Learning from correlations:
What parts of quantum states tell about the whole

Dissertation

zur Erlangung des Grades eines Doktors
der Naturwissenschaften

vorgelegt von
M. Sc. Nikolai Wyderka

„Wo man sich rangibt, da hat man Last mit.“

Abstract

The aim of this thesis is to deepen the understanding of correlations between particles in quantum mechanical systems. It focuses on finding relationships between the correlations among different parts of the system, as well as revealing their limitations in multi-qubit states.

In particular, new answers to the quantum marginal problem are found, i.e., the question of whether knowledge of the subsystems of certain particle numbers allows fixing a global quantum state uniquely. Among other things, it is shown that in many cases, certain sets of two-particle reduced states determine a joint four-particle state uniquely. Furthermore, it is shown that the set of correlations in multi-qubit states naturally decomposes into an odd and an even component, where often one component uniquely fixes the other. This finding is consequently applied to the problem of entanglement detection and the characterization of ground states of Hamiltonians.

In the second part of the thesis, interrelations between correlation quantifiers of degree two, known as Sector lengths, are established and connected to quantum mechanical properties of states. It is shown that Sector lengths are helpful for the detection of entanglement, and that they are subject to monogamy-like constraints, limiting the amount of concurrent correlations between different particles. Consequently, it is investigated which additional information for the task of entanglement detection is yielded by higher-order invariants, in particular higher moments of the distribution of correlation measurements.

The third part considers the problem of entanglement detection in experimentally limited scenarios: It analyses the capabilities of entanglement detection having access to expectation values of two product observables only. In systems of restricted dimensionality, necessary and sufficient criteria to be useful for such tasks are developed for pairs of such observables.

The last chapter extends the scope of the thesis via a theoretical assessment of quantum memories. As important building blocks for future applications of quantum mechanics, like quantum computers and quantum communication, these memory devices need to store quantum states faithfully for the corresponding task. In order to being able to characterize this property of quantum memories sufficiently, abstract criteria for memory performance measures are developed. Consequently, three such measures based on the coherence of quantum states are defined and their properties are determined.

Zusammenfassung

Das Ziel dieser Dissertation ist es, das Verständnis quantenmechanischer Korrelationen zu vertiefen, indem Abhängigkeiten zwischen und Beschränkungen von Korrelationen unterschiedlicher Teile von Mehrteilchenzuständen gefunden werden.

Um dieses Ziel zu erreichen, wird zunächst das Quantenmarginalienproblem untersucht. Dieses beschäftigt sich mit der Frage, ob die Kenntnis der Zustände physikalischer Subsysteme ausreicht, um den globalen Zustand eindeutig zu bestimmen. Hier wird unter anderem gezeigt, dass bestimmte Zweiteilchen-Subsysteme einen gemeinsamen Vierteilchen-Zustand eindeutig bestimmen. Anschließend wird das Marginalienproblem verallgemeinert und gezeigt, dass die Menge aller Korellationen in Systemen mehrerer Qubits auf natürliche Weise in zwei Komponenten zerfällt; die Menge der Korrelationen zwischen einer ungeraden, und solchen zwischen einer geraden Anzahl von Teilchen. In vielen Fällen wird die eine Komponente durch die andere eindeutig bestimmt. Schließlich werden Anwendungen zur Verschränkungsdetektierung und Charakterisierung von Grundzuständen aufgezeigt.

Im zweiten Teil der Dissertation werden Sektorlängen als geeignete Größen zur Charakterisierung der Korrelationsstärke zwischen verschiedenen Zahlen von Teilchen eingeführt und mit den quantenmechanischen Eigenschaften des Systems in Verbindung gebracht. Insbesondere wird aufgezeigt, dass Sektorlängen für die Verschränkungsdetektion geeignet sind und monogamieartiger Beschränkungen unterliegen, die die gleichzeitige Korrelation verschiedener Teile des Systems einschränken. Daraufhin wird untersucht, inwiefern Verteilungen von Korrelationsmessungen als Invarianten höheren Grades dabei helfen können, Verschränkungseigenschaften von Quantensystemen zu charakterisieren.

Der dritte Teil beschäftigt sich mit der Detektion von Verschränkung trotz eingeschränkter experimenteller Möglichkeiten. Hier wird untersucht, in welchen Fällen die Kenntnis von Erwartungswerten zweier Produkt-Observablen ausreichen kann, um Verschränkung nachzuweisen. Schließlich werden in Systemen beschränkter Dimension notwendige und hinreichende Kriterien für die Nützlichkeit eines solchen Observablenpaares gefunden.

Im letzten Kapitel wird der Blick auf die theoretische Charakterisierung von Quantenspeichern gerichtet. Solche Speicher sind wichtige Bestandteile künftiger Anwendungsgebiete wie Quantenrechnern und Quantenkommunikation, und müssen als solche in der Lage sein, Quantenzustände originalgetreu zu speichern. Um die Leistung solcher Quantensysteme ausreichend beurteilen zu können, werden abstrakte

Kriterien für Qualitätsmaße von Quantenspeichern entwickelt. Anschließend werden drei solche Maße definiert und deren Eigenschaften untersucht.

Table of contents

1 Introduction

Throughout the history of science, the observation of correlations has been a driving force to gain insight into the underlying laws of physics. To mention only a few early examples, Archimedes' principle was derived from noticing correlations between the density of objects and displaced liquid, and heliocentrism was proposed as a simple model to explain correlations between the celestial orbits of the planets [1]. The list continues to the times of modern physics: the detection of missing correlations between the intensity of light and the energy of electrons in experiments on the photoelectric effect pushed the development of quantum theory [2], and correlations between temperature deviations in the cosmic microwave background are deeply connected to fundamental parameters of cosmic models, like the age of the universe and the relative amount of dark matter and dark energy [3].

These examples make clear that a fundamental comprehension of correlations lies at the heart of the cognitive process associated with theoretical physics. This thesis is concerned with deepening this understanding in the context of quantum mechanics. Quantum mechanics was developed following a number of observations that could not be sufficiently explained classically, like the frequency dependence of the intensity of a black-body radiator [4] and the already mentioned energy spectrum of electrons emitted through the photoelectric effect [2]. Even though these findings could be explained phenomenologically by introducing the notion of quanta in the early twentieth century, it was not until 1925 that a concise mathematical theory of quantum mechanics was developed [5].

The rapid derivation of the uncertainty principle [6], stating that certain observables cannot be measured with great precision at the same time lead to the formulation of the Copenhagen interpretation of quantum mechanics, a fundamental shift of paradigm that is popular until today. It states that physical objects do not have defined physical properties until they are measured. The ambiguity of what exactly defines a measurement process is a question at the boundary of physics and philosophy and still a source of vivid discussions in the physics community.

In contrast, most physicists agree that studying correlations between observables is an impartial way of describing the striking phenomena predicted by quantum mechanics. One of these is the existence of non-local correlations between far apart particles, known as entanglement and fundamentally different from correlations that are present in classical systems. It allows for an observer to measure a property of one part of an entangled system, and, by the Copenhagen interpretation, fix this property in the same process not only for the part at hand but for the whole entangled system, independent from where in the universe it is located. It is a common misunderstanding that entanglement would allow for faster-than-light communication: In order to become entangled, the two systems have to interact physically, i.e., be in causal contact before, and it is not possible to transmit information faster than the speed of light with the help of entanglement.

Nevertheless, entanglement enables applications as quantum teleportation and quantum cryptography, as well as advanced computation schemes in quantum computers. While the first two applications are of interest in the context of secure communication, as they allow for an uninterceptable key exchange, the latter application is of great interest due to the ability of quantum computers to solve problems that are intractable on classical computers, as the simulation of quantum systems or prime factorization,

The recurrent theme of this thesis is to understand the capabilities, but also the limitations of the correlations present in quantum systems. While the set of admissible quantum correlations is larger than the set of classical correlations, this additional freedom is also the source of many possible dependencies between the properties of different parts of quantum mechanical states. We study these relations in the first two scientific chapters of this thesis: In Chapter 3 we consider the question of what one can learn about a composite quantum system from the knowledge of correlations between subsystems of certain sizes, a question relevant for secure communication, the characterization of ground states of Hamiltonians and quantum chemistry. In Chapter 4, we generalize the same question to larger sets of correlations, not only those of certain subsystems. As it turns out, the correlations of systems of multiple particles with two internal degrees of freedom, called qubits, factorize naturally into two components, where one component often completely determines the other.

Chapter 5 is concerned with quantifying the size of correlations in quantum systems. To that end, we introduce a measure of correlation strength for different sizes of subsystems, called sector lengths, and show that knowledge of these sizes allows inferring many of the non-local properties of quantum states.

We then turn to more practically relevant topics in Chapter 6, where we consider the question of how one can maximize the inferred information about systems from correlation measurements. As it turns out, knowledge of the distribution of expectation values yields access to more properties of the state than expectation values alone.

As entanglement is a key resource for many applications of quantum mechanics, we tackle the problem of determining the minimal experimental requirements that allow for entanglement detection in Chapter 7. Finally, we put the focus on practical implementations of basic building blocks of quantum computers in Chapter 8: We explain why quantum memories are important for quantum computation and communication and how one can evaluate their performance using coherence, another kind of non-classical property of quantum mechanics.

The chapters are written such that they can be understood independently from one another, even though we highlight the many connections between the topics in the text. The common mathematical foundation needed to understand the chapters is developed in Chapter 2. In order to guide the impatient reader, we display a list of prerequisites, i.e., a collection of sections from Chapter 2 necessary to understand the following text, at the beginning of each chapter.

2 Mathematical toolbox

2.1 Introduction

We begin by explaining the basic concepts of quantum mechanics and build our set of tools upon it. To that end, we will introduce the axioms of quantum mechanics and review the notion of pure and mixed quantum states. For the latter, we will introduce a very expedient basis, called the Bloch basis, that is used throughout this thesis in order to describe correlations in multi-qubit states.

After introducing the notion of marginal states, which correspond to states of subsystems of a global state, we will introduce the concept of entanglement, which is, apart from coherence, probably the most important non-classical feature of quantum mechanics. After stating the definition, we will introduce useful measures of entanglement and review prominent results about the monogamy of entanglement, which states that even though quantum mechanics allows for entanglement, it also limits it in interesting ways.

Next, we introduce quantum channels as an important tool to describe physical manipulations of states. Mathematically speaking, they correspond to mappings between states even if applied to only parts of a global state. Quantum channels will be of importance when we look at quantum memories in Chapter 8.

An important quantum informational quantity is the entropy of a system. We introduce two different entropies, the von Neumann entropy as a generalization of the usual Shannon entropy to quantum states, and, as an approximation, the easier to compute linear entropy, and highlight the differences between the two quantities.

Consequently, we have a look at coherence as a quantifier of superposition, the second important non-classical feature of quantum mechanics and finally introduce the concept of semidefinite programs, a class of optimization problems that are ubiquitous in quantum information and in some cases allow for analytical statements about the existence and optimality of solutions.

2.2   Quantum mechanics and quantum states

The theory of quantum mechanics is based upon a number of axioms that define the mathematical structure as well as the notion of measurement processes. Here, we follow the outline given in [7]:

— *The state of a system is given by a vector in a Hilbert space.*

Throughout this thesis, we are concerned with finite-dimensional systems. For these, the Hilbert space $\mathcal{H}$ is given by $\mathbb{C}^d$ where d denotes the dimension of the system. Vectors in this space are usually denoted by $|\psi\rangle$, called *ket*-vector. The hermitian adjoint of $|\psi\rangle$ is denoted by $|\psi\rangle^\dagger = \langle\psi|$, called *bra*-vector. We assume pure states to be vectors that are normalized according to the usual inner product $(|\psi\rangle, |\phi\rangle) := \langle\psi|\phi\rangle$, that is, $\langle\psi|\psi\rangle = 1$. Furthermore, vectors differing by only a complex phase are considered equivalent pure states. Technically, this means that the set of states corresponds to the projective space $\mathbb{C}P^{d-1}$. Finally, we denote the canonical basis of $\mathbb{C}^d$ by $|0\rangle, |1\rangle, \ldots, |d-1\rangle$.

While each isolated physical system is always in a pure state, it might be unknown in which state it is exactly. As an example, consider a photon that is emitted from a light bulb. The photon is polarized in a certain direction relative to a given basis, thus its state is described by a normalized vector of the form $a|H\rangle + b|V\rangle$, where $|H\rangle$ and $|V\rangle$ denote horizontally and vertically polarized photons, respectively. However, this direction is random for each emitted photon. This is why we use mixed states to capture this classical randomness. A mixed state (sometimes called density matrix) ρ is a convex combination of projectors onto pure states, or

$$\rho = \sum_{i=1}^{r} p_i |\psi_i\rangle\langle\psi_i|, \tag{2.1}$$

where $p_i > 0, \sum_i p_i = 1$. The vectors $|\psi_i\rangle$ can be chosen to be orthonormal, in which case the number of addends, r, denotes the rank of the state.

It sometimes makes sense to treat pure states as operators as well by switching from the vector representation $|\psi\rangle$ to the operator representation $|\psi\rangle\langle\psi|$. Then, the set of all mixed and pure states is given by the set of all positive semidefinite hermitian operators of trace one, i.e.,

$$\rho = \rho^\dagger, \quad \mathrm{Tr}\,(\rho) = 1, \quad \rho \geq 0. \tag{2.2}$$

Here, positive semidefinite means that the eigenvalues of the matrix representation are non-negative.

— The time evolution of a pure state is given by the Schrödinger equation.

Let H denote the Hamiltonian of the system, i.e., a hermitian operator governing the interactions. Then a pure state evolves according to the Schrödinger equation via

$$i\hbar\partial_t|\psi(t)\rangle = i\partial_t|\psi(t)\rangle = H|\psi(t)\rangle, \tag{2.3}$$

where we use natural units here and in the following such that $\hbar = 1$. If the Hamiltonian is not explicitly time dependent, one can formally write

$$|\psi(t)\rangle = e^{-iHt}|\psi(0)\rangle \tag{2.4}$$

for some initial state $|\psi(0)\rangle$.

— Observables are represented by hermitian matrices on the Hilbert space.

Each observable A can be written in a spectral decomposition,

$$A = \sum_{i=1}^{K} \alpha_i|a_i\rangle\langle a_i|. \tag{2.5}$$

The possible outcomes of a measurement of A are given by the eigenvalues α_i. If the system is in the state ρ prior to the measurement, the probability of obtaining α_i is given by $\langle a_i|\rho|a_i\rangle$. Therefore, the expectation value of the measurement is given by $\langle A \rangle = \sum_i \alpha_i\langle a_i|\rho|a_i\rangle = \mathrm{Tr}(\rho A)$. After the measurement, the state is in an eigenstate of A corresponding to the measurement result α_i.

Measurements in an eigenbasis of an observable are called projective measurements. More generally, however, one can also consider projective measurements on a larger system, consisting of the original system and an environment. This leads to the notion of POVMs (positive operator valued measures). Instead of a set of projections to the eigenvectors of an observable, one obtains a set of N positive observables $\{E_k\}_{k=1}^N$, called effects, that sum to the identity, i.e.,

$$\sum_{k=1}^{N} E_k = \mathbb{1}. \tag{2.6}$$

Such a generalized measurement yields the outcome k with probability

$$p_k = \mathrm{Tr}(\rho E_k). \tag{2.7}$$

As each effect E_k is hermitian and positive, it can be decomposed into measurement operators A_i, such that $E_k = A_k^\dagger A_k$, although the A_k are not uniquely determined,

except for the case of projective measurements. Given a decomposition into measurement operators, the post-measurement state after obtaining outcome k is given by

$$\rho_k = \frac{A_k \rho A_k^\dagger}{p_k}. \tag{2.8}$$

The case of projective measurements is recovered by choosing $E_k = |\psi_k\rangle\langle\psi_k|$ as the projectors onto the eigenvectors of the observable.

In the case of projective measurements, a direct consequence of the projection onto eigenstates during the measurement process is that a state cannot yield certain results w.r.t. two non-commuting observables, if the state lies in the non-commuting subspace. This observation leads to famous results like the Heisenberg uncertainty principle [6]. For POVMs, the notion of incompatibility is less straight-forwardly characterized. We call a set of m POVMs, $\{\{E_k^{(1)}\},\dots,\{E_k^{(m)}\}\}$ *compatible*, or *jointly measurable*, if there exists a joint measurement POVM $\{E_{\vec{k}}\}$ where $\vec{k} = (k_1,\dots,k_m)$ is a vector of individual measurement results for the corresponding $\{E_k^{(j)}\}$, and the marginals of $\{E_{\vec{k}}\}$ yield the individual measurements, i.e.,

$$\sum_{k_1}\cdots\sum_{k_{j-1}}\sum_{k_{j+1}}\cdots\sum_{k_m} E_{\vec{k}} = E_{k_j}^{(j)} \tag{2.9}$$

for each $j = 1,\dots,m$.

Finally, we explicitly state another axiom that usually is hidden in the mathematical formalism:

— *The Hilbert space of a composite system is given by the tensor product of the Hilbert spaces of the individual systems.*

The composite system of n systems of dimension d is given by $\mathbb{C}^d \otimes \dots \otimes \mathbb{C}^d \cong \mathbb{C}^{d^n}$. We denote the canonical basis of this space by $|i_1 \dots i_n\rangle = |i_1\rangle \otimes \dots \otimes |i_n\rangle$, where $i_j \in \{0,\dots,d-1\}$ for each j.

2.3 Qubits and the Bloch basis

In this thesis, we will be mainly concerned with multi-qubit states, that is, we consider states in a composite system of n two-level systems. In the language of the previous section, this means $d = 2$ and the quantum states are called qubit states. More generally, states consisting of d-level systems are called qudits. For qubit states,

we introduce a particularly useful basis, called the Bloch basis. We start by introducing it for a single qubit [7].

A qubit is the smallest quantum mechanical system and has dimension $d = 2$. A physical example of such a system would be the spin of an electron, which can be in a superposition of up, ($|0\rangle$) and down ($|1\rangle$). Taking into account the normalization and equivalence under a global phase, the electron's state can be written as

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle. \tag{2.10}$$

Thus, of the four real dimensions of $\mathbb{C}^2$ only two dimensions survive. The set of physical pure states can be interpreted as the surface of a unit sphere in three dimensions, called Bloch sphere, with inclination θ and azimuth φ. This interpretation becomes more compelling when considering also mixed states. To that end, we choose as a basis for the space of 2 by 2 matrices the Pauli matrices, given by

$$\sigma_0 = \mathbb{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_1 = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2 = Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_3 = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{2.11}$$

This is a hermitian, orthogonal basis under the Hilbert-Schmidt inner product, i.e., $(\sigma_i, \sigma_j) := \text{Tr}(\sigma_i\sigma_j) = 2\delta_{ij}$, called Bloch basis. Furthermore, X, Y and Z are traceless, and, as $\sigma_i^2 = \mathbb{1}$ for all i, they are unitary matrices, too.

We can now write each mixed state in this basis as

$$\rho = \frac{1}{2}(a_0\sigma_0 + a_1\sigma_1 + a_2\sigma_2 + a_3\sigma_3). \tag{2.12}$$

Imposing the constraints from Eq. (2.2) yields the following: The coefficients a_i are real, as $\rho = \rho^\dagger$; $a_0 = 1$, as $\text{Tr}(\rho) = 1$ and the only non-traceless basis element is σ_0. This also why we choose the normalization of $1/2$ in Eq. (2.12). Requiring positivity of ρ yields $a_1^2 + a_2^2 + a_3^2 \leq 1$. This motivates defining the vectors $\vec{a} := (a_1, a_2, a_3)^\text{T}$ and $\vec{\sigma} := (\sigma_1, \sigma_2, \sigma_3)^\text{T}$, and writing

$$\rho = \frac{1}{2}(\mathbb{1} + \vec{a} \cdot \vec{\sigma}). \tag{2.13}$$

Thus, physical mixed states of single qubits are parameterized by a three-dimensional vector $\vec{a}$ whose length must not exceed one. This corresponds to points inside of a three-dimensional unit sphere. Calculating the projector $|\psi\rangle\langle\psi|$ from the vector $|\psi\rangle$ in Eq. (2.10) yields in the Bloch basis $a_1 = \sin\theta\cos\varphi$, $a_2 = \sin\theta\sin\varphi$ and $a_3 = \cos\theta$, i.e., exactly the point on the surface of the sphere with inclination θ and azimuth φ.

What is more, the basis coefficients a_i can be directly measured, as the basis is hermitian: $a_i = \langle\sigma_i\rangle$.

Finally, we can augment the single-qubit basis to a multi-qubit one by taking the n-fold tensor product of all combinations of single-qubit basis matrices σ_i:

$$\rho = \frac{1}{2^n} \sum_{i_1,\dots,i_n=0}^{3} a_{i_1\dots i_n} \sigma_{i_1} \otimes \dots \otimes \sigma_{i_n}. \qquad (2.14)$$

The basis elements inherit many of their properties from the single qubit case: The only element in the basis that is not traceless is the identity, i.e., $\sigma_0 \otimes \dots \otimes \sigma_0$ with a trace of 2^n, fixing $a_{0\dots0} = 1$. Furthermore, the basis elements are hermitian and unitary, and form an orthogonal basis with $\mathrm{Tr}[(\sigma_{i_1} \otimes \dots \otimes \sigma_{i_n})(\sigma_{j_1} \otimes \dots \otimes \sigma_{j_n})] = 2^n \delta_{i_1 j_1} \dots \delta_{i_n j_n}$. Imposing $\rho = \rho^\dagger$ translates into the constraint that the coefficients $a_{i_1\dots i_n}$ must be real. They can again be expressed as $a_{i_1\dots i_n} = \langle \sigma_{i_1} \otimes \dots \otimes \sigma_{i_n} \rangle$. However, the positivity of quantum states imposes a plethora of high-degree constraints on the coefficients that lack a simple geometrical interpretation as in the single-qubit case. In fact, some interesting features of quantum mechanics, like monogamy of entanglement and the findings of Chapter 5 are due to this positivity constraint.

Note further that the basis elements $\sigma_{i_1} \otimes \dots \otimes \sigma_{i_n}$ occurring in the Bloch decomposition have a certain number of identity matrices in them, meaning that they act trivially on the corresponding qubit. Therefore, we define the weight of a basis element as the number of nontrivial (meaning non-identity) Pauli matrices in it, or mathematically

$$\mathrm{wt}(\sigma_{i_1} \otimes \dots \otimes \sigma_{i_n}) := |\{j | i_j \neq 0\}|. \qquad (2.15)$$

It will be useful later on to group the terms of a state ρ given in the Bloch decomposition in Eq. (2.14) according to their weight. We define

$$P_k(\rho) := \sum_{\substack{i_1,\dots,i_n=0 \\ \mathrm{wt}(\sigma_{i_1}\otimes\dots\otimes\sigma_{i_n})=k}}^{3} a_{i_1\dots i_n} \sigma_{i_1} \otimes \dots \otimes \sigma_{i_n}, \qquad (2.16)$$

such that

$$\rho = \frac{1}{2^n} \sum_{k=0}^{n} P_k(\rho). \qquad (2.17)$$

The only term of weight 0 consists of identities only, with the prefactor fixed by the unit trace of the state. Thus $P_0(\rho) = \sigma_0 \otimes \dots \otimes \sigma_0 = \mathbb{1}_{2^n \times 2^n}$, which is why we usually write this term explicitly: $\rho = \frac{1}{2^n}[\mathbb{1} + \sum_{k=1}^{n} P_k(\rho)]$. If the state under consideration is clear from the context, we simply write P_k.

A particularly useful quantity will be the square of the Hilbert-Schmidt norm of the operators P_k, which are called sector lengths [8]:

$$A_k(\rho) := \frac{1}{2^n} \text{Tr}[P_k(\rho)^2]. \tag{2.18}$$

Note, that we call A_k a length, even though it is the square of the norm. The sector length A_k captures the amount of k-partite correlations in the state and is useful to describe the properties of a state for two reasons: First of all, by definition, they are invariant under local unitary rotations (LU-invariant), i.e., changes of the local basis. Second of all, using the Löwner-Heinz theorem, one can show that they are convex, i.e., $A_k(\sum_i p_i \rho_i) \leq \sum_i p_i A_k(\rho_i)$ [9]. This also implies that the extremal values are realized by pure states.

One important LU-invariant of a state is its purity, $\text{Tr}(\rho^2)$. This quantity equal to one for pure states and minimal for maximally mixed states of dimension d, $\rho = \frac{1}{d}\mathbb{1}_{d \otimes d}$, taking a value of $\frac{1}{d}$. Note that from Eq. (2.17) it follows directly that

$$\text{Tr}(\rho^2) = \frac{1}{2^n}[1 + \sum_{k=1}^{n} A_k(\rho)]. \tag{2.19}$$

2.4 Marginal states

Consider a global state of n particles of dimension d each. Sometimes, one is interested in the subsystem of $k < n$ of the parties only. For example, the global state could be consisting of an experimentally accessible part of k parties and an inaccessible environment of $n - k$ parties, or one is limited in the lab to measurements on at most k different parties at the same time. In these cases, one is interested in the marginal, or reduced state, of the k parties only. The state of this subsystem is also a proper quantum state, and it is obtained from the global state by taking the partial trace over the inaccessible subsystems. Mathematically speaking, we denote by ρ the global state of the n-partite system. Let $S \subset \{1, \ldots, n\}$ be a subset of the parties of cardinality k, and $\bar{S} = \{1, \ldots, n\} \setminus S$ its complement. Then the k-body marginal of parties S is defined via

$$\rho_S := \text{Tr}_{\bar{S}}(\rho). \tag{2.20}$$

Here, $\text{Tr}_{\bar{S}}$ denotes the partial trace that maps operators on $\mathcal{H}_S \otimes \mathcal{H}_{\bar{S}}$ linearly onto operators on $\mathcal{H}_S$ via $\text{Tr}_{\bar{S}}(A_S \otimes A_{\bar{S}}) = \text{Tr}(A_{\bar{S}})A_S$ for all operators A_S on $\mathcal{H}_S$ and operators $A_{\bar{S}}$ on $\mathcal{H}_{\bar{S}}$.

2.4.1 The marginal problem

The quantum marginal problem consists of several existence and compatibility questions related to the marginal states of quantum systems. It is best understood looking at its classical analogon: Shining parallel light under a certain angle on an opaque three-dimensional object creates a shadow (a projection) of the object. The classical marginal problem is now the following uniqueness question: Having a set of shadows and their corresponding angles, does this data allow to uniquely reconstruct the bulk object? It is easy to see that in this very general example, uniqueness of a reconstructed object can almost never be ensured, as one can always carve out a hole in the bulk object without changing any projection.

A second question related to the marginal problem is very similar: Given the shadows only, does there exist a compatible bulk object, i.e., an object that produces exactly the shadows at hand. Interestingly, the classical answer to this problem is almost always yes [10]. This allows for example for the construction of digital sundials, that produce the image of a digital clock showing the correct time, depending on the angle of incidence of the sunlight.

The answers to the analogous quantum marginal questions are different but highly relevant in many scenarios. Before we state known results there, we rephrase the set of questions mathematically. Note that we give a more physically motivated list of applications of the quantum marginal at the beginning of Chapter 3.

2.4.2 Mathematical description

Consider a quantum system of n parties, and a set of subsystems $\mathcal{S} = \{S_i\}$, where each $S_i \subset \{1, \ldots, n\}$. Associated to each subsystem, we have a quantum state ρ_{S_i} living on that system.

Following the notation of Ref. [11], we define the joining set of the set of states $\{\rho_{S_i}\}$:

Definition 2.1. The *mixed joining set* $\mathcal{M}_{\mathcal{S}}$ of a set of marginal states $\{\rho_{S_i} \mid S_i \in \mathcal{S}\}$ denotes the set of compatible n-partite states, i.e.,

$$\mathcal{M}_{\mathcal{S}}(\{\rho_{S_i}\}) := \{\rho \mid \forall i \ \mathrm{Tr}_{\bar{S}_i}(\rho) = \rho_{S_i}\}. \tag{2.21}$$

The *pure joining set* denotes the set of compatible pure n-partite states;

$$\mathcal{M}_{\mathcal{S}}^{\mathrm{p}} := \{\rho \in \mathcal{M}_{\mathcal{S}} \mid \rho^2 = \rho\}. \tag{2.22}$$

If $\mathcal{S}$ consists of all subsystems of size k, i.e., $\mathcal{S} = \{S \subset \{1, \ldots, n\} \, | \, |S| = k\}$, then we denote the joining set simply by $\mathcal{M}_k$.

With this definition, we are in position to pose the two marginal problems, namely the uniqueness and the compatibility problem, mathematically [12]:

Definition 2.2. A pure n-partite state $|\psi\rangle$ is called

- k-uniquely determined among all states (k-UDA), if there exists no other (mixed) state ρ with the same k-body marginals: $|\mathcal{M}_k| = 1$;

- k-uniquely determined among pure states (k-UDP), if there exists no other pure state ρ with the same k-body marginals: $|\mathcal{M}_k^{\mathrm{p}}| = 1$.

Here, the joining sets are formed w.r.t. the k-body marginals of $|\psi\rangle$.

Clearly, k-UDA implies k-UDP, but the converse is not true [13].

While the sets in the uniqueness problem are known to contain at least one element, namely the original state $|\psi\rangle$, this is unknown in the case of the compatibility question [14, 15]:

Definition 2.3. A set of marginal states $\{\rho_{S_i} \, | \, S_i \in \mathcal{S}\}$ is called compatible, (sometimes called n-representable in the context of fermionic systems), w.r.t. $\mathcal{S}$, if there exists a pure joining global n-partite state: $|\mathcal{M}_{\mathcal{S}}^{\mathrm{p}}(\{\rho_{S_i}\})| > 0$.

The compatibility problem has been shown to be QMA-complete [16, 17]. QMA-completeness is the quantum analog to NP-completeness, meaning that a) the problem is in QMA (there exists a quantum verifier that can be convinced of the right answer in polynomial time with high probability), and b) every problem in QMA can be reduced to the problem at hand [17]. Just like NP-complete problems, QMA-complete problems are considered very hard to solve, even with the help of quantum computers.

2.4.3 Previous results

The marginal problem, and in particular the question of uniqueness, was subject to intense study before. The compatibility question was posed first in the context of fermionic systems and their two-body reduced states [18]. This restricted scenario was finally solved [19]. Similar compatibility problems in non-fermionic systems have consequently been investigated as well [14, 20, 21].

The question of uniqueness was analyzed in detail first by Linden, Popescu and Wootters, who showed that almost all pure three-qubit states are determined among all mixed states by their two-body marginals [22]. In this context, *almost all* means that the statement is true for all states but a subset of measure zero. Later, Diósi showed that two of the three two-body marginals suffice to characterize uniquely a pure three-particle state among all other pure states [23]. In two major steps, it was then first shown that in qubit systems, the marginals of a certain fraction of roughly two-thirds of the parties suffice for uniquely fixing almost all quantum states [24]. Finally, this result has been improved and extended to higher dimensional systems: it was shown that almost all states of n qudits are uniquely determined by certain sets of reduced states of just more than half of the parties, whereas the reduced states of fewer than half of the parties are not sufficient [25]. Note that the marginals of a state are determined by the lower-order correlations. Thus, uniqueness can be interpreted as the higher-order correlations being determined by the lower-order ones.

2.5 Entanglement

We already noted that multipartite states live on the tensor product space of the individual parties. As the dimension of the product space is given by the product of the individual dimensions, this means that there is space for many more states than just the possible combinations of the individual (local) states. This is in contrast to the classical world: If we consider a classical system, like a pixel on a computer screen, then its state can be described by three real numbers, namely the red, the green and the blue intensity. The state of two such pixels could then be described by six numbers. In the quantum world, however, the joint system would be nine-dimensional, leaving space for three extra dimensions.

2.5.1 Bipartite entanglement

Let us consider the simplest case of a pure two-partite system. We call its state $|\psi\rangle$ *separable* or *product*, if it can be written as [26]

$$|\psi\rangle = |\phi_A\rangle \otimes |\phi_B\rangle, \tag{2.23}$$

where $|\phi_{A/B}\rangle$ are pure single-particle states. Separable states are the analog to the classical states in the example above. An example of such a state of two qubits would be the state $|00\rangle = |0\rangle \otimes |0\rangle$. However, not all states can be written in that form. For example, the state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ cannot be decomposed, as a simple

calculation with an ansatz $|\phi_A\rangle = a|0\rangle + b|1\rangle$, $|\phi_B\rangle = c|0\rangle + d|1\rangle$ shows, as then $ac = bd = \frac{1}{\sqrt{2}}$, whereas $ad = bc = 0$, leading to a contradiction. Non-separable pure states like $|\Phi^+\rangle$ are called *entangled* [26].

In order to check whether a given bipartite pure state is entangled, one can use the Schmidt decomposition [27]: We can write each state in the canonical basis as

$$|\psi\rangle = \sum_{i,j=0}^{d-1} a_{ij}|ij\rangle. \tag{2.24}$$

The complex valued coefficients a_{ij} define a $d \times d$-dimensional matrix A, that we can write as $A = U\Sigma V$ using the singular value decomposition, where U and V are unitary matrices and Σ is a diagonal matrix with non-negative numbers $\sqrt{\lambda_0}, \ldots, \sqrt{\lambda_{d-1}}$ on its diagonal. Thus, we can write

$$|\psi\rangle = \sum_{i,j,k=0}^{d-1} u_{ik}\sqrt{\lambda_k}v_{kj}|ij\rangle \tag{2.25}$$

$$= \sum_{k=0}^{d-1} \sqrt{\lambda_k} \left(\sum_{i=0}^{d-1} u_{ik}|i\rangle\right) \left(\sum_{j=0}^{d-1} v_{kj}|j\rangle\right) \tag{2.26}$$

$$\equiv \sum_{k=0}^{d-1} \sqrt{\lambda_k}|k\rangle_A \otimes |k\rangle_B, \tag{2.27}$$

where $|k\rangle_A = \sum_{i=0}^{d-1} u_{ik}|i\rangle$ and $|k\rangle_B = \sum_{j=0}^{d-1} v_{kj}|j\rangle$ are called the local Schmidt basis of party A and B, respectively, and form orthonormal bases due to the properties of the unitary matrices U and V. The numbers $\sqrt{\lambda_k}$ are called Schmidt coefficients of $|\psi\rangle$. The number of non-vanishing Schmidt coefficients is called the Schmidt rank of $|\psi\rangle$. The state is a product state, iff it has Schmidt rank one [27]. If, however, the Schmidt rank is equal to d and all Schmidt coefficients are equal, the state is called *maximally entangled*.

