables $\{A_{x|i}\}_{i=1}^{N}$ only acts on the party x of the network, with $x \in [n]$, it directly follows that Γ_{NCDS} has a block structure,

$$\Gamma_{\text{NCDS}} = \begin{pmatrix} \Gamma_1 & \gamma_{12} & \cdots & \gamma_{1N} \\ \gamma_{12}^T & \Gamma_2 & \cdots & \gamma_{2N} \\ \vdots & \vdots & \ddots & \vdots \\ \gamma_{1N}^T & \gamma_{2N}^T & \cdots & \Gamma_N \end{pmatrix}. \tag{B.27}$$

Let us investigate the structure of Γ_x for a BNCDS network state ϱ_{BNCDS}, with $x \in [n]$. We recall that

$$\Gamma_x = \Gamma\left(\{A_{x^1|i} \otimes \cdots \otimes A_{x^{n_x}|i}\}_{i=1}^{N}, \varrho_{\text{BNCDS}}^{(x)}\right) \tag{B.28}$$

where $\varrho_{\text{BNCDS}}^{(x)} = \text{tr}_{\hat{x}}(\varrho_{\text{BNCDS}})$, $\hat{x} = [n] \setminus \{x\}$. For the sake of readability, we drop the subscript BNCDS until the end of the proof. As $\varrho^{(x)}$ is a product state, Γ_x can be decomposed following Lemma B.1, i.e.,

$$\Gamma_x = \bigotimes_{\alpha=1}^{n}\left(\mathbf{x}_\alpha \mathbf{x}_\alpha^T + \Gamma(\{A_{x^\alpha|i_\alpha}\}_{i_\alpha=1}^{N}, \varrho^{(x^\alpha)})\right) - \bigotimes_{\alpha=1}^{n} \mathbf{x}_\alpha \mathbf{x}_\alpha^T, \tag{B.29}$$

with $\langle A_{x^\alpha|i_\alpha}\rangle_{\varrho^{(x^\alpha)}}$ being the vector entries of $\mathbf{x}_\alpha \mathbf{x}_\alpha^T$, for all $i_\alpha \in [N]$. Therein, the summands

$$\Gamma(\{A_{x^\alpha|i_\alpha}\}, \varrho^{(x^\alpha)}) \bigotimes_{\beta\neq\alpha,\beta=1}^{n_x} |\mathbf{x}_\beta\rangle\langle\mathbf{x}_\beta| \tag{B.30}$$

can be written as

$$\Gamma\left(\{A_{x^\alpha|i_\alpha}^{\text{RED}}\}, \varrho^{(x^\alpha)}\right), \tag{B.31}$$

with

$$A_{x^\alpha|i_\alpha}^{\text{RED}} = \left(\prod_{\beta\neq\alpha,\beta=1}^{n_x} \langle A_{x^\beta|i_\beta}\rangle_{\varrho^{(x^\beta)}}\right) A_{x^\alpha|i_\alpha}. \tag{B.32}$$

Now, we analyse the off-diagonal blocks for $x \neq y$, $x, y \in [n]$ that have matrix entries

$$[\gamma_{xy}]_{ij} = \langle A_{x|i} \otimes A_{y|j}\rangle_{\varrho^{(xy)}} - \langle A_{x|i}\rangle_{\varrho^{(x)}} \langle A_{y|j}\rangle_{\varrho^{(y)}} \quad \forall i, j \in [N]. \tag{B.33}$$

They are trivially equal to zero when the nodes x and y are not connected as in that case, $\varrho^{(xy)} = \varrho^{(x)} \otimes \varrho^{(y)}$. On the other hand, if they do are connected,

it is by one source exactly. Without loss of generality, we assume that x^1 and y^1 are connected by the same source, and the state can be written as

$$\varrho^{(xy)} = \varrho^{(x^1y^1)} \bigotimes_{\alpha=2}^{n_x} \varrho^{(x^\alpha)} \bigotimes_{\beta=2}^{n_y} \varrho^{(y^\beta)}. \tag{B.34}$$

Therefore, Eq. (B.33) reads

$$\begin{aligned}\left[\gamma_{xy}\right]_{ij} = &\left(\langle A_{x^1|i_1} \otimes A_{y^1|j_1}\rangle_{\varrho^{(x^1y^1)}} - \langle A_{x^1|i_1}\rangle_{\varrho^{(x^1)}} \langle A_{y^1|i_1}\rangle_{\varrho^{(y^1)}}\right) \\ &\prod_{\alpha=2}^{n_x} \langle A_{x^\alpha|i_\alpha}\rangle_{\varrho^{(x^\alpha)}} \prod_{\beta=2}^{n_y} \langle A_{y^\beta|i_\beta}\rangle_{\varrho^{(y^\beta)}},\end{aligned} \tag{B.35}$$

which, with the reduced observables of Eq. (B.32) can be written as

$$\left[\gamma_{xy}\right]_{ij} = \langle A^{\text{RED}}_{x^1|i_1} \otimes A^{\text{RED}}_{y^1|j_1}\rangle_{\varrho^{(x^1y^1)}} - \langle A^{\text{RED}}_{x^1|i_1}\rangle_{\varrho^{(x^1)}} \langle A^{\text{RED}}_{y^1|i_1}\rangle_{\varrho^{(y^1)}}. \tag{B.36}$$

Finally, putting everything together, we obtain

$$\Gamma\left(\{A_{x|i} \mid x \in [n]\}_{i=1}^N, \varrho\right) = \sum_{s\in \mathrm{S}} \Gamma\left(\{A^{\text{RED}}_{x^\alpha|i} \mid x^\alpha \in s\}_{i=1}^N, \varrho_s\right) + \bigoplus_{x=1}^{n} R_x, \tag{B.37}$$

where

$$\begin{aligned}R_x = &\bigotimes_{\alpha=1}^{n_x} \left(\mathbf{x}_\alpha \mathbf{x}_\alpha^T + \Gamma(\{A_{x^\alpha|i_\alpha}\}, \varrho_\alpha)\right) - \bigotimes_{\alpha=1}^{n_x} |\mathbf{x}_\alpha\rangle\langle\mathbf{x}_\alpha| \\ &- \sum_{\alpha=1}^{n_x} \left(\Gamma(\{A_{x^\alpha|i_\alpha}\}, \varrho_\alpha) \bigotimes_{\beta\neq\alpha,\beta=1}^{n_x} \mathbf{x}_\beta \mathbf{x}_\beta^T\right)\end{aligned} \tag{B.38}$$

is PSD. □

Now that we have the explicit structure of CMs for product observables on BNCDS network states, it directly follows that in this case, the CMs have a block decomposition as described in Proposition 4.7. We use the following lemma to argue that the block decomposition holds for any set of local observables, which follows from a direct calculation [C].

Lemma B.3 ([C]). *Let $\Gamma\left(\{X_i\}_{i=1}^N\}, \varrho\right)$ be a* CM. *Let C be a real matrix such that $Y_j = \sum_{i=1}^N C_{ij} X_i$, $j = 1, \ldots, M$. Then*

$$\Gamma\left(\{Y_j\}_{j=1}^M, \varrho\right) = C^T \Gamma\left(\{X_i\}_{i=1}^N, \varrho\right) C. \tag{B.39}$$

Combining all those results, we are now ready to prove Proposition 4.7.

Proof of Proposition 4.7. From Lemma B.2, we know that the block decomposition holds for BNCDS network states with product observables. When those product observables are chosen to be a complete set of observables, Lemma B.3 shows that the block decomposition holds for any observable set acting on BNCDS network states. Finally, an analogous reasoning to the cases of UTN and CTN leads to the conclusion that the block decomposition holds for states of NCDS networks with local operations. □

Publication list

[A] K. Hansenne*, Z.-P. Xu*, T. Kraft, and O. Gühne. Symmetries in quantum networks lead to no-go theorems for entanglement distribution and to verification techniques. *Nature Communications*, 13:496, 2022. DOI: 10.1038/s41467-022-28006-3

[B] C. de Gois*, K. Hansenne*, and O. Gühne. Uncertainty relations from graph theory. *Physical Review A*, 107:062211, 2023. DOI: 10.1103/PhysRevA.107.062211

[C] K. Hansenne and O. Gühne. Covariance-matrix-based criteria for network entanglement. *Entropy*, 25:1260, 2023. DOI: 10.3390/e25091260

[D] L. T. Weinbrenner, N. Prasannan, K. Hansenne, S. Denker, J. Sperling, B. Brecht, C. Silberhorn, and O. Gühne. Certifying the topology of quantum networks: theory and experiment. *Physical Review Letters*, 132:240802, 2024. DOI: 10.1103/PhysRevLett.132.240802

[E] K. Hansenne, R. Qu, L. T. Weinbrenner, C. de Gois, H. Wang, Y. Ming, Z. Yang, P. Horodecki, W. Gao, and O. Gühne. Optimal overlapping tomography. *ArXiv preprint*, arXiv:2408.05730, 2024. DOI: 10.48550/arXiv.2408.05730

* These authors contributed equally.

Bibliography

[1] S. Aaronson. Shadow tomography of quantum states. In *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing*, pages 325–338, 2018. DOI: 10.1145/3188745.3188802.

[2] A. A. Abbott, P.-L. Alzieu, M. J. W. Hall, and C. Branciard. Tight state-independent uncertainty relations for qubits. *Mathematics*, 4, 2016. DOI: 10.3390/math4010008.

[3] J. Åberg, R. Nery, C. Duarte, and R. Chaves. Semidefinite tests for quantum network topologies. *Physical Review Letters*, 125:110505, 2020. DOI: 10.1103/PhysRevLett.125.110505.

[4] E. R. Anschuetz, D. Gamarnik, and B. T. Kiani. Bounds on the ground state energy of quantum p-spin hamiltonians. *ArXiv preprint*, arXiv:2404.07231, 2024. DOI: 10.48550/arXiv.2404.07231.

[5] B. G. Araújo, M. M. Taddei, D. Cavalcanti, and A. Acín. Local quantum overlapping tomography. *Physical Review A*, 106:062441, 2022. DOI: 10.1103/PhysRevA.106.062441.

[6] A. Aspect, J. Dalibard, and G. Roger. Experimental test of Bell's inequalities using time-varying analyzers. *Physical Review Letters*, 49:1804, 1982. DOI: 10.1103/PhysRevLett.49.1804.

[7] G. Avis, F. Rozpedek, and S. Wehner. Analysis of multipartite entanglement distribution using a central quantum-network node. *Physical Review A*, 107: 012609, 2023. DOI: 10.1103/PhysRevA.107.012609.

[8] K. Azuma, S. E. Economou, D. Elkouss, P. Hilaire, L. Jiang, H.-K. Lo, and I. Tzitrin. Quantum repeaters: from quantum networks to the quantum internet. *Reviews of Modern Physics*, 95:045006, 2023. DOI: 10.1103/RevModPhys.95.045006.

[9] P. Badziag, P. Horodecki, R. Horodecki, and R. Augusiak. Separability in terms of a single entanglement witness. *Physical Review A*, 88:010301, 2013. DOI: 10.1103/PhysRevA.88.010301.

[10] J. Bae and L.-C. Kwek. Quantum state discrimination and its applications. *Journal of Physics A: Mathematical and Theoretical*, 48:083001, 2015. DOI: 10.1088/1751-8113/48/8/083001.

[11] S. Beigi and M.-O. Renou. Covariance decomposition as a universal limit on correlations in networks. *IEEE Transactions on Information Theory*, 68:384, 2021. DOI: 10.1109/TIT.2021.3119651.