For mixed states, the notion of entanglement is a bit more involved. Apart from product states $\rho = \rho_A \otimes \rho_B$, also classical convex mixtures of product states, i.e.,

$$\rho_{\text{sep}} = \sum_{i=1}^{r} p_i \rho_A^{(i)} \otimes \rho_B^{(i)}, \tag{2.28}$$

need to be considered as separable states [26]. However, it is much more complicated to decide whether a mixed state is entangled or not, and there are necessary and sufficient criteria only in some special cases. In fact, deciding whether a given state is separable or not, is NP-hard [28].
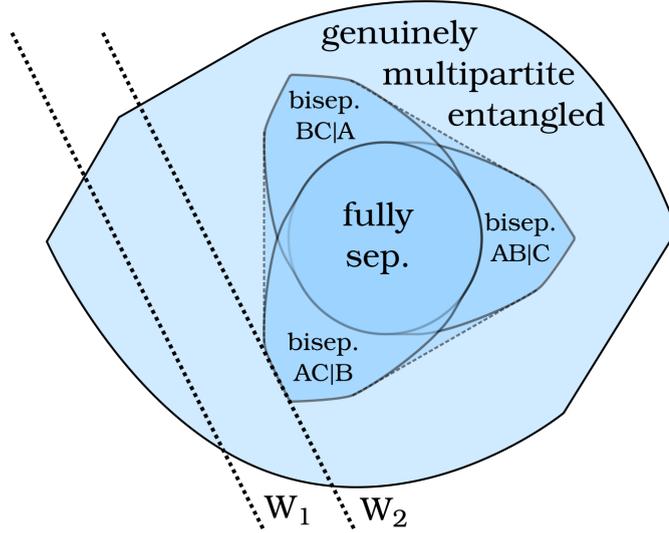
FIGURE 2.1: The convex set of all tripartite states and the subsets of biseparable and fully separable states. The dotted line corresponds to states of vanishing expectation value w.r.t. the witness observable W_1 and the optimal W_2, respectively.

A simple necessary criterion is the PPT (positive partial transpose) criterion: We define the partial transpose map via its action on the canonical operator basis element $|ij\rangle\langle kl|$ via

$$|ij\rangle\langle kl|^{T_B} = |il\rangle\langle kj|. \tag{2.29}$$

As this map is linear, its effect on separable states of the form in Eq. (2.28) is given by

$$\rho_{\text{sep}}^{T_B} = \sum_{i=1}^{r} p_i \rho_A^{(i)} \otimes (\rho_B^{(i)})^T, \tag{2.30}$$

which is still positive, as $(\rho_B^{(i)})^T$ is again a state. If, however, the state is not separable, the partial transpose might map it to something which is not positive anymore, proving that it is entangled.

The PPT criterion is very powerful, as it is necessary and sufficient for qubit-qubit and qubit-qutrit states. In larger-dimensional systems, however, there exist entangled states with positive partial transpose [26].

2.5.2 Multipartite entanglement

If we want to generalize the notion of entanglement to the multipartite scenario, we need to consider different kinds of entanglement, which are displayed in Fig. 2.1. In particular, a bipartite state of parties *A*, *B* and *C* is called *fully separable*, iff it can be

decomposed in terms of three products [26], i.e.,

$$\rho_{ABC} = \sum_i p_i \rho_A^{(i)} \otimes \rho_B^{(i)} \otimes \rho_C^{(i)}. \tag{2.31}$$

However, it could be the case that the state is not fully separable, but instead entangled between party B and C, while being separable between A and systems B and C. In this case, the state can be decomposed as

$$\rho_{ABC} = \sum_i p_i \rho_A^{(i)} \otimes \rho_{BC}^{(i)}, \tag{2.32}$$

in which case we call it *biseparable* w.r.t. the biseparation $A|BC$.

Convex combinations of biseparable states from any of the three different biseparability-classes are called *biseparable* [26]. Note that these can be mixtures of biseparable states w.r.t. different partitions as well, forming a convex subset in the whole convex state space, indicated by the dashed boundary in Fig. 2.1. Finally, states which are not biseparable are called genuinely multipartite entangled, or GME in short [26].

This concept can be generalized easily to more than three parties, yielding even more different entanglement types.

2.5.3   Entanglement measures

In the multipartite scenario, there is no unique notion of maximal entanglement anymore. Instead, there exist different methods to quantify the entanglement in such states, each of which giving rise to different sets of maximally entangled states. In this thesis, we are going to use two different entanglement measures as well as the method of entanglement witnesses in order to quantify multipartite entanglement.

An entanglement measure E is a map that assigns a numerical value to a state, exhibiting a set of properties. These properties are not uniquely defined in the literature, here we follow the definition of [29]. For a discussion about the different definitions, see for example [7].

Definition 2.4. We call a map E a (mixed-state) *entanglement measure*, if it fulfills the following:

E1 If ρ is separable, $E(\rho) = 0$.

E2 $E(\rho)$ should be invariant under a local change of basis, i.e., $E(U_A \otimes U_B \ldots \rho U_A^\dagger \otimes U_B^\dagger \ldots) = E(\rho)$ for all unitary maps U_A, U_B, $\ldots$.

E3 *E* should not increase under any local operation assisted by classical communication (a set of operations called LOCC), that is, $E[\Lambda(\rho)] \leq E(\rho)$ for all LOCC operations Λ.

E4 *E* should be convex, i.e., $E(\sum_i p_i \rho_i) \leq \sum_i p_i E(\rho_i)$.

E5 *E* should be extensive, which means that $E(\rho^{\otimes n}) = nE(\rho)$.

E6 *E* should be subadditive, meaning that $E(\rho \otimes \sigma) \leq E(\rho) + E(\sigma)$.

If a map *E* fulfills only E2 and E3, it is called an *entanglement monotone* [7].

Sometimes, entanglement measures are defined for pure states only, in which case the convexity property is dropped. Nevertheless, one can sometimes lift it to a mixed-state entanglement measure by using the convex roof construction [30]. To a mixed state ρ, it assigns the value

$$E(\rho) = \min_{\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|} \sum_i p_i E(|\psi_i\rangle), \tag{2.33}$$

where the minimization is taken over all pure state decompositions of ρ. This construction has the advantage that the quantity is convex by construction, and oftentimes it is straight-forward to see whether the other properties are inherited from the measure for pure states. However, it is a difficult task to perform the minimization analytically, except for some special choices of *E* for pure states, as in the case of the concurrence discussed below.

For our purposes, a particularly useful entanglement measure for qubits is the bipartite concurrence [31, 32] and one of its multipartite generalizations, the so-called *n*-concurrence, sometimes called θ-concurrence [29].

In order to define it, we define a useful map for quantum states, called universal state inversion.

Definition 2.5. The *universal state inversion* of an *n*-qubit state ρ is given by

$$\tilde{\rho} = Y^{\otimes n} \rho^T Y^{\otimes n}, \tag{2.34}$$

where *Y* is the Pauli matrix σ_2. In terms of the Bloch decomposition in Eq. (2.17), the state $\rho = \frac{1}{2^n} \sum_k P_k$ is mapped to

$$\tilde{\rho} = \frac{1}{2^n} \sum_{k=0}^{n} (-1)^k P_k. \tag{2.35}$$

Indeed, the action of the map is to flip the sign of all nontrivial Pauli matrices. Interestingly, this map is positive, meaning that $\tilde{\rho} \geq 0$ if $\rho \geq 0$ [33]. Furthermore, it maps

pure states to pure states, where it maps $|\psi\rangle$ to $|\tilde{\psi}\rangle = (iY)^{\otimes n}K|\psi\rangle = (iY)^{\otimes n}|\psi^\star\rangle$, where K denotes the anti-unitary complex conjugation operation, performed in the canonical basis, and $|\psi^\star\rangle$ denotes the complex conjugate of $|\psi\rangle$.

Applying this map twice on the level of mixed states yields the original state again. However, on the level of pure states,

$$|\tilde{\tilde{\psi}}\rangle = Y^{\otimes n}KY^{\otimes n}K|\psi\rangle \qquad (2.36)$$

$$= (-1)^n Y^{\otimes n}Y^{\otimes n}K^2|\psi\rangle \qquad (2.37)$$

$$= (-1)^n|\psi\rangle. \qquad (2.38)$$

As a consequence, it induces a relative phase if n is odd. Therefore, by the property of anti-unitary operations, $\langle\psi|\tilde{\psi}\rangle = \langle\tilde{\psi}|\tilde{\tilde{\psi}}\rangle^\star = \langle\tilde{\tilde{\psi}}|\tilde{\psi}\rangle = (-1)^n\langle\psi|\tilde{\psi}\rangle$. Thus, $\langle\psi|\tilde{\psi}\rangle = 0$ if n is odd, meaning that universal state inversion maps states to orthogonal states.

This feature can be used in the context of entanglement detection. If we have a two-qubit product state $|\psi\rangle = |\phi_1\rangle \otimes |\phi_2\rangle$, then $|\langle\psi|\tilde{\psi}\rangle| = |\langle\phi_1|\tilde{\phi_1}\rangle\langle\phi_2|\tilde{\phi_2}\rangle| = 0$. For non-product states, however, the magnitude of the overlap can be anything between 0 and 1. This motivates the definition of the concurrence [32]:

Definition 2.6. The *concurrence C* of a pure two-qubit state $|\psi\rangle$ is given by

$$C(|\psi\rangle) := |\langle\psi|\tilde{\psi}\rangle|. \qquad (2.39)$$

The concurrence is one of the few measures where the convex roof construction in Eq. (2.33) can be performed analytically. One obtains for the concurrence of a mixed two-qubit state ρ,

$$C(\rho) = \max(0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4), \qquad (2.40)$$

where λ_1 to λ_4 denote, in decreasing order, the real eigenvalues of the operator $\sqrt{\sqrt{\rho}\tilde{\rho}\sqrt{\rho}}$.

The value of the concurrence is between 0 and 1. It assigns 0 to separable states and 1 to the maximally entangled state $|\Phi^+\rangle := \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and all states that are equivalent to $|\Phi^+\rangle$ under local unitary transformations, i.e., the Bell states

$$|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), \qquad (2.41)$$

$$|\Psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle). \qquad (2.42)$$

There are several ways to generalize the concurrence to more than two parties. In this thesis, we will make use of one such generalization, called n-concurrence [29]. It is defined completely analogous to the two-qubit case:

Definition 2.7. The *n-concurrence* C_n of an n-qubit state $|\psi\rangle$ where n is even, is given by

$$C_n(|\psi\rangle) := |\langle\psi|\tilde{\psi}\rangle|. \tag{2.43}$$

For mixed states, C_n is given by the convex roof construction in Eq. (2.33).

Note that this definition makes sense only for an even number of qubits, as otherwise $C_n(\rho) = 0$ for all states as discussed above. The n-concurrence assigns 0 to fully separable states, but not necessarily to biseparable ones. Furthermore, it assigns maximal entanglement to many different states, including the n-partite GHZ state, defined as

$$|\mathrm{GHZ}_n\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes n} + |1\rangle^{\otimes n}), \tag{2.44}$$

with $|\mathrm{GHZ}_2\rangle = |\Phi^+\rangle$.

2.5.4 Monogamy of entanglement

As mentioned before, the positivity constraint on quantum states gives rise to some intrinsic limitations to quantum correlations in multipartite systems. One such constraint is known as monogamy of entanglement, as it limits the amount of shared entanglement between one of the parties and the rest.

The first occurrence of these kinds of constraints was found by Coffman, Kundu and Wootters in Ref. [34]. They showed that for a pure three-qubit state $|\psi\rangle_{ABC}$, the squared concurrence of the two-body marginals fulfill

$$C^2(\rho_{AB}) + C^2(\rho_{AC}) \leq C^2(\rho_{A(BC)}). \tag{2.45}$$

Here, $C^2(\rho)$ denotes the square of the concurrence given by Eq. (2.40), and $C^2(\rho_{A(BC)})$ denotes the squared concurrence of the state if parties B and C are treated as a single ququart system. As we have no definition for the concurrence for such systems, we use the fact that the reduced state ρ_{BC} has at most rank 2, if the tripartite state is pure. This follows immediately from the Schmidt decomposition of the state in Eq. (2.25) for a cut between party A and parties BC. Thus, we can treat the combined system BC as an effective qubit state.

Eq. (2.45) can be interpreted as follows: As $C^2(\rho_{A(BC)}) \leq 1$, the entanglement that is shared between parties A and B, and the entanglement shared between A and C,

cannot be arbitrarily large, but is mutually exclusive. For instance, if A and B share a Bell state with $C^2(\rho_{AB}) = 1$, then A and C must be completely unentangled with $C^2(\rho_{AC}) = 0$.

This result was later generalized by Osborne and Verstraete to more than three parties [35], and since then many similar inequalities involving different entanglement quantifiers have been found [36–41]. More generally, it was shown that among correlation measures, apart from some special cases, only entanglement measures can be strictly monogamous [42].

Apart from their philosophical relevance, monogamy relations are also useful in the context of privacy proofs for quantum key distribution protocols. For example, the security of the Ekert protocol is based on the fact that each eavesdropper that is correlated to the communicating parties would reduce the entanglement between their shared states [43].

2.5.5 Witnesses

The evaluation of entanglement measures for mixed states can be very costly, for example, if the measure is constructed using the convex roof method and/or cannot be performed analytically. Additionally, many measures require full knowledge of the quantum state, which is an unrealistic scenario. This motivates the definition of entanglement witnesses, which correspond observables with the following properties [26]:

Definition 2.8. An entanglement witness is an observable W with

- $\text{Tr}(W\rho) \geq 0$ for all separable states ρ,

- $\text{Tr}(W\rho) < 0$ for at least one entangled state ρ.

Here, the notion separable stands for any kind of separability if ρ is multipartite, i.e., it can be fully separable, biseparable, etc.

The idea of entanglement witnesses is the following: The set of separable states forms a proper convex subset of the set of all states. The trace function defines an inner product on this space, known as the Hilbert-Schmidt inner product, defined via $(A, B)_{\text{HS}} := \text{Tr}(AB^{\dagger})$ for two operators A and B. Thus, the condition $\text{Tr}(W\rho) = c$ defines a hyperplane of constant overlap c between W and C. This is visualized in Fig. 2.1 by the dotted line. A witness corresponds to an operator such that the hyperplane $\text{Tr}(W\rho) = 0$ separates the set of separable states from at least one entangled

state. This means, that the separable subset is located on one side of the hyperplane (corresponding to $\text{Tr}(W\rho) \geq 0$), and that there is at least one state on the other side (with $\text{Tr}(W\rho) < 0$). States with negative expectation value must then be entangled and are called *detectable* by W.

Of course, we cannot expect a single witness to detect all entangled states. Nevertheless, as the set of separable states is convex and closed, for each entangled state ρ there exists an entanglement witness detecting it [44].

Sometimes, an existing witness can be improved by shifting and rotating it, such that it detects more entangled states than before. For example, one could improve the witness W_1 displayed in Fig. 2.1 by shifting it to W_2, which touches the set of separable states. Mathematically, this corresponds to subtracting a positive observable A from W_1, such that for all states $\text{Tr}(W_2\rho) = \text{Tr}((W_1 - A)\rho) \leq \text{Tr}(W_1\rho)$. If no such observable A exists, we call W *optimal* [26].

While evaluating the overlap with a witness is usually easy, constructing the witness in the first place is not. A common ansatz in order to create witnesses for non-biseparability is to choose

$$W = g\mathbb{1} - |\psi\rangle\langle\psi|,\tag{2.46}$$

with some pure state $|\psi\rangle$ that is known to be entangled [26]. This ansatz ensures that there always exists an entangled state, namely $|\psi\rangle$, that is detected, as long as $g < 1$. The free parameter g must then be optimized in order to ensure positivity on all separable states. Here, it suffices to optimize over pure product states, as those are the extremal points of the separable set, i.e.,

$$g = \sup_{|\phi_1\rangle, |\phi_2\rangle} |(\langle\phi_1| \otimes \langle\phi_2|)|\psi\rangle|^2.\tag{2.47}$$

The resulting operator in Eq. (2.46) is a witness, provided that $g < 1$.

Note, that there exist many other methods to construct witnesses as well [26].

2.6 Quantum channels

Physical transformations among quantum states play an important role in quantum information processing. These transformation are represented by maps called quantum channels. In principle, they correspond to mappings from the space of operators on the Hilbert space of one system (the incoming state), to the operator space of another system (the outgoing state), subject to certain constraints, ensuring that states

are mapped to states, as well as that they correspond the physical manipulations of the state. We define [7]:

Definition 2.9. A *quantum channel M* is map between operators on the Hilbert space $\mathcal{H}_{\text{in}}$ to operators on the Hilbert space $\mathcal{H}_{\text{out}}$, s.t.

- states are mapped to states: $M(\rho) \geq 0$ if $\rho \geq 0$, $\text{Tr}[M(\rho)] = \text{Tr}(\rho) = 1$ and $M(\rho)^\dagger = M(\rho)$,

- M is completely positive: For each d-dimensional extension of the space, the map $M \otimes \mathbb{1}_{d \times d}$ is positive as well.

The second condition in this definition is necessary for the map to be physical: If we apply it to only one part of a multipartite system, we expect the outgoing operator still to be a state.

Another notion we are going to use is that of a *unital* channel. Unital channels map the identity to itself, i.e., $M(\mathbb{1}) = \mathbb{1}$.

An important subclass of quantum channels are *entanglement-breaking channels*. These channels completely unentangle the input state from any possible other state. Incidentally, they correspond exactly to channels which can be realized via measure-and-prepare schemes [45]:

Definition 2.10. A measure-and-prepare (M&P) channel M is a quantum channel that can be written as

$$M(\rho) = \sum_k \text{Tr}(E_k \rho) \rho_k, \tag{2.48}$$

where the E_k form a POVM and the ρ_k are quantum states.

As the name and the definition indicate, these channels can be realised by measuring the input state and preparing the output state according to the measurement result.

The notion of M&P channels, or entanglement breaking channels, is important in order to distinguish good quantum memories from bad ones (see Chapter 8). Ideally, these memories preserve all quantum properties of the input state by storing a quantum state faithfully. M&P channels, however, can be realized storing classical data and they destroy all entanglement of a state.

There are multiple representations of quantum channels. In this thesis, we are going to make use of two of them, the Kraus representation and the Choi-Jamiołkowski isomorphism.

2.6.1 The Kraus representation

A powerful way to describe quantum channels is the Kraus representation. It states that each completely positive map M from Hilbert space $\mathcal{H}_{\text{in}}$ of dimension d_{in} to the Hilbert space $\mathcal{H}_{\text{out}}$ of dimension d_{out} can be written as [46, 47]

$$M(\rho) = \sum_{k=1}^{D} K_k \rho K_k^{\dagger}, \tag{2.49}$$

where $D \leq d_{\text{in}} d_{\text{out}}$ and the K_k are $d_{\text{out}} \times d_{\text{in}}$-dimensional matrices satisfying

$$\sum_{k=1}^{D} K_k^{\dagger} K_k \leq \mathbb{1}. \tag{2.50}$$

The matrices K_k are called Kraus operators and can always be chosen orthogonal, i.e., $\text{Tr}(K_i^{\dagger} K_j) \propto \delta_{ij}$. The minimal D needed in order to represent the channel is called the Kraus rank. If the map is also trace preserving (i.e., it is a quantum channel), then Eq. (2.50) becomes an equality. Unital channels additionally satisfy

$$\sum_{k=1}^{D} K_k K_k^{\dagger} = \mathbb{1}. \tag{2.51}$$

Finally, there is a connection between a measure-and-prepare channel and its Kraus representation: A channel is M&P iff it can be written using Kraus operators of rank one only [45].

2.6.2 The Choi-Jamiołkowski isomorphism

The Choi-Jamiołkowski isomorphism connects quantum channels and quantum states. For a quantum channel M from $\mathcal{H}_{\text{in}}$ to $\mathcal{H}_{\text{out}}$, we define the Choi state living on $\mathcal{H}_{\text{in}} \otimes \mathcal{H}_{\text{out}}$ as [48–50]

$$\eta_M := (\mathbb{1}_{d_{\text{in}}} \otimes M)(|\phi^+\rangle\langle\phi^+|), \tag{2.52}$$

where $|\phi^+\rangle = \frac{1}{\sqrt{d_{\text{in}}}} \sum_{j=0}^{d_{\text{in}}-1} |jj\rangle$ is a maximally entangled state on $\mathcal{H}_{\text{in}} \otimes \mathcal{H}_{\text{in}}$. The channel can be reconstructed from η_M via [46]

$$M(\rho) = d_{\text{in}} \text{Tr}_A[(\rho^{\text{T}} \otimes \mathbb{1}_{d_{\text{out}}})\eta_M]. \tag{2.53}$$

The properties of the channel map to properties of the Choi state in the following way:

- $\text{Tr}[M(\rho)] = 1 \Leftrightarrow \text{Tr}_B(\eta_M) = \mathbb{1}/d_{\text{in}}$,

- M completely positive $\Leftrightarrow \eta_M \geq 0$,

- M is unital $\Leftrightarrow \mathrm{Tr}_A(\eta_M) = \mathbb{1}/d_{\mathrm{in}}$,

- M is M&P $\Leftrightarrow \eta_M$ is separable.

This correspondence is a one-to-one mapping between quantum channels and certain quantum states. The isomorphism is quite powerful, as it allows to study properties of the channel by looking at the properties of quantum states. For example, the complete positivity is a rather abstract property of a channel, whereas in the space of quantum states it corresponds to the usual positivity of a matrix. Furthermore, deciding whether a channel is measure-and-prepare can now be tackled using the tools developed for deciding whether a state is entangled or not.

2.7 Entropy

One of the most important consequences of the adoption of the theory of quantum mechanics is the paradigm shift from theories predicting outcomes of measurements to a theory that predicts only probability distributions of outcomes. As such, quantities describing properties of these distributions become important for understanding the properties of the system. One such quantity is the classical Shannon entropy. For a probability distribution $\{p_i\}$ with $\sum_i p_i = 1$, it is defined as [27]

$$H(\{p_i\}) := -\sum_i p_i \log(p_i), \tag{2.54}$$

where the logarithm is defined w.r.t. base two. The Shannon entropy is closely related to the amount of uncertainty comprised in the distribution. For a probability distribution of n different outcomes, the entropy is maximal for uniform distributions where $p_i = \frac{1}{n}$, with $H = \log(n)$. On the other hand, for a distribution where $p_1 = 1$, $p_j = 0$ for $j > 1$, the entropy vanishes (here and in the following, we set $0\log(0) = 0$ according to the limit $p_j \searrow 0$). Incidentally, the Shannon entropy corresponds roughly to the average number of bits needed to describe the outcome of a random event efficiently: For a uniform distribution, the best strategy is to just encode the outcome, which is a number between 1 and n, as a binary number, for which $\log(n)$ bits are needed. For the distribution with $p_1 = 1$, however, no information is needed to be encoded, as the outcome will always be 1.

2.7.1 The von Neumann entropy

In quantum mechanics, the analogon to the classical probability distribution is the density matrix. One can generalize the definition of the Shannon entropy to the notion of density matrix, yielding the von Neumann entropy S:

$$S_\mathrm{N}(\rho) := -\operatorname{Tr}[\rho \log(\rho)]. \tag{2.55}$$

The von Neumann entropy corresponds to the Shannon entropy of the eigenvalues of ρ.

There is a close connection between entanglement and entropies as quantifiers of uncertainty. This connection becomes apparent, if we consider the example of the maximally entangled two-qubit Bell state $|\Phi^+\rangle$ again. The marginal state of party A of the Bell state is the maximally mixed state $\rho_A = \mathbb{1}/2$. This can be interpreted as all information on the state being embodied in the correlations between the two parties, i.e., being non-local, as the single party information reveals nothing about the global state. This is reflected in the entropy of the reduced state, $S_\mathrm{N}(\rho_A) = \log(2)$, being maximal. For product states, on the other hand, the reduced state is pure and $S_\mathrm{N}(\rho_A) = 0$.

It should come to no surprise that this allows for the definition of an entanglement measure, called *entanglement of formation*, defined for pure bipartite states as

$$E_f(|\psi\rangle) := S_\mathrm{N}[\operatorname{Tr}_B(|\psi\rangle\langle\psi|)], \tag{2.56}$$

and for mixed states via the convex roof construction in Eq. (2.33).

As mentioned before, there is no unique notion of maximal entanglement for more than two partite systems. One such notion, however, is based on the entropy argument given above:

Definition 2.11. A pure n-partite $|\psi\rangle$ is called absolutely maximally entangled, if for each bipartition $A|B$ with $A \subset \{1,\ldots,n\}$, $B = \{1,\ldots,n\} \setminus A$ and $|A| \leq |B|$, the entropy $S_\mathrm{N}[\operatorname{Tr}_B(|\psi\rangle\langle\psi|)]$ is maximal, i.e., $\operatorname{Tr}_B(|\psi\rangle\langle\psi|) \propto \mathbb{1}$.

To decide whether or not these states exist for given n and internal dimension d, is an open problem and subject to ongoing research. For a summary of known results, we refer to [51] and the references therein. A table of known results for different d and n is provided in Ref. [52].

The von Neumann entropy exhibits some additional properties which makes it useful for several tasks [27]:

(Sub-)Additivity $S_\text{N}(\rho_A \otimes \rho_B) = S_\text{N}(\rho_A) + S_\text{N}(\rho_B)$ and $S_\text{N}(\rho_{AB}) \leq S_\text{N}(\rho_A) + S_\text{N}(\rho_B)$.

Triangle inequality $S_\text{N}(\rho_{AB}) \geq |S_\text{N}(\rho_A) - S_\text{N}(\rho_B)|$.

Concavity $S_\text{N}(\sum_i p_i \rho_i) \geq \sum_i p_i S_\text{N}(\rho_i)$.

Strong subadditivity $S_\text{N}(\rho_{ABC}) + S_\text{N}(\rho_B) \leq S_\text{N}(\rho_{AB}) + S_\text{N}(\rho_{BC})$.

These properties have many important consequences, for which we refer to the literature [7, 27]. Here, we will only comment on some inferences of the strong subadditivity property [27]. To that end, we introduce some related quantities.

Definition 2.12. The *conditional entropy* of a composite quantum state ρ_{AB} is given by

$$S_\text{N}(A|B) := S_\text{N}(\rho_{AB}) - S_\text{N}(\rho_B). \tag{2.57}$$

The *mutual information* between systems A and B is given by

$$I_\text{N}(A:B) := S_\text{N}(\rho_A) + S_\text{N}(\rho_B) - S_\text{N}(\rho_{AB}). \tag{2.58}$$

The interpretation of these two quantities is as follows: The conditional entropy quantifies the uncertainty in the joint state ρ_{AB} that is left when the marginal state ρ_B is known. The sum $S_\text{N}(\rho_A) + S_\text{N}(\rho_B)$ contains the information that is bound to A and B twice. Thus, by subtracting this common entropy, the mutual information between A and B amounts to only that contribution.

Using these two quantities, we can formulate the main consequences of the strong subadditivity as follows [27]:

- Knowing more reduces the uncertainty: $S_\text{N}(A|BC) \leq S_\text{N}(A|B)$.

- Loosing a particle reduces mutual information: $I_\text{N}(A:BC) \geq I_\text{N}(A:B)$.

- Local operations reduce mutual information: If $\rho_{A'B'} = (\mathbb{1} \otimes \Lambda)(\rho_{AB})$ for some quantum channel Λ, then $I_\text{N}(A:B) \geq I_\text{N}(A':B')$.

2.7.2 The linear entropy

While the von Neumann entropy satisfies all desired properties for an uncertainty quantifier, it is not the only function doing so. Furthermore, it might be hard to evaluate, as it requires diagonalization of the corresponding density matrix. Therefore, computationally easier but similar quantities are considered as well. One such choice

is the linear entropy: It is obtained by expanding the logarithm in the definition of the von Neumann entropy around pure states and taking just the leading contribution into account:

Definition 2.13. The *linear entropy* of a quantum state ρ is defined as

$$S_{\mathrm{L}}(\rho) = 2[1 - \mathrm{Tr}(\rho^2)]. \tag{2.59}$$

Like the von Neumann entropy, the linear entropy vanishes for pure states and takes its maximal value for completely mixed states, where it reaches $S_{\mathrm{L}}(\mathbb{1}/d) = 2\frac{d-1}{d}$. The linear entropy shares many properties with the von Neumann entropy while being easier to compute. However, it does not obey the strong subadditivity, a counterexample is given by the three-qubit state $\rho_{ABC} = \mathbb{1}/2 \otimes |\Phi^+\rangle\langle\Phi^+|$.

An interesting connection exists between the linear entropy and the sector lengths introduced in Eq. (2.18). As the linear entropy is defined via the purity of the state, it can be expressed as a linear combination of sector lengths. Furthermore, one can find a one-to-one correspondence between the sector lengths A_k, and the linear entropies of the marginals of the state. This connection is explored in detail in Chapter 5.

2.8 Coherence

We already introduced entanglement as one of the main non-classical features of quantum mechanics. Another major distinction between classical and quantum physics is called coherence. In contrast to entanglement, coherence is also a local feature as it describes the amount of superposition w.r.t. a given (classical) basis present in a quantum state. For example, a single-qubit realized by the spin of an electron can be in state $|0\rangle$ (spin up) or $|1\rangle$ (spin down), but also in any linear combination, called superposition, of these two. Coherence plays an important role in many areas of quantum information, including quantum metrology and quantum communication [53]. In contrast to entanglement, coherence depends on the choice of local basis.

2.8.1 Coherence measures

There are several ways to quantify coherence, each of which should satisfy some natural assumptions for such a quantifier [54]: First of all, it should assign a value of zero to incoherent basis states, as well as to their classical mixtures, i.e., the set of all diagonal density matrices. This convex (and basis dependent) set is denoted by $\mathcal{I}$.

Second, it should not increase under certain incoherent channels, which map incoherent states to incoherent states. These are channels, where the Kraus operators satisfy $K_k \mathcal{I} K_k^\dagger \subset \mathcal{I}$. There are two types of such operations: Apart from the usual channel given by $M(\rho) = \sum_k K_k \rho K_k^\dagger$, one can also allow for selective operations, which retain measurement results for the POVM $\{K_k^\dagger K_k\}$ formed from the Kraus operators. In this case, one obtains the post-measurement state $\rho_k = K_k \rho K_k^\dagger / p_k(M)$ with probability $p_k(M) = \text{Tr}(K_k^\dagger K_k \rho)$. In sum, this leads to two conditions for a coherence quantifier C: $C(\rho) \geq C(M(\rho))$ and $C(\rho) \geq \sum_k p_k(M) C[\rho_k(M)]$, meaning that C should not increase on average for all incoherent channels M.

Finally, C should be convex, i.e., $C(\sum_k p_k \rho_k) \leq \sum_k p_k C(\rho_k)$.

Any quantity satisfying these criteria is called a *coherence measure*. The abstract criteria are not concerned with a notion of maximally coherent state. Intuitively, these should be given by equal superpositions of the basis states with relative phases, i.e.,

$$|\psi^{\vec{\alpha}}\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} e^{i\alpha_j} |j\rangle \tag{2.60}$$

where $\vec{\alpha} = (\alpha_0, \alpha_1, \ldots, \alpha_{d-1})$ is a vector of local phases. Indeed, one can show that each coherence measure is maximized by this set of states [55]. However, some coherence measures assign this maximal value also to other states, which, depending on the application, might be disfavored. That is why it is sometimes required that any valid coherence measure is maximized only by the states in Eq. (2.60) [55]. Indeed, most of the commonly used coherence measures, including the ones we illuminate in the following, fulfill this additional property.

2.8.2 The l_1-norm of coherence and robustness of coherence

Probably the easiest quantifier obeying the properties for coherence measures is the l_1-norm of coherence:

Definition 2.14. The l_1-*norm of coherence* of a quantum state ρ is given by

$$C_{l_1}(\rho) := \sum_{i \neq j} |\rho_{ij}|. \tag{2.61}$$

Intuitively, it quantifies the size of all off-diagonal entries of the density matrix.

While this measure is easy to compute, it lacks a direct physical interpretation. This is why we introduce another measure, called robustness of coherence [56]:
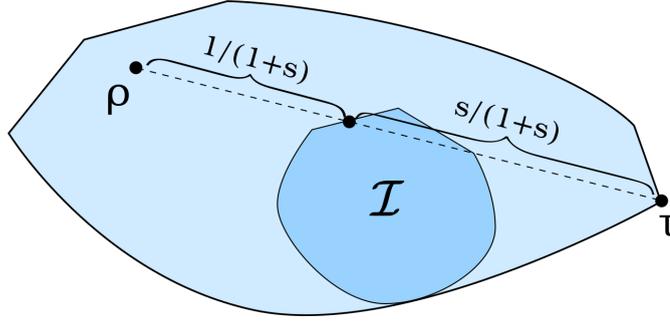
FIGURE 2.2: A visualization of the convex set of incoherent states $\mathcal{I}$ as a subset of all quantum states, and the optimal linear combination of a state ρ and τ from the definition of the robustness of coherence in Eq. (2.62). The optimization minimizes the distance from ρ to the incoherent set $\mathcal{I}$ along a straight line to a quantum state τ relative to the distance between ρ and τ.

Definition 2.15. The *robustness of coherence* of a quantum state ρ is defined as

$$C_R(\rho) := \min_{\tau \in \mathcal{D}, s \geq 0} \left\{ s \,\Big|\, \frac{\rho + s\tau}{1+s} \in \mathcal{I} \right\}, \tag{2.62}$$

where $\mathcal{D}$ denotes the set of density matrices.

The robustness of coherence quantifies the distance of the state ρ from the convex set $\mathcal{I}$. This is visualized in Fig. 2.2.

Both quantifiers, the l_1-norm of coherence and the robustness, take values between 0 and $d-1$ where d is the dimension of the system.

In contrast to the l_1-norm of coherence, the robustness has a direct operational interpretation in a phase discrimination task as follows [56]: Suppose that an initial state ρ undergoes a unitary evolution w.r.t. $U_\phi = \sum_{j=0}^{d-1} e^{ij\phi} |j\rangle\langle j|$, such that the output state is given by $\rho' = U_\phi \rho U_\phi^\dagger$. The phase ϕ is chosen at random from a set $\{\phi_k\}$ with probabilities $\{p_k\}$. The task is now to prepare an input state ρ and perform a POVM measurement $\{E_k\}$ on the output in order to determine the randomly chosen phase from the output. The success probability for this task depends on the specific instance (i.e., the chosen set of phases and probabilities), but also on the input state ρ and the chosen measurement. The latter should be chosen such that the success probability $p^\star(\{\phi_k, p_k\})$ is maximal, i.e.,

$$p^\star_{\{\phi_k, p_k\}}(\rho) = \max_{\{E_k\}} \sum_k p_k \operatorname{Tr}(\rho' E_k) \tag{2.63}$$

The question remains which input states are useful for this task. Incoherent input states, i.e., diagonal states, are commuting with the diagonal unitary rotation. Therefore, no reminiscence of the phase is encoded into them, and no measurement can

reveal any information about the phase. In this case, the best guess is the phase that is chosen with the highest probability, $p^{\star}_{\{\phi_k,p_k\}}(\mathcal{I}) = \max_k p_k$.

Indeed, choosing a coherent input state instead yields better success probabilities. One can show that the maximal success probability for a fixed input state ρ when optimizing the game instances $\{\phi_k, p_k\}$ and the measurements $\{E_k\}$, is given by [56]

$$p_{\max}(\rho) \equiv \max_{\{\phi_k,p_k\}} \frac{p^{\star}_{\{\phi_k,p_k\}}(\rho)}{p^{\star}_{\{\phi_k,p_k\}}(\mathcal{I})} = 1 + C_{\mathrm{R}}(\rho). \tag{2.64}$$

In other words, the achievable relative advantage over choosing just the phase with the highest probability, is given by the robustness of coherence of the input state.

2.9 Semidefinite programs

Many problems in the context of quantum information and entanglement detection can be formulated as optimization problems involving linear and semidefinite constraints. Such optimization tasks are called semidefinite programs (SDPs) and received a lot of attention in mathematical optimization theory [57, 58] (for a comprehensive overview, see also Ref. [59] and the references given therein). In its most basic form, an SDP can be written as [60]

$$
\begin{aligned}
\min_{X} \quad & \mathrm{Tr}(CX) & \text{(2.65)} \\
\text{subject to} \quad & \mathrm{Tr}(A_i X) = b_i \quad \text{for } i = 1, \dots, m, \\
& X \geq 0,
\end{aligned}
$$

where the optimization is performed over positive semidefinite symmetric (or hermitian) $n \times n$-matrices X. Due to the restriction to the semidefinite domain, these optimizations form a larger class than linear programs. However, SDPs can still be efficiently numerically optimized using interior point methods [59].

What makes SDPs so prominent in quantum information is the fact that sometimes the optimality of a found solution can be proven (within machine precision), and, if there is no feasible solution at all, its absence can be shown. To that end, we introduce

the dual form of the SDP (2.65) as

$$\max_{y,S} \quad \sum_{i=1}^{m} y_i b_i \tag{2.66}$$

$$\text{subject to} \quad \sum_{i=1}^{m} y_i A_i + S = C,$$

$$S \geq 0.$$

Consequently, we call (2.65) the primal of the SDP. The power of switching to the dual representation is revealed by the so-called weak duality [60]:

Theorem 2.16. *If the primal and the dual of an SDP are feasible (i.e., there exists a solution satisfying the constraints) with solutions X and (y, S), respectively, then*

$$\text{Tr}(CX) - \sum_{i=1}^{m} y_i b_i = \text{Tr}(SX) \geq 0. \tag{2.67}$$

If equality holds, then X and (y, S) are optimal solutions.

The proof of the theorem is straight-forward and can be found, for example, in Ref. [61].

The left-hand side of Eq.(2.67) is called duality gap. The theorem shows that if one finds solutions to the primal and the dual problem such that the duality gap vanishes, then the found solutions are optimal.

A priori, there is no guarantee that a given SDP converges to the optimal value. However, there is a range of sufficient conditions for the convergence. The most prominent one is Slater's condition, stating that the optimal value is reached if there are feasible points in the interior of the optimization region [60, 62]:

Theorem 2.17. *If there exist feasible solutions X and (y, S) of the primal and the dual of an SDP such that $X > 0$ and $S > 0$, then the primal and the dual attain their optimal values.*

As an example, we consider the problem of creating an entanglement witness for a given bipartite state $|\psi\rangle$. As noted in Section 2.5, a good ansatz for such a witness is given by

$$W = g\mathbb{1} - |\psi\rangle\langle\psi|, \tag{2.68}$$

with

$$g = \sup_{|\phi_1\rangle, |\phi_2\rangle} |(\langle\phi_1| \otimes \langle\phi_2|)|\psi\rangle|^2 \tag{2.69}$$

$$= \sup_{\rho_1, \rho_2} \text{Tr}(\rho_1 \otimes \rho_2 |\psi\rangle\langle\psi|). \tag{2.70}$$

The optimization can be approximated by an SDP. While it is not possible to enforce the tensor product structure, as this is a quadratic constraint, it is possible to optimize over the slightly larger set of PPT states:

$$\max_{\sigma} \quad \mathrm{Tr}(\sigma |\psi\rangle\langle\psi|) \tag{2.71}$$
$$\text{subject to} \quad \sigma \geq 0,$$
$$\mathrm{Tr}(\sigma) = 1,$$
$$\sigma^{T_B} \geq 0.$$

An optimal value of less than unity yields a suitable value for g in Eq. (2.69).

Another example is that of symmetric extensions [63–65]. For any bipartite separable state,

$$\rho_{AB} = \sum_{i=1}^{k} p_i |a_i\rangle\langle a_i| \otimes |b_i\rangle\langle b_i|, \tag{2.72}$$

one can define the symmetric extension of order m as

$$\rho_{ABA_1\ldots A_m} = \sum_{i=1}^{k} p_i |a_i\rangle\langle a_i| \otimes |b_i\rangle\langle b_i| \otimes |a_i\rangle\langle a_i| \otimes \ldots \otimes |a_i\rangle\langle a_i|. \tag{2.73}$$

This extension fulfills the following properties:

- $\mathrm{Tr}_{A_1\ldots A_m}(\rho_{ABA_1\ldots A_m}) = \rho_{AB}$,

- $\rho_{ABA_1\ldots A_m}$ is symmetric under exchange of any of the systems $A, A_1, \ldots, A_m$,

- $\rho_{ABA_1\ldots A_m}^{T_S} \geq 0$ for every $S \subset \{A, B, A_1, \ldots, A_m\}$.

The existence of a symmetric extension of order m is only guaranteed for separable states, and it can be shown that for each entangled state there exists an order m_0 such that a symmetric extension of order larger or equal to m_0 does not exist [63, 65]. Whether or not a symmetric extension of fixed order exists can be formulated in terms of an SDP. As noted above, the non-existence of a feasible solution can be certified in many cases, yielding a numerical tool that is capable of proving that a given state is entangled.

3 The marginal problem

Prerequisites

3.1 Introduction

The quantum marginal problem is, as noted in Section 2.4, concerned with the following two problems:

Is a global quantum state uniquely determined by a set of its marginal states? And, given a set of marginal states, are they compatible, i.e., does there exist a global state exhibiting these marginals?

We already introduced a mathematical language suited for tackling these questions and listed known results about the problem. Before we continue with our results on how to extend these results for four- and more qudit systems, we motivate the marginal problem physically by listing applications in the context of ground states of local Hamiltonians and quantum chemistry. We then look in detail at the connection between uniquely determined states and ground states. Consequently, we investigate in detail the four-particle case, for which we show that certain subsets of the two-body marginals almost always suffice to determine a state among pure states.

Finally, we generalize the results to more particles and list some exceptional states that are not determined. We conclude with a discussion.

3.2 Motivation

The aforementioned uniqueness question is highly relevant for the characterization of the ground state space of local Hamiltonians. A *k*-local Hamiltonian is a hermitian

operator H which can be written as

$$H = \sum_{\substack{S \subset \{1,\dots,n\}, \\ |S| \leq k}} h_S, \tag{3.1}$$

where each h_S acts nontrivially only on the parties in S. As most interactions in quantum systems are limited in range, many relevant Hamiltonians are of this form for small k. It is of fundamental interest to decide whether such a Hamiltonian has a unique ground state. For example, a strategy to prepare certain quantum states is given by constructing a Hamiltonian with the target state as ground state. This procedure can only be successful if the target state is the non-degenerate ground state of the Hamiltonian. In other scenarios, one tries to steer the ground state of an initial system to the ground state of a final system by adiabatically changing the Hamiltonian. A criterion for success for such transformations is given by the adiabatic theorem of quantum mechanics, requiring that at each fixed time there is a finite energy gap between the ground state and the first excited state [66, 67]. A necessary criterion for this is that the time evolved Hamiltonian has non-degenerate ground state at each time step.

Non-degeneracy of ground states of k-local Hamiltonians is closely related to the before-mentioned uniqueness problem: Given the ground state ρ_0 of a k-local Hamiltonian H, its energy is given by

$$E_0 = \mathrm{Tr}(H\rho_0) = \sum_{\substack{S \subset \{1,\dots,n\}, \\ |S| \leq k}} \mathrm{Tr}(\rho_{0,S} h_S). \tag{3.2}$$

It is therefore a function of the k-body marginals of ρ_0 only. Thus, if ρ_0 the unique ground state of H then there must not exist any other state with the same k-body marginals [68, 69]. This we denote as ρ_0 being k-uniquely determined among all states. We will highlight the connection between unique ground states and uniquely determined states in more detail in Section 3.3.

A second motivation comes from quantum chemistry [18]. There, many relevant properties of fermionic quantum states can be calculated from two-point functions, derived from the two-body marginal of the global fermionic quantum state. It is therefore of fundamental interest to decide whether given two-point data can originate from a global n-partite state or not [19]. This is known as the n-representability problem. Also in non-fermionic systems, the compatibility problem has been investigated [14, 18, 20, 21].

Finally, the marginal problem is connected to the phenomenon of entanglement. As we will see below, pure states of two parties are determined by their one-body marginals only if the state is a product state. Consequently, entangled states can contain correlations among many parties that are lost when having access to the marginals only. This connection between the properties of the parts and the global quantum state has been subject to many previous works [70–73].

3.3 Unique ground states and uniquely determined states

Recall from Section 2.4 that we call a state k-UDP (uniquely determined among pure states) if there is no other pure state exhibiting the same k-body marginals, and k-UDA (uniquely determined among all states) if there is no other compatible pure or mixed state.

It is illustrative to explore the connection between ground states of local Hamiltonians and uniquely determined states in more detail. As mentioned in the motivation section, every unique ground state of a k-local Hamiltonian must be k-UDA. The converse, however, is not true, and an explicit counterexample of a six-qubit state being 2-UDA, but not a ground state of a 2-local Hamiltonian was found recently [11].

The reason for this discrepancy has geometric origins: Let $\mathcal{O}$ denote the set of $d^n \times d^n$ hermitian matrices and $\mathcal{B} \subset \mathcal{O}$ the subset of density matrices. Using the Bloch representation in Eq. (2.17), we define $\mathcal{P}_k$ to be the projector to the subspace of $\mathcal{O}$ having up to k-partite correlations only. In the case of qubits, this subspace is spanned by the multipartite Pauli matrices of weight equal to or less than k.

In the projected space, the k-UDA states are extremal points of the subset $P_k(\mathcal{B})$:

Lemma 3.1. *Let $|\psi\rangle$ be a state that is k-UDA. Then $\mathcal{P}_k(|\psi\rangle\langle\psi|)$ is an extremal point in $\mathcal{P}_k(\mathcal{B})$.*

Proof. Assume that $\mathcal{P}_k(|\psi\rangle\langle\psi|)$ was not an extremal point. Then it could be written as

$$\mathcal{P}_k(|\psi\rangle\langle\psi|) = p\mathcal{P}_k(\rho_1) + (1-p)\mathcal{P}_k(\rho_2), \tag{3.3}$$

where ρ_1 and ρ_2 are states in $\mathcal{B}$. As $|\psi\rangle$ is k-UDA, the inverse image is unique and $p\rho_1 + (1-p)\rho_2$ is a valid decomposition of $|\psi\rangle\langle\psi|$ in $\mathcal{B}$. But $|\psi\rangle\langle\psi|$ is a pure state and therefore $\rho_1 = \rho_2 = |\psi\rangle\langle\psi|$. $\square$

Now consider a k-local Hamiltonian H, i.e., it lives in $\mathcal{P}_k(\mathcal{O})$. As $\text{Tr}(\rho H)$ yields the energy of ρ, as well as the Hilbert-Schmidt distance, states with fixed energy E lie on a
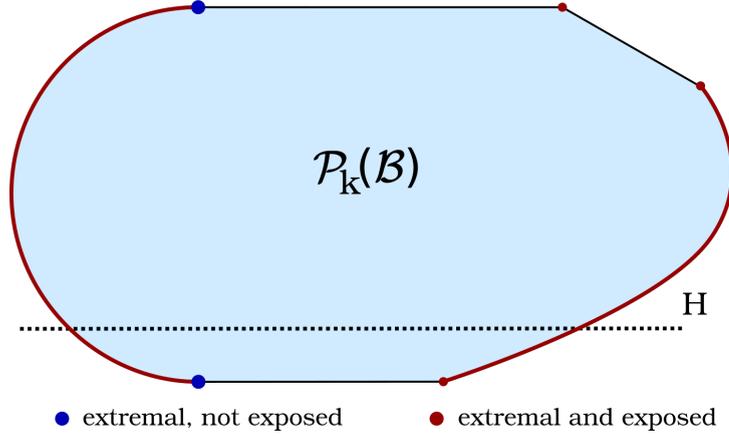
FIGURE 3.1: The space of all n-partite density matrices projected onto the reduced space of k-partite and lower correlations only. The extremal and exposed points of the convex set are displayed in dark red, whereas the two extremal but not exposed points are displayed in dark blue. These two points cannot be expressed as unique ground states of k-local Hamiltonians, as every Hamiltonian H with a non-exposed ground state is at least two-fold degenerate.

hyperplane in $\mathcal{P}_k(\mathcal{B})$. States with different energy lie on hyperplanes that are moved in parallel. For ρ to be the unique ground state of H, it needs to be the only state minimizing $\mathrm{Tr}(\rho H)$. Such states are called exposed [74]. Every exposed point is also an extremal point, but not every extremal point is exposed. This scenario is displayed in Fig. 3.1, where a convex set with two non-exposed extremal points is shown. This implies that there might be non-exposed k-UDA states, which can never be unique ground states of k-local Hamiltonians.

It can be shown, however, that the set of exceptions is quite small. Indeed, the set of non-exposed extremal points is of measure zero in the set of all extremal points [74].

The fact that the set of counterexamples is quite small can also be seen in the language of semidefinite programming, introduced in Section 2.9. To that end, we denote the set of states which are unique ground states of k-local Hamiltonians as k-UGS, and, by slight abuse of notation, the set of k-UDA states simply by k-UDA. Then we have that their closures coincide:

Theorem 3.2. $\overline{k\text{-}UGS} = \overline{k\text{-}UDA}.$

Proof. Deciding whether a fixed state $|\phi\rangle$ is k-UDA can be cast in terms of the SDP

$$\min_{\sigma} \quad \mathrm{Tr}(\sigma|\phi\rangle\langle\phi|) \tag{3.4}$$

$$\text{subject to} \quad \sigma \geq 0,$$

$$\mathcal{P}_k(\sigma) = \mathcal{P}_k(|\phi\rangle\langle\phi|),$$

the dual problem of which is given by [11]

$$\max_{H} \quad \mathrm{Tr}(H|\phi\rangle\langle\phi|) \tag{3.5}$$

$$\text{subject to} \quad H + |\phi\rangle\langle\phi| \geq 0,,$$

$$\mathcal{P}_k(H) = H,$$

$$H = H^{\dagger}.$$

Let α and β denote the optimal values of the primal and the dual problem, respectively. Strong duality holds due to Slater's condition from Theorem 2.17, thus $\alpha = \beta$. The pure state $|\phi\rangle\langle\phi|$ is k-UDA iff $\alpha = 1$. Thus, in this case also $\beta = 1$ and in principle, the optimal H of the dual problem would be a Hamiltonian with $|\phi\rangle$ being its unique ground state and having the right marginals. However, the dual optimization is unbounded and the actual optimal H might be unbounded, too, and therefore never reachable, leading to counterexamples to the UDA = UGS conjecture. Nevertheless, we will show that each k-UDA state can be approximated arbitrarily well by k-UGS states.

Strong duality implies that there is a sequence of Hamiltonians H_n with

$$f_n := -\mathrm{Tr}(H_n|\phi\rangle\langle\phi|) \overset{n\to\infty}{\longrightarrow} 1 \tag{3.6}$$

and w.l.o.g. we assume $f_n > 0$ (otherwise, we truncate the first sequence elements that violate this condition). We now show that the ground states $|\phi_n\rangle$ of the H_n are non-degenerate and have a finite gap, from which we conclude that the sequence of ground states $|\phi_n\rangle$ approximates $|\phi\rangle$.

To that end, assume that the ground state space of H_n was degenerate. Then there exists a state $|\psi_n\rangle$ in the ground state space that is perpendicular to $|\phi\rangle$ and has energy

$$-e_n := \langle\psi_n|H|\psi_n\rangle \leq -f_n < 0, \tag{3.7}$$

as $|\phi\rangle$ cannot have less energy than the ground state. However, condition (3.6) implies

$$-e_n = \langle\psi_n|(H + |\phi\rangle\langle\phi|)|\psi_n\rangle \overset{!}{\geq} 0, \tag{3.8}$$

which is in violation with Eq. (3.7). Thus, all H_n have a non-degenerate ground state. From this argument also follows that $|\phi_n\rangle$ is the only eigenstate of H_n having a negative expectation value, because otherwise a suitable linear combination of the negative

energy state and the ground state would be perpendicular to $|\phi\rangle$, leading to the same contradiction. Thus, the energy gap of H_n is finite.

Finally, this implies again by Eq. (3.6),

$$\langle \phi_n | (H_n + |\phi\rangle\langle\phi|) | \phi_n \rangle = -e_n + |\langle\phi|\phi_n\rangle|^2 \geq 0, \tag{3.9}$$

thus

$$1 \geq |\langle\phi|\phi_n\rangle|^2 \geq e_n \geq f_n \longrightarrow 1. \tag{3.10}$$

Therefore, the sequence $|\phi_n\rangle$ of unique ground states of quasi-local Hamiltonians approximates $|\phi\rangle$ and therefore $\overline{k\text{-UGS}} = \overline{k\text{-UDA}}$. $\qquad\square$

3.4 The four particle case

In the remainder of this chapter, we investigate the case of four-particle states having equal internal dimensions. As mentioned before, unique ground states of k-local Hamiltonians must be k-UDA. As many relevant interaction Hamiltonians are two-local, this case is of particular interest. It is known that most three-particle states are 2-UDA [22, 24], while most five-particle states are not [69]. Thus, the only open case is that of four particles.

We make an important step towards solving this case by showing that generic pure states of four particles are 2-UDP by certain sets of their two-body marginals. To that end, we begin by defining precisely what we mean by generic states. We then prove our main result, first for the case of qubits and subsequently for the general case of qudits. The theorem is then generalized to generic n-particle states, which can be shown to be determined in a similar way by certain sets of three of their $(n-2)$-body marginals. Finally, we list some specific examples for the exceptional case of states of four particles that are not determined by their two-body marginals.

3.4.1 Generic states

Generic states are understood to be states drawn randomly according to the Haar measure. Here, we adopt a special procedure to obtain such random states in a Schmidt decomposed form. To that end, consider a four-particle pure state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C \otimes \mathcal{H}_D$, where $\dim \mathcal{H}_A = \dim \mathcal{H}_B = \ldots = d$. Using the Schmidt decomposition from Eq. (2.25) along the bipartition $(AB|CD)$, the state can be written
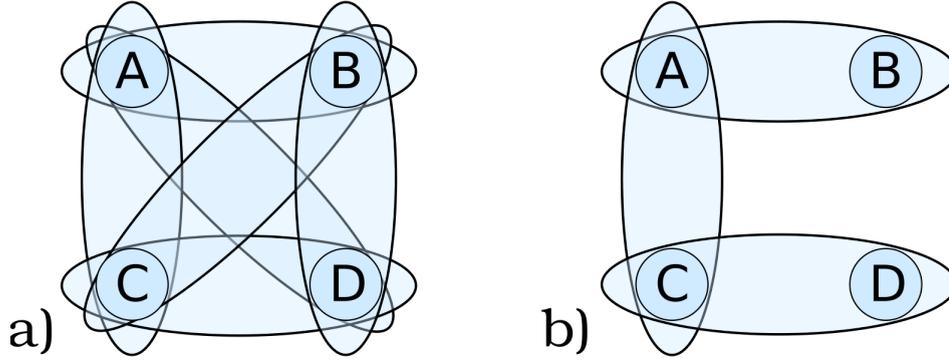
FIGURE 3.2: Illustration of two different sets of two-body marginals: a) the set of all six two-body marginals, b) a set of three two-body marginals that is shown to suffice to uniquely determine generic pure states.

as

$$|\psi\rangle = \sum_{i=1}^{d^2} \sqrt{\lambda_i} |i\rangle_{AB} \otimes |i\rangle_{CD},\qquad(3.11)$$

where $\sum_i \lambda_i = 1$. If the state has full Schmidt rank, i.e., $\lambda_i \neq 0$ for all i, then the sets $|i\rangle_{AB}$ and $|i\rangle_{CD}$ form orthonormal bases in the composite Hilbert spaces $\mathcal{H}_A \otimes \mathcal{H}_B$ and $\mathcal{H}_C \otimes \mathcal{H}_D$, respectively.

Definition 3.3. A *generic* four-particle pure state is a state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C \otimes \mathcal{H}_D$ drawn randomly according to the Haar measure. Writing such state as in Eq. (3.11), the Schmidt bases and the set of Schmidt coefficients are independent from each other. The distribution of the Schmidt coefficients is given by [75, 76]

$$P(\lambda_1,\ldots,\lambda_4)\mathrm{d}\lambda_1\ldots\mathrm{d}\lambda_4 = N\delta\left(1 - \sum_{i=1}^{4}\lambda_i\right)\prod_{1\leq i<j\leq 4}(\lambda_i - \lambda_j)^2\mathrm{d}\lambda_1\ldots\mathrm{d}\lambda_4 \qquad(3.12)$$

and the Schmidt bases are distributed according to the Haar measure of unitary operators on the smaller Hilbert spaces.

The mutual independence of the two Schmidt bases and the coefficients can be seen from the fact that in the Haar measure, for the probability distribution $p(|\psi\rangle)$ to obtain state $|\psi\rangle$ holds $p(|\psi\rangle) = p(\mathbb{1}_{AB} \otimes U_{CD}|\psi\rangle) = p(U_{AB} \otimes \mathbb{1}_{CD}|\psi\rangle)$.

Generic states as defined above exhibit two other important properties: They have full Schmidt rank and pairwise distinct Schmidt coefficients. We would like to add that while the definition above makes use of the Haar measure, we do not explicitly require it. Any measure with the same independence properties between the two Schmidt bases and Schmidt coefficients would work as well, as long as the sets of states having non-full Schmidt rank or degenerate Schmidt coefficients are also of measure zero.

3.4.2 The case of qubits

To begin with, we investigate the qubit case, where $d = 2$. Let $|\psi\rangle = \sum_{i=1}^{4} \sqrt{\lambda_i}|i\rangle_{AB} \otimes |i\rangle_{CD}$ be a generic state in the sense defined above. The two-body marginal of parties A and B is given by

$$\rho_{AB} = \text{Tr}_{CD}(|\psi\rangle\langle\psi|) = \sum_{i=1}^{4} \lambda_i |i\rangle\langle i|_{AB} \tag{3.13}$$

and similarly for CD. This is the starting point for the proof of the following theorem.

Theorem 3.4. *Almost all four-qubit pure states are uniquely determined among pure states by the three two-body marginals ρ_{AB}, ρ_{CD} and ρ_{BD}. In particular, this implies that they are 2-UDP.*

Proof. Let $|\psi\rangle$ be a generic state in the Schmidt decomposed form in Eq. (3.11). We arrange the Schmidt bases such that the Schmidt coefficients are in decreasing order, i.e. $\lambda_i \geq \lambda_{i+1}$. Suppose that there is another pure state $|\phi\rangle$ which exhibits the same two-body marginals ρ_{AB} and ρ_{CD} as $|\psi\rangle$. As the λ_i are pairwise distinct and in decreasing order, the Schmidt bases of $|\phi\rangle$ and $|\psi\rangle$ have to coincide up to a phase. Thus, $|\phi\rangle$ must be of the form

$$|\phi\rangle = \sum_{i=1}^{4} e^{i\varphi_i}\sqrt{\lambda_i}|i\rangle_{AB} \otimes |i\rangle_{CD}. \tag{3.14}$$

Therefore, the only degrees of freedom left of $|\phi\rangle$ are the four phases φ_i.

We now demand that also the marginals of parties B and D coincide, in other words, $\text{Tr}_{AC}(|\psi\rangle\langle\psi|) = \text{Tr}_{AC}(|\phi\rangle\langle\phi|)$ (but any other marginal would be fine, too):

$$\begin{aligned}\rho_{BD} &= \sum_{i,j=1}^{4}\sqrt{\lambda_i\lambda_j}\,\text{Tr}_{AC}(|i\rangle\langle j|_{AB} \otimes |i\rangle\langle j|_{CD}) \\ &\overset{!}{=} \sum_{i,j=1}^{4}e^{i(\varphi_i-\varphi_j)}\sqrt{\lambda_i\lambda_j}\,\text{Tr}_{AC}(|i\rangle\langle j|_{AB} \otimes |i\rangle\langle j|_{CD}).\end{aligned} \tag{3.15}$$

The sum runs over operators on the space of parties B and D. For every pair i, j, this operator is given by

$$O_{ij} = \text{Tr}_{AC}(|i\rangle\langle j|_{AB} \otimes |i\rangle\langle j|_{CD}). \tag{3.16}$$

The 16 operators O_{ij} span a subspace in the 16-dimensional space of operators on $\mathcal{H}_B \otimes \mathcal{H}_D$. As we will see later, this subspace is only 13-dimensional, thus the operators must be linearly dependent. Therefore, we cannot simply compare both sides of Eq. (3.15) term by term to conclude that $\varphi_i = \varphi_j$. Instead, let us interpret the 16 operators O_{ij}

as vectors in the 16-dimensional operator space. Thus, we are looking for solutions of the equation

$$\sum_{i,j=1}^{4} (1 - e^{i(\varphi_i - \varphi_j)}) \sqrt{\lambda_i \lambda_j} O_{ij} \equiv \sum_{i,j=1}^{4} \gamma_{ij} O_{ij} = 0_{4\times 4}, \tag{3.17}$$

where

$$\gamma_{ij} := (1 - e^{i(\varphi_i - \varphi_j)}) \sqrt{\lambda_i \lambda_j}. \tag{3.18}$$

These are 16 equations, one for every entry of the resulting 4×4 matrix. We can treat Eq. (3.17) as a system of linear equations for the γ_{ij} and look for solutions that can be written in the specific form in Eq. (3.18). It implies that

$$\gamma_{ii} = 0, \tag{3.19}$$

$$\gamma_{ij} = \bar{\gamma}_{ji}, \tag{3.20}$$

Therefore, there are effectively six undetermined complex-valued variables γ_{ij} for $1 \leq i < j \leq 4$.

Let us now investigate the linear system in Eq. (3.17) in more detail. Note that every O_{ij} can be written as a product

$$O_{ij} = \text{Tr}_A(|i\rangle\langle j|_{AB}) \otimes \text{Tr}_C(|i\rangle\langle j|_{CD}) \equiv Q_{ij} \otimes R_{ij}, \tag{3.21}$$

where $Q_{ij} = \text{Tr}_A(|i\rangle\langle j|_{AB})$, $R_{ij} = \text{Tr}_C(|i\rangle\langle j|_{CD})$. The matrices Q_{ij} and R_{ij} inherit some properties from the underlying orthonormal bases:

$$\text{Tr}(Q_{ij}) = \delta_{ij},$$

$$Q_{ij}^{\dagger} = Q_{ji} \tag{3.22}$$

and similarly for R_{ij}.

Using these properties together with Eqs. (3.19) and (3.20), Eq. (3.17) can be written as

$$\sum_{i<j} \gamma_{ij} Q_{ij} \otimes R_{ij} + \bar{\gamma}_{ij} Q_{ij}^{\dagger} \otimes R_{ij}^{\dagger} \overset{!}{=} 0. \tag{3.23}$$

For $i \neq j$, $\text{Tr}(Q_{ij}) = \text{Tr}(R_{ij}) = 0$ and we can write Q_{ij} and R_{ij} explicitly as

$$Q_{ij} = \begin{pmatrix} q_{ij}^{11} & q_{ij}^{12} \\ q_{ij}^{21} & -q_{ij}^{11} \end{pmatrix}, \tag{3.24}$$

$$R_{ij} = \begin{pmatrix} r_{ij}^{11} & r_{ij}^{12} \\ r_{ij}^{21} & -r_{ij}^{11} \end{pmatrix}. \tag{3.25}$$

Thus,

$$
\begin{aligned}
0 &= \sum_{i<j} \gamma_{ij} Q_{ij} \otimes R_{ij} + \bar{\gamma}_{ij} Q_{ij}^\dagger \otimes R_{ij}^\dagger \\
&= \sum_{i<j} \begin{pmatrix} \gamma_{ij} q_{ij}^{11} R_{ij} + \bar{\gamma}_{ij} \bar{q}_{ij}^{11} R_{ij}^\dagger & \gamma_{ij} q_{ij}^{12} R_{ij} + \bar{\gamma}_{ij} \bar{q}_{ij}^{21} R_{ij}^\dagger \\ \gamma_{ij} q_{ij}^{21} R_{ij} + \bar{\gamma}_{ij} \bar{q}_{ij}^{12} R_{ij}^\dagger & -(\gamma_{ij} q_{ij}^{11} R_{ij} + \bar{\gamma}_{ij} \bar{q}_{ij}^{11} R_{ij}^\dagger) \end{pmatrix} \\
&= \begin{pmatrix} A & B \\ B^\dagger & -A \end{pmatrix}.
\end{aligned}
\tag{3.26}
$$

Now we treat each submatrix A and B individually. Demanding $A = 0$ yields

$$
\sum_{i<j} \gamma_{ij} q_{ij}^{11} R_{ij} = - \sum_{i<j} \bar{\gamma}_{ij} \bar{q}_{ij}^{11} R_{ij}^\dagger,
\tag{3.27}
$$

thus $\sum_{i<j} \gamma_{ij} q_{ij}^{11} R_{ij}$ must be skew-hermitian. As R_{ij} has zero trace, we extract the following set of equations:

$$
\Re(\sum_{i<j} \gamma_{ij} q_{ij}^{11} r_{ij}^{11}) = 0,
\tag{3.28}
$$

$$
\sum_{i<j} \gamma_{ij} q_{ij}^{11} r_{ij}^{12} + \sum_{i<j} \bar{\gamma}_{ij} \bar{q}_{ij}^{11} \bar{r}_{ij}^{21} = 0.
\tag{3.29}
$$

On the other hand, demanding $B = 0$ yields

$$
\sum_{i<j} \gamma_{ij} q_{ij}^{12} r_{ij}^{11} + \sum_{i<j} \bar{\gamma}_{ij} \bar{q}_{ij}^{21} \bar{r}_{ij}^{11} = 0,
\tag{3.30}
$$

$$
\sum_{i<j} \gamma_{ij} q_{ij}^{12} r_{ij}^{12} + \sum_{i<j} \bar{\gamma}_{ij} \bar{q}_{ij}^{21} \bar{r}_{ij}^{21} = 0,
\tag{3.31}
$$

$$
\sum_{i<j} \gamma_{ij} q_{ij}^{12} r_{ij}^{21} + \sum_{i<j} \bar{\gamma}_{ij} \bar{q}_{ij}^{21} \bar{r}_{ij}^{12} = 0.
\tag{3.32}
$$

Treating real and imaginary part separately, these are $3 + 6 = 9$ real equations for the six complex values γ_{ij}.

Before continuing with the proof, we have to ensure that these equations are linearly independent. This can be checked for by expanding the Schmidt bases $|i\rangle_{\text{AB}}$ and $|i\rangle_{\text{CD}}$ in terms of the computational basis, i.e.

$$
|i\rangle_{\text{AB}} = \sum_{a,b=0}^{1} \mu_{ab}^i |ab\rangle,
\tag{3.33}
$$

$$
|i\rangle_{\text{CD}} = \sum_{c,d=0}^{1} \nu_{cd}^i |cd\rangle,
\tag{3.34}
$$

where the only dependence among the $|i\rangle_{AB}$ is

$$\langle i|j\rangle_{AB} = \sum_{a,b} \mu^i_{ab}\bar{\mu}^j_{ab} = \delta_{ij} \tag{3.35}$$

and similarly for $|i\rangle_{CD}$. Expressing the numbers q_{ij} in terms of the coefficients μ,

$$q^{bb'}_{ij} = \sum_a \mu^i_{ab}\bar{\mu}^j_{ab'}, \tag{3.36}$$

shows that the only dependence among the q_{ij} is $q^{11}_{ij} = -q^{22}_{ij}$, which has already been taken into account. Thus, the numbers q^{11}_{ij}, q^{12}_{ij} and q^{21}_{ij} do not fulfill any additional constraints. The same is true for the r_{ij}. As the orthonormal bases have been chosen independently and randomly, the q_{ij} and r_{ij} are also independent of each other.

Returning to the proof, there is a three dimensional (real) solution space for the γ_{ij} due to Eqs. (3.28) to (3.32) if we do not impose the constraints (3.18) yet. As $\gamma_{ij} = 0$ for all i, j is certainly a solution, we can parametrize this solution space by

$$\gamma_{ij} = \sum_{a=1}^{3} x_a v^a_{ij}, \tag{3.37}$$

where the x_a are the three real-valued parameters.