[12] J. S. Bell. On the Einstein Podolsky Rosen paradox. *Physics Physique Fizika*, 1: 195, 1964. DOI: 10.1103/PhysicsPhysiqueFizika.1.195.

[13] F. Benatti, R. Floreanini, and M. Piani. Non-decomposable quantum dynamical semigroups and bound entangled states. *Open Systems & Information Dynamics*, 11:325, 2004. DOI: 10.1007/s11080-004-6622-6.

[14] C. H. Bennett and G. Brassard. Quantum cryptography: public key distribution and coin tossing. *Theoretical Computer Science*, 560:7, 2014. DOI: 10.1016/j.tcs.2014.05.025.

[15] 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*, 70:1895, 1993. DOI: 10.1103/PhysRevLett.70.1895.

[16] J. Biamonte, M. Faccin, and M. De Domenico. Complex networks from classical to quantum. *Communications Physics*, 2:53, 2019. DOI: 10.1038/s42005-019-0152-6.

[17] R. Blume-Kohout. Optimal, reliable estimation of quantum states. *New Journal of Physics*, 12:043034, 2010. DOI: 10.1088/1367-2630/12/4/043034.

[18] X. Bonet-Monroig, R. Babbush, and T. E. O'Brien. Nearly optimal measurement scheduling for partial tomography of quantum states. *Physical Review X*, 10:031064, 2020. DOI: 10.1103/PhysRevX.10.031064.

[19] J. L. Bönsel, O. Gühne, and A. Cabello. Generating multipartite nonlocality to benchmark quantum computers. *ArXiv preprint*, arXiv:2406.07659, 2024. DOI: 10.48550/arXiv.2406.07659.

[20] S. Bose, V. Vedral, and P. L. Knight. Multiparticle generalization of entanglement swapping. *Physical Review A*, 57:822, 1998. DOI: 10.1103/PhysRevA.57.822.

[21] M. Bourennane, M. Eibl, C. Kurtsiefer, S. Gaertner, H. Weinfurter, O. Gühne, P. Hyllus, D. Bruß, M. Lewenstein, and A. Sanpera. Experimental detection of multipartite entanglement using witness operators. *Physical Review Letters*, 92:087902, 2004. DOI: 10.1103/PhysRevLett.92.087902.

[22] A. Bretto. *Hypergraph theory: An introduction*. Mathematical Engineering. Springer Cham, 2013. DOI: 10.1007/978-3-319-00080-0.

[23] H. J. Briegel and R. Raussendorf. Persistent entanglement in arrays of interacting particles. *Physical Review Letters*, 86:910, 2001. DOI: 10.1103/PhysRevLett.86.910.

[24] A. Broadbent, J. Fitzsimons, and E. Kashefi. Universal blind quantum computation. In *50th Annual IEEE Symposium on Foundations of Computer Science*, pages 517–526. IEEE, 2009. DOI: 10.1109/FOCS.2009.36.

[25] L. Bugalho, B. C. Coutinho, F. A. Monteiro, and Y. Omar. Distributing multipartite entanglement over noisy quantum networks. *Quantum*, 7:920, 2023. DOI: 10.22331/q-2023-02-09-920.

[26] T. Bullock and P. Busch. Measurement uncertainty relations: characterising optimal error bounds for qubits. *Journal of Physics A: Mathematical and Theoretical*, 51:283001, 2018. DOI: 10.1088/1751-8121/aac729.

[27] P. Busch, P. Lahti, and R. F. Werner. Colloquium: Quantum root-mean-square error and measurement uncertainty relations. *Reviews of Modern Physics*, 86: 1261, 2014. DOI: 10.1103/RevModPhys.86.1261.

[28] M. S. Byrd and N. Khaneja. Characterization of the positivity of the density matrix in terms of the coherence vector representation. *Physical Review A*, 68: 062322, 2003. DOI: 10.1103/PhysRevA.68.062322.

[29] D. Cavalcanti and P. Skrzypczyk. Quantum steering: a review with focus on semidefinite programming. *Reports on Progress in Physics*, 80:024001, 2016. DOI: 10.1088/1361-6633/80/2/024001.

[30] T.-Y. Chen, X. Jiang, S.-B. Tang, L. Zhou, X. Yuan, H. Zhou, J. Wang, Y. Liu, L.-K. Chen, W.-Y. Liu, et al. Implementation of a 46-node quantum metropolitan area network. *npj Quantum Information*, 7:134, 2021. DOI: 10.1038/s41534-021-00474-3.

[31] M. Chudnovsky, N. Robertson, P. Seymour, and R. Thomas. The strong perfect graph theorem. *Annals of mathematics*, page 51, 2006. DOI: 10.4007/annals.2006.164.51.

[32] V. Cimini, E. Polino, F. Belliardo, F. Hoch, B. Piccirillo, N. Spagnolo, V. Giovannetti, and F. Sciarrino. Experimental metrology beyond the standard quantum limit for a wide resources range. *npj Quantum Information*, 9:20, 2023. DOI: 10.1038/s41534-023-00691-y.

[33] C. J. Colbourn. Covering array tables for t=2,3,4,5,6. URL: https://www.public.asu.edu/~ccolbou/src/tabby/catable.html.

[34] C. J. Colbourn. Combinatorial aspects of covering arrays. *Le Matematiche*, 59: 125, 2004.

[35] P. J. Coles, M. Berta, M. Tomamichel, and S. Wehner. Entropic uncertainty relations and their applications. *Reviews of Modern Physics*, 89:015002, 2017. DOI: 10.1103/RevModPhys.89.015002.

[36] P. Contreras-Tejada, C. Palazuelos, and J. I. de Vicente. Asymptotic survival of genuine multipartite entanglement in noisy quantum networks depends on the topology. *Physical Review Letters*, 128:220501, 2022. DOI: 10.1103/PhysRevLett.128.220501.

[37] A. C. Costa, R. Uola, and O. Gühne. Steering criteria from general entropic uncertainty relations. *Physical Review A*, 98:050104, 2018. DOI: 10.1103/PhysRevA.98.050104.