Luckily, we have additional constraints at hand as the γ_{ij} are not independent. Let us define the normalized variables $c_{ij} := (\lambda_i\lambda_j)^{-1/2}\gamma_{ij}$. Then

$$\begin{aligned}
c_{ij}c_{jk} &= (1 - e^{i(\varphi_i - \varphi_j)})(1 - e^{i(\varphi_j - \varphi_k)}) \\
&= 1 - e^{i(\varphi_i - \varphi_j)} - e^{i(\varphi_j - \varphi_k)} + e^{i(\varphi_i - \varphi_k)} \\
&= c_{ij} + c_{jk} - c_{ik}, \tag{3.38}
\end{aligned}$$

for all i, j, k. This implies also (setting $i = k$)

$$|c_{ij}|^2 = c_{ij} + \bar{c}_{ij}. \tag{3.39}$$

Substituting for c_{ij} the solution (3.37) yields for all $i < j$

$$\sum_{a,b=1}^{3} x_a x_b v^a_{ij}\bar{v}^b_{ij} = \sqrt{\lambda_i\lambda_j} \sum_{a=1}^{3} x_a(v^a_{ij} + \bar{v}^a_{ij}). \tag{3.40}$$

There are six equations for the three variables x_a. Taking the four equations for $i = 1$, $j = 1,\ldots,4$, yields four independent equations as each equation makes use of a different, independent Schmidt coefficient λ_i. Additionally, any of the equations can be solved for any of the x_a and the Schmidt coefficients λ_i have not been used to obtain

the solutions in Eq. (3.37). Therefore, only the trivial solution $x_a = 0$ exists, thus

$$c_{ij} = \gamma_{ij} = 0.\tag{3.41}$$

Consequently, all phases $\varphi_i = \varphi$ must be equal. Thus $|\phi\rangle = e^{i\varphi}|\psi\rangle$ which corresponds to the same physical state. □

The same result is also true for other configurations of known marginals that result from relabeling the particles.

3.4.3 The case of higher-dimensional systems

The proof can seamlessly be extended to the case of qudits having higher internal dimension d.

Theorem 3.5. *Almost all four-qudit pure states of internal dimension d are uniquely determined among pure states by the three two-body marginals of particles ρ_{AB}, ρ_{CD} and ρ_{BD}. In particular, this implies that they are 2-UDP.*

Proof. The proof follows exactly the same steps as in the qubit case. The bases of the subspaces A, B and C, D are then d^2-dimensional, thus i and j run from 1 to d^2 and there are d^2 free phases [$(d^2 - 1)$ if ignoring a global phase]. There are then $\frac{d^2(d^2-1)}{2}$ different complex-valued γ_{ij} with $i < j$. The Eq. (3.26) consists in this case of $d \times d$ submatrices:

$$\sum_{i<j} \begin{pmatrix} \gamma_{ij}q_{ij}^{11}R_{ij} + \bar{\gamma}_{ij}\bar{q}_{ij}^{11}R_{ij}^\dagger & \cdots & \gamma_{ij}q_{ij}^{1d}R_{ij} + \bar{\gamma}_{ij}\bar{q}_{ij}^{d1}R_{ij} \\ \vdots & \ddots & \vdots \\ \gamma_{ij}q_{ij}^{d1}R_{ij} + \bar{\gamma}_{ij}\bar{q}_{ij}^{1d}R_{ij}^\dagger & \cdots & \end{pmatrix} = 0.\tag{3.42}$$

Again, the lower left submatrices are the adjoints of the upper right ones, thus it suffices to set the upper right ones to zero. All submatrices on the diagonal must be skew-hermitian, and the last diagonal matrix can be expressed by the other diagonal entries due to tracelessness:

- Every off-diagonal submatrix such as $\gamma_{ij}q_{ij}^{12}R_{ij} + \bar{\gamma}_{ij}\bar{q}_{ij}^{21}R_{ij}^\dagger$ yields $2(d^2 - 1)$ real equations, as R_{ij} is a traceless $d \times d$ matrix, thus $r_{ij}^{dd} = -r_{ij}^{11} - \ldots - r_{ij}^{d-1,d-1}$. There are $\frac{d(d-1)}{2}$ off-diagonal submatrices on the upper right, thus they yield $(d^2 - 1)d(d - 1)$ real equations.

- Every diagonal submatrix is skew-hermitian, which exhibits $d + 2\frac{d(d-1)}{2} = d^2$ real equations, and traceless, which removes one of the diagonal equations, leaving

$d^2 - 1$ equations. There are $d - 1$ diagonal submatrices, yielding a total of $(d - 1)(d^2 - 1)$ real equations.

Thus, there is a total of $(d - 1)(d^2 - 1) + d(d - 1)(d^2 - 1) = (d^2 - 1)^2$ (real) equations. Consequently, the $\frac{d^2(d^2-1)}{2}$ complex-valued γ_{ij} are reduced to $2\frac{d^2(d^2-1)}{2} - (d^2 - 1)^2 = d^2 - 1$ real parameters, which matches again the number of free phases in the ansatz.

From the compatibility equations (3.38), we can choose those with $i = 1$, $j = 1 \ldots d^2$ to obtain a set of d^2 independent quadratic equations, as there are by assumption d^2 independent Schmidt coefficients. Therefore, the only solution is $\gamma_{ij} = 0$ as in the qubit case, implying that $|\phi\rangle = e^{i\varphi}|\psi\rangle$ for some phase φ. $\qquad\square$

3.5 States of n particles

Even though above theorem is limited to states of four particles, the result sheds some light on states of more parties.

Corollary 3.6. *For $n \geq 4$, almost all n-qudit pure states of parties $A, B, C, D, E_1, \ldots E_{n-4}$ of internal dimension d are uniquely determined among pure states by the three $(n-2)$-body marginals of particles $\rho_{ABE_1\ldots}$, $\rho_{CDE_1\ldots}$ and $\rho_{BDE_1\ldots}$. In particular, this implies that they are $(n-2)$-UDP.*

Proof. We denote by E all the parties $E_1, \ldots, E_{n-4}$. Consider a generic pure n-particle state $|\psi\rangle$ with known $(n-2)$-body marginals ρ_{ABE}, ρ_{ACE} and ρ_{CDE}. From these, one can obtain the $(n-4)$-particle marginal ρ_E. This allows us to decompose a generic state into

$$|\psi\rangle = \sum_{i=1}^{\min(d^4, d^{n-4})} \sqrt{\lambda_i}|\psi_i\rangle \otimes |i\rangle_E, \tag{3.43}$$

where the Schmidt basis $|i\rangle_E$ and Schmidt coefficients λ_i are determined by ρ_E and the Schmidt vectors $|\psi_i\rangle$ on $ABCD$ have yet to be determined. On the one hand, knowing the $(n-2)$-body marginal ρ_{ABE} allows us to determine all expectation values of the form

$$\langle\psi|O_A \otimes O_B \otimes |i\rangle\langle i|_E|\psi\rangle = \text{Tr}(O_A \otimes O_B \otimes |i\rangle\langle i|_E \rho_{ABE}) \tag{3.44}$$

for all i, where O_A and O_B are some local observables of parties A and B, respectively. On the other hand, this is equivalent to knowing all expectation values $\langle\psi_i|O_A \otimes O_B|\psi_i\rangle$ of the pure four-particle constituent $|\psi_i\rangle$, yielding its reduced state $\rho_{AB}^{(i)}$. The same can be done for parties AC and parties CD. According to Theorem 3.5, this determines
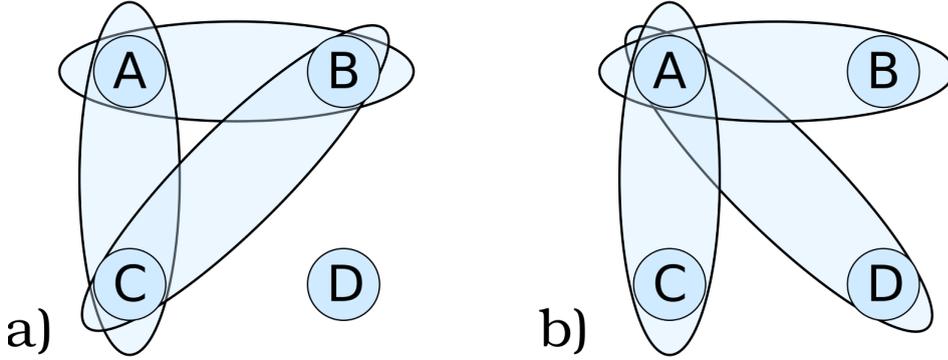
FIGURE 3.3: Illustration of the two other possible sets of three two-body marginals: a) a set of marginals, which clearly does not determine the global state, as ρ_D is not fixed. b) a set of marginals to which our proof does not apply. Nevertheless, we have numerical evidence that these marginals still determine the state uniquely for qubits.

the states $|\psi_i\rangle$ uniquely up to a phase. Thus, the joint state on $ABCDE$ has to have the form

$$|\psi'\rangle = \sum_{i=1}^{\min(d^4, d^{n-4})} e^{i\varphi_i} \sqrt{\lambda_i} |\psi_i\rangle \otimes |i\rangle_{\mathrm{E}}. \tag{3.45}$$

However, from this family only the choice $\varphi_i = \varphi_j$ for all i, j is compatible with the known reduced state ρ_{ABE}: The reduced state

$$\rho'_{\mathrm{ABE}} = \sum_{i,j} e^{i(\varphi_i - \varphi_j)} \sqrt{\lambda_i \lambda_j} \, \mathrm{Tr}_{\mathrm{CD}}(|\psi_i\rangle\langle\psi_j|) \otimes |i\rangle\langle j|_{\mathrm{E}} \tag{3.46}$$

can be compared term by term with the known marginal, as the $|i\rangle_{\mathrm{E}}$ are orthogonal. Therefore, $|\psi'\rangle = e^{i\varphi}|\psi\rangle$ for some phase φ and the state is determined again. □

It must be stressed that the main statement of this Corollary is the fact that three of the $(n-2)$-body marginals can already suffice to fix the state. The fact that pure states are $(n-2)$-UDP is not surprising, as usually already less knowledge is sufficient to make a pure state UDA, see Ref. [25] for a discussion.

3.6 States that are not UDP

As the proof above is valid for generic states only, it is natural to ask whether there are special four-particle states that are not UDP. This is indeed the case. In the following, we give an incomplete list of undetermined four-particle qubit states. Note that if any two states $|\psi\rangle$ and $|\phi\rangle$ share the same two-body marginals, then also all local unitary equivalent states $|\psi\rangle' = U_A \otimes U_B \otimes U_C \otimes U_D|\psi\rangle$ and $|\phi\rangle' = U_A \otimes U_B \otimes U_C \otimes U_D|\phi\rangle$ share the same marginals. Thus, we restrict ourselves to states $|\psi\rangle = \sum \alpha_{ijkl}|ijkl\rangle$ of the

standard form introduced in Ref. [77], where

$$\alpha_{0000}, \alpha_{0001}, \alpha_{0010}, \alpha_{0100}, \alpha_{1000} \quad \in \quad \mathbb{R},$$
$$\alpha_{0111}, \alpha_{1011}, \alpha_{1101}, \alpha_{1110} \quad = \quad 0 \tag{3.47}$$

and all other coefficients being complex. In the following list, the states are always assumed to be normalized. To shorten the notation, we make use of the *W*-state

$$|W_4\rangle = \frac{1}{2}(|0001\rangle + |0010\rangle + |0100\rangle + |1000\rangle)$$

and of the Dicke state

$$|D_2^4\rangle \quad = \quad \frac{1}{\sqrt{6}}(|0011\rangle + |0101\rangle + |1001\rangle$$
$$+ |0110\rangle + |1010\rangle + |1100\rangle).$$

Due to the standard form, we have in the following $a, b \in \mathbb{R}$, while $r, s \in \mathbb{C}$. The claimed properties of the states can directly be computed.

- For fixed a, b and s, the family

$$|\psi\rangle = a|0000\rangle + b|W_4\rangle + se^{i\varphi}|1111\rangle \tag{3.48}$$

  shares the same two-body marginals for all values of φ.

- For the same state with $a = 0, b = \frac{2}{\sqrt{6}}$ and $s = \frac{1}{\sqrt{3}}$,

$$|\phi\rangle = \frac{1}{2}|0000\rangle + \frac{1}{\sqrt{2}}e^{i\varphi}|D_2^4\rangle - \frac{1}{2}e^{2i\varphi}|1111\rangle \tag{3.49}$$

  shares the same marginals for all values of φ.

- For every state
$$|\psi\rangle = a|0000\rangle + r|D_2^4\rangle + s|1111\rangle, \tag{3.50}$$

  the state
$$|\phi\rangle = a|0000\rangle + re^{i\varphi_r}|D_2^4\rangle + se^{i\varphi_s}|1111\rangle \tag{3.51}$$

  shares the same marginals if $\bar{r}se^{i\varphi_s} = are^{i\varphi_r}(1 - e^{i\varphi_r}) + \bar{r}se^{i\varphi_r}$, which is feasible for e.g., $a = 0$.

All of our examples are superpositions of Dicke states and generalized GHZ states. By a local unitary operation, these examples also include the Dicke state with three excitations. The examples prove that Theorem 3.4 does not hold for all four-particle states, but only for generic states.

3.7 Conclusions

We have shown that generic four-qudit pure states are uniquely determined among pure states by three of their six different marginals of two parties. Interestingly, from this, it follows that pure states of an arbitrary number of qudits are determined by certain subsets of size three of their $(n-2)$-body marginals. The proof required knowledge of two marginals of distinct systems, for instance, ρ_{AB} and ρ_{CD}, in order to fix the Schmidt decomposition of the compatible state. However, there are two other sets of three two-body marginals, illustrated in Fig. 3.3. The first one, namely knowledge of ρ_{AB}, ρ_{AC} and ρ_{BC}, is certainly not sufficient to fix the state, as we do not have any knowledge of particle D in this case: Every product state $\rho_{ABC} \otimes \rho_D$ with arbitrary state ρ_D is compatible. The situation for the second configuration, namely knowledge of the three marginals ρ_{AB}, ρ_{AC} and ρ_{AD}, is not that clear. In a numerical survey testing random four-qubit states, we could not find pairs of different pure states which have these coinciding marginals. Thus, we conjecture that any marginal configuration involving all four parties determines generic states. In any case, knowledge of any set of four two-body marginals fixes the state, as there are always two marginals of distinct particle pairs present in these sets.

The question remains which pure four-qubit states are also uniquely determined among all mixed states by their two-body marginals. The results from Ref. [25] suggest that generic states are not UDA, and Ref. [69] shows that for the case of four qutrits, there exists a witness detecting states which are not UDA. On the other hand, in the same reference, a numerical procedure indicated that for generic pure four-qubit states the compatible mixed states (having the same marginals) are never of full rank. Clarifying this situation is an interesting problem for further research.

4 Even and odd correlations

Prerequisites

4.1 Introduction

In the last chapter, we regarded the marginal problem. It can be rephrased as the question of whether the correlations between many of the particles are determined by the correlations between restricted subsets of them. In the language of Section 2.3, this can be stated as follows: For a fixed number k, are the correlations $P_{k+1}, \ldots, P_n$ (uniquely) determined by the correlations $P_1, \ldots, P_k$? It is a natural step to generalize this question in the following way: Which subset of the correlations $\{P_1, \ldots, P_n\}$ determines the whole state? This will be the focus of interest in this chapter.

As an example consider a state of three parties, denoted by A, B and C. Three different contributions to the correlations of the state can be distinguished, which are also depicted in Fig. 4.1: First, there are single-body terms, acting on individual parties alone and determining the single party density matrices. In Section 2.3, we denoted them as P_1. Second, there are two-body correlations acting on the pairs AB, BC, and AC, denoted by P_2. Finally, there are three-body correlations acting on all three particles ABC, called P_3. Thus the question arises: Are these three contributions independent of each other or is one of them determined by the others?

In this chapter, we present an approach to answering this and more general questions for multi-qubit systems. We identify two components of the correlations, depending on the question of whether they act on an odd or even number of particles. We prove that the even correlations and odd correlations obey strong relations, one component often completely determining the other one. Besides of the fundamental interest, these results have several practical applications: We prove that all pure qubit states with an odd number of qubits are uniquely determined among all mixed states by

$$P_e = P_2 \qquad\qquad P_o = P_1 + P_3$$

$$\rho \propto \mathbb{1} + P_e + P_o$$
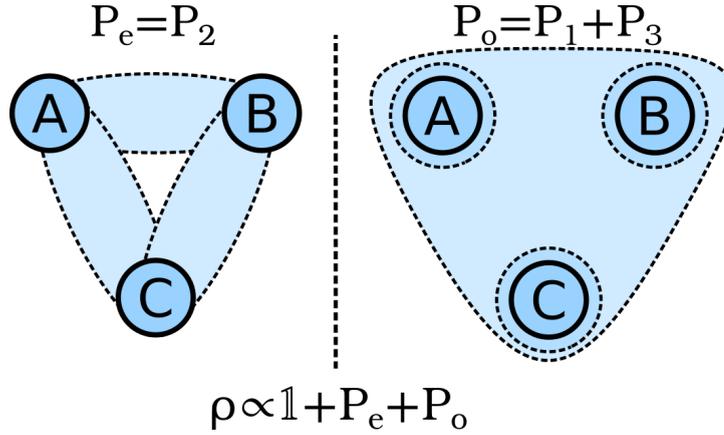
FIGURE 4.1: Visualization of the decomposition of a three-particle state ρ into even and odd correlations. A state ρ is expanded in Bloch representation as $\rho \propto \mathbb{1} + P_1 + P_2 + \ldots$, where P_j denotes all terms containing j-body correlations. We prove that the even correlations P_e are determined by the odd correlations P_o for pure states of an odd number of qubits, so the three qubit state is completely determined by P_o.

the odd component of the correlations. This generalizes the findings of the last chapter. In addition, our approach can be used to characterize ground states arising from Hamiltonians having even or odd interactions only, and the behavior of the correlation components under time evolution governed by Hamiltonians having odd components only. Finally, we apply our insights to simplify the task of entanglement detection in certain scenarios. While the results are obtained mainly for pure states, we finally generalize some of them to certain families of mixed states.

4.2 The even-odd decomposition

Recall from Section 2.3, that we write multi-qubit states in the Bloch basis, i.e., the n-fold tensor product of the Pauli basis, as

$$\rho = \frac{1}{2^n}\left(\mathbb{1}^{\otimes n} + \sum_{k=1}^{n} P_k\right), \qquad (4.1)$$

where P_k denotes the sum over all contributions acting on exactly k of the parties non-trivially. We call P_k the k-body correlations of the state, being determined by the expectation values taken on groups of k particles. As an example, consider the two-qubit Bell state $|\Psi^+\rangle = (|01\rangle + |10\rangle)/\sqrt{2}$, for which the corresponding density operator reads

$$|\Psi^+\rangle\langle\Psi^+| = \frac{1}{4}(\mathbb{1} \otimes \mathbb{1} + X \otimes X + Y \otimes Y - Z \otimes Z), \qquad (4.2)$$

so we have $P_1 = 0$ and $P_2 = X \otimes X + Y \otimes Y - Z \otimes Z$.

As our main ansatz, we further group the operators according to the parity of their weight and define

$$P_\mathrm{e} := \sum_{\substack{j \text{ even,} \\ j \neq 0}} P_j, \qquad P_\mathrm{o} := \sum_{j \text{ odd}} P_j. \tag{4.3}$$

Note that $P_0 = \mathbb{1}^{\otimes n}$ is excluded from P_e. Then we can write states in the even-odd decomposition (see Fig. 4.1)

$$\rho = \frac{1}{2^n}(\mathbb{1} + P_\mathrm{e} + P_\mathrm{o}). \tag{4.4}$$

Here and in the following, we write $\mathbb{1}$ instead of $\mathbb{1}^{\otimes n}$ in order to shorten the notation. The central result of this chapter will be strong relations between the even and the odd component, P_e and P_o.

Our approach is based on the state inversion map, introduced in Eq. (2.34). On the level of pure states, the state inversion map can be represented by the anti-unitary inversion operator $F := (iY)^{\otimes n}K$, where K denotes the complex conjugation in the default basis [78]. We have that $F^\dagger = (-1)^n F$ and for pure states we write $|\tilde{\psi}\rangle = F|\psi\rangle$. It follows that pure states remain pure under the state inversion. Note that for single-qubit Pauli matrices we have $F\sigma_i F^\dagger = -\sigma_i$ for $i \neq 0$. Thus, in Bloch decomposition, F flips the sign of each term that acts on an odd number of parties non-trivially. Starting from Eq. (4.4), we can also write

$$\tilde{\rho} = \frac{1}{2^n}(\mathbb{1} + P_\mathrm{e} - P_\mathrm{o}). \tag{4.5}$$

This allows for an easier representation of the even and odd correlations, namely,

$$\mathbb{1} + P_\mathrm{e} = 2^{n-1}(\rho + \tilde{\rho}), \qquad P_\mathrm{o} = 2^{n-1}(\rho - \tilde{\rho}). \tag{4.6}$$

The key observation is that under the state inversion, pure states of an odd number of qubits are mapped to orthogonal states. This fact was known before [79–83], however, we give a proof that allows for generalization to qudit systems, for which the statement is new.

Lemma 4.1. *For pure n-qudit states $\rho = |\psi\rangle\langle\psi|$ with n odd we have that*

$$\rho\tilde{\rho} = 0. \tag{4.7}$$

Proof. Let $\rho = |\psi\rangle\langle\psi|$ be the pure quantum state and let $M \subset \{1, 2, \ldots, n\}$ denote a subset of the parties. Using the Schmidt decomposition for the bipartition $M|\bar{M}$, i.e.,

$$|\psi\rangle = \sum_i \sqrt{\lambda_i}|i\rangle_M \otimes |i\rangle_{\bar{M}}, \tag{4.8}$$

allows to derive the following relation for the reduced state $\rho_M := \mathrm{Tr}_{\bar{M}}(\rho)$:

$$\rho(\rho_M \otimes \mathbb{1}_{\bar{M}}) = \sum_{i,j} \sqrt{\lambda_i \lambda_j^3} |i\rangle\langle j|_M \otimes |i\rangle\langle j|_{\bar{M}} = \rho(\mathbb{1}_M \otimes \rho_{\bar{M}}). \tag{4.9}$$

Then, state inversion can be written as an alternating sum over the marginals of the state [33],

$$\tilde{\rho} = \sum_{M \subset \{1,\ldots,n\}} (-1)^{|M|} \rho_M \otimes \mathbb{1}_{\bar{M}} \tag{4.10}$$

$$= \mathbb{1} - \rho_A - \rho_B - \ldots + \rho_{AB} + \ldots \pm \rho. \tag{4.11}$$

Note that complementary reductions have the opposite sign since n is odd. Thus, multiplying this equation with ρ and using Eq. (4.9), every term cancels one of the others and we have $\rho\tilde{\rho} = 0$. $\qquad\square$

In the qudit case, pure states do not stay pure under the state inversion but are mapped to positive operators. This generalization is studied in Section 4.6.2.

As we will see, the operator identity in Eq. (4.7) has strong implications on correlations in pure qubit states. For even n, this result is not true in general. However, there are certain states like the W-state for $n \geq 4$ and in particular graph states of type I [84], for which the statement still holds, as will be discussed later.

4.3   Results for an odd number of qubits

Throughout this section, we consider pure qubit states of an odd number of parties, denoted by $|\psi^{odd}\rangle$. We can directly prove our first main result.

Theorem 4.2. *For pure n-qubit states $|\psi^{odd}\rangle$, written in the even-odd decomposition as in Eq. (4.4), we have that*

(1) *the even and odd components of the correlations commute: $[P_e, P_o] = 0$;*

(2) *the odd correlations uniquely determine the even correlations via*

$$\mathbb{1} + P_e = \frac{1}{2^{n-1}} P_o^2; \tag{4.12}$$

(3) the eigenvalues $\Lambda = (\lambda_1, \ldots, \lambda_{2^n})$ of P_e and P_o are given by

$$
\begin{aligned}
\Lambda(P_e) &= (2^{n-1} - 1, 2^{n-1} - 1, -1, \ldots, -1), \\
\Lambda(P_o) &= (2^{n-1}, -2^{n-1}, 0, \ldots, 0).
\end{aligned}
\tag{4.13}
$$

Proof. We use Eq. (4.6) to write

$$
\begin{aligned}
P_o &= 2^{n-1}(|\psi^{odd}\rangle\langle\psi^{odd}| - |\tilde{\psi}^{odd}\rangle\langle\tilde{\psi}^{odd}|), \\
\mathbb{1} + P_e &= 2^{n-1}(|\psi^{odd}\rangle\langle\psi^{odd}| + |\tilde{\psi}^{odd}\rangle\langle\tilde{\psi}^{odd}|).
\end{aligned}
\tag{4.14}
$$

From Lemma 4.1 it follows that both $\mathbb{1} + P_e$ and P_o are diagonal in the same basis and commute. The eigenvalues then can be read off. Furthermore, Eq. (4.12) can be directly verified in the common eigenbasis. $\qquad\square$

The fact that P_e is given by P_o for pure states can be restated in the language of uniqueness: Pure qubit states of an odd number of parties are uniquely determined among pure states (UDP) by the odd correlations. Note that we will later show that they are also determined among all mixed states (UDA) by P_o. This leads to the converse question of whether these states are also determined by the even correlations P_e. The answer to this question is negative, but the set of compatible states is small.

Corollary 4.3. *Given the even correlations P_e of a pure n-qubit state $|\psi^{odd}\rangle$, the set of admissible odd correlations P_o to retrieve a pure state again is a two-parameter family.*

Proof. Let $\rho = |\psi^{odd}\rangle\langle\psi^{odd}|$ and $\tilde{\rho} = |\tilde{\psi}^{odd}\rangle\langle\tilde{\psi}^{odd}|$, and write $\mathbb{1} + P_e = 2^{n-1}(\rho + \tilde{\rho})$. Thus, the eigenvectors with eigenvalue 2^{n-1} of $\mathbb{1} + P_e$ are a superposition of $|\psi^{odd}\rangle$ and $|\tilde{\psi}^{odd}\rangle$. Given only P_e, one can choose any of its eigenvectors $|\eta\rangle$ from the two-dimensional subspace of eigenvalue $2^{n-1} - 1$. As $|\tilde{\eta}\rangle$ is orthogonal to $|\eta\rangle$, it follows that $\mathbb{1} + P_e = 2^{n-1}(|\eta\rangle\langle\eta| + |\tilde{\eta}\rangle\langle\tilde{\eta}|)$. Therefore, every choice of an eigenvector gives rise to compatible correlations $P_o^{(r)}$ via

$$
P_o^{(r)} = 2^{n-1}(|\eta\rangle\langle\eta| - |\tilde{\eta}\rangle\langle\tilde{\eta}|),
\tag{4.15}
$$

resulting in the total state $\rho = |\eta\rangle\langle\eta|$. By fixing one of the eigenstates $|\eta\rangle$, one can parametrize all valid solutions by

$$
\begin{aligned}
P_o^{(r)}(\theta, \phi) = 2^{n-1}[&\cos\theta(|\eta\rangle\langle\eta| - |\tilde{\eta}\rangle\langle\tilde{\eta}|) \\
&+ \sin\theta(e^{i\phi}|\tilde{\eta}\rangle\langle\eta| + e^{-i\phi}|\eta\rangle\langle\tilde{\eta}|)]
\end{aligned}
\tag{4.16}
$$

for all real valued θ and ϕ. $\qquad\square$

So far, we have shown that for an odd number of parties, the odd correlations uniquely determine the state among pure states. It is natural to ask whether a state is determined also among all states (UDA).

Corollary 4.4. *Consider a pure qubit state $|\psi\rangle$ of n parties where n is odd. Then the state is uniquely determined among all mixed states by P_o.*

Proof. Recall that in the even-odd decomposition, the state reads

$$|\psi\rangle\langle\psi| = \frac{1}{2^n}(\mathbb{1} + P_e + P_o). \tag{4.17}$$

Suppose there were a mixed state ρ with the same odd correlations. Then we could write it as a convex sum of pure states,

$$\rho = \sum_i p_i \frac{1}{2^n}(\mathbb{1} + P_e^{(i)} + P_o^{(i)}), \tag{4.18}$$

where $\sum_i p_i = 1$ and $\sum_i p_i P_o^{(i)} = P_o$. From Theorem 4.2 we know that P_o has two non-vanishing eigenvalues $\lambda_{o_\pm} = \pm 2^{n-1}$, and the same holds for every $P_o^{(i)}$ as they originate from pure states. Because the largest eigenvalue of the sum equals the sum of all the maximal eigenvalues, all $P_o^{(i)}$ must share the same corresponding eigenvector. The same is true for the smallest eigenvalue. Thus, $P_o^{(i)} = P_o^{(j)}$ for all i, j follows. As the $P_e^{(i)}$ are uniquely determined by the $P_o^{(i)}$, they also coincide and therefore $\rho = |\psi\rangle\langle\psi|$. $\square$

This result can be seen as a generalization of the uniqueness question of the marginal problem. For example, recall that it was shown that almost all three-qubit states are determined among all states by P_1 and P_2 [22]. Corollary 4.4 shows that *all* three-qubit states are determined among all states by P_1 and P_3, and, remarkably, this generalizes to all odd numbers of parties.

An immediate consequence of Corollary 4.4 is that all pure states of an odd number of parties are unique ground states of odd-body Hamiltonians. More precisely, choosing $H = -P_o = 2^{n-1}(|\tilde{\psi}^{\text{odd}}\rangle\langle\tilde{\psi}^{\text{odd}}| - |\psi^{\text{odd}}\rangle\langle\psi^{\text{odd}}|)$ yields a specific example of such a Hamiltonian.

4.4 Results for an even number of qubits

We now turn to the case of even n, and throughout this section, $|\psi^{\text{even}}\rangle$ denotes a pure state on an even number of qubits. Although in this case $|\psi\rangle$ and $|\tilde{\psi}\rangle$ do not need to be perpendicular, one can gain some insight into the even and odd components of the

correlations. We denote the overlap by $|\langle\tilde{\psi}|\psi\rangle| = \alpha$ with a positive number α such that $\mathrm{Tr}(\rho\tilde{\rho}) = \alpha^2$. Note that α coincides with the n-concurrence defined in Eq. (2.43) in Section 2.5.

For our purpose, we need to distinguish three cases: The case where $\alpha = 0$, the case of $0 < \alpha < 1$ and that of $\alpha = 1$.

If $\alpha = 0$, we recover the case of an odd number of qubits. Examples for such states are the W-state, $|W\rangle = (|0\ldots01\rangle + \ldots + |10\ldots0\rangle)/\sqrt{n}$, and all completely separable states. In this case, all the results from the previous sections apply and P_{o} determines P_{e}.

If $\alpha = 1$, $|\psi\rangle \propto |\tilde{\psi}\rangle$, which means that there are only even correlations present in $|\psi\rangle$ and $P_{\mathrm{o}} = 0$. In this case, the even correlations are not determined by the odd correlations at all. One prominent example for such a state is the n-party Greenberger-Horne-Zeilinger (GHZ) state, $|\mathrm{GHZ}\rangle = (|0\ldots0\rangle + |1\ldots1\rangle)/\sqrt{2}$.

If $0 < \alpha < 1$, even though the results from the previous section do not apply, the spectrum of P_{e} is still rather fixed, leading to the following observation:

Theorem 4.5. *Let $|\psi^{even}\rangle$ be a pure qubit state with $|\langle\psi^{even}|\tilde{\psi}^{even}\rangle|^2 = \alpha^2 \neq 0$. Write $|\psi^{even}\rangle$ in the even-odd decomposition as in Eq. (4.4). Then*

(1) the even correlations P_{e} uniquely determine the odd correlations P_{o} up to a sign,

(2) the family of pure states having the same odd correlations P_{o} as $|\psi^{even}\rangle$ is one-dimensional. The even correlations can be parameterized in terms of P_{o}.

Proof. Let $\rho = |\psi^{\mathrm{even}}\rangle\langle\psi^{\mathrm{even}}|$. Before proving the statements, we investigate the eigenvectors and eigenvalues of P_{e} and P_{o}. As $\mathbb{1} + P_{\mathrm{e}} = 2^{n-1}(\rho + \tilde{\rho})$, it must be of rank two if $\alpha \neq 1$. Thus, it has two non-vanishing eigenvalues, lying in the span of $|\psi\rangle$ and $|\tilde{\psi}\rangle$. Calculating

$$\begin{aligned}(\mathbb{1} + P_{\mathrm{e}})|\psi\rangle &= 2^{n-1}(|\psi\rangle + \alpha e^{i\phi}|\tilde{\psi}\rangle), \\ (\mathbb{1} + P_{\mathrm{e}})|\tilde{\psi}\rangle &= 2^{n-1}(|\tilde{\psi}\rangle + \alpha e^{-i\phi}|\psi\rangle)\end{aligned} \qquad (4.19)$$

yields the two non-vanishing eigenvalues

$$1 + \lambda_{\mathrm{e}_{\pm}} = 2^{n-1}(1 \pm \alpha) \qquad (4.20)$$

and the corresponding orthonormal eigenvectors

$$|e_{\pm}\rangle = \frac{1}{\sqrt{2(1 \pm \alpha)}}(|\psi\rangle \pm e^{i\phi}|\tilde{\psi}\rangle). \qquad (4.21)$$

We can also determine the action of P_o on these eigenvectors, which reveals that it is purely off-diagonal in the eigenbasis of P_e,

$$P_o|e_\pm\rangle = 2^{n-1}(\rho - \tilde{\rho})|e_\pm\rangle = 2^{n-1}\sqrt{1-\alpha^2}|e_\mp\rangle. \tag{4.22}$$

Thus, the eigenvectors of P_o are given by

$$|o_\pm\rangle = \frac{1}{\sqrt{2}}(|e_+\rangle \pm |e_-\rangle) \tag{4.23}$$

and the eigenvalues are given by

$$\lambda_{o_\pm} = \pm 2^{n-1}\sqrt{1-\alpha^2}. \tag{4.24}$$

We are now in position to prove the claims. Let us prove statement two first:

(2) By assumption, P_o is known. The eigenvalues determine the overlap α by Eq. (4.24). Knowledge of α fixes the eigenvalues of any admissible reconstructed $P_e^{(r)}$. The admissible eigenvectors of $P_e^{(r)}$ can be obtained from Eq. (4.23) to read

$$|e_\pm\rangle = \frac{1}{\sqrt{2}}(|o_+\rangle \pm |o_-\rangle). \tag{4.25}$$

However, the eigenvectors $|o_\pm\rangle$ are only unique up to a phase. Taking into account this extra phase while omitting a global phase yields

$$|e_\pm\rangle = \frac{1}{\sqrt{2}}(|o_+\rangle \pm e^{i\varphi}|o_-\rangle). \tag{4.26}$$

This allows us to write all compatible even correlations as

$$\begin{aligned}
\mathbb{1} + P_e^{(r)} &= (1+\lambda_{e_+})|e_+\rangle\langle e_+| + (1+\lambda_{e_-})|e_-\rangle\langle e_-| \\
&= 2^{n-1}(|o_+\rangle\langle o_+| + \alpha e^{-i\varphi}|o_+\rangle\langle o_-| \\
&\quad + |o_-\rangle\langle o_-| + \alpha e^{i\varphi}|o_-\rangle\langle o_+|).
\end{aligned} \tag{4.27}$$

This is a one-dimensional space of admissible reconstructed even correlations, parameterized by φ.