[38] J. Cotler and F. Wilczek. Quantum overlapping tomography. *Physical Review Letters*, 124:100401, 2020. DOI: 10.1103/PhysRevLett.124.100401.

[39] M. Cramer, M. B. Plenio, S. T. Flammia, R. Somma, D. Gross, S. D. Bartlett, O. Landon-Cardinal, D. Poulin, and Y.-K. Liu. Efficient quantum state tomography. *Nature Communications*, 1:149, 2010. DOI: 10.1038/ncomms1147.

[40] C. de Gois. PhD thesis, Universität Siegen (Germany). In preparation.

[41] C. de Gois and M. Kleinmann. User-friendly confidence regions for quantum state tomography. *Physical Review A*, 109:062417, 2024. DOI: 10.1103/PhysRevA.109.062417.

[42] S. Denker. Characterizing multiparticle entanglement using the Schmidt decomposition of operators. Master's thesis, Universität Siegen (Germany), 2023. DOI: 10.1007/978-3-658-43203-4.

[43] R. Diestel. *Graph Theory*. Graduate Texts in Mathematics. Springer Berlin, Heidelberg, fifth edition, 2018. DOI: 10.1007/978-3-662-53622-3.

[44] W. Dür, G. Vidal, and J. I. Cirac. Three qubits can be entangled in two inequivalent ways. *Physical Review A*, 62:062314, 2000. DOI: 10.1103/PhysRevA.62.062314.

[45] K. Eckert, J. Schliemann, D. Bruß, and M. Lewenstein. Quantum correlations in systems of indistinguishable particles. *Annals of physics*, 299:88, 2002. DOI: 10.1006/aphy.2002.6268.

[46] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47:777, 1935. DOI: 10.1103/PhysRev.47.777.

[47] A. K. Ekert. Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67:661, 1991. DOI: 10.1103/PhysRevLett.67.661.

[48] C. Eltschka, M. Huber, S. Morelli, and J. Siewert. The shape of higher-dimensional state space: Bloch-ball analog for a qutrit. *Quantum*, 5:485, 2021. DOI: 10.22331/q-2021-06-29-485.

[49] R. P. Feynman, F. L. Vernon Jr, and R. W. Hellwarth. Geometrical representation of the Schrödinger equation for solving maser problems. *Journal of Applied Physics*, 28:49, 1957. DOI: 10.1063/1.1722572.

[50] S. J. Freedman and J. F. Clauser. Experimental test of local hidden-variable theories. *Physical Review Letters*, 28:938, 1972. DOI: 10.1103/PhysRevLett.28.938.

[51] N. Friis, O. Marty, C. Maier, C. Hempel, M. Holzäpfel, P. Jurcevic, M. B. Plenio, M. Huber, C. Roos, R. Blatt, and B. Lanyon. Observation of entangled states of a fully controlled 20-qubit system. *Physical Review X*, 8:021012, 2018. DOI: 10.1103/PhysRevX.8.021012.

[52] N. Friis, G. Vitagliano, M. Malik, and M. Huber. Entanglement certification from theory to experiment. *Nature Reviews Physics*, 1:72, 2019. DOI: 10.1038/s42254-018-0003-5.

[53] G. García-Pérez, M. A. C. Rossi, B. Sokolov, E.-M. Borrelli, and S. Maniscalco. Pairwise tomography networks for many-body quantum systems. *Physical Review Research*, 2:023393, 2020. DOI: 10.1103/PhysRevResearch.2.023393.

[54] G. Giedke, B. Kraus, M. Lewenstein, and J. Cirac. Entanglement criteria for all bipartite Gaussian states. *Physical Review Ketters*, 87:167904, 2001. DOI: 10.1103/PhysRevLett.87.167904.

[55] P. Giorda, L. Maccone, and A. Riccardi. State-independent uncertainty relations from eigenvalue minimization. *Physical Review A*, 99:052121, 2019. DOI: 10.1103/PhysRevA.99.052121.

[56] O. Gittsovich, O. Gühne, P. Hyllus, and J. Eisert. Unifying several separability conditions using the covariance matrix criterion. *Physical Review A*, 78:052319, 2008. DOI: 10.1103/PhysRevA.78.052319.

[57] D. Gottesman. Class of quantum error-correcting codes saturating the quantum hamming bound. *Physical Review A*, 54:1862, 1996. DOI: 10.1103/PhysRevA.54.1862.

[58] D. M. Greenberger, M. A. Horne, and A. Zeilinger. Going beyond Bell's theorem. In *Bell's Theorem, Quantum Theory and Conceptions of the Universe*, Fundamental Theories of Physics, pages 69–72. Springer Dordrecht, 1989. DOI: 10.1007/978-94-017-0849-4.

[59] D. Gross, Y.-K. Liu, S. T. Flammia, S. Becker, and J. Eisert. Quantum state tomography via compressed sensing. *Physical Review Letters*, 105(15):150401, 2010. DOI: 10.1103/PhysRevLett.105.150401.

[60] O. Gühne and G. Tóth. Entanglement detection. *Physics Reports*, 474:1, 2009. DOI: 10.1016/j.physrep.2009.02.004.

[61] O. Gühne, P. Hyllus, D. Bruß, A. Ekert, M. Lewenstein, C. Macchiavello, and A. Sanpera. Detection of entanglement with few local measurements. *Physical Review A*, 66:062305, 2002. DOI: 10.1103/PhysRevA.66.062305.

[62] O. Gühne, G. Tóth, P. Hyllus, and H. J. Briegel. Bell inequalities for graph states. *Physical Review Letters*, 95:120405, 2005. DOI: 10.1103/PhysRevLett.95.120405.

[63] O. Gühne, P. Hyllus, O. Gittsovich, and J. Eisert. Covariance matrices and the separability problem. *Physical Review Letters*, 99:130504, 2007. DOI: 10.1103/PhysRevLett.99.130504.