We now show the first statement:

(1) Assume that now P_e is given. Can we uniquely reconstruct in the odd correlations P_o from knowledge of P_e? Unfortunately, the eigenvectors $|e_\pm\rangle$ are again only

determined up to a phase. Therefore, every reconstructed operator $P_{\mathrm{o}}^{(r)}$ of the form

$$
\begin{aligned}
P_{\mathrm{o}}^{(r)} &= \lambda_{\mathrm{o}_+} |o_+\rangle\langle o_+| + \lambda_- |o_-\rangle\langle o_-| && (4.28) \\
&= \lambda_{\mathrm{o}_+} (e^{i\varphi}|e_+\rangle\langle e_-| + e^{-i\varphi}|e_-\rangle\langle e_+|) && (4.29)
\end{aligned}
$$

for all $\varphi \in \mathbb{R}$ would be a valid operator, such that

$$
\frac{1}{2^n}(\mathbb{1} + P_{\mathrm{e}} + P_{\mathrm{o}}^{(r)}) \tag{4.30}
$$

is a pure state again. However, only certain choices of φ recreate a P_{o} which exhibits solely odd correlation in Bloch decomposition. This can be seen as follows: As we will show at the end of the proof, $|e_\pm\rangle\langle e_\pm|$ can only exhibit even correlations. This means that $|e_\pm\rangle$ are eigenvectors of the inversion operator F introduced above, i.e. $F|e_\pm\rangle \propto |e_\pm\rangle$. Recall that for n even, $F^\dagger = F$. Thus, $F|e_+\rangle\langle e_-|F^\dagger = e^{i\Lambda}|e_+\rangle\langle e_-|$ for some Λ. The condition that $P_{\mathrm{o}}^{(r)}$ contains only odd correlations can be written as

$$
P_{\mathrm{o}}^{(r)} + \tilde{P}_{\mathrm{o}}^{(r)} = P_{\mathrm{o}}^{(r)} + F P_{\mathrm{o}}^{(r)} F^\dagger = 0. \tag{4.31}
$$

Eq. (4.29) translates this to

$$
e^{i\varphi} + e^{-i(\varphi-\Lambda)} = 0, \tag{4.32}
$$

which exhibits exactly two solutions for φ. Thus, there are only two possible reconstructions $P_{\mathrm{o}}^{(r)}$, corresponding to the original P_{o} and its negation, $-P_{\mathrm{o}}$.

All that is left is to show the used assumption that the eigenvectors $|e_\pm\rangle$ exhibit only even correlations. Note, that this is a special case of Kramers' theorem [85], stating that the eigenvectors of a Hamiltonian exhibiting even correlations only is either at least two-fold degenerate or exhibits itself only even correlations.

The statement can be seen as follows: Let $P = \lambda_+|p_+\rangle\langle p_+| + \lambda_-|p_-\rangle\langle p_-|$ be a hermitian operator which exhibits only even correlations in the Bloch decomposition, $\langle p_+|p_-| =\rangle 0$ and $\lambda_- < \lambda_+$. We regard P as a Hamiltonian with the unique ground state $|p_-\rangle$. As P has even correlations only, $FPF^\dagger = P$. Thus

$$
\begin{aligned}
\lambda_- &= \mathrm{Tr}(P|p_-\rangle\langle p_-|) = \mathrm{Tr}(FPF^\dagger|p_-\rangle\langle p_-|) \\
&= \mathrm{Tr}(PF|p_-\rangle\langle p_-|F^\dagger), \tag{4.33}
\end{aligned}
$$

as $F^\dagger = F$ if n is even. Thus, also $F|p_-\rangle$ is a ground state of P. As by assumption the ground state is unique, $F|p_-\rangle \propto |p_-\rangle$ must hold true and therefore, $|p_-\rangle\langle p_-|$ exhibits only even correlations. This implies that also $|p_+\rangle\langle p_+|$ has even correlations only. $\square$

	n even and $0 < \alpha < 1$	n odd or $\alpha = 0$
P_o given	One-dimensional solution space for P_e	P_e is uniquely determined
P_e given	$\pm P_\text{o}$ is uniquely determined up to the sign	Two-dimensional solution space for P_o

TABLE 4.1: Summary of the relations between the even and odd components of pure state correlations as derived in Theorems 4.2 and 4.5 and Corollary 4.3. The detailed relations can be found in the corresponding proofs. Additionally, if n is even and $\alpha = 1$, the state exhibits only even correlations and given P_e, only $P_\text{o} = 0$ is compatible.

All of our results on the relations between even and odd components are summarized in Table 4.1.

A statement similar to Corollary 4.4 is not true for an even number of parties with $\alpha \neq 0$, as the family of mixed states $p\rho + (1 - p)\tilde{\rho} = [\mathbb{1} + P_\text{e} + (2p - 1)P_\text{o}]/2^n$ shares the same even body correlations, unless $\alpha = 1$, in which case $P_\text{o} = 0$ and the state is determined.

As a final remark, note that pure states mixed with white noise can be reconstructed as well from knowledge of P_o (P_e) for n odd (n even), as the noise parameter can be deduced from the eigenvalues of the operators.

4.5 Applications

4.5.1 Ground states of Hamiltonians

Some of the results of this chapter can be related to Kramers' theorem [85]. Consider a Hamiltonian that contains even-body interactions only, such as the Ising model without external field [86], or the t-J-model [87–89]. A unique ground state of such a Hamiltonian must have even correlations only. This, however, is not possible if n is odd, in which case odd correlations must be present according to Eq. (4.12). Thus, every ground state of an even-body Hamiltonian must be degenerate if n is odd. On the other hand, if n is even, then the ground state must belong to the class of even states, i.e., $\alpha = 1$. Second, consider Hamiltonians with odd-body interactions only. The ground-state energy of such Hamiltonians is a function of P_o only. Thus, a unique ground state for n even can only be a state which is determined uniquely by P_o, which are exactly the states perpendicular to their inverted states, i.e., having $\alpha = 0$ like the W-state or product states.

4.5.2 Unitary time evolution

Another application concerns the orbits of certain states under the time evolution governed by certain Hamiltonians. Here, our approach allows to re-derive and understand previous results from Ref. [80], where a completely different approach was used. Consider a Hamiltonian H_o consisting of odd-body interactions only. Then, any operator P evolves in time as

$$P(t) = e^{-iH_o t} P e^{iH_o t} = \sum_{m=0}^{\infty} \frac{(-it)^m}{m!} [H_o, P]_m, \tag{4.34}$$

where $[H_o, P]_m := [H_o, [H_o, P]_{m-1}]$ denotes the m-times nested commutator given by $[H_o, P]_0 = P$.

Now, let us denote the number of particles a tensor product T of Pauli matrices acts upon non-trivially by $\mathrm{wt}(T)$ as defined in Eq. (2.15). For these weights, Lemma 1 from Ref. [90], adapted for the case of commutators, can be used. It states that for the weight of the commutator of two tensor products S and T one has that:

$$\mathrm{wt}([S,T]) \equiv \mathrm{wt}(S) + \mathrm{wt}(T) + 1 \quad (\mathrm{mod}\ 2), \tag{4.35}$$

provided that the commutator does not vanish. This lemma encodes the commutator rules of the Pauli matrices. Therefore, by linearity, commuting two odd or two even hermitian operators yields an odd operator, while commuting an even and an odd operator yields an even operator.

Consider, for example, the three-qubit operators $S = X \otimes Y \otimes Z + \mathbb{1} \otimes \mathbb{1} \otimes Y$ and $T = \mathbb{1} \otimes X \otimes Z$. Then, S has odd and T has even weight. Their commutator is given by $[S,T] = -2iX \otimes Z \otimes \mathbb{1} + 2i\mathbb{1} \otimes X \otimes X$, which has even weight.

Thus, if H and P are odd, all the nested commutators in Eq. (4.34) are odd too, and $P(t)$ stays odd for all times t. On the other hand, if H is odd but P is even, then $P(t)$ remains even. By Eqs. (4.4) and (4.5), the inverted state $\tilde{\rho}$ evolves as $\exp(-iHt)\tilde{\rho}\exp(iHt)$ as well, as the state inversion and the time evolution commute in this case. Therefore, given a quantum state ρ, the overlap $\alpha^2 = \mathrm{Tr}(\rho\tilde{\rho})$ stays constant for all times. This is also true for mixed states. In that case, the result also holds for the n-concurrence C_n, given by the convex roof construction for α, as the value of $\mathrm{Tr}(\rho\tilde{\rho})$ stays constant for any decomposition of ρ into a sum over pure states [91]. In summary, the following theorem holds:

Theorem 4.6. *Any quantum state $\rho(t)$, whose time evolution is governed by an odd-body interacting Hamiltonian has a constant value of α and C_n.*

61

This result can be useful as follows: Recent experiments enabled the observation of the spreading of quantum correlations under interacting Hamiltonians for systems out of thermal equilibrium [92, 93]. Theorem 4.6 shows that large classes of Hamiltonians preserve certain properties of a quantum state and deviations thereof may be used to characterize the actually realized Hamiltonian. For instance, Refs. [94, 95] proposed methods to engineer Hamiltonians with three-qubit interactions only. Experimentally, the n-concurrence is not easy to measure; however, bounds can be found with simple methods [96–98]. A simple scheme that detects even-body terms in the Hamiltonian is the following.

Start with any state $|\psi(0)\rangle$ with zero n-concurrence and let it evolve under the Hamiltonian in question. We denote by $|\mathrm{GHZ}_n\rangle$ the n-partite GHZ state from Eq. (2.44) with n-concurrence equal to one. After a fixed time t_0, the state can be decomposed as

$$|\psi(t_0)\rangle = \sqrt{F}|\mathrm{GHZ}_n\rangle + \sqrt{1-F}|\chi\rangle \tag{4.36}$$

with $\langle \mathrm{GHZ}_n|\chi\rangle = 0$. The n-concurrence of the state is given by

$$
\begin{aligned}
C_n(|\psi(t_0)\rangle) &= |\langle\psi(t_0)|\tilde{\psi}(t_0)\rangle| \\
&= |F\langle\mathrm{GHZ}_n|\mathrm{GHZ}_n\rangle + (1-F)\langle\chi|Y^{\otimes n}|\chi^*\rangle \\
&\quad + \sqrt{F(1-F)}(\langle\mathrm{GHZ}_n|Y^{\otimes n}|\chi^*\rangle + \mathrm{h.c.})| \\
&= |F + (1-F)\langle\chi|\tilde{\chi}\rangle|, \tag{4.37}
\end{aligned}
$$

as $\langle\mathrm{GHZ}_n|Y^{\otimes n}|\chi^*\rangle = \langle\mathrm{GHZ}_n|\chi^*\rangle = \langle\mathrm{GHZ}_n|\chi\rangle^* = 0$. The right hand side is always lower bounded by

$$C_n(|\psi(t)\rangle) \geq F - (1-F). \tag{4.38}$$

If $F > 50\%$, the concurrence is non-zero and even-body interactions must have been present. Therefore, low-concurrence states cannot approximate the GHZ state under the time evolution with odd-body Hamiltonians.

Combining this result with the one about ground states of odd-body Hamiltonians, we obtain the following corollary.

Corollary 4.7. *If n is even, it is not possible to produce a GHZ state from a W-state (or any state with $C_n = 0$) by unitary or adiabatic time evolution under Hamiltonians with odd interactions only.*

4.5.3 Entanglement detection

The results of this chapter yield insight into the structure of pure quantum states that is still subject to ongoing research [99].

Consider a pure state of n qubits with n being odd. Suppose that the odd correlations $P_1, P_3, \ldots, P_{n-2}$ are given. If the state is biseparable, there are $(n-1)/2$ different possibilities of biseparation: It could be biseparable along a cut between one qubit and the other $n-1$ qubits, or between two qubits and $n-2$, etc., up to $(n-1)/2$ qubits and $(n+1)/2$ qubits. The first case can be tested for by checking for each party whether the corresponding one-particle reduced state is pure. This can be done due to the knowledge of P_1. The second case, namely, two qubits vs. $n-2$ qubits can be tested by assuming that the $(n-2)$-qubit state is pure and trying to reconstruct the appropriate even correlations. According to Corollary 4.4, this is only possible if the state was indeed pure. This procedure can be applied to all other splittings as well. Thus, the information on genuine multipartite entanglement in pure states is embodied in the odd correlations $P_1, P_3, \ldots, P_{n-2}$ already, where no knowledge of the highest correlations P_n is needed. This is in contrast to the case of mixed states.

4.6 Generalizations

4.6.1 Mixed states

Most of the results obtained so far are only valid for pure quantum states. However, some of the results can be generalized to mixed states as well. To that end, consider a (mixed) quantum state ρ of n qubits, written in the even-odd decomposition as

$$\rho = \frac{1}{2^n}(\mathbb{1} + P_e + P_o). \tag{4.39}$$

We are interested in the subset of states which are orthogonal to their inversion, i.e., $\text{Tr}(\rho\tilde{\rho}) = 0$. Examples for such three-qubit states can be found in Section 5.4.3, where such states are constructed for all admissible sector length configurations.

Note that for positive semidefinite matrices, one can always find positive square roots, thus $\text{Tr}(\rho\tilde{\rho}) = \text{Tr}(\sqrt{\rho}\sqrt{\rho}\sqrt{\tilde{\rho}}\sqrt{\tilde{\rho}}) = \text{Tr}[(\sqrt{\rho}\sqrt{\tilde{\rho}})(\sqrt{\rho}\sqrt{\tilde{\rho}})^{\dagger}] = 0$. As this expression corresponds to the square of the Hilbert-Schmidt norm of $\sqrt{\rho}\sqrt{\tilde{\rho}}$, this implies that already $\sqrt{\rho}\sqrt{\tilde{\rho}} = 0$ on an operator level and therefore $\rho\tilde{\rho} = 0$.

For mixed states, we do not have the additional constraint $\rho^2 = \rho$ at our disposal. However, expanding $\rho\tilde\rho = 0$ in the even-odd decomposition yields

$$(\mathbb{1} + P_{\mathrm{e}})^2 - (P_{\mathrm{o}})^2 + [P_{\mathrm{o}}, P_{\mathrm{e}}] = 0. \tag{4.40}$$

As the right-hand side is hermitian, the skew-hermitian commutator on the left-hand side must vanish, as well as the hermitian $(\mathbb{1} + P_{\mathrm{e}})^2 - (P_{\mathrm{o}})^2$. Thus, P_{e} and P_{o} can be simultaneously diagonalized. We denote the eigenvectors by $|v_i\rangle$ and write

$$P_{\mathrm{o}} = \sum_{i=1}^{2^n} \lambda_{\mathrm{o},i} |v_i\rangle\langle v_i|, \qquad P_{\mathrm{e}} = \sum_{i=1}^{2^n} \lambda_{\mathrm{e},i} |v_i\rangle\langle v_i|. \tag{4.41}$$

As $(\mathbb{1} + P_{\mathrm{e}})^2 = (P_{\mathrm{o}})^2$, it holds that $\lambda_{\mathrm{o},i} = \pm(1 + \lambda_{\mathrm{e},i})$ for all i. We have to distinguish two cases for each i; if $\lambda_{\mathrm{o},i} = 0$ or $\lambda_{\mathrm{o},i} = -(1 + \lambda_{\mathrm{e},i})$, then the corresponding eigenvector $|v_i\rangle$ belongs to the kernel of ρ, as $\rho|v_i\rangle = 0$. If, however, $0 \neq \lambda_{\mathrm{o},j} = +(1 + \lambda_{\mathrm{e},j})$, then $|v_j\rangle$ is an eigenvector of ρ with non-vanishing eigenvalue $\frac{1}{2^{n-1}}\lambda_{\mathrm{o},j}$. For each such eigenvector we can write

$$2^n \rho|v_i\rangle = (\mathbb{1} + P_{\mathrm{e}} + P_{\mathrm{o}})|v_i\rangle = 2\lambda_{\mathrm{o},i}|v_i\rangle. \tag{4.42}$$

If we apply the anti-unitary inversion operator F to this equation, we obtain

$$(\mathbb{1} + P_{\mathrm{e}} - P_{\mathrm{o}})|\tilde v_i\rangle = 0. \tag{4.43}$$

This means that the inverted state $|\tilde v_i\rangle$ belongs to the kernel of ρ as well. This has interesting consequences, which we summarize in the following corollary.

Corollary 4.8. *For an n-qubit state ρ with $\mathrm{Tr}(\rho\tilde\rho) = 0$ holds:*

1. *For each state $|\psi\rangle$ in the range of ρ, the state $|\tilde\psi\rangle$ is in the kernel;*

2. *For each state $|\psi\rangle$ in the range of ρ holds $\langle\tilde\psi|\psi\rangle = 0$.*

Proof. We showed the first statement in the text above. In order to prove the second, we write $|\psi\rangle = \rho|\phi\rangle$ for an appropriate $|\phi\rangle$. Then

$$\langle\tilde\psi|\psi\rangle = \langle\tilde\phi|\tilde\rho\rho|\phi\rangle = 0. \tag{4.44}$$

$\square$

Some comments on this result are in order: First of all, it immediately implies that matrices being orthogonal to their inverted states can be at most of rank 2^{n-1}. Second

of all, it can help with entanglement detection using the range criterion [100]. It states that if ρ is a fully separable state, then its range must be spanned by product vectors. If a product vector $|\psi\rangle = |a\rangle \otimes \ldots$ is known to be in the range of ρ, then the product vector $|\tilde{\psi}\rangle = |\tilde{a}\rangle \otimes \ldots$ cannot be in the range, which might be helpful if one wants to show that there are not enough product states in the range for them to span the whole space, thus proving entanglement. Finally, note that the second statement of Corollary 4.8 is trivial if n is odd.

4.6.2 Higher dimensional systems

While the results obtained before are valid for qubit systems only, some extensions to higher-dimensional systems are possible, as we will discuss now. The state inversion map can be generalized to systems of internal dimension d by taking Eq. (4.11) as a definition (see also the discussion in Ref. [101]):

$$\tilde{\rho} := \sum_{M \subset \{1,\ldots,n\}} (-1)^{|M|} \rho_M \otimes \mathbb{1}_{\bar{M}}. \tag{4.45}$$

This yields a positive operator [33, 102], which can be normalized to a proper state. In a higher dimensional Bloch decomposition, the inversion reads

$$\tilde{\rho} = \frac{(d-1)^n}{d^n} \sum_{j=0}^{n} \left(\frac{1}{1-d}\right)^j P_j. \tag{4.46}$$

However, for $n > 1$ and $d > 2$ pure states do not stay pure under the state inversion. Thus, the state inversion cannot be represented as an operator acting on vectors in Hilbert space anymore, but only as a channel. Nevertheless, this generalization has recently been used to gain insight into the distribution of entanglement in higher dimensional many-body systems [101].

4.6.3 Generalized inversions

Another generalization concerns the nature of the inversion operator. Instead of flipping the sign of all non-trivial Pauli operators, one can generalize this to only flipping certain ones. The most general form of such an operator acting on a single qubit reads

$$F_\alpha = iC \left(i\alpha_0 \mathbb{1} + \sum_{i=1}^{3} \alpha_i \sigma_i \right) \tag{4.47}$$

where the four dimensional vector $\vec{\alpha}$ is normalized. The choice $\alpha = (0, 0, 1, 0)^\mathrm{T}$ corresponds to the flip considered above (the signs of all Pauli matrices are flipped),

whereas $\alpha = (1,0,0,0)^{\mathrm{T}}$ flips just Y (which corresponds to a transposition of the state), $\alpha = (0,1,0,0)^{\mathrm{T}}$ flips Z, and $\alpha = (0,0,0,1)^{\mathrm{T}}$ flips X. Other values of $\vec{\alpha}$ correspond to superpositions of these flips. Indeed, $F_\alpha |\psi\rangle$ is a pure state again. For example, setting $\alpha = (0,0,0,1)^{\mathrm{T}}$ allows for a decomposition of states by the number of X appearing in each term, thus, P_{e} would consist of all terms with an even number of X. Using this decomposition, analogous results can be derived with similar uniqueness properties.

4.7 Conclusions

In this chapter, we introduced the decomposition of multipartite qubit states in terms of even and odd correlations. For pure states, we showed that the even and odd correlations are deeply connected, and often one type of correlations determines the other. This allowed us to derive several applications, ranging from the unique determination of a state by its odd correlations to invariants under Hamiltonian time evolution and entanglement detection.

For future work, it would be highly desirable to generalize the approach to higher-dimensional systems. Some facts about state inversion are collected in the previous section, but developing a general theory seems challenging. Furthermore, it may be very useful if one can extend our theory to a quantitative theory, where the correlations within some subset of particles are measured with some correlation measure and then monogamy relations between the different types of correlations are developed. In part, this procedure is carried out in the next chapter.

5 Sector lengths

Prerequisites

5.1 Introduction

One of the main messages of the first chapters of this thesis states that correlations in quantum mechanics are more powerful than classical correlations, nevertheless, they are constrained in many ways due to the underlying framework, especially the positivity of quantum states. We saw manifestations of these restrictions in the context of the marginal problem in Chapter 3, and the even-odd relations in Chapter 4. Furthermore, these restrictions give rise to the monogamy relations discussed in Section 2.5.4.

A useful concept to describe the correlation structure of quantum states is the so-called sector length, defined in Eq. (2.18). Roughly said, sector lengths for n-partite quantum states are quadratic expressions and quantify, for different $k \leq n$, the amount of k-partite correlations in the state. Thus, to any n-qubit state one assigns a tuple $(A_1, \ldots A_n)$ of sector lengths and infers properties of the state based on the sector length configuration. Sector lengths are, as all correlation measures, invariant under local unitary transformations [103]. They are expressible in terms of purities of the reduced states of a system, and as such, they can be experimentally characterized by randomized measurements on a single copy of the state [104].

Consequently, sector lengths have been used for many purposes, for example, entanglement detection [105], deriving monogamy relations [39] and excluding the existence of certain absolutely maximally entangled states [90]. In the context of quantum coding theory, sector lengths are known as weight enumerator theory and are used

to characterize quantum codes [106]. Furthermore, bounds on k-sector lengths with $k < n$ can be used to find necessary conditions for a set of reduced density matrices of up to k of the parties to be compatible with a global state and are thus useful in the context of the representability problem introduced in Section 2.4.

In this chapter we first find exact bounds on individual sectors A_k for $k \in \{2, 3, n\}$. Furthermore, we fully classify the set of admissible tuples of sector lengths for two- and three-qubit states by characterizing all bounds on linear combinations of the sector lengths. Interestingly, we show that in these cases, the admissible sector lengths form a convex polytope that can be characterized by few constraints. One of these constraints can be viewed as a symmetrized version of strong subadditivity (SSA) of the linear entropy introduced in Section 2.7.

This chapter is structured as follows: First, we will define sector lengths and review known relations between them. Then, we find tight bounds on the individual sectors A_2, A_3 and A_n in n-qubit states. There, we highlight connections to monogamy of entanglement and apply our results to the representability problem and the problem of entanglement detection. Next, we extensively study the cases of two and three qubits. To that end, we describe how to translate between sector lengths, linear entropies and mutual linear entropies, which are in one-to-one correspondence. We completely characterize the allowed sector length configurations by considering a symmetrized SSA for linear entropies for three-qubit systems. While it is known that SSA does not hold in general for the linear entropy [107], we show, using techniques from semidefinite programming (SDP), that the symmetrized version is true for three qubits.

Finally, have a glance at the four-qubit case. Here, we list examples of corresponding states for all admissible integer tuples of sector lengths.

5.2 Basic definitions

Consider a quantum state ρ of n qubits. We expand the state in terms of the Bloch basis, i.e., in terms of tensor products of Pauli matrices, and group the terms according to the number of non-trivial Pauli matrices in each term as described in Eq. (2.16), i.e.,

$$\rho = \frac{1}{2^n}(\mathbb{1} + P_1 + P_2 + \ldots + P_n), \qquad (5.1)$$

Here, P_k contains the sum of all terms with k non-trivial Pauli matrices, i.e., terms of weight k. As ρ is hermitian, the P_k are hermitian as well. Note that the only term that is not traceless is the unit operator, thus the normalization 2^{-n} is chosen such that $\text{Tr}(\rho) = 1$.

As an example, consider again the Greenberger-Horne-Zeilinger (GHZ) state of three particles, $|\text{GHZ}\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$. In terms of Pauli operators, the density matrix reads

$$\rho_{\text{GHZ}} = \frac{1}{2^3}(\mathbb{1}\mathbb{1}\mathbb{1} + ZZ\mathbb{1} + Z\mathbb{1}Z + \mathbb{1}ZZ + XXX - XYY - YXY - YYX). \qquad (5.2)$$

Here and in the following, we skip the tensor product symbol for better readability. Thus, $\mathbb{1}ZZ$ means $\mathbb{1} \otimes Z \otimes Z$. In this example, $P_1 = 0$, $P_2 = ZZ\mathbb{1} + Z\mathbb{1}Z + \mathbb{1}ZZ$ and $P_3 = XXX - XYY - YXY - YYX$.

The sector length A_k captures the amount of k-body correlations in a state. We already defined it in Eq. (2.18) as the normalized square of the Hilbert-Schmidt norm of the P_k, i.e.,

$$A_k(\rho) := \frac{1}{2^n} \text{Tr}[P_k(\rho)^2] = \sum_{\Xi_k} \text{Tr}[\Xi_k \rho]^2, \qquad (5.3)$$

where the sum spans over all Pauli operators Ξ_k of weight k. Note that $A_0 = 1$ by normalization. As an example, the GHZ state above has sector length configuration $(A_1, A_2, A_3) = (0, 3, 4)$. We stress that while we used an explicit choice of a basis to define the A_i they are invariant under local unitary operations, and as such, they are independent of the choice of the local basis.

Considering the set of all quantum states of n parties, we are interested in the tuples $(A_1, \ldots, A_n)$ that are attainable. First, we find tight bounds on the individual sectors. These bounds can always be realised by pure states, as the quantity A_i is convex as shown in Section 2.3: $A_i(\rho) \leq \sum_j p_j A_i(|\psi_j\rangle)$ if $\rho = \sum_j p_j |\psi_j\rangle\langle\psi_j|$. Thus, we start by listing some basic facts about sector lengths of pure states. In this case, $\rho = \rho^2$ and therefore $\sum_{k=0}^n A_k = 2^n$. In fact, the sum of all sector lengths is equal to the purity of the state up to a factor of 2^n.

Additionally, there are many relations among the A_i for pure states: Choosing $\rho = |\psi\rangle\langle\psi|$ and a subsystem $S \subset \{1, \ldots, n\}$, one can define the reduced state of particles S, $\rho_S := \text{Tr}_{\bar{S}}(\rho)$, where $\bar{S} = \{1, \ldots, n\} \setminus S$. Using the Schmidt decomposition from Eq. (2.25) between systems S and $\bar{S}$, one can write the pure state $|\psi\rangle$ as

$$|\psi\rangle = \sum_i \sqrt{\lambda_i} |i\rangle_S \otimes |i\rangle_{\bar{S}}. \qquad (5.4)$$

An immediate consequence is that ρ_S and $\rho_{\bar{S}}$ are diagonal in the respective Schmidt bases, and their spectra coincide. Furthermore, recall from Eq. (4.9) that

$$\rho(\rho_S \otimes \mathbb{1}_{\bar{S}}) = \rho(\mathbb{1}_S \otimes \rho_{\bar{S}}). \qquad (5.5)$$

Summing this identity over all subsets of size $m \leq n$ yields an equation for pure states that is expressible in terms of sector lengths [84]:

$$M_m := 2^m \sum_{j=0}^{n-m} \binom{n-j}{m} A_j - 2^{n-m} \sum_{j=0}^{m} \binom{n-j}{n-m} A_j = 0 \tag{5.6}$$

for all integer $0 \leq m \leq n$, where for $m = 0$ one obtains the purity equality, $\sum_i A_i = 2^n$. The relations $M_m = 0$ are known in the more general context of coding theory as MacWilliams' identities [108]. A subset of $\lceil \frac{n}{2} \rceil$ of them are linearly independent equations and allows for the elimination of certain A_i if the state is known to be pure.

5.3 Bounds on individual sector lengths

We start by proving some bounds on the smallest sector lengths. First of all, it is known that

$$A_1 \leq n \tag{5.7}$$

for n-qubit states, which is attained for pure product states like $|0 \ldots 0\rangle$. This is because $A_1(\rho)$ is given by the sum of all $A_1(\rho_i)$ of the one-party reduced states ρ_i of ρ, corresponding to the squared magnitude of the Bloch vector, which is bounded by one.

5.3.1 Bounds on A_2

While the bound (5.7) is trivial, the tight bounds on A_2 are only known for $n = 2$ and $n = 3$ so far. For $n = 2$, the bound is given by $A_2 \leq 3$, as for the purity holds $\text{Tr}(\rho^2) = 2^{-2}[1 + A_1(\rho) + A_2(\rho)] \leq 1$. For $n = 3$, however, we obtain from $M_1 = 0$ in (5.6) for pure states that $A_2 = 3$, and therefore by convexity for all states $A_2 \leq 3$. We will show here that for $n \geq 3$, the bound is given by $A_2 \leq \binom{n}{2}$, using the following Lemma.

Lemma 5.1. *If for all quantum states ρ of n_0 qubits it holds that $A_k(\rho) \leq \binom{n_0}{k}$, then for all states ρ' of $n \geq n_0$ qubits, it holds that $A_k(\rho') \leq \binom{n}{k}$.*

Proof. We prove the Lemma by induction over the number of qubits n. Let the statement be true for a fixed $n \geq n_0$ and consider a state ρ of $n+1$ parties. There are $n+1$ different n-party marginal states of ρ, $\rho_{\bar{j}} := \text{Tr}_j(\rho)$ for $j \in \{1, \ldots, n+1\}$. For each of them it holds by assumption that $A_k(\rho_{\bar{j}}) \leq \binom{n}{k}$.

Every k-body correlation among the parties $i_1, \ldots, i_k$ that is present in ρ is also present in the reduced states that contain the parties $i_1, \ldots, i_k$. This is the case for $(n + 1 - k)$ of the $(n + 1)$ different reductions. Thus,

$$\sum_{j=1}^{n+1} A_k(\rho_{\bar{j}}) = (n + 1 - k) A_k(\rho). \tag{5.8}$$

The left hand side of this equation is bounded by assumption by $(n + 1)\binom{n}{k}$, thus we have that

$$A_k(\rho) \leq \frac{n+1}{n+1-k} \binom{n}{k} = \binom{n+1}{k}. \tag{5.9}$$

$\square$

Proposition 5.2. *For all qubit states of $n \geq 3$ parties, it holds that $A_2 \leq \binom{n}{2}$. The bound is tight.*

Proof. For $n = 3$, from $M_1 = 0$ in (5.6) we have that $A_2 = 3 = \binom{3}{2}$. Thus, Lemma 5.1 applies and therefore $A_2 \leq \binom{n}{2}$ for all n-qubit states with $n \geq 3$.

Concerning the tightness, consider the pure product state $|0\ldots0\rangle\langle0\ldots0| = (\frac{\mathbb{1}+Z}{2})^{\otimes n}$. It has weights given by $(A_1, A_2, \ldots, A_n) = (\binom{n}{1}, \binom{n}{2}, \ldots, \binom{n}{n})$ and reaches the bound.

$\square$

Note that in [109] the authors prove a weaker statement of Proposition 5.2 for the sum of all bipartite correlation terms involving X and Y only, for which the same bound is obtained.

Using the same induction technique and the base case of four qubits, we can prove an even stronger, non-symmetric version of Proposition 5.2 for $n \geq 4$, by summing only those contributions to A_2 that involve correlations with the (arbitrarily chosen) first qubit.