[64] O. Gühne, C.-Y. Lu, W.-B. Gao, and J.-W. Pan. Toolbox for entanglement detection and fidelity estimation. *Physical Review A*, 76:030305, 2007. DOI: 10.1103/PhysRevA.76.030305.

[65] O. Gühne, Y. Mao, and X.-D. Yu. Geometry of faithful entanglement. *Physical Review Letters*, 126:140503, 2021. DOI: 10.1103/PhysRevLett.126.140503.

[66] L. Gurvits. Classical deterministic complexity of Edmonds' problem and quantum entanglement. In *Proceedings of the 35th Annual ACM Symposium on Theory of Computing*, pages 10–19, 2003. DOI: 10.1145/780542.780545.

[67] K. Hansenne. Quantum entanglement: a study of recent separability criteria. Master's thesis, Université de Liège (Belgium), 2020. URL: `http://hdl.handle.net/2268.2/9319`.

[68] A. S. Hedayat, N. J. A. Sloane, and J. Stufken. *Orthogonal Arrays: Theory and Applications*. Springer Series in Statistics. Springer New York, NY, 1999. DOI: 10.1007/978-1-4612-1478-6.

[69] M. Hein, J. Eisert, and H. J. Briegel. Multiparty entanglement in graph states. *Physical Review A*, 69:062311, 2004. DOI: 10.1103/PhysRevA.69.062311.

[70] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. Van den Nest, and H.-J. Briegel. Entanglement in graph states and its applications. In *Quantum Computers, Algorithms and Chaos*, pages 115–218. IOS Press, 2006. DOI: 10.3254/978-1-61499-018-5-115.

[71] T. Heinosaari and M. Ziman. *The Mathematical Language of Quantum Theory: From Uncertainty to Entanglement*. Cambridge University Press, 2011. DOI: 10.1017/CBO9781139031103.

[72] W. Heisenberg. Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik. *Zeitschrift für Physik*, 43:172, 1927. DOI: 10.1007/BF01397280.

[73] W. Hoeffding. Probability inequalities for sums of bounded random variables. *Journal of the American Statistical Association*, 58:13–30, 1963. DOI: 10.1080/01621459.1963.10500830.

[74] H. F. Hofmann and S. Takeuchi. Violation of local uncertainty relations as a signature of entanglement. *Physical Review A*, 68:032103, 2003. DOI: 10.1103/PhysRevA.68.032103.

[75] R. A. Horn and C. R. Johnson. *Matrix Analysis*. second edition, 2013.

[76] M. Horodecki, P. Horodecki, and R. Horodecki. Separability of mixed states: necessary and sufficient conditions. *Physics Letters A*, 223:1–8, 1996. DOI: 10.1016/S0375-9601(96)00706-2.

[77] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki. Quantum entanglement. *Reviews of Modern Physics*, 81:865, 2009. DOI: 10.1103/RevModPhys.81.865.

[78] H.-Y. Huang, R. Kueng, and J. Preskill. Predicting many properties of a quantum system from very few measurements. *Nature Physics*, 16:1050, 2020. DOI: 10.1038/s41567-020-0932-7.

[79] Y. Huang. Variance-based uncertainty relations. *Physical Review A*, 86:024101, 2012. DOI: 10.1103/PhysRevA.86.024101.

[80] L. P. Hughston, R. Jozsa, and W. K. Wootters. A complete classification of quantum ensembles having a given density matrix. *Physics Letters A*, 183:14, 1993. DOI: 10.1016/0375-9601(93)90880-9.

[81] F. Hulpke, D. Bruss, M. Lewenstein, and A. Sanpera. Simplifying Schmidt number witnesses via higher-dimensional embeddings. *Quantum Information & Computation*, 4:207, 2004.

[82] P. C. Humphreys, N. Kalb, J. P. Morits, R. N. Schouten, R. F. Vermeulen, D. J. Twitchen, M. Markham, and R. Hanson. Deterministic delivery of remote entanglement on a quantum network. *Nature*, 558:268, 2018. DOI: 10.1038/s41586-018-0200-5.

[83] Z. Ji, J. Chen, Z. Wei, and M. Ying. The LU-LC conjecture is false. *Quantum Information & Computation*, 10:97, 2010. DOI: 10.26421/QIC10.1-2-8.

[84] R. M. Karp. Reducibility among combinatorial problems. In *Complexity of computer computations*, pages 85–103. Springer, Boston, MA, 1972. DOI: 10.1007/978-1-4684-2001-2˙9.

[85] E. H. Kennard. Zur Quantenmechanik einfacher Bewegungstypen. *Zeitschrift für Physik*, 44:326, 1927. DOI: 10.1007/BF01391200.

[86] C. Khatri and C. R. Rao. Solutions to some functional equations and their applications to characterization of probability distributions. *Sankhyā: The Indian Journal of Statistics, Series A*, page 167, 1968.

[87] S. Khatri, C. T. Matyas, A. U. Siddiqui, and J. P. Dowling. Practical figures of merit and thresholds for entanglement distribution in quantum networks. *Physical Review Research*, 1:023032, 2019. DOI: 10.1103/PhysRevResearch.1.023032.

[88] H. J. Kimble. The quantum internet. *Nature*, 453:1023, 2008. DOI: 10.1038/nature07127.

[89] G. Kimura. The Bloch vector for N-level systems. *Physics Letters A*, 314:339, 2003. DOI: 10.1016/S0375-9601(03)00941-1.

[90] R. King, D. Gosset, R. Kothari, and R. Babbush. Triply efficient shadow tomography. *ArXiv preprint*, arXiv:2404.19211, 2024. DOI: 10.48550/arXiv.2404.19211.