Proposition 5.3. *For all qubit states of $n \geq 4$ parties, it holds that*

$$\sum_{j=2}^{n} A_2(\rho_{1j}) \equiv \sum_{j=2}^{n} A_2^{(1j)} \leq n - 1. \tag{5.10}$$

Proof. We prove the claim for $n = 4$ first. In this case, we distribute all of the 27 Pauli operators whose expectation values contribute to the bipartite sector lengths

into anticommuting sets,

$$M_1 = \{XX\mathbb{1}\mathbb{1}, XY\mathbb{1}\mathbb{1}, XZ\mathbb{1}\mathbb{1}, \ Y\mathbb{1}X\mathbb{1}, Y\mathbb{1}Y\mathbb{1}, Y\mathbb{1}Z\mathbb{1}, \ Z\mathbb{1}\mathbb{1}X, Z\mathbb{1}\mathbb{1}Y, Z\mathbb{1}\mathbb{1}Z \},$$

$$M_2 = \{YX\mathbb{1}\mathbb{1}, YY\mathbb{1}\mathbb{1}, YZ\mathbb{1}\mathbb{1}, \ Z\mathbb{1}X\mathbb{1}, Z\mathbb{1}Y\mathbb{1}, Z\mathbb{1}Z\mathbb{1}, \ X\mathbb{1}\mathbb{1}X, X\mathbb{1}\mathbb{1}Y, X\mathbb{1}\mathbb{1}Z \},$$

$$M_3 = \{Z\,X\mathbb{1}\mathbb{1}, Z\,Y\mathbb{1}\mathbb{1}, ZZ\mathbb{1}\mathbb{1}, \ X\mathbb{1}X\mathbb{1}, X\mathbb{1}Y\mathbb{1}, X\mathbb{1}Z\mathbb{1}, \ Y\mathbb{1}\mathbb{1}X, Y\mathbb{1}\mathbb{1}Y, Y\mathbb{1}\mathbb{1}Z \},$$

such that in each set all operators pairwise anticommute. Here, $XX\mathbb{1}\mathbb{1}$ means again $X \otimes X \otimes \mathbb{1} \otimes \mathbb{1}$. For any anticommuting set M, it holds that $\sum_{m \in M} \langle m \rangle^2 \leq 1$ [110–112]. The sets are chosen such that

$$\sum_{j=2}^{4} A_2(\rho_{1j}) = \sum_{i=1}^{3} \sum_{m \in M_i} \langle m \rangle^2 \leq 3. \tag{5.11}$$

To augment the proof to the case of $n > 4$, we consider all $\binom{n-1}{3}$ subsets of four of the parties containing the first one, i.e., for $n = 5$ we would consider the sets $\{1,2,3,4\}, \{1,2,3,5\}, \{1,2,4,5\}$ and $\{1,3,4,5\}$. For each of these subsets, the inequality for four parties holds. Summing these inequalities yields, on the one hand, an upper bound of $3\binom{n-1}{3}$. On the other hand, we obtain each of the two-body correlations $A_2(\rho_{1j})$ exactly $\binom{n-2}{2}$ times. Dividing both sides by this factor proves the claim. $\qquad\square$

Interestingly, the method of anticommuting sets is also suitable for proving Proposition 5.2 for $n \geq 6$ in an easy graphical way by solving Sudoku-like games. We explain this method in Appendix A.

Proposition 5.3 states that in a multi-qubit state, the bipartite correlations of a party with any of the other parties, on average cannot exceed one. Note that maximally entangled bipartite reduced states would obey $A_2 = 3$, and separable two-qubit states obey $A_2 \leq 1$. Thus, Propositions 5.2 and 5.3 can be seen as monogamy relations limiting the shared entanglement between a party with the rest, and Proposition 5.3 is in close connection to the Osborne-Verstraete relation [35].

Furthermore, these bounds are useful in the context of the 2-representability problem [14, 15, 113]. There, one wants to decide whether a set of two-body marginals is compatible with a common global state. While the 1-representability problem for qubits is solved (i.e., the same problem with a set of one-body marginals) [113] and yields a polytope of compatible eigenvalues, the k-representability problem for $k > 1$ is in general hard to decide [16]. However, Proposition 5.3 can be turned into a set of necessary conditions on the spectra of a set of two-body marginals in order to be compatible:

Corollary 5.4. *Let $\{\rho_{ij}\}_{1\leq i<j\leq n}$ denote a set of two-qubit states with eigenvalues $\lambda_k^{(ij)}$. Let their compatible one-qubit marginals be denoted by $\{\rho_i\}_{1\leq i\leq n}$ with spectra $\lambda_k^{(i)}$. If they originate from a common global state, then for the spectra of the matrices it holds that for all $1 \leq i \leq n$:*

$$2\sum_{j\neq i}\sum_{k=1}^{4}(\lambda_k^{(ij)})^2 \leq \sum_{j\neq i}\sum_{k=1}^{2}(\lambda_k^{(j)})^2 + (n-1)\sum_{k=1}^{2}(\lambda_k^{(i)})^2. \tag{5.12}$$

Proof. Note that for an n-qubit state ρ, $\text{Tr}(\rho^2) = \sum_{k=1}^{2^n}\lambda_k^2$, where λ_k are the eigenvalues of ρ. Additionally, for the two-body marginal ρ_{ij}, the purity is given by $\text{Tr}(\rho_{ij}^2) = \frac{1}{4}(1 + A_1^{(i)} + A_1^{(j)} + A_2^{(ij)})$.

This allows to write $A_2^{(ij)}$ as a function of purities and thus as a function of eigenvalues, i.e.

$$A_2^{(ij)} = 4\sum_{k=1}^{4}(\lambda_k^{(ij)})^2 - 2\sum_{k=1}^{2}[(\lambda_k^{(i)})^2 + (\lambda_k^{(j)})^2] + 1, \tag{5.13}$$

where $\lambda_k^{(ij)}$ are the eigenvalues of ρ_{ij} and $\lambda_k^{(i)}, \lambda_k^{(j)}$ the eigenvalues of ρ_i, ρ_j, respectively. Then for each fixed choice of i, the claim follows by using $\sum_{j=1, j\neq i}^{n} A_2^{(ij)} \leq n-1$ from Proposition 5.3. $\square$

5.3.2 Bounds on A_3 and higher sectors

Up to here, the results involved two-body correlations only. In this section, we generalize some of the statements to three-body correlations and the sector length A_3. Recalling the statement of Lemma 5.1, we know that if for some $n_0 \geq 3$, $A_3(\rho) \leq \binom{n_0}{3}$ for all ρ of n_0 qubits, then the same bound holds for all $n > n_0$ as well. The question arises whether such an n_0 exists. For $n = 3$, $A_3(|\text{GHZ}\rangle) = 4 > \binom{3}{3} = 1$. For $n = 4$, there exist states with $A_3 = 8 > \binom{4}{3} = 4$, for example the highly entangled state [26, 114, 115]

$$|\chi\rangle = \frac{1}{\sqrt{6}}(|0001\rangle + |0010\rangle + |0100\rangle + |1000\rangle + \sqrt{2}|1111\rangle). \tag{5.14}$$

But for $n \geq 5$, the bound holds. To show this, we need to introduce an additional technique, namely the so-called shadow inequalities [116].

Let M and N be two positive semidefinite hermitian operators acting on an n-particle space. Then for all $T \subset \{1, \ldots, n\}$ [116, 117],

$$\sum_{S\subset\{1,...,n\}} (-1)^{|S\cap\bar{T}|} \text{Tr}[\text{Tr}_{\bar{S}}(M)\,\text{Tr}_{\bar{S}}(N)] \geq 0. \tag{5.15}$$

Origin	Eq. (5.7)	Proposition 5.2
Min. n	$n \geq 1$	$n \geq 3$
Sector len.	$A_1 \leq n$	$A_2 \leq \binom{n}{2}$
Lin. ent.	$S_{\mathrm{L}}^{(1)} \geq 0$	$S_{\mathrm{L}}^{(2)} \geq \frac{n-1}{2} S_{\mathrm{L}}^{(1)}$
Mut. ent.	$I_{\mathrm{L}}^{(1)} \geq 0$	$I_{\mathrm{L}}^{(2)} \leq \frac{n-1}{2} I_{\mathrm{L}}^{(1)}$
Origin	Proposition 5.5	Proposition 5.9
Min. n	$n \geq 5$	$n \geq 3$
Sector len.	$A_3 \leq \binom{n}{3}$	$\binom{n}{3} + A_3 \geq \frac{1}{3}\binom{n-1}{2} A_1 + \frac{n-2}{3} A_2$
Lin. ent.	$S_{\mathrm{L}}^{(3)} \geq \frac{n-2}{2} S_{\mathrm{L}}^{(2)} - \frac{1}{4}\binom{n-1}{2} S_{\mathrm{L}}^{(1)}$	$S_{\mathrm{L}}^{(3)} \leq \frac{n-2}{3} S_{\mathrm{L}}^{(2)} - \frac{1}{3}\binom{n-1}{2} S_{\mathrm{L}}^{(1)}$
Mut. ent.	$I_{\mathrm{L}}^{(3)} \geq \frac{n-2}{2} I_{\mathrm{L}}^{(2)} - \frac{1}{4}\binom{n-1}{2} I_{\mathrm{L}}^{(1)}$	$I_{\mathrm{L}}^{(3)} \leq \frac{n-2}{3} I_{\mathrm{L}}^{(2)}$

TABLE 5.1: Translation of the various sector bounds into inequalities for linear entropy and mutual linear entropy.

Here, $\bar{S} = \{1, \ldots, n\} \setminus S$ and $\mathrm{Tr}_{\bar{S}}$ denotes the partial trace of systems $\bar{S}$.

Summing over all T with $|T| = k$ yields a set of inequalities $B_k \geq 0$:

$$B_k := \sum_{\substack{T,S \subset \{1,\ldots,n\}, \\ |T|=k}} (-1)^{|S \cap \bar{T}|} \mathrm{Tr}[\mathrm{Tr}_{\bar{S}}(M) \, \mathrm{Tr}_{\bar{S}}(N)] \geq 0. \tag{5.16}$$

Choosing $M = N = \rho$, the right-hand side can be evaluated in terms of the sector lengths to read [118, 119]

$$B_k = \frac{1}{2^n} \sum_{r=0}^{n} (-1)^r K_k(r;n) A_r \geq 0 \tag{5.17}$$

with the Kravchuk polynomials

$$K_k(r;n) = \sum_{j=0}^{k} (-1)^j 3^{k-j} \binom{r}{j} \binom{n-r}{k-j}. \tag{5.18}$$

For $k = 0$, $B_0 = \frac{1}{2^n}[\sum_{j=0}^{n}(-1)^j A_j] \geq 0$ is equivalent to the positivity of state inversion, introduced in Eq. (2.34). Note that other references denote the inequalities B_k by S_k. Here, we chose B_k instead in order to avoid confusion with the linear entropy.

Using these inequalities, we are in position to prove the following bound:

Proposition 5.5. *For all qubit states of $n \geq 5$, it holds that $A_3 \leq \binom{n}{3}$. For $n = 3$, the bound is given by $A_3 \leq 4$; for $n = 4$, it is given by $A_3 \leq 8$. The bounds are tight.*

Proof. For $n = 3$ and $n = 4$, we use a linear program that involves the purity $M_0 = 0$ from (5.6) and state inversion inequality $B_0 \geq 0$. For $n = 3$, these two equations read

$$1 + A_1 + A_2 + A_3 = 8, \tag{5.19}$$

$$1 - A_1 + A_2 - A_3 \geq 0. \tag{5.20}$$

Subtracting the second inequality from the first and using $A_1 \geq 0$, we obtain $A_3 \leq 4$. The same works for $n = 4$.

For $n \geq 5$, we prove the statement for $n = 5$. By use of Lemma 5.1, the result will then be true for larger n as well. We can assume that the total state is pure, as convex combinations of pure states will never increase any sector length. Using a linear program involving relations $M_j = 0$ for $j \in \{0, 1, 2\}$ from (5.6), $B_1 \geq 0$ reduces to $A_3 \leq 10 = \binom{5}{3}$.

Concerning the tightness, consider the GHZ state for $n = 3$ having $A_3 = 4$ and the state $|\chi\rangle$ for $n = 4$, given in Eq. (5.14). For $n \geq 5$, consider any product state like $|0\rangle^{\otimes n}$ with sector lengths $A_k = \binom{n}{k}$. $\qquad\square$

Numerically, a similar statement seems to hold for A_4 for states of at least 8 qubits, but using a linear program, one can show that shadow inequalities are insufficient to show it. Still, we conjecture:

Conjecture 5.6. For all k there exists an n_0, such that for all $n \geq n_0$, $A_k \leq \binom{n}{k}$ holds for states of n-qubits.

5.3.3 Bounds on A_n

Finally, we look at the full-body correlations of states, i.e. A_n of an n-qubit state. Lower bounds on this quantity can be used to detect entanglement [105, 120]. Upper bounds, however, were only known for the case of odd n until recently [120]. In this case, combining again the purity $M_0 = 0$ from (5.6) and state inversion inequality $B_0 \geq 0$ from (5.17) yields for odd n

$$2^{n-1} \geq \sum_{\substack{k \text{ odd,} \\ k \leq n}} A_k \geq A_n. \tag{5.21}$$

For example, the n-partite GHZ state for odd n fulfills $A_n = 2^{n-1}$, thus this bound is tight.

n	Constraint	Sector length	Linear entropy	Mutual entropy
2	Purity	$A_1 + A_2 \leq 3$	$S_L^{(2)} \geq 0$	$I_L^{(2)} \leq I_L^{(1)}$
2	State inv.	$A_1 - A_2 \leq 1$	$S_L^{(2)} \leq S_L^{(1)}$	$I_L^{(2)} \geq 0$
3	Purity	$A_1 + A_2 + A_3 \leq 7$	$S_L^{(3)} \geq 0$	$I_L^{(3)} \geq I_L^{(2)} - I_L^{(1)}$
3	State inv.	$A_1 - A_2 + A_3 \leq 1$	$S_L^{(3)} \geq S_L^{(2)} - S_L^{(1)}$	$I_L^{(3)} \geq 0$
3	Schmidt dec.	$A_2 \leq 3$	$S_L^{(2)} \geq S_L^{(1)}$	$I_L^{(2)} \leq I_L^{(1)}$
3	SSSA	$A_1 + A_2 \leq 3(1 + A_3)$	$3S_L^{(3)} \leq 2S_L^{(2)} - S_L^{(1)}$	$I_L^{(3)} \leq \frac{1}{3}I_L^{(2)}$

TABLE 5.2: Translation of the complete sets of sector bounds of two- and three-qubit states into linear entropy and mutual linear entropy inequalities. The trivial bounds $A_j \geq 0$ are omitted. The translation among the representations is given by (5.33) - (5.34). The constraints are due to purity, state inversion [$B_0 \geq 0$ from (5.17)], Schmidt decomposition [(5.6)] and symmetric strong subadditivity (SSSA, Theorem 5.8).

For n even, this trick does not work. In this case, the GHZ state fulfills $A_n = 2^{n-1} + 1$, which is why it was conjectured in [120] that this is the upper bound. Here, we show that this is true at least up to $n = 10$.

For small n, this follows from the shadow inequality B_1 in (5.17). Evaluating $B_1 \geq 0$ for $n = 2$ yields

$$A_2 \leq 3 = 2^{2-1} + 1, \tag{5.22}$$

which is the well known bound on the two-body correlations in two-qubit states and is compatible with the conjecture. For $n = 4$, $B_1 \geq 0$ yields

$$A_4 \leq 3 - 2A_1 + A_2 \leq 3 + \binom{4}{2} = 2^{4-1} + 1 = 9, \tag{5.23}$$

where we used the result of Proposition 5.2. For higher n, we observe that for every state ρ, the even mixture with its state inversion from Eq. (2.34), $\hat{\rho} = \frac{1}{2}(\rho + \tilde{\rho})$ has the same even correlations P_{2k} and vanishing odd correlations P_{2k+1}. This fact was established already in Chapter 4. Thus, the bounds on an even sector length can be obtained by setting w.l.o.g. the odd correlations to zero, i.e. $A_{2k+1} = 0$.

For $n = 6$, we investigate $B_1 \geq 0$ and $B_3 \geq 0$ and combine them to eliminate A_4. This yields, using Proposition 5.2 again,

$$A_6 \leq 18 + A_2 \leq 33. \tag{5.24}$$

For $n = 8$, we combine B_1, B_3 and B_5 to yield the bound, for $n = 10$ we combine B_k for $k = 1, 3, 5, 7$:

Theorem 5.7. *For n-qubit states with $n \leq 10$, n even, it holds that $A_n \leq 2^{n-1} + 1$. The bound is tight.*

If Conjecture 5.6 is true for $k = 4$ and $n_0 \leq 12$, as numerical calculation indicates, then the same method works for $n = 12$, $n = 14$, $n = 16$ as well.

Finally, we note that recently an alternative proof was found, establishing the bound for all even n [121].

5.3.4 Application to entanglement detection

Before continuing, we highlight some applications of the bounds found in this section to the detection of entanglement. As mentioned before, sector lengths are convex and invariant under local unitaries, making them useful for entanglement detection [105]. This can be exploited by noticing that for product states $\rho = \rho_A \otimes \rho_B$, where ρ_A consists of n_A and ρ_B of n_B particles, it holds that

$$A_k(\rho_A \otimes \rho_B) = \sum_{j=0}^{k} A_j(\rho_A) A_{k-j}(\rho_B),\tag{5.25}$$

where we set $A_k(\rho) = 0$ if k exceeds the number of particles in ρ.

For $n_A = n_B = 1$, $A_2(\rho_A \otimes \rho_B) = A_1(\rho_A)A_1(\rho_B)$. Due to convexity of the sector lengths, it follows that

$$A_2 \leq 1 \tag{5.26}$$

for all separable states.

For more than two parties, different entanglement structures occur, as explained in Section 2.5.2. Here, we are interested in detecting genuine multipartite entanglement, thus, we want to find a criterion excluding biseparability.

For $n = 3$, we showed that $A_3 \leq 4$, on the other hand, all biseparable states obey

$$A_3 \leq 3,\tag{5.27}$$

as for states $\rho = \rho_A \otimes \rho_{BC}$ it holds that $A_3(\rho) = A_1(\rho_A)A_2(\rho_{BC}) \leq 3$. Therefore, also in this case, the highest sector length can be used to detect genuine multipartite entanglement.

For $n = 4$, however, the situation is different: One can show with the same argument as above that biseparable states fulfill $A_4 \leq 9$, an example is given in Section 5.4.5. But, as seen before, $A_4 \leq 9$ is already the bound for all states. Thus, A_4 does not allow for detection of genuine multipartite entanglement. However, there is a nontrivial biseparability bound on A_3 of 7. To see this, we have to consider two possibilities. On

the one hand, product states of the form $\rho_A \otimes \rho_{BCD}$ fulfill

$$A_3(\rho_A \otimes \rho_{BCD}) = A_3(\rho_{BCD}) + A_1(\rho_A)A_2(\rho_{BCD}) \leq 4 + 3 = 7, \qquad (5.28)$$

where we used the previously derived bounds of $A_1 \leq n$, as well as $A_2 \leq 3$ and $A_3 \leq 4$ for three-qubit states. On the other hand, product states of the form $\rho_{AB} \otimes \rho_{CD}$ fulfill

$$A_3(\rho_{AB} \otimes \rho_{CD}) = A_1(\rho_{AB})A_2(\rho_{CD}) + A_2(\rho_{AB})A_1(\rho_{CD}) \qquad (5.29)$$
$$\leq A_1(\rho_{AB})[3 - A_1(\rho_{CD})] + A_1(\rho_{CD})[3 - A_1(\rho_{AB})] \qquad (5.30)$$
$$\leq 6. \qquad (5.31)$$

Here, we have used the purity bound $A_1 + A_2 \leq 3$ and the bound $A_1 \leq 2$ for two-qubit states. Instead, for general four-qubit states, the bound of Proposition 5.5 due to positivity of the state is given by $A_3 \leq 8$. Therefore, not the highest, but the next-to-highest correlations allow for entanglement detection. This already yields an entanglement criterion which can detect states not detectable by known criteria using the sector lengths [105], an example being again the highly entangled state $|\chi\rangle$ from Eq. (5.14) with sector length configuration $(A_1, A_2, A_3, A_4) = (0, 2, 8, 5)$. Note that it is known that even vanishing highest order correlations do not exclude genuine multipartite entanglement [122–125]. Finally, let us note that while sector lengths are quadratic expressions in the quantum state, the additional knowledge of similar quantities of higher order, i.e. higher moments, allows for more refined entanglement detection. This will be explored in more detail in Chapter 6.

5.4 Bounds on linear combinations of sector lengths

We now turn to the problem of finding bounds on linear combinations of sector lengths. This is related to the question of whether linear constraints are enough to fully characterize the set, meaning that the set of states forms a polytope in the sector length picture. As mentioned before, sector lengths are in one-to-one correspondence with linear entropies and the mutual entropy for linear entropies. It turns out that some of the obtained inequalities are easier understood in the language of linear entropies.

5.4.1 Translation into entropy inequalities

Recall from Section 2.7 that the linear entropy of a state ρ is defined as $S_{\mathrm{L}}(\rho) = 2[1 - \mathrm{Tr}(\rho^2)]$. As $\mathrm{Tr}(\rho^2)$, the purity of ρ, is up to a factor equal to the sum of all sector lengths of ρ, we can express S_{L} in terms of sector lengths. We define the sector entropy of sector k by summing over all linear entropies of reduced states of k particles, i.e.

$$S_{\mathrm{L}}^{(k)} := \sum_{\substack{K \subset \{1,\dots,n\} \\ |K| = k}} S_{\mathrm{L}}(\rho_K)$$
$$= \frac{1}{2^{k-1}} \left[\binom{n}{k} 2^k - \sum_{j=0}^{k} \binom{n-j}{k-j} A_j \right], \tag{5.32}$$

which can be inverted to yield

$$A_k = \binom{n}{k} - \sum_{j=1}^{k} (-1)^{k-j} 2^{j-1} \binom{n-j}{k-j} S_{\mathrm{L}}^{(j)}. \tag{5.33}$$

Furthermore, it will be useful to define the k-partite mutual linear entropy,

$$I_{\mathrm{L}}^{(k)} := \sum_{j=1}^{k} (-1)^{j-1} \binom{n-j}{k-j} S_{\mathrm{L}}^{(j)}. \tag{5.34}$$

For $k = 2$ and $n = 2$, it resembles the usual mutual entropy, $I_{\mathrm{L}}^{(2)} = S_{\mathrm{L}}(\rho_A) + S_{\mathrm{L}}(\rho_B) - S_{\mathrm{L}}(\rho_{AB})$. Note that the definition is analogous to the mutual information of von Neumann entropy. However, in the case of linear entropy, the name mutual linear entropy is preferred, as the quantity is not additive and does not vanish for product states [126]. Table 5.1 lists the non-trivial bounds on the sector lengths found above, translated into the two other representations.

Using the results above, we can now characterize the allowed values of sector length tuples $(A_1, \dots, A_n)$ for two-qubit and three-qubit states. It turns out that in both cases the set of admissible values is a convex polytope. This is interesting as the convexity is not trivial because the sector lengths are nonlinear in the state. In addition, it is surprising that only a finite number of linear constraints corresponding to the surfaces of the polytope is sufficient for a full description. This reminds of a similar polytope for separable states if variances of collective spin-observables are considered [111].
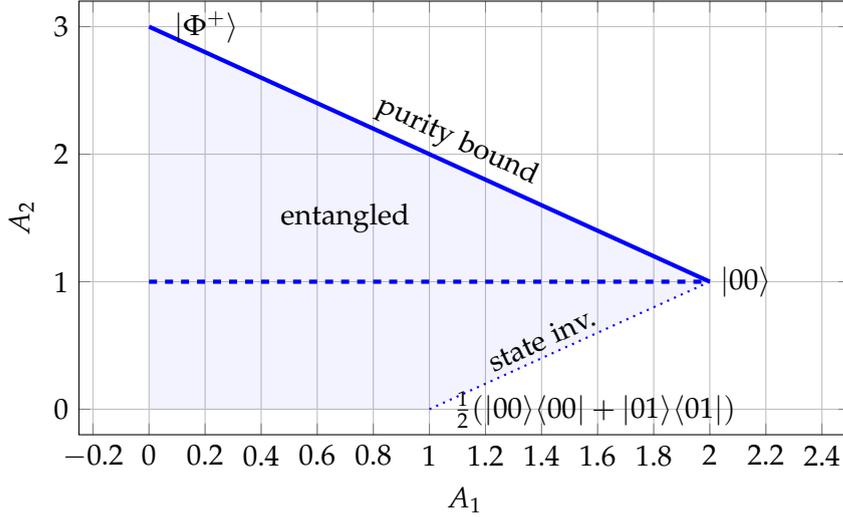
FIGURE 5.1: The total set of attainable pairs A_1 and A_2 in two-qubit states, displayed in light blue.

5.4.2 Characterization of two-qubit states

It is easy to verify that in the case of $n = 2$, pure product states obey $A_1 = 2$ and $A_2 = 1$ [see (5.25)]. The Bell state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ obeys $A_1 = 0$, $A_2 = 3$. The purity bound $\text{Tr}(\rho^2) \leq 1$ translates into $1 + A_1 + A_2 \leq 4$. By superposing a pure product state and the Bell state, one can obtain pure states with $A_1 \in [0, 2]$ and $A_2 = 3 - A_1$. Exceeding the value of 2 for A_1 is impossible due to the bound $A_1 \leq n$ from Eq. (5.7).

However, the state inversion bound $B_0 \geq 0$ from (5.17) yields another bound on A_1 and A_2 due to positivity; namely $A_1 - A_2 \leq 1$. States reaching this bound are given by the family $(1 - p)|00\rangle\langle00| + p|01\rangle\langle01|$. All other states can be reached by mixing the boundary states with the maximally mixed state $\mathbb{1}/4$, as these states lie on a straight line connecting the boundary state with the origin. This yields the whole set of admissible pairs of A_1 and A_2 and is displayed in Fig. 5.1.

5.4.3 Characterization of three-qubit states

While all the bounds in the case of two qubits are known, the case of three qubits shows an interesting new result that is connected to strong subadditivity of linear entropy.

We start by collecting all inequalities that we know: The state inversion bound $B_0 \geq 0$ from (5.17), the bound $A_1 \leq 3$, the shadow inequality $B_1 \geq 0$ and the bound from
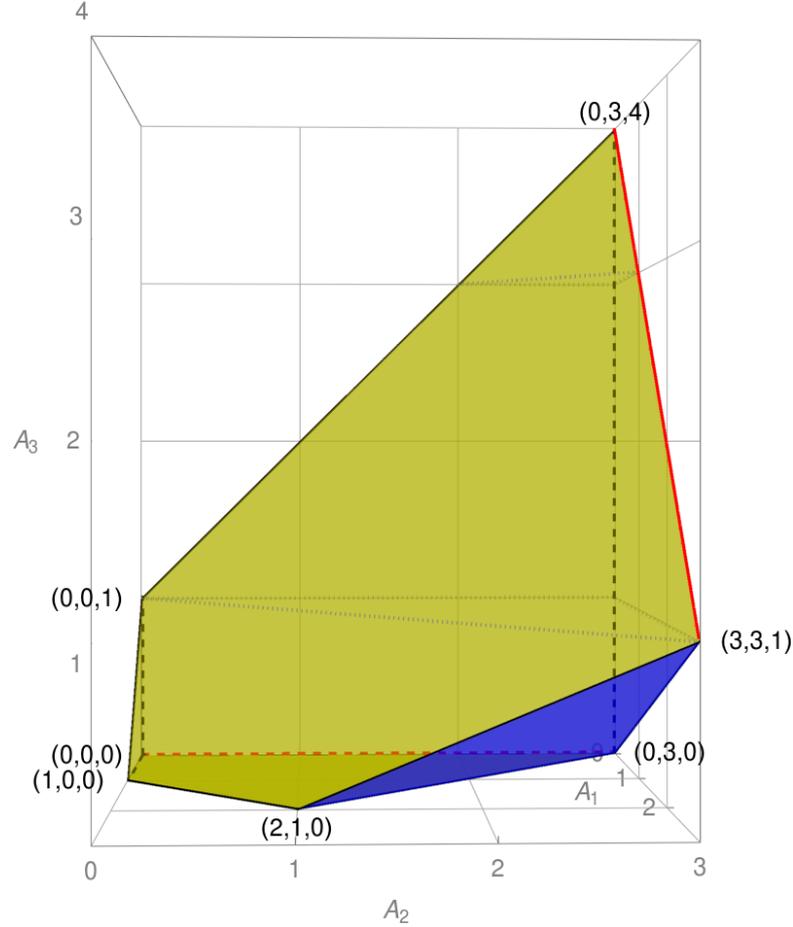
FIGURE 5.2: The polytope of admissible sector length configurations of three-qubit states. The yellow surface corresponds to the state inversion bound $B_0 \propto 1 - A_1 + A_2 - A_3 \geq 0$, the blue surface originates from symmetric strong subadditivity [(5.37)]. Pure states lie on the red solid line connecting $(3, 3, 1)$ (product states) and $(0, 3, 4)$ (GHZ state). The A_2-axis is displayed by a red dashed line. States above the lower gray dotted line are not fully separable, states above the upper gray dotted line are genuinely multipartite entangled. The surface of the polytope is displayed in Fig. 5.3.

Proposition 5.2 yield a set of four inequalities,

$$1 - A_1 + A_2 - A_3 \geq 0, \qquad A_1 \leq 3, \tag{5.35}$$

$$9 - 5A_1 + A_2 + 3A_3 \geq 0, \qquad A_2 \leq 3, \tag{5.36}$$

from which the bound $\mathrm{Tr}(\rho^2) \leq 1$ can be obtained using a linear program. These inequalities define a polytope in the three-dimensional space of tuples (A_1, A_2, A_3).

However, as numerical search indicates, these bounds are not tight. As it turns out, there is a single additional linear constraint replacing the constraint $B_1 \geq 0$.

Theorem 5.8. *For 3-qubit states, it holds that*

$$A_1 + A_2 \leq 3(1 + A_3). \tag{5.37}$$

Proof. Consider the map

$$\rho' = M(\rho) := (YY\mathbb{1})\rho^{\mathrm{T}_{12}}(YY\mathbb{1}) + (Y\mathbb{1}Y)\rho^{\mathrm{T}_{13}}(Y\mathbb{1}Y) + (\mathbb{1}YY)\rho^{\mathrm{T}_{23}}(\mathbb{1}YY), \qquad (5.38)$$

where $\rho^{\mathrm{T}_{ij}}$ is the partial transpose of ρ w.r.t. systems i and j. This map can be seen as a sum of partial state inversions of subsystems of size two, flipping the sign of the Pauli matrices of that particular subsystems. Using the Bloch decomposition, it can easily be seen that $\mathrm{Tr}(\rho\rho') = \frac{1}{8}(3 - A_1 - A_2 + 3A_3)$. Note that the map defined above is not positive, however, we will show that $\mathrm{Tr}(\rho\rho') \geq 0$ for all ρ, yielding the claim.

To that end, we consider the Choi matrix η of the map, given by Eq. (2.52) as

$$\eta = (\mathbb{1} \otimes M)(|\phi^+\rangle\langle\phi^+|) \qquad (5.39)$$

with $|\phi^+\rangle = \frac{1}{\sqrt{8}}\sum_{i=0}^{7}|ii\rangle$. The map can be reconstructed according to Eq. (2.53) via $M(\rho) = 2^3 \mathrm{Tr}_A[(\rho^{\mathrm{T}} \otimes \mathbb{1})\eta]$. Thus, the quantity in question can be written in terms of the Choi matrix as $\mathrm{Tr}(\rho\rho') = 2^3 \mathrm{Tr}[(\rho \otimes \rho)\eta^{\mathrm{T}_A}]$. As M is not positive, η is not positive as well, and one can directly calculate that η^{T_A} has a single negative eigenvalue of $-3/2$. Nevertheless, it is positive for symmetric product states $\rho \otimes \rho$. To see this, we use an SDP to minimize $\mathrm{Tr}(\sigma\eta^{\mathrm{T}_A})$ over symmetric states σ and trying to enforce the product structure on σ using some relaxations of this property.

To begin with, the matrix η^{T_A} can be written in Bloch decomposition as

$$
\begin{aligned}
\eta^{\mathrm{T}_A} \propto\; & 3\mathbb{1}\mathbb{1}\mathbb{1}\,\mathbb{1}\mathbb{1}\mathbb{1} && - \sum_{a\in\{x,y,z\}} \sigma_a\mathbb{1}\mathbb{1}\,\sigma_a\mathbb{1}\mathbb{1} && - \sum_{a\in\{x,y,z\}} \mathbb{1}\sigma_a\mathbb{1}\,\mathbb{1}\sigma_a\mathbb{1} && - \sum_{a\in\{x,y,z\}} \mathbb{1}\mathbb{1}\sigma_a\,\mathbb{1}\mathbb{1}\sigma_a \\
& - \sum_{a,b\in\{x,y,z\}} \sigma_a\sigma_b\mathbb{1}\,\sigma_a\sigma_b\mathbb{1} && - \sum_{a,b\in\{x,y,z\}} \sigma_a\mathbb{1}\sigma_b\,\sigma_a\mathbb{1}\sigma_b && - \sum_{a,b\in\{x,y,z\}} \mathbb{1}\sigma_a\sigma_b\,\mathbb{1}\sigma_a\sigma_b \\
& + 3 \sum_{a,b,c\in\{x,y,z\}} \sigma_a\sigma_b\sigma_c\,\sigma_a\sigma_b\sigma_c. && && && (5.40)
\end{aligned}
$$

Note that due to the special symmetric form of the basis elements, the matrix can also be written as a combination of local flip operators. This allows to write the matrix also in terms of projectors onto the symmetric and antisymmetric subspaces. This representation of the problem is explained in more detail in Appendix B.

The matrix η^{T_A} exhibits many symmetries; it is symmetric under the exchange of the first three and the second three parties. Also, it is symmetric under any permutation among the first three parties, if the same permutation is applied to the second three parties as well. Furthermore, it is invariant under single qubit local unitaries $V\mathbb{1}\mathbb{1}V\mathbb{1}\mathbb{1}$ for $V \in \{X, Y, Z, \Pi, T, H\}$ where $\Pi = \mathrm{diag}(1, i)$, $T = \mathrm{diag}(1, \exp(i\pi/4))$ and H being the Hadamard gate.

All of these symmetries do not alter the product structure of $\rho \otimes \rho$ and can, therefore, be imposed for the optimal state as well.

Apart from the symmetries, we can try to impose the product structure of σ. However, this is a non-linear constraint and thus not exactly tractable by an SDP. Nevertheless, we find a set of linear constraints that brings us close enough to the set of product states to prove the claim.

First of all, product states are separable by definition and must have a positive partial transpose, i.e. $\sigma^{\mathrm{T}_A} \geq 0$ [127]. Next, using the positivity of Breuer-Hall maps, for separable states σ and skew symmetric unitaries U, i.e., $U^{\mathrm{T}} = -U$, it holds that $\sigma_{\mathrm{BH}} = \mathrm{Tr}_{4,5,6}(\sigma) \otimes \mathbb{1}\mathbb{1}\mathbb{1} - \sigma - (\mathbb{1}\mathbb{1}\mathbb{1} \otimes U)\sigma^{\mathrm{T}_B}(\mathbb{1}\mathbb{1}\mathbb{1} \otimes U^{\dagger}) \geq 0$ [128, 129]. It turns out that the choice of $U = YYY$ is suitable in our case.

As a last constraint, for product states, $\langle A \otimes A \rangle_{\rho \otimes \rho} = \langle A \rangle_{\rho}^2 \geq 0$ for all three-qubit observables A. Here, we consider the special choice of $A = X\mathbb{1}\mathbb{1}$. For product states, it should hold that $\langle A \otimes A \rangle_{\sigma} = \langle A \otimes \mathbb{1}\mathbb{1}\mathbb{1} \rangle_{\sigma}^2$, as σ is symmetric as noted before. To make this constraint linear, note that for Pauli observables, $|\langle A \rangle| \leq 1$. Thus, $\langle A \otimes A \rangle_{\sigma} \leq |\langle A \otimes \mathbb{1}\mathbb{1}\mathbb{1} \rangle_{\sigma}|$. Now, there are two possibilities. Either, the optimal state obeys $\langle A \otimes \mathbb{1}\mathbb{1}\mathbb{1} \rangle_{\sigma} \geq 0$ or $\langle A \otimes \mathbb{1}\mathbb{1}\mathbb{1} \rangle_{\sigma} \leq 0$. Therefore, we run the SDP twice, once with the constraint $\langle A \otimes A \rangle_{\sigma} \leq \langle A \otimes \mathbb{1}\mathbb{1}\mathbb{1} \rangle_{\sigma}$ and once with $\langle A \otimes A \rangle_{\sigma} \leq -\langle A \otimes \mathbb{1}\mathbb{1}\mathbb{1} \rangle_{\sigma}$.

To summarize, we run the following SDP:

$$
\begin{aligned}
\min_{\sigma} \quad & \mathrm{Tr}(\sigma \eta^{\mathrm{T}_A}) && (5.41) \\
\text{subject to} \quad & \sigma \geq 0, \\
& \sigma \text{ symmetric}, \\
& (V\mathbb{1}\mathbb{1}\, V\mathbb{1}\mathbb{1})\sigma(V\mathbb{1}\mathbb{1}\, V\mathbb{1}\mathbb{1}) = \sigma \text{ for } V \in \{X, Y, Z, \Pi, T, H\}, \\
& \sigma^{\mathrm{T}_A} \geq 0, \sigma_{\mathrm{BH}} \geq 0, \\
& \mathrm{Tr}[(A \otimes A)\sigma] \geq 0 \text{ for all observables } A, \\
& \mathrm{Tr}[(X\mathbb{1}\mathbb{1}\, X\mathbb{1}\mathbb{1})\sigma] \leq \pm \mathrm{Tr}[(X\mathbb{1}\mathbb{1}\, \mathbb{1}\mathbb{1}\mathbb{1})\sigma].
\end{aligned}
$$

Here, the symmetry constraint means both, symmetric under exchange of the first three with the last three parties, as well as symmetric under exchange among the first three and the same exchange among the last three parties. The last three constraints are the linear approximations of the product structure, where the $\pm$ in the last constraint means that we run the SDP once for each choice. Both cases yield a minimal trace of zero within machine precision, proving the claim. $\qquad \square$

Note that the method presented here can also be used to prove bounds for arbitrary linear combinations $\sum_k c_k A_k$. In this case, one has to choose $\eta^{T_A} = \sum_k c_k \sum_{\Xi_k} \Xi_k \otimes \Xi_k$, where the inner sum iterates over all Pauli operators Ξ_k acting on k of the parties nontrivially, as well as choosing appropriate relaxations of the product structure.

The polytope defined by (5.35)-(5.37) is displayed in Fig. 5.2 and Fig. 5.3.

It remains to show that the obtained polytope is tight by showing the existence of states for every point in the polytope, including the boundary. In fact, it suffices to find states on the yellow and the blue surface in Fig. 5.2, corresponding to the state inversion bound $1 - A_1 + A_2 - A_3 \geq 0$ and the bound $A_1 + A_2 \leq 3(1 + A_3)$ from Theorem 5.8. This follows from the observation that for every state ρ, also the state inversion $\tilde{\rho} := Y^{\otimes n} \rho^T Y^{\otimes n}$ is a proper state, with the same coefficients in the Bloch decomposition up to a minus sign for all coefficients of an odd number of Pauli operators as shown in Chapter 4. Thus, the family $\rho(p) = p\rho + (1-p)\tilde{\rho}$ corresponds to states with sector lengths $((1-2p)^2 A_1(\rho), A_2(\rho), (1-2p)^2 A_3(\rho))$, yielding a family of states lying on a straight line connecting a point in the polytope with the point $(0, A_2, 0)$ on the red dashed A_2-axis with the same value of A_2. Therefore, states filling the yellow and the blue surface and their straight-line connections to the A_2-axis fill the whole polytope.

First, we give families of states covering the yellow surface, corresponding to the state inversion bound:

$$\rho_A(p, \alpha) = p|G(\alpha)\rangle\langle G(\alpha)| + \frac{1-p}{8}(\mathbb{1} + XXX), \tag{5.42}$$

$$\rho_B(p, \alpha) = p|H(\alpha)\rangle\langle H(\alpha)| + \frac{1-p}{8}[\mathbb{1} + \cos(\alpha)Z\mathbb{1}\mathbb{1} + \sin(\alpha)XXX], \tag{5.43}$$

$$\rho_C(p, q) = \frac{p}{2}\mathbb{1} \otimes |00\rangle\langle 00| + \frac{q}{2}\mathbb{1} \otimes |01\rangle\langle 01| + (1 - p - q)|000\rangle\langle 000|, \tag{5.44}$$

with the abbreviations

$$|G(\alpha)\rangle = \frac{1}{\sqrt{1 + \cos(\frac{\alpha}{2})\sin(\frac{\alpha}{2})}}\left[\cos(\frac{\alpha}{2})|GHZ\rangle + \sin(\frac{\alpha}{2})|+++\rangle\right], \tag{5.45}$$

$$|H(\alpha)\rangle = \left[\cos(\frac{\alpha}{2})|0\rangle - \sin(\frac{\alpha}{2})|1\rangle\right] \otimes |+-\rangle, \tag{5.46}$$

with $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$, and $0 \leq p \leq 1$, $0 \leq q \leq p$ and $0 \leq \alpha \leq \pi$.

Second, the blue surface corresponding to Theorem 5.8 is spanned by the states

$$\rho_D(\alpha, \beta) = \frac{p}{2}|\Phi(\alpha)\rangle\langle\Phi(\alpha)| \otimes \mathbb{1} + \frac{1-p}{2}|\Phi(\beta)\rangle\langle\Phi(\beta)| \otimes \mathbb{1} \tag{5.47}$$
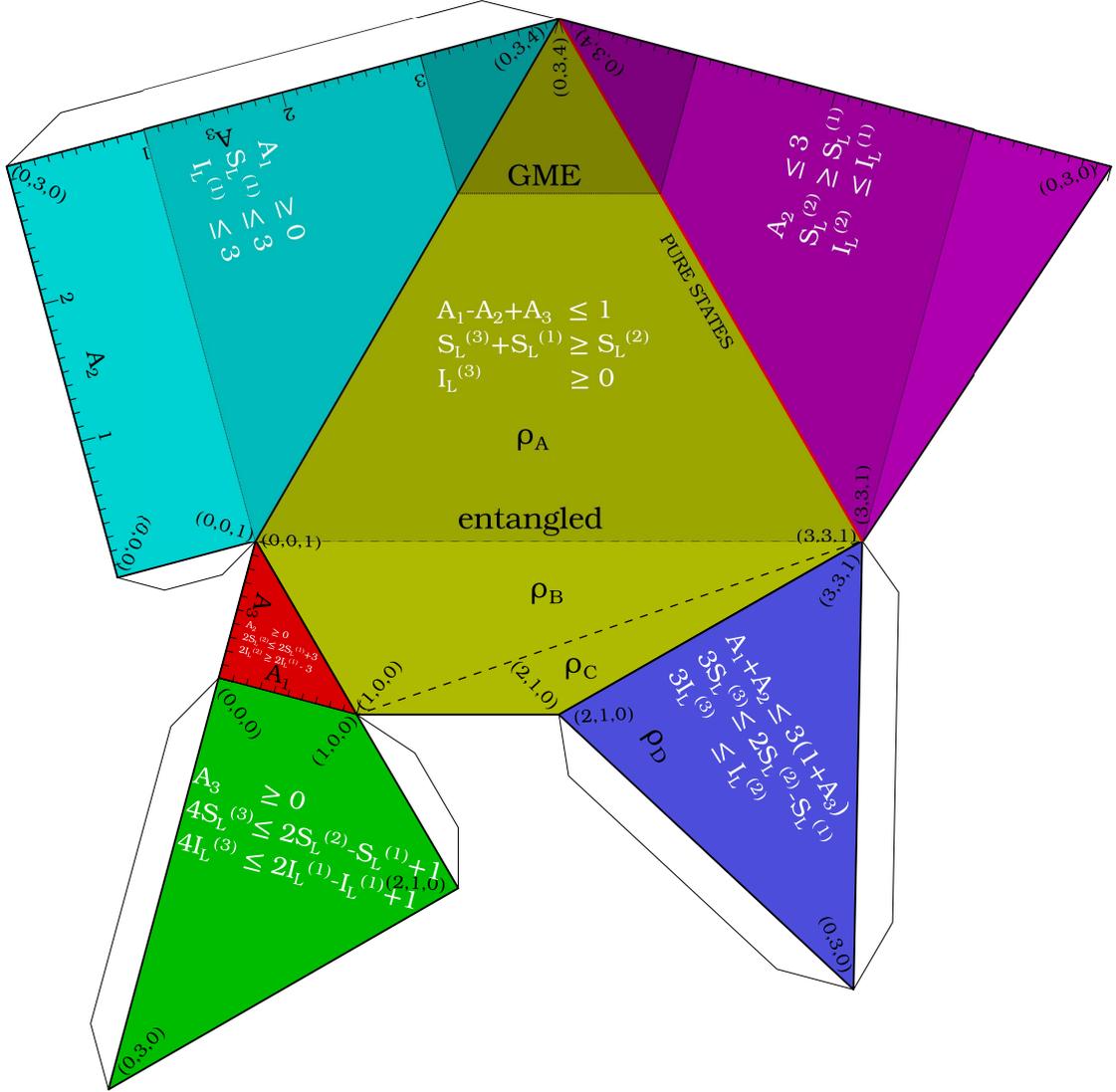
FIGURE 5.3: The surface of the polytope of admissible sector lengths of three-qubit states with the regions covered by the families of states (5.42) - (5.44) on the yellow surface corresponding to the state inversion bound $A_1 - A_2 + A_3 = 1$. The family of states (5.47) covers the whole of the blue surface corresponding to symmetric strong subadditivity $A_1 + A_2 \leq 3(1 + A_3)$.

where $|\Phi(\alpha)\rangle = \cos(\alpha/2)|00\rangle + \sin(\alpha/2)|11\rangle$ and $p = \sin(\beta)/[\sin(\alpha) + \sin(\beta)]$. The angles α and β take arbitrary values between 0 and π.

All other states can be reached by mixing these states with their inverted states, defined by $\tilde{\rho} := Y^{\otimes n} \rho^{\mathrm{T}} Y^{\otimes n}$.

5.4.4 Connection to strong subadditivity

Theorem 5.8 is closely related to strong subadditivity (SSA). One formulation of SSA for the specially chosen particle B is $S(\rho_{ABC}) + S(\rho_B) \leq S(\rho_{AB}) + S(\rho_{BC})$. However,

Num.	A_1	A_2	A_3	A_4	State(s)
1	0	6	0	9	$|\text{GHZ}_4\rangle, |\Phi^+\rangle \otimes |\Phi^+\rangle, |s_4\rangle$
2	0	5	2	8	
3	0	4	4	7	$\cos(\alpha)|s_4\rangle + \sin\alpha|\chi\rangle$
4	0	3	6	6	
5	0	2	8	5	$|\chi\rangle$
6	1	6	1	7	
7	2	6	2	5	$\cos(\beta)|0000\rangle + \sin(\beta)|1111\rangle$
8	3	6	3	3	
9	1	3	7	4	$|W_4\rangle, |\text{GHZ}\rangle \otimes |0\rangle$
10	2	4	6	3	$|\Phi^+\rangle \otimes |00\rangle$
11	3	5	5	2	$[\cos(\pi/8)|00\rangle + \sin(\pi/8)|11\rangle] \otimes |00\rangle$
12	4	6	4	1	$|0000\rangle$

TABLE 5.3: List of pure four-qubit states realizing integer tuples of sector lengths at the boundary of the pure state region displayed in Fig. 5.4. In the list, $|\text{GHZ}_4\rangle = \sqrt{2}^{-1}(|0000\rangle + |1111\rangle)$, $|s_4\rangle = \sqrt{3}^{-1}(|0011\rangle + |1100\rangle - |\Psi^+\rangle \otimes |\Psi^+\rangle)$, $|\chi\rangle$ is given in Eq. (5.14) and $|W_4\rangle = 2^{-1}(|0001\rangle + |0010\rangle + |0100\rangle + |1000\rangle)$. The entries depending on α and β denote families of states covering the whole boundary, and the integer tuples are obtained for suitable choices of the angles.

it holds for the von Neumann entropy only and fails to hold for the linear entropy, a counterexample being the state $|\Phi^+\rangle\langle\Phi^+| \otimes \frac{1}{2}$. Nevertheless, summing SSA over all particles to symmetrize it, yields

$$3S_L(\rho_{ABC}) + S_L(\rho_A) + S_L(\rho_B) + S_L(\rho_C) \leq 2[S_L(\rho_{AB}) + S_L(\rho_{AC}) + S_L(\rho_{BC})], \quad (5.48)$$

or in our language,

$$3S_L^{(3)} + S_L^{(1)} \leq 2S_L^{(2)}. \quad (5.49)$$

This is, using the correspondence (5.33), equivalent to the statement of Theorem 5.8. Thus, linear entropy for three-qubit states obeys a symmetric SSA, which implies that usual SSA holds for at least one choice of special particle. Another formulation in terms of mutual linear entropies yields the inequality $I_L^{(3)} \leq \frac{1}{3}I_L^{(2)}$.

We state the full set of restrictions for $n = 2$ and $n = 3$ in all three representations in Table 5.2.

Finally, note that the statement of Theorem 5.8 can be generalized to states of more particles using the same induction trick as in the proof of Lemma 5.1. We get:

Corollary 5.9. *For n-qubit states with $n \geq 3$, it holds that $I_L^{(3)} \leq \frac{n-2}{3}I_L^{(2)}$.*

In terms of sector lengths, the bound reads

$$\binom{n}{3} - \frac{1}{3}\binom{n-1}{2}A_1 - \frac{1}{3}\binom{n-2}{1}A_2 + A_3 \geq 0. \quad (5.50)$$
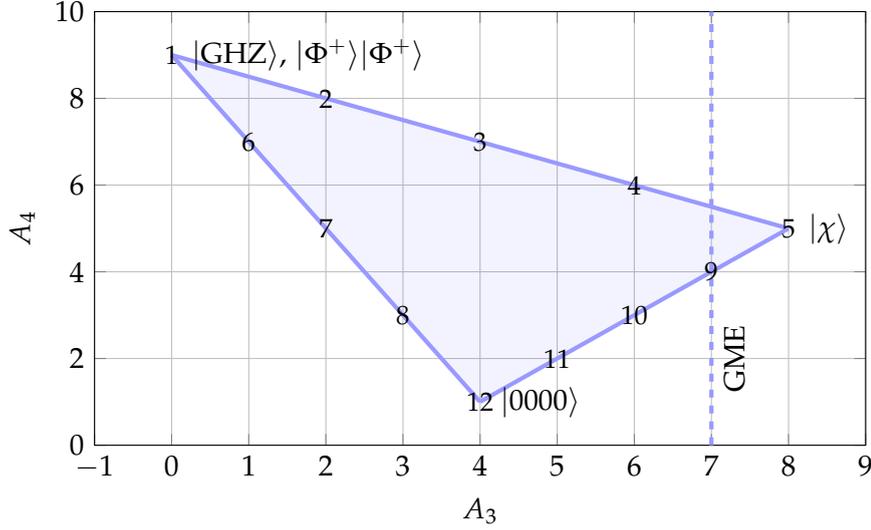
FIGURE 5.4: The region of (A_3, A_4)-pairs of pure four-qubit states. The sector lengths A_1 and A_2 are determined by Eqs. (5.51) and (5.52). The numbers indicate the row in Table 5.3 containing pure state realisations of the respective points.

Using a linear program, it is evident that this equation is stronger than the shadow inequalities (5.17). As this bound is complementary to the bound $A_3 \leq \binom{n}{3}$, we list it as well in Table 5.1.

5.4.5 A list of pure four-qubit states

While a complete characterization of admissible sector lengths of four-qubit states is out of the scope of this chapter, it is nevertheless instructive to consider the subset of pure states only.

From the purity relations $M_0 = 0$ and $M_1 = 0$ from Eq. (5.6) we obtain two independent relations among the A_i, namely

$$A_1 = -\frac{1}{3}A_3 - \frac{2}{3}A_4 + 6, \tag{5.51}$$

$$A_2 = -\frac{2}{3}A_3 - \frac{1}{3}A_4 + 9. \tag{5.52}$$

Furthermore, according to Proposition 5.2, we have $A_2 \leq 6$, translating into $2A_3 + A_4 \geq 9$. We are now in position to plot the remaining (A_3, A_4) plane. For each integer pair of (A_3, A_4) on the boundary of the region, we list some pure state realizations. Recall that while A_4 itself is incapable of detecting genuine multipartite entanglement, a value of $A_3 > 7$ indicates GME.

The plot is visible in Fig. 5.4, the list of states is given in Table 5.3.

5.5 Conclusions

In this chapter, we showed how to combine methods from quantum mechanics, coding theory and semidefinite programming to obtain strict bounds on linear combinations of sector lengths for multi-qubit systems. As a result, we obtained a full characterization of the allowed tuples of sector lengths for $n \leq 3$, where for $n = 3$ one of the constraints is related to a symmetrized version of strong subadditivity of linear entropies. Our results can be understood in the language of entropy inequalities and monogamy relations, they can also be used in the context of entanglement detection and the representability problem.

Our results highlight several problems for further research. First of all, the natural question of a complete characterization of sector bounds for $n \geq 4$, but also for higher-dimensional systems beyond qubits arises. The notion of sector lengths can be extended to higher-dimensional states as well, and many of the techniques like state inversion can be generalized. This has been used in the past to obtain some bounds [101, 117], however, a complete characterization is still out of reach. Interestingly, we found that for $n \leq 3$, the allowed region of sector bounds turned out to be a polytope, perfectly described by a few linear constraints. The reason for this remains elusive and deserves further attention, as it may yield deep insight into the complicated structure of the positivity constraints. It might well be that this is a feature exclusive to qubit systems, or systems of few particles only. Apart from a similar characterization of higher-dimensional states of more parties, a deeper understanding of the associated entropy inequalities is crucial. For instance, the question of whether the inequality holds for other entropies is relevant.

Finally, we used the bounds on the individual sector lengths for the task of entanglement detection and showed, for instance, that A_4 alone does not allow for entanglement detection in four-qubit states. The question of whether linear combinations of sector lengths allow for better entanglement criteria in this scenario is worth to be investigated in the future.

6 Learning about entanglement from higher moments

Prerequisites

6.1 Introduction

An ongoing challenge in quantum information is the detection of entanglement in quantum states. While many criteria exist, their experimental realization remains a major challenge in contemporary setups.

One particular difficulty arises for setups aiming to prove entanglement in quantum states shared between spatially separated parties, for example in the setting of quantum cryptography. Many entanglement criteria, especially those using Bell inequalities and often also those involving witnesses, require the parties to align their measurement apparatus [26, 130, 131], which is a technically challenging task.

In order to solve this issue, several different approaches have been used, like using local measurements only under the assumption that the global state is pure [72], or encoding the physical state into a logical subspace that is protected against rotations [132, 133]. Another method that we have exploited already in Chapter 5 is the formulation of LU-invariant entanglement criteria using correlations [8, 105, 123, 134–138]. Such criteria are sometimes called reference frame independent, as they can be evaluated without alignment of the measurements apparatus [139]. However, a drawback might be that the individual parties need good control over their measurements. This might be the case if one is required to measure in orthogonal measurement directions.

In this chapter, we will define a family of LU-invariants with the additional advantage that they can be evaluated using random measurement settings at the local sites, and use this family for the task of entanglement detection as follows. Typical experimental setups yield more data than designed for. For example, measuring the sector length

A_2 in a two-qubit state is equivalent to random measurements on both of the parties in a sense to be defined in the next section. The corresponding measurement data yields not only the mean value but also a distribution of measurement results. Good knowledge of the distribution, in turn, yields a set of its higher moments, forming higher-degree LU-invariants of the state.

Fig. 6.1 displays the simulated distribution of such randomized measurements for product states, the two-body marginal of the W-state

$$|W\rangle = \frac{1}{\sqrt{3}}(|100\rangle + |010\rangle + |001\rangle), \tag{6.1}$$

as well as the Werner state [140]

$$\rho_W(p) = p|\Phi^+\rangle\langle\Phi^+| + \frac{1-p}{4}\mathbb{1} \otimes \mathbb{1} \tag{6.2}$$

for $p = \frac{1}{\sqrt{3}}$. All of these distributions have a vanishing mean value and identical variances, which are equivalent to the sector length A_2 as we will show later. However, the distribution for the entangled W-state marginal and the entangled Werner state clearly differ from the distribution of the product state. While this difference is not visible in the first two moments (the mean value and the variance), and therefore not detectable by any criterion using the sector length A_2, it manifests itself in the higher moments of the distributions.

These findings motivate to consider higher moments of randomized measurements for the task of entanglement detection in bipartite systems in this chapter. To that end, we begin with the definition of a set of higher-degree invariants using moments of random correlations. We then introduce spherical t-designs to transform the abstractly defined moments into finite sums of powers of mean values. Finally, we use a subset of the invariants of degree two (sector lengths) and four to derive improved entanglement criteria. In fact, these criteria can be regarded as a refinement of the criterion in Eq. (5.26).

6.2 Moments of random correlation measurements

To begin with, we define a family of intrinsically LU-invariant numbers for an arbitrary n-qubit state. To that end, assume that each party $k = 1, \ldots, n$ picks a random measurement basis by picking a random unitary $U_k \in U(2)$ according to the Haar measure, and defining the measurement basis $|b_i\rangle_k = U_k|i\rangle_k$ with $i \in \{0,1\}$.
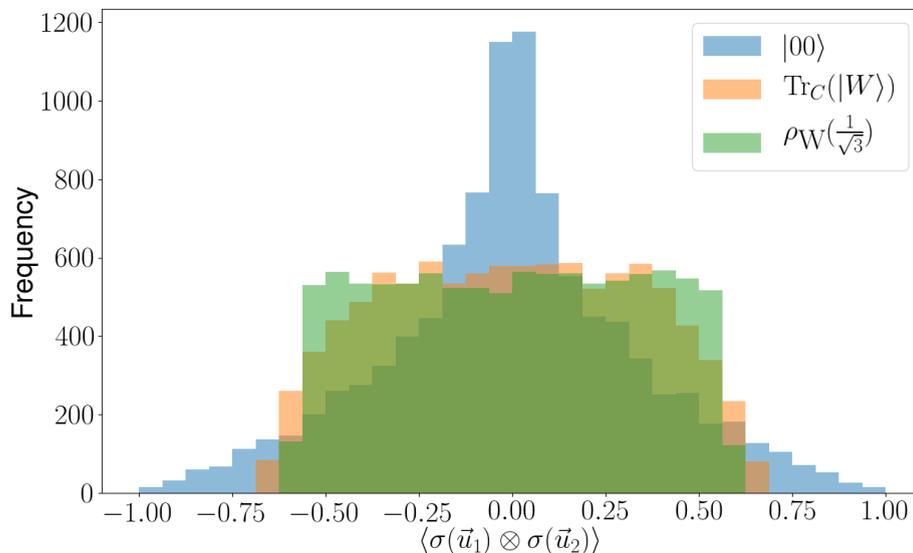
FIGURE 6.1: Sample distributions for random bipartite measurements for different two-qubit states: a product state (blue), the two-body marginal state of the tripartite W-state (orange) and a specific Werner state (green). The variance of the distributions corresponds to $\mathcal{R}^{(2)}$ and is equal to $\frac{1}{9}$ for all distributions shown here. The kurtosis corresponds to $\mathcal{R}^{(4)}$ in Eq. (6.4) and allows for entanglement detection.

The measurement basis defines a point on the Bloch sphere, corresponding to $|b_0\rangle$, and its antipodal $|b_1\rangle$. Instead of picking Haar random unitaries, the parties can pick uniformly a random point on the Bloch sphere, given by a unit vector $\vec{u}_k$. The corresponding operator that is measured is given by the rotated Pauli matrix

$$\sigma(\vec{u}_k) = \vec{u}_k \cdot \vec{\sigma} \tag{6.3}$$

with $\vec{\sigma} = (X, Y, Z)^{\mathrm{T}}$.

The n parties then evaluate the expectation value $\langle \sigma(\vec{u}_1) \otimes \sigma(\vec{u}_2) \otimes \ldots \otimes \sigma(\vec{u}_n) \rangle_\rho$ on the joint state ρ and repeat the experiment many times. This yields a distribution of measured expectation values. The t-th moment $\mathcal{R}^{(t)}$ of this distribution is then given by

$$\mathcal{R}^{(t)}(\rho) = \frac{1}{(4\pi)^n} \int \langle \sigma(\vec{u}_1) \otimes \ldots \otimes \sigma(\vec{u}_n) \rangle_\rho^t \, \mathrm{d}\vec{u}_1 \ldots \mathrm{d}\vec{u}_n, \tag{6.4}$$

where the domain of integration is given by n unit spheres S^2.

As a local unitary transformation on party k of the state ρ corresponds to rotations of the corresponding measurement direction $\vec{u}_k$, the moments are by definition LU-invariant. Furthermore, due to linearity of the expectation value, substituting any $\vec{u}_k$ with $-\vec{u}_k$ in the t-th power of the expectation value yields a factor of $(-1)^t$, implying that $\mathcal{R}^{(t)}(\rho) = 0$ whenever t is odd. Furthermore, for $t = 0$, we obtain $\mathcal{R}^{(0)}(\rho) = 1$.
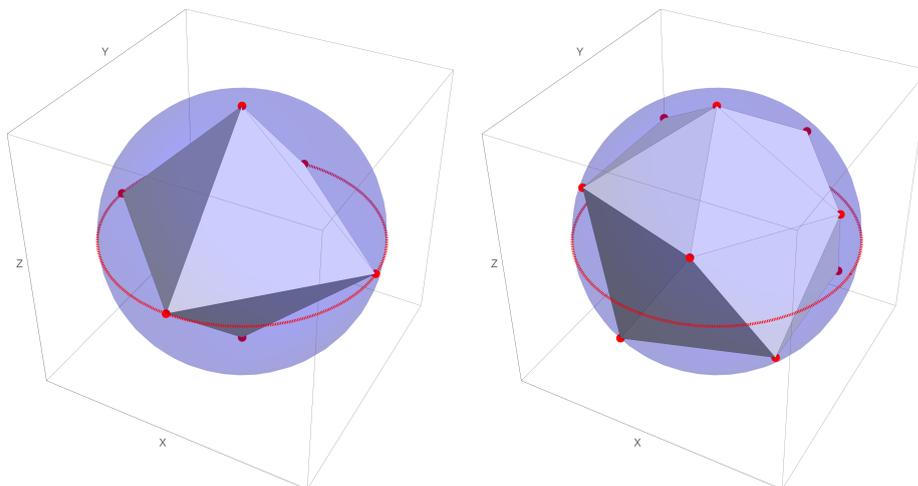
FIGURE 6.2: Left: The points of a spherical 3-design, forming an octahedron. Its points correspond to measurements in the usual X, Y and Z direction. Right: The points of a spherical 5-design, forming an icosahedron.

Therefore, the first two non-trivial moments are given by $\mathcal{R}^{(2)}(\rho)$ and $\mathcal{R}^{(4)}(\rho)$, on which we will focus in the following.

6.3 Spherical designs

The question remains how to evaluate the integral in Eq. (6.4). Luckily, averages of polynomials of degree t on the unit sphere can be replaced by a sum over a certain finite subset of points on the sphere [141]:

Definition 6.1. A set $\{\vec{d}_1, \ldots, \vec{d}_m\}$ of m points on the unit sphere is called a spherical t-design of dimension d, if

$$\int_{S^d} F(\vec{u}) \, d\vec{u} = \frac{1}{m} \sum_{j=1}^{m} F(\vec{d}_j) \tag{6.5}$$

for all polynomials F of degree t or less with their domain being the d-dimensional unit sphere S^d.

One can show that for each t and dimension d, for sufficiently large m a spherical t-design of dimension d exists [141]. However, there is no constructive method to obtain such designs and the minimal number of points m needed for such designs is unknown. However, there are many designs known, especially for $d = 2$ [142].

In order to rewrite Eq. (6.4) for $t = 2$ and $t = 4$, we need two-dimensional 2-designs and 4-designs.

For $t = 2$, we use the six points

$$\vec{d}_1 = (1,0,0)^\mathrm{T}, \qquad \vec{d}_2 = (0,1,0)^\mathrm{T}, \qquad \vec{d}_3 = (0,0,1)^\mathrm{T},$$
$$\vec{d}_4 = (-1,0,0)^\mathrm{T}, \qquad \vec{d}_5 = (0,-1,0)^\mathrm{T}, \qquad \vec{d}_6 = (0,0,-1)^\mathrm{T}, \tag{6.6}$$

displayed in Fig. 6.2. In fact, these points even form a 3-design [142]. However, we are using it for two reasons: First, there exists a 2-designs with only four points arranged like a tetrahedron. However, the 3-design presented above has the advantage that for every point also its antipodal is contained in the set. We noted already that substituting $\vec{u}_k$ by $-\vec{u}_k$ does not change the t-th power of the expectation value for even t. Thus, we do not have to evaluate the function for all six points in order to determine $\mathcal{R}^{(2)}$, but only for half of them. Second, the points of the 3-design correspond to measurements of the usual Pauli matrices X, Y and Z. This yields a correspondence between $\mathcal{R}^{(2)}$ and the sector length A_n as defined in Eq. (2.18):

Lemma 6.2. *For an n-qubit quantum state ρ holds that*

$$A_n(\rho) = 3^n \mathcal{R}^{(2)}(\rho). \tag{6.7}$$

Proof. Using the 3-design defined by the points in Eq. (6.6), we obtain

$$\mathcal{R}^{(2)}(\rho) = \frac{1}{6^n} \sum_{j_1,\ldots j_n=1}^{6} \langle \vec{d}_{j_1} \cdot \vec{\sigma} \otimes \ldots \otimes \vec{d}_{j_n} \cdot \vec{\sigma} \rangle_\rho^2 \tag{6.8}$$

$$= \frac{1}{3^n} \sum_{j_1,\ldots j_n=1}^{3} \langle \sigma_{j_1} \otimes \ldots \otimes \sigma_{j_n} \rangle_\rho^2 \tag{6.9}$$

$$= \frac{1}{3^n} A_n(\rho). \tag{6.10}$$

For the second line we have used the invariance under point inversion, and the last equality is just the definition of the sector length A_n. $\square$

This correspondence shows that any entanglement criterion using the moments is a generalization of the criterion in Eq. (5.26).

Finally, we have to evaluate $\mathcal{R}^{(4)}$. To that end, we use the spherical 5-design given by the 12 vertices of an icosahedron as displayed in Fig. 6.2. Again, for each point also its antipodal is part of the set, thus it suffices to evaluate the expectation value on six directions per site. Denoting these vertices as $\vec{e}_1$ to $\vec{e}_6$, we obtain

$$\mathcal{R}^{(4)} = \frac{1}{6^n} \sum_{j_1,\ldots,j_n=1}^{6} \langle \vec{e}_{j_1} \cdot \vec{\sigma} \otimes \ldots \otimes \vec{e}_{j_n} \cdot \vec{\sigma} \rangle_\rho^4. \tag{6.11}$$
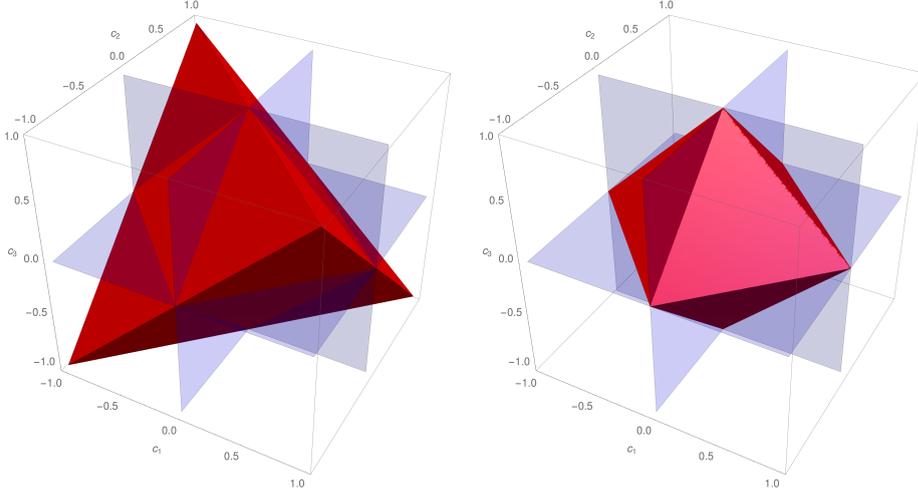
FIGURE 6.3: Left: The parameters c_1, c_2, c_3 that yield positive bipartite Bell diagonal states form a tetrahedron, given by the constraints in Eq. (6.16). Right: The subset of parameters yielding separable Bell diagonal states form an octahedron within the tetrahedron, given by the constraint $|c_1| + |c_2| + |c_3| \leq 1$.