[91] C. M. Knaut, A. Suleymanzade, Y.-C. Wei, D. R. Assumpcao, P.-J. Stas, Y. Q. Huan, B. Machielse, E. N. Knall, M. Sutula, G. Baranes, N. Sinclair, C. DeEknamkul, D. S. Levonian, M. K. Bhaskar, H. Park, M. Lončar, and M. D. Lukin. Entanglement of nanophotonic quantum memory nodes in a telecom network. *Nature*, 629:573, 2024. DOI: 10.1038/s41586-024-07252-z.

[92] D. E. Knuth. The sandwich theorem. *Electronic Journal of Combinatorics*, 1:A1, 1994. DOI: 10.37236/1193.

[93] J. I. Kokkala, K. Meagher, R. Naserasr, K. J. Nurmela, P. R. Östergård, and B. Stevens. On the structure of small strength-2 covering arrays. *Journal of Combinatorial Designs*, 28:5, 2020. DOI: 10.1002/jcd.21671.

[94] T. Kraft, S. Designolle, C. Ritz, N. Brunner, O. Gühne, and M. Huber. Quantum entanglement in the triangle network. *Physical Review A*, 103: L060401, 2021. DOI: 10.1103/PhysRevA.103.L060401.

[95] P. Kurzyński, T. Paterek, R. Ramanathan, W. Laskowski, and D. Kaszlikowski. Correlation complementarity yields Bell monogamy relations. *Physical Review Letters*, 106:180402, 2011. DOI: 10.1103/PhysRevLett.106.180402.

[96] L. Lamata, J. León, D. Salgado, and E. Solano. Inductive classification of multipartite entanglement under stochastic local operations and classical communication. *Physical Review A*, 74:052336, 2006. DOI: 10.1103/PhysRevA.74.052336.

[97] L. T. Ligthart, M. Gachechiladze, and D. Gross. A convergent inflation hierarchy for quantum causal structures. *Communications in Mathematical Physics*, 401:2673, 2023. DOI: 10.1007/s00220-023-04697-7.

[98] J.-L. Liu, X.-Y. Luo, Y. Yu, C.-Y. Wang, B. Wang, Y. Hu, J. Li, M.-Y. Zheng, B. Yao, D. T. Zi Yan, J.-W. Jiang, X.-B. Liu, X.-P. Xie, J. Zhang, Q.-H. Mao, X. Jiang, Q. Zhang, X.-H. Bao, and J.-W. Pan. Creation of memory–memory entanglement in a metropolitan quantum network. *Nature*, 629:579, 2024. DOI: 10.1038/s41586-024-07308-0.

[99] S. Liu. Matrix results on the Khatri-Rao and Tracy-Singh products. *Linear Algebra and its Applications*, 289:267, 1999. DOI: 10.1016/S0024-3795(98)10209-4.

[100] L. Lovász. On the shannon capacity of a graph. *IEEE Transactions on Information Theory*, page 1, 1979. DOI: 10.1109/TIT.1979.1055985.

[101] M.-X. Luo. New genuinely multipartite entanglement. *Advanced Quantum Technologies*, 4:2000123, 2021. DOI: 10.1002/qute.202000123.

[102] L. Maccone and A. K. Pati. Stronger uncertainty relations for all incompatible observables. *Physical Review Letters*, 113:260401, 2014. DOI: 10.1103/PhysRevLett.113.260401.

[103] O. Makuta, L. T. Ligthart, and R. Augusiak. No graph state is preparable in quantum networks with bipartite sources and no classical communication. *npj Quantum Information*, 9:117, 2023. DOI: 10.1038/s41534-023-00789-3.

[104] H. Markowits. Portfolio selection. *The Journal of Finance*, 7:71, 1952. DOI: 10.2307/2975974.

[105] N. D. Mermin. Extreme quantum entanglement in a superposition of macroscopically distinct states. *Physical Review Letters*, 65:1838, 1990. DOI: 10.1103/PhysRevLett.65.1838.

[106] M. B. Morán and F. Huber. Uncertainty relations from state polynomial optimization. *Physical Review Letters*, 132:200202, 2024. DOI: 10.1103/PhysRevLett.132.200202.

[107] S. Morelli, H. Yamasaki, M. Huber, and A. Tavakoli. Entanglement detection with imprecise measurements. *Physical Review Letters*, 128:250501, 2022. DOI: 10.1103/PhysRevLett.128.250501.

[108] T. Moroder and O. Gittsovich. Calibration-robust entanglement detection beyond Bell inequalities. *Physical Review A*, 85:032301, 2012. DOI: 10.1103/PhysRevA.85.032301.

[109] T. Moroder, P. Hyllus, G. Tóth, C. Schwemmer, A. Niggebaum, S. Gaile, O. Gühne, and H. Weinfurter. Permutationally invariant state reconstruction. *New Journal of Physics*, 14:105001, 2012. DOI: 10.1088/1367-2630/14/10/105001.

[110] G. Murta, F. Grasselli, H. Kampermann, and D. Bruß. Quantum conference key agreement: a review. *Advanced Quantum Technologies*, 3:2000025, 2020. DOI: 10.1002/qute.202000025.

[111] M. Navascués, E. Wolfe, D. Rosset, and A. Pozas-Kerstjens. Genuine network multipartite entanglement. *Physical Review Letters*, 125:240505, 2020. DOI: 10.1103/PhysRevLett.125.240505.

[112] B. C. Nichol, R. Srinivas, D. Nadlinger, P. Drmota, D. Main, G. Araneda, C. Ballance, and D. Lucas. An elementary quantum network of entangled optical atomic clocks. *Nature*, 609:689, 2022. DOI: 10.1038/s41586-022-05088-z.

[113] S. Niekamp, M. Kleinmann, and O. Gühne. Entropic uncertainty relations and the stabilizer formalism. *Journal of Mathematical Physics*, 53:012202, 2012. DOI: 10.1063/1.3678200.

[114] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, tenth edition, 2010. DOI: 10.1017/CBO9780511976667.

[115] N. P. K. and S. R. Kola. The-distance chromatic number of trees and cycles. *AKCE International Journal of Graphs and Combinatorics*, 16:230, 2019. DOI: 10.1016/j.akcej.2017.11.007.

[116] J.-W. Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger. Experimental entanglement swapping: entangling photons that never interacted. *Physical Review Letters*, 80:3891, 1998. DOI: 10.1103/PhysRevLett.80.3891.

[117] C. H. Papadimitriou and K. Steiglitz. *Combinatorial Optimization: Algorithms and Complexity*. Dover Books on Computer Science. Dover Publications, 1998.

[118] W. Pauli. Zur Quantenmechanik des magnetischen Elektrons. *Zeitschrift für Physik*, 43:601, 1927. DOI: 10.1007/BF01397326.

[119] A. Pickston, J. Ho, A. Ulibarrena, F. Grasselli, M. Proietti, C. L. Morrison, P. Barrow, F. Graffitti, and A. Fedrizzi. Conference key agreement in a quantum network. *NPJ Quantum Information*, 9:82, 2023. DOI: 10.1038/s41534-023-00750-4.

[120] M. Plávala. General probabilistic theories: an introduction. *Physics Reports*, 1033:1, 2023. DOI: 10.1016/j.physrep.2023.09.001.

[121] M. Pompili, S. L. Hermans, S. Baier, H. K. Beukers, P. C. Humphreys, R. N. Schouten, R. F. Vermeulen, M. J. Tiggelman, L. dos Santos Martins, B. Dirkse, et al. Realization of a multinode quantum network of remote solid-state qubits. *Science*, 372:259, 2021. DOI: 10.1126/science.abg1919.

[122] C. Portmann and R. Renner. Security in quantum cryptography. *Reviews of Modern Physics*, 94:025008, 2022. DOI: 10.1103/RevModPhys.94.025008.

[123] C. R. Rao. Factorial experiments derivable from combinatorial arrangements of arrays. *Supplement to the Journal of the Royal Statistical Society*, 9:128, 1947. DOI: 10.2307/2983576.

[124] R. Raussendorf and H. J. Briegel. A one-way quantum computer. *Physical Review Letters*, 86:5188, 2001. DOI: 10.1103/PhysRevLett.86.5188.

[125] H. P. Robertson. The uncertainty principle. *Physical Review*, 34:163, 1929. DOI: 10.1103/PhysRev.34.163.

[126] P. P. Rohde. *The Quantum Internet: The Second Quantum Revolution*. Cambridge University Press, 2021. DOI: 10.1017/9781108868815.

[127] L. Rückle, J. Budde, J. de Jong, F. Hahn, A. Pappa, and S. Barz. Experimental anonymous conference key agreement using linear cluster states. *Physical Review Research*, 5:033222, 2023. DOI: 10.1103/PhysRevResearch.5.033222.

[128] B. Sagan. *The Symmetric Group: Representations, Combinatorial Algorithms, and Symmetric Functions*. Graduate Texts in Mathematics. Springer New York, NY, second edition, 2013. DOI: 10.1007/978-1-4757-6804-6.

[129] E. Schrödinger. Die gegenwärtige situation in der Quantenmechanik. *Naturwissenschaften*, 23:844, 1935. DOI: 10.1007/BF01491914.

[130] R. Schwonnek, L. Dammeier, and R. F. Werner. State-independent uncertainty relations and entanglement detection in noisy systems. *Physical Review Letters*, 119:170404, 2017. DOI: 10.1103/PhysRevLett.119.170404.

[131] M. Seevinck and J. Uffink. Local commutativity versus Bell inequality violation for entangled states and versus non-violation for separable states. *Physical Review A*, 76:042105, 2007. DOI: 10.1103/PhysRevA.76.042105.

[132] J. Shang, H. K. Ng, A. Sehrawat, X. Li, and B.-G. Englert. Optimal error regions for quantum state estimation. *New Journal of Physics*, 15:123026, 2013. DOI: 10.1088/1367-2630/15/12/123026.

[133] E. Shchukin, F. Schmidt, and P. van Loock. Waiting time in quantum repeaters with probabilistic entanglement swapping. *Physical Review A*, 100:032322, 2019. DOI: 10.1103/PhysRevA.100.032322.

[134] C. Simon. Towards a global quantum network. *Nature Photonics*, 11:678, 2017. DOI: 10.1038/s41566-017-0032-0.

[135] P. Skrzypczyk and D. Cavalcanti. *Semidefinite Programming in Quantum Information Science*. 2053-2563. IOP Publishing, 2023. DOI: 10.1088/978-0-7503-3343-6.

[136] N. J. A. Sloane. A library of orthogonal arrays. URL: http://neilsloane.com/oadir/#3_2.

[137] L. Stephenson, D. Nadlinger, B. Nichol, S. An, P. Drmota, T. Ballance, K. Thirumalai, J. Goodwin, D. Lucas, and C. Ballance. High-rate, high-fidelity entanglement of qubits across an elementary quantum network. *Physical Review Letters*, 124:110501, 2020. DOI: 10.1103/PhysRevLett.124.110501.

[138] K. Szymański. *Numerical ranges and geometry in quantum information: Entanglement, uncertainty relations, phase transitions, and state interconversion*. PhD thesis, Uniwersytet Jagielloński (Poland), 2022. DOI: 10.48550/arXiv.2303.07390.

[139] K. Szymański and K. Życzkowski. Geometric and algebraic origins of additive uncertainty relations. *Journal of Physics A: Mathematical and Theoretical*, 53: 015302, 2019. DOI: 10.1088/1751-8121/ab4543.

[140] Y. S. Teo. *Introduction to Quantum-State Estimation*. World Scientific, 2015. DOI: 10.1142/9617.

[141] B. M. Terhal and P. Horodecki. Schmidt number for density matrices. *Physical Review A*, 61:040301, 2000. DOI: 10.1103/PhysRevA.61.040301.

[142] J. Torres-Jimenez. Uniform CA. URL: https://www.tamps.cinvestav.mx/~oc/.

[143] J. Torres-Jimenez and I. Izquierdo-Marquez. Survey of covering arrays. In *15th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing*, pages 20–27. IEEE, 2013. DOI: 10.1109/SYNASC.2013.10.

[144] G. Tóth and O. Gühne. Entanglement detection in the stabilizer formalism. *Physical Review A*, 72:022340, 2005. DOI: 10.1103/PhysRevA.72.022340.

[145] N. Tsimakuridze and O. Gühne. Graph states and local unitary transformations beyond local Clifford operations. *Journal of Physics A: Mathematical and Theoretical*, 50:195302, 2017. DOI: 10.1088/1751-8121/aa67cd.

[146] R. Uola, A. C. Costa, H. C. Nguyen, and O. Gühne. Quantum steering. *Reviews of Modern Physics*, 92:015001, 2020. DOI: 10.1103/RevModPhys.92.015001.

[147] M. Van den Nest, J. Dehaene, and B. De Moor. Graphical description of the action of local clifford transformations on graph states. *Physical Review A*, 69: 022316, 2004. DOI: 10.1103/PhysRevA.69.022316.

[148] M. Van den Nest, J. Dehaene, and B. De Moor. Local unitary versus local clifford equivalence of stabilizer states. *Physical Review A*, 71:062323, 2005. DOI: 10.1103/PhysRevA.71.062323.

[149] T. van Leent, M. Bock, R. Garthoff, K. Redeker, W. Zhang, T. Bauer, W. Rosenfeld, C. Becher, and H. Weinfurter. Long-distance distribution of atom-photon entanglement at telecom wavelength. *Physical Review Letters*, 124:010510, 2020. DOI: 10.1103/PhysRevLett.124.010510.

[150] F. Verstraete, J. Dehaene, B. De Moor, and H. Verschelde. Four qubits can be entangled in nine different ways. *Physical Review A*, 65:052112, 2002. DOI: 10.1103/PhysRevA.65.052112.

[151] Y.-X. Wang, Z.-P. Xu, and O. Gühne. Quantum LOSR networks cannot generate graph states with high fidelity. *npj Quantum Information*, 10:11, 2024. DOI: 10.1038/s41534-024-00806-z.

[152] J. Watrous. *The Theory of Quantum Information*. Cambridge University Press, 2018. DOI: 10.1017/9781316848142.

[153] S. Wehner and A. Winter. Higher entropic uncertainty relations for anti-commuting observables. *Journal of Mathematical Physics*, 49, 2008. DOI: 10.1063/1.2943685.

[154] S. Wehner, D. Elkouss, and R. Hanson. Quantum internet: a vision for the road ahead. *Science*, 362:eaam9288, 2018. DOI: 10.1126/science.aam9288.

[155] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger. Violation of bell's inequality under strict einstein locality conditions. *Physical Review Letters*, 81:5039, 1998. DOI: 10.1103/PhysRevLett.81.5039.

[156] M. Weilenmann, B. Dive, D. Trillo, E. A. Aguilar, and M. Navascués. Entanglement detection beyond measuring fidelities. *Physical Review Letters*, 124: 200502, 2020. DOI: 10.1103/PhysRevLett.124.200502.

[157] L. T. Weinbrenner. PhD thesis, Universität Siegen (Germany). In preparation.

[158] R. F. Werner and M. M. Wolf. Bound entangled Gaussian states. *Physical Review Letters*, 86:3658, 2001. DOI: 10.1103/PhysRevLett.86.3658.

[159] H. Weyl. Quantenmechanik und Gruppentheorie. *Zeitschrift für Physik*, 46:1, 1927. DOI: 10.1007/BF02055756.

[160] E. Wolfe, R. W. Spekkens, and T. Fritz. The inflation technique for causal inference with latent variables. *Journal of Causal Inference*, 7:20170020, 2019. DOI: 10.1515/jci-2017-0020.

[161] E. Wolfe, A. Pozas-Kerstjens, M. Grinberg, D. Rosset, A. Acín, and M. Navascués. Quantum inflation: a general approach to quantum causal compatibility. *Physical Review X*, 11:021043, 2021. DOI: 10.1103/PhysRevX.11.021043.

[162] Z.-P. Xu. Characterizing arbitrary quantum networks in the noisy intermediate-scale quantum era. *Physical Review A*, 108:L040201, 2023. DOI: 10.1103/PhysRevA.108.L040201.

[163] Z.-P. Xu, R. Schwonnek, and A. Winter. Bounding the joint numerical range of Pauli strings by graph parameters. *PRX Quantum*, 5:020318, 2024. DOI: 10.1103/PRXQuantum.5.020318.

[164] X. Yang, Y.-H. Yang, and M.-X. Luo. Strong entanglement distribution of quantum networks. *Physical Review Research*, 4:013153, 2022. DOI: 10.1103/PhysRevResearch.4.013153.

[165] Z. Yang, S. Ru, L. Cao, N. Zheludev, and W. Gao. Experimental demonstration of quantum overlapping tomography. *Physical Review Letters*, 130:050804, 2023. DOI: 10.1103/PhysRevLett.130.050804.

[166] J. Yin, Y. Cao, Y.-H. Li, S.-K. Liao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai, G.-B. Li, Q.-M. Lu, Y.-H. Gong, Y. Xu, S.-L. Li, F.-Z. Li, Y.-Y. Yin, Z.-Q. Jiang, M. Li, J.-J. Jia, G. Ren, D. He, Y.-L. Zhou, X.-X. Zhang, N. Wang, X. Chang, Z.-C. Zhu, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan. Satellite-based entanglement distribution over 1200 kilometers. *Science*, 356:1140, 2017. DOI: 10.1126/science.aan3211.

[167] M. Żukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert. "Event-ready-detectors" Bell experiment via entanglement swapping. *Physical Review Letters*, 71:4287, 1993. DOI: 10.1103/PhysRevLett.71.4287.