6.4 The two-qubit case

We are now going to use the moments $\mathcal{R}^{(2)}$ and $\mathcal{R}^{(4)}$ for entanglement detection in the case of two-qubit states. First of all, we expand Eq. (6.11) for $n = 2$. To that end, we define

$$Q^{(4)} := \sum_{i,j,k,l=1}^{3} \langle \sigma_i \otimes \sigma_j \rangle \langle \sigma_k \otimes \sigma_l \rangle \langle \sigma_i \otimes \sigma_l \rangle \langle \sigma_k \otimes \sigma_j \rangle. \tag{6.12}$$

Inserting the points of the spherical 5-design into Eq. (6.11) for $n = 2$ yields

$$\mathcal{R}^{(4)} = \frac{1}{75}[2Q^{(4)} + 81(\mathcal{R}^{(2)})^2] \tag{6.13}$$

$$= \frac{1}{75}[2Q^{(4)} + (A_2)^2]. \tag{6.14}$$

Before considering arbitrary two-qubit states, we concentrate on Bell diagonal states (BDS). They form a three-parameter subclass of all mixed two-qubit states and are defined via [143]

$$\rho_{\text{BDS}} = \frac{1}{4}(\mathbb{1} \otimes \mathbb{1} + \sum_{i=1}^{3} c_i \sigma_i \otimes \sigma_i), \tag{6.15}$$

where the c_i are real numbers. In order to yield a positive matrix, the c_i have to obey

$$1 - c_1 - c_2 - c_3 \geq 0, \qquad 1 - c_1 + c_2 + c_3 \geq 0,$$
$$1 + c_1 - c_2 + c_3 \geq 0, \qquad 1 + c_1 + c_2 - c_3 \geq 0. \tag{6.16}$$

The set of admissible numbers c_i forms a tetrahedron and is displayed on the left-hand side in Fig. 6.3.

The concurrence of a Bell diagonal state can easily be calculated using Eq. (2.40) by observing that $\tilde{\rho} = \rho$, and reads

$$C(\rho_{\text{BDS}}) = \max\{0, 2\lambda_{\max} - 1\} \tag{6.17}$$

$$= \max\{0, \sum_{i=1}^{3} |c_i| - 1\}. \tag{6.18}$$

The separable BDS states, i.e., those with vanishing concurrence, form an octahedron, characterized by $\sum_{i=1}^{3} |c_i| \leq 1$, displayed on the right-hand side in Fig. 6.3.

The importance of the class of Bell diagonal states stems from the following fact:

Lemma 6.3. *For each two-qubit state ρ, there exists a Bell diagonal state ρ_{BDS}, s.t.*

a) $C(\rho_{BDS}) \leq C(\rho)$,

b) $\mathcal{R}^{(k)}(\rho_{BDS}) = \mathcal{R}^{(k)}(\rho)$ *for all k.*

Proof. In order to prove a), we first note that due to Eq. (2.40), the concurrence of a state ρ and its inversion $\tilde{\rho}$ coincide. This implies, using the convexity property E4 in Def. 2.4 of entanglement measures, that

$$C(\frac{1}{2}\rho + \frac{1}{2}\tilde{\rho}) \leq C(\rho). \tag{6.19}$$

The mixture on the left-hand side of this equation can be evaluated using Eq. (4.5): It has the same bipartite correlations as ρ, but vanishing one-particle contributions. More precisely, $\frac{1}{2}(\rho + \tilde{\rho}) = \frac{1}{4}(\mathbb{1} \otimes \mathbb{1} + \sum_{i,j=1}^{3} t_{ij}\sigma_i \otimes \sigma_j)$.

Using appropriate local unitary transformations $U_A \otimes U_B$, the 3×3 correlation matrix t_{ij} can be diagonalized, yielding the Bell diagonal state

$$\rho_{\text{BDS}} := U_A \otimes U_B \frac{1}{2}(\rho + \tilde{\rho})U_A^\dagger \otimes U_B^\dagger. \tag{6.20}$$

As local unitary transformations do not change the entanglement of the state, the claim $C(\rho_{\text{BDS}}) \leq C(\rho)$ follows.

For the proof of statement b), we note that $\mathcal{R}^{(k)}$ is a function of the bipartite correlations t_{ij} only, as well as being invariant under local unitary rotations by definition. Thus, the moments of ρ and the rotated and mixed ρ_{BDS} coincide. $\qquad\square$

The statement of Lemma 6.3 yields a simplified recipe to characterize the landscape of admissible $(\mathcal{R}^{(2)}, \mathcal{R}^{(4)})$-values of bipartite entangled and separable quantum states, by consideration of the reduced class of Bell diagonal states only.

6.4.1 The landscape of all two-qubit states

We begin with the characterization of admissible $\mathcal{R}^{(2)}, \mathcal{R}^{(4)}$-pairs of all bipartite quantum states. As each realizable pair is also realizable by a Bell diagonal state, it suffices to consider obtainable values of this subset of states.

We begin by rewriting explicitly Eqs. (6.8) and (6.13) for Bell diagonal states. Writing $\rho_{\mathrm{BDS}} = \frac{1}{4}(\mathbb{1} \otimes \mathbb{1} + \sum_{i=1}^{3} c_i \sigma_i \otimes \sigma_i)$, we obtain

$$\mathcal{R}^{(2)} = \frac{1}{9}(c_1^2 + c_2^2 + c_3^2), \tag{6.21}$$

$$\mathcal{R}^{(4)} = \frac{2}{75}(c_1^4 + c_2^4 + c_3^4) + \frac{27}{25}(\mathcal{R}^{(2)})^2. \tag{6.22}$$

Thus, we have to solve the following optimization problem:

$$\min_{c_1, c_2, c_3}/\max \ c_1^4 + c_2^4 + c_3^4 \tag{6.23}$$

$$\text{subject to} \ \ c_1^2 + c_2^2 + c_3^2 = k,$$

$$1 - c_1 - c_2 - c_3 \geq 0,$$

$$1 - c_1 + c_2 + c_3 \geq 0,$$

$$1 + c_1 - c_2 + c_3 \geq 0,$$

$$1 + c_1 + c_2 - c_3 \geq 0.$$

Geometrically, this corresponds to minimizing/maximizing the size of a deformed sphere such that it still intersects with a sphere of radius $\sqrt{k}$, with the intersections lying inside of the positivity tetrahedron. The constrained optimization is displayed in Fig. 6.4. Due to symmetry, it suffices to consider the case $c_1 \geq c_2 \geq 0, c_3 \leq 0$, as the target function is invariant under exchange of the c_i, as well as under reflection $c_i \to -c_i$, and the constraints are less restrictive in the octants where one (or all) of the c_i are negative.

In this region, only the positivity constraints $1 - c_1 - c_2 - c_3 \geq 0$ and $1 - c_1 + c_2 + c_3 \geq 0$ are still relevant.

Next, using Lagrange multipliers, it is easy to see that the minimum (or maximum) size of the deformed sphere such that it intersects with the sphere of radius $\sqrt{k}$ is
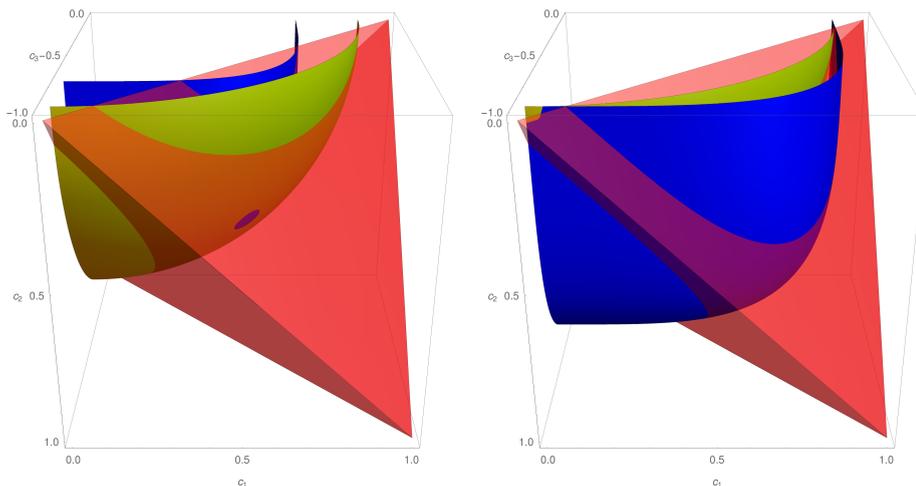
FIGURE 6.4: The minimization (left) and maximization (right) of the size of a deformed sphere (blue), such that its intersection with a sphere of radius $\sqrt{k}$ (yellow) lies inside of the constrained red region, corresponding to the set of Bell diagonal states.

given by $k^2/3$ (or k^2), where the points of intersection are located at points $|c_i| = |c_j|$ (or $c_1 = \sqrt{k}, c_2 = 0, c_3 = 0$).

The global minimum can always be attained, even for $k > \frac{1}{3}$, as long as $k \leq 3$. The maximum, however, is constrained by positivity as soon as $k > 1$, when the maximal point touches the tetrahedron. For that region, both remaining positivity constraints are fulfilled exactly, yielding $c_1 = 1, c_2 = -c_3$ for the optimal point. From the spherical constraint we obtain $c_2 = \sqrt{\frac{k-1}{2}}$, yielding a maximal size of the deformed sphere of $1 + \frac{(k-1)^2}{2}$. Combining both cases and using $k = 9\mathcal{R}^{(2)}$, we obtain the following bounds on $\mathcal{R}^{(4)}$:

$$\frac{9}{5}(\mathcal{R}^{(2)})^2 \leq \mathcal{R}^{(4)} \leq \begin{cases} \frac{81}{25}(\mathcal{R}^{(2)})^2 & 0 \leq \mathcal{R}^{(2)} \leq \frac{1}{9}, \\ \frac{54}{25}(\mathcal{R}^{(2)})^2 - \frac{6}{25}\mathcal{R}^{(2)} + \frac{1}{25} & \frac{1}{9} \leq \mathcal{R}^{(2)} \leq \frac{1}{3}. \end{cases} \tag{6.24}$$

These bounds are displayed as blue lines in Fig. 6.6.

6.4.2 The subset of separable two-qubit states

We now have to perform a similar optimization for the subset of separable Bell diagonal states, which are described by the additional octahedral constraint $|c_1| + |c_2| + |c_3| \leq 1$, replacing the former positivity constraints, as the separability constraint is stronger.

In this case, we can perform the optimization in any octant, as all constraints and target functions are symmetric under reflection and exchange of the c_i. Thus, we concentrate on the case $c_1 \geq c_2 \geq c_3 \geq 0$. The optimization is displayed in Fig. 6.5.
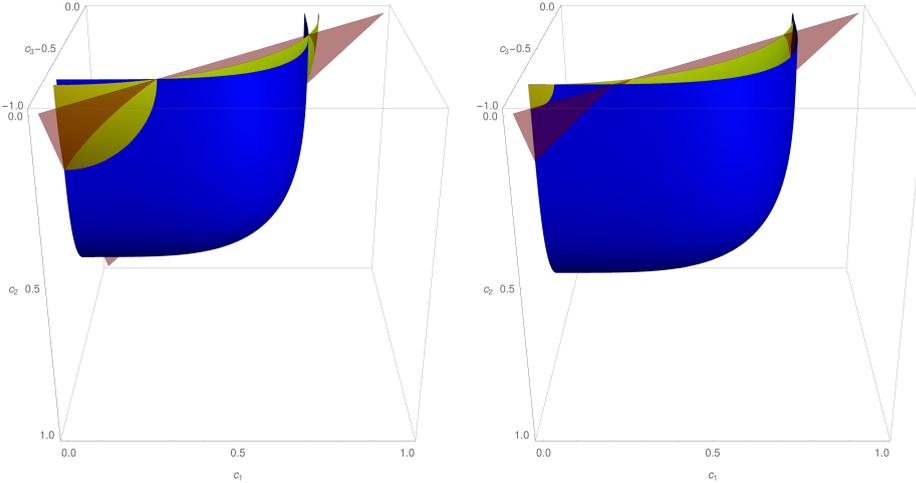
FIGURE 6.5: The minimization (left) and maximization (right) of the size of a deformed sphere (blue), such that its intersection with a sphere of radius k (yellow) lies inside of the constrained red region, corresponding to the set of separable Bell diagonal states. For the minimization, several different cases have to be considered.

As before, for $k \leq \frac{1}{3}$, the sphere lies completely inside of the octahedron, yielding the same upper and lower bound as in the general case.

The maximum, located at $c_2 = c_3 = 0$, is attainable up to $k = 1$. For $k > 1$, the octahedron lies inside of the sphere, and no solution can be found anymore.

The minimum, however, splits into several distinct cases. For $\frac{1}{3} \leq k \leq \frac{1}{2}$, the cut of the octahedron with the sphere yields a circle, on which the optimum must lie. Solving the exactly fulfilled constraints $|c_1| + |c_2| + |c_3| = c_1 + c_2 + c_3 = 1$, as well as $c_1^2 + c_2^2 + c_3^2 = k$ for c_2 and c_3, and plugging them into the target function allows for a one-dimensional optimization, yielding the minimum $\frac{1}{54}(27k^2 + 18k - 7 - 4\sqrt{2}\sqrt{3k-1}^3)$.

Finally, in the region $\frac{1}{2} \leq k \leq 1$, the cut of octahedron and sphere is an incomplete sphere, where the minimum fulfills the additional constraint $c_3 = 0$, yielding immediately the minimum of $\frac{1}{2}(k^2 + 2k - 1)$. Rephrasing these lower bounds in terms of $\mathcal{R}^{(2)}$ and $\mathcal{R}^{(4)}$ yields for separable states the same upper bound as for all states, namely

$$\mathcal{R}^{(4)} \leq \frac{81}{25}(\mathcal{R}^{(2)})^2, \tag{6.25}$$

as long as $\mathcal{R}^{(2)} \leq \frac{1}{9}$. The lower bound is given by

$$\mathcal{R}^{(4)} \geq \begin{cases} \frac{9}{5}(\mathcal{R}^{(2)})^2 & 0 \leq \mathcal{R}^{(2)} \leq \frac{1}{27}, \\ \frac{1}{2025}[4374(\mathcal{R}^{(2)})^2 + 162\mathcal{R}^{(2)} - 7 - 4\sqrt{2}\sqrt{27\mathcal{R}^{(2)} - 1}^3] & \frac{1}{27} \leq \mathcal{R}^{(2)} \leq \frac{1}{18}, \\ \frac{1}{75}[162(\mathcal{R}^{(2)})^2 + 18\mathcal{R}^{(2)} - 1] & \frac{1}{18} \leq \mathcal{R}^{(2)} \leq \frac{1}{9}. \end{cases} \tag{6.26}$$
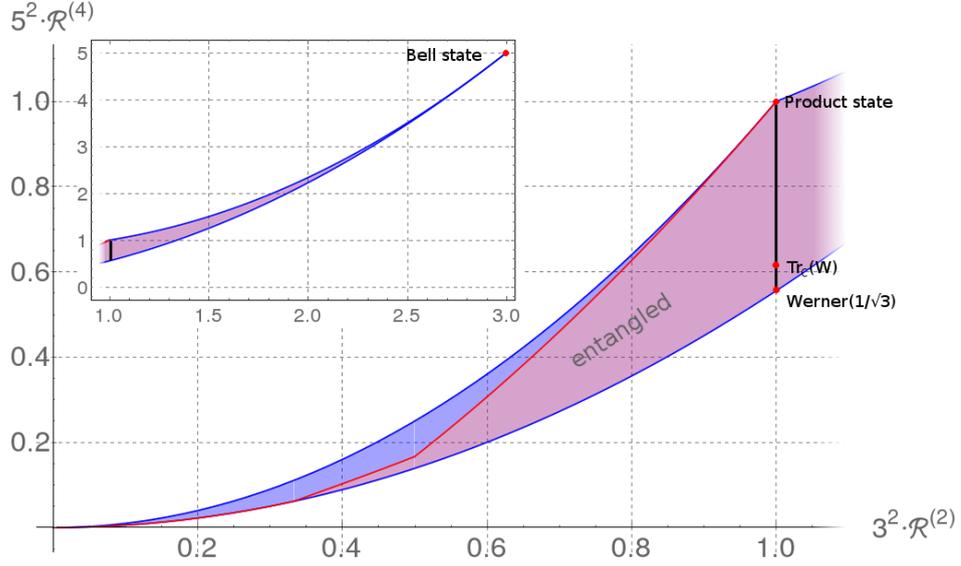
FIGURE 6.6: The set of admissible $\mathcal{R}^{(2)}$-$\mathcal{R}^{(4)}$ pairs in two-qubit states. The blue region contains all separable and some entangled states, the red region contains entangled states only. The red line that separates the two regions corresponds to the function in Eq. (6.26) and acts as an entanglement criterion that can detect states like the two-body marginal of a three-partite W-state and all entangled Werner states, lying on the lower bound of the set. The weaker criterion from Eq. (5.26) using $\mathcal{R}^{(2)}$ only is displayed as a thick black line.

All of the obtained bounds are displayed in Fig. 6.6. As one can see, the set of separable states is clearly distinguishable from the set of entangled states, and the bounds allow for entanglement detection in the following way: If a two-qubit state is separable, then also its corresponding Bell diagonal states from Lemma 6.3 is separable, lying in the separable subset in Fig. 6.6. Thus, if a two-qubit state lies outside of the subset, it must be entangled. Whether or not it lies outside can be phrased as follows:

Theorem 6.4. *If for a two-qubit state ρ it holds that*

- $\mathcal{R}^{(2)}(\rho) > \frac{1}{9}$, *or*

- $\frac{1}{18} \leq \mathcal{R}^{(2)} \leq \frac{1}{9}$ *and* $\mathcal{R}^{(4)} < \frac{1}{75}[162(\mathcal{R}^{(2)})^2 + 18\mathcal{R}^{(2)} - 1]$, *or*

- $\frac{1}{27} \leq \mathcal{R}^{(2)} \leq \frac{1}{18}$ *and* $\mathcal{R}^{(4)} < \frac{1}{2025}[4374(\mathcal{R}^{(2)})^2 + 162\mathcal{R}^{(2)} - 7 - 4\sqrt{2}\sqrt{27\mathcal{R}^{(2)} - 1}^3]$,

then ρ is entangled.

The criterion of Theorem 6.4 can be regarded as a generalization of the criterion in Eq. (5.26), which detects the entanglement if $\mathcal{R}^{(2)}(\rho) > \frac{1}{9}$ only (black line in Fig. 6.4).

As a first example, consider the prominent family of Werner states, given in Eq. (6.2). It is entangled iff $p > \frac{1}{3}$, as can be checked using the PPT criterion. As $\mathcal{R}^{(t)}[\rho_W(p)] =$

$p^t \mathcal{R}^{(t)}(|\Phi^+\rangle)$, the criterion in Eq. (5.26) detects the entanglement of this state for $p > \frac{1}{\sqrt{3}}$ only. However, this family lies on the global lower bound of the state space in Fig. 6.6 with $\mathcal{R}^{(4)} = \frac{9}{5}(\mathcal{R}^{(2)})^2$. Thus, using the refined criterion of Theorem 6.4, the entanglement of Werner states is detected for the full range of $p > \frac{1}{3}$.

As a second example, consider the marginal state ρ_{AB} of the three-partite W-state in Eq. (6.1). Its marginal state $\rho_{AB} = \frac{1}{3}|00\rangle\langle00| + \frac{2}{3}|\Psi^+\rangle\langle\Psi^+|$ is known to be entangled, with a concurrence of $C(\rho_{AB}) = \frac{2}{3}$. With moment values of $3^2\mathcal{R}^{(2)}(\rho_{AB}) = 1$ and $5^2\mathcal{R}^{(4)}(\rho_{AB}) = \frac{49}{81}$, it is only detectable by the refined criterion.

6.5   Boundary states

The optimization performed above yields directly the Bell diagonal states lying at the boundary of the corresponding sets. Here, we list for each point on the boundaries a corresponding Bell diagonal state. Note, however, that these states are usually not the unique states realizing these points.

As stated above, the global minimum is traced by Werner states, corresponding to Bell diagonal states with parameters $(c_1, c_2, c_3) = (p, -p, p)$ with $0 \leq p \leq 1$, being entangled iff $p > \frac{1}{3}$.

The global upper bound for $3^2\mathcal{R}^{(2)} \leq \frac{1}{3}$, connecting the product states with the origin, is traced by mixtures of product states with maximally mixed states, where the corresponding Bell diagonal state is given by $(0, 0, p)$ with $0 \leq p \leq 1$. The quadratic upper bound connecting the product states with the Bell state, however, is traced by Bell diagonal states with parameters $(p, -p, 1)$.

The lower bound of the separable set is a piecewise function. For $3^2\mathcal{R}^{(2)} \leq \frac{1}{3}$, it is realised by separable states with parameters (p, p, p), where $0 \leq p \leq \frac{1}{3}$. If $\frac{1}{3} \leq 3^2\mathcal{R}^{(2)} \leq \frac{1}{2}$, the family $(p, p, 1-2p)$ for $\frac{1}{3} \leq p \leq \frac{1}{2}$ reaches the bound. Finally, the bound for $\frac{1}{2} \leq 3^2\mathcal{R}^{(2)} \leq 1$ is realized by states of the form $(p, 1-p, 0)$ with $\frac{1}{2} \leq p \leq 1$.

6.6   Multipartite entanglement

There are several ways to generalize the results of this chapter. One such track is to consider multipartite states, as the definition in Eq. (6.4), as well as the reformulation in terms of designs, can be directly generalized to n-partite states.
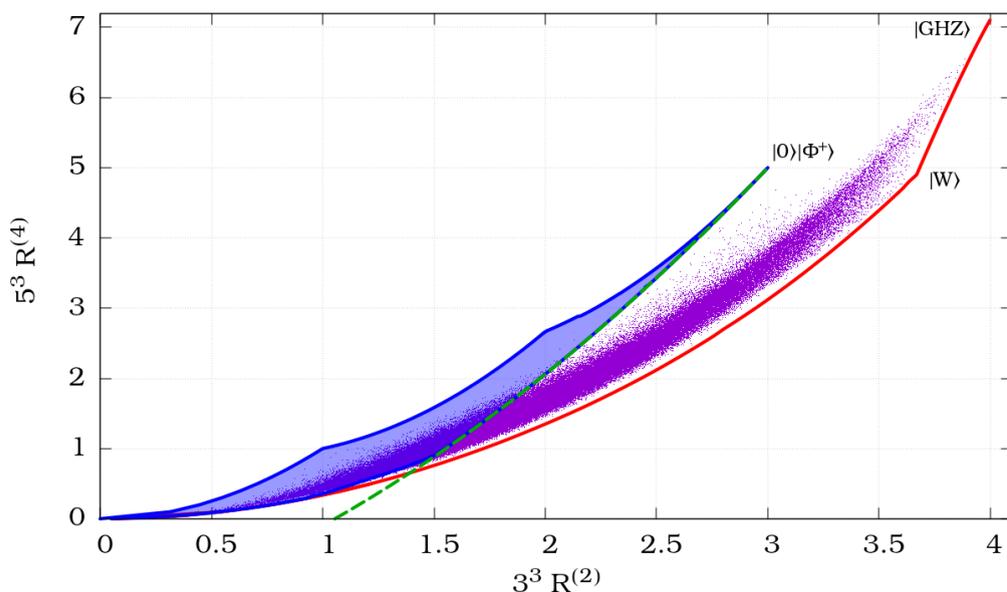
FIGURE 6.7: The set of three-qubit states in the $\mathcal{R}^{(2)}$, $\mathcal{R}^{(4)}$-landscape. The (numerically obtained) subset of biseparable states is displayed in light blue with thick blue boundaries. The lower bound of the set of all states is displayed in red, and some random three-qubit states are displayed in violet. The conjectured criterion in Eq. (6.28) is displayed as a dashed, green line. For reference, the highly entangled GHZ state and W-state, as well as a biseparable product state, have been added to the plot.

Let us consider the case of three qubits. Using Lemma 6.2 we can express $\mathcal{R}^{(2)}(\rho)$ in terms of the sector length A_3, i.e.,

$$\mathcal{R}^{(2)}(\rho) = \frac{1}{27} A_3(\rho). \tag{6.27}$$

From Eq. (5.27), we know that a value of $A_3 > 3$ certifies genuine multipartite entanglement, and we can ask again the question whether additional knowledge of $\mathcal{R}^{(4)}$ allows for a refined criterion.

In contrast to the bipartite case, we treat this case numerically. Thus, we optimize numerically over three-partite quantum states using the BFGS algorithm [144–147]. Additionally, we optimize over the set of biseparable states only. The results are presented in Fig. 6.7 and show a large area occupied by genuinely multipartite entangled states only. Thus, it is possible to formulate a refined criterion. While we are not able to infer an analytical form of the boundary between the two sets, we can approximate it quadratically, which allows us to formulate the following conjecture:

Conjecture 6.5. For each biseparable three-qubit state ρ_{bisep}, it holds that

$$\mathcal{R}^{(4)}(\rho_{\text{bisep}}) \geq \frac{1}{425}[972(\mathcal{R}^{(2)})^2 + 90\mathcal{R}^{(2)} - 5]. \tag{6.28}$$

Finally, we note that also the discrimination of different entanglement classes is possible. Indeed, it is possible to detect states outside of the *W*-class. Furthermore, it is possible to detect multipartite entanglement from the two-body marginals. These two generalizations are described in Ref. [148].

6.7 Conclusions

Higher moments of distributions of measurement results are a natural byproduct of measurement processes. As such, it is of great interest to harvest this additional information for the measurement task at hand. In this chapter, we considered how higher moments of the statistics of random correlation measurements can help to detect entanglement. These random measurements are useful in cases where no shared reference frame can be established, or when the measurement devices are insufficiently characterized.

We showed that in the case of two-qubit states, the additional knowledge of higher moments allows indeed for a more refined entanglement detection compared to knowing only the first two moments. In order to obtain analytical results, we used the theory of spherical designs.

Finally, we gave numerical evidence that also in multipartite scenarios entanglement detection can be improved using higher moments.

It would be desirable to generalize the results from this chapter to higher-dimensional systems beyond qubits as well. In this case, one has to replace spherical designs by unitary designs, as there exists no appropriate Bloch sphere representation of higher dimensional systems.

A great advantage of using the moments of random correlation measurements is their invariance under local unitary rotations. However, it is probably also possible to use higher moments of a restricted set of measurement results to improve the ability to detect entanglement, for example in spin squeezing measurements [149–152]. Prospecting these more general measurement settings could be beneficial for improving the amount of information that can be obtained from measurement results in many different experiments.

7 Detecting entanglement using product observables

Prerequisites

7.1 Introduction

Entanglement is an important resource for many applications of quantum mechanics. For example, the security of the Ekert protocol for key distribution using quantum cryptography relies on the two parties being able to quantify the entanglement in a shared quantum state [43]. Another example is that of measurement-based quantum computation, where the actual computation is performed by measurements (and appropriate classical pre- and post-processing) of a previously created resource state [153, 154]. It is believed that states that allow for universal quantum computing require certain entanglement quantifiers to reach a maximum [155]. Given the prominent role of entanglement in such tasks, it is evident that the ability to certify and quantify entanglement using appropriate measurements is of great importance.

However, measurement abilities are usually limited. First, in typical setups, the devices are limited to local measurements, for instance, if the individual particles of a multipartite state are spatially separated. Second, measuring expectation values of these observables can be expensive as usually many copies of the state are required.

In this chapter, we are therefore asking the following question: What is the minimal effort required to detect entanglement using expectation value measurements in bipartite quantum states?

To answer this question, we investigate the case of measuring the expectation values of two product observables and give necessary and sufficient conditions on these observables in order to detect entanglement in qubit-qubit and qubit-qutrit systems. Finally, we highlight connections of the results to jointly measurable observables.

7.2 The setting

We consider bipartite quantum states and local measurement observables. We start by considering the case of a single observable $C = C_A \otimes C_B$. In this case, entanglement detection is not possible, as can be seen as follows: Let ρ be an entangled quantum state with $c = \langle C \rangle = \text{Tr}(\rho C_A \otimes C_B)$. Then, as $\text{Tr}(\rho) = 1$, the value of c must lie between the smallest and the largest eigenvalue ($\lambda_{\min}$ and $\lambda_{\max}$) of $C_A \otimes C_B$. As $C_A \otimes C_B$ is product, its eigenvectors are product states, too. Thus, there exist two product states, $|a_{\min}\rangle \otimes |b_{\min}\rangle$ and $|a_{\max}\rangle \otimes |b_{\max}\rangle$, yielding the expectation value $\lambda_{\min}$ and $\lambda_{\max}$, respectively, when measuring C.

As the set of pure states is connected, one can find two continuous families of states, $|a(t)\rangle$ and $|b(t)\rangle$ with

$$|a(0)\rangle = |a_{\min}\rangle, \quad |a(1)\rangle = |a_{\max}\rangle, \tag{7.1}$$

$$|b(0)\rangle = |b_{\min}\rangle, \quad |b(1)\rangle = |b_{\max}\rangle. \tag{7.2}$$

As the trace is a continuous map, there exists a value $0 \le t_c \le 1$, such that $|c\rangle := |a(t_c)\rangle \otimes |b(t_c)\rangle$ yields the same expectation value $\text{Tr}(|c\rangle\langle c|C_A \otimes C_B) = c$ as ρ.

How about having access to an additional measurement observable, $L = L_A \otimes L_B$? In this case, entanglement detection is clearly possible, as we have already shown in Section 5.3.4. There, we showed that if for a bipartite qubit system, the sector length $A_2 = \sum_{i,j}\langle \sigma_i \otimes \sigma_j \rangle^2$ exceeds a value of one, then the state is entangled. This bound is already violated if $\langle X \otimes X \rangle^2 + \langle Z \otimes Z \rangle^2 > 1$, which is, for instance, the case for all Bell states. Thus, having access to the expectation values of the two product observables $X \otimes X$ and $Z \otimes Z$, one can indeed detect entanglement.

The question arises whether any pair of product observables can be used for entanglement detection. To that end, consider the two observables $X \otimes X$ and $X \otimes Z$. As we have seen in Section 5.3.1, the sum of squares of their expectation values cannot exceed one, as the operators anticommute, thus they cannot violate the bound given above. Indeed, as we will show below, one cannot formulate any entanglement criterion using only the two expectation values $\langle X \otimes X \rangle$ and $\langle X \otimes Z \rangle$.

In the following, we investigate this case of two product observables C and L in great detail in order to find necessary and sufficient properties for these two operators that enables them to detect entanglement.

7.3 Relation to entanglement witnesses

The scenario described above has close connections to the question of whether or not an observable can be interpreted as an entanglement witness. As introduced in Section 2.5, an entanglement witness is a hermitian operator W with $\langle W \rangle \geq 0$ for all separable states, and $\langle W \rangle < 0$ for at least one entangled state. Any entanglement witness can be written as

$$W = g\mathbb{1} - B, \tag{7.3}$$

where B the observable to be measured and g is chosen such that $\langle W \rangle \geq 0$ for all separable states. This means that the optimal choice for g is given by

$$g = \sup_{\sigma} \mathrm{Tr}(\sigma B), \tag{7.4}$$

where the supremum is over all separable quantum states σ. As discussed in Section 2.5, the set of separable quantum states is given by all convex combinations of pure product states, implying that the set of separable states is convex and there always exists a pure product state yielding a maximal value of $\mathrm{Tr}(\sigma B)$. Thus, the maximization of Eq. (7.4) can be performed considering pure product states only, making it much more efficient. Furthermore, for many reasonable choices of B, the maximum can be calculated analytically.

Finally, note that not all choices for B yield useful entanglement witnesses. As we have seen above, choosing $B = C_A \otimes C_B$ results in the optimization in Eq. (7.4) yielding the maximal eigenvalue of B, thus $W \geq 0$ and there is no entangled state detected by it.

This observation makes it clear that, in order for B to allow for the construction of an entanglement witness, its eigenstate corresponding to its highest eigenvalue needs to be entangled (and if instead the ground state is entangled, we can use $-B$ to construct an entanglement witness).

If, however, in addition to $\langle C \rangle$, also $\langle L \rangle$ is known, then this allows for the determination of the expectation value of $B = \alpha C + \beta L$ for all α and β, and therefore any witness of the form

$$W(\alpha, \beta) = g(\alpha, \beta)\mathbb{1} - \alpha C - \beta L \tag{7.5}$$

can be evaluated. Owing to the convexity of the set of all separable states, this also means that for each entangled state that can be detected from knowledge of $\langle C \rangle$ and $\langle L \rangle$, there exists a witness of the form of Eq. (7.5) for some α and β detecting it.

7.4 Systems of two qubits

We start with the easiest case of bipartite qubit systems. In this case, easy necessary and sufficient conditions for their ability to detect entanglement can be found:

Theorem 7.1. *In a two-qubit system, the product observables $C = C_A \otimes C_B$ and $L = L_A \otimes L_B$ can be used for entanglement detection, if and only if $[C_A, L_A] \neq 0$ and $[C_B, L_B] \neq 0$.*

Proof. One direction of the proof is trivial: If $[C_A, L_A] = 0$, then C and L cannot be used for entanglement detection, because in this case, Alice is effectively performing only a single measurement M_A. So, any possible linear combination $B = \alpha C + \beta L$ can be evaluated from the statistics of a product measurement $M_A \otimes M_B(\alpha, \beta)$, and, as shown above, the probabilities of such measurements can always be mimicked by a separable state. The same applies if $[C_B, L_B] = 0$.

As argued above, in order to be useful for entanglement detection, there must exist numbers α, β such that

$$B = \alpha C + \beta L \tag{7.6}$$

has an entangled ground state. This ground state can then be certified by the appropriate combination of C and L, thus its entanglement can be detected. Therefore, in order to show the other direction, we have to show that such numbers α and β exist whenever the local observables do not commute.

To that end, let us consider $\alpha = 1$ and $\beta = \lambda$, where λ is a small real number. We can assume that the operators C_A and C_B are diagonal in their respective local computational basis, so C is diagonal in $|kl\rangle$, $k, l \in \{0, 1\}$ with eigenvalues γ_{kl}. We need to distinguish two cases, depending on whether the operator C has a degenerate ground state or not.

Non-degenerate ground state: Let us assume, without loss of generality, that C has the unique ground state $|00\rangle$. Considering λL as a perturbation to C, we now prove that the perturbed ground state is entangled by reductio ad absurdum. To that end, assume that the ground state of the operator $C + \lambda L$ is always a product state. For small values of λ, the ground state can, according to perturbation theory, be expanded as

$$|\psi(\lambda)\rangle = |00\rangle + \lambda|\psi_1\rangle + \lambda^2|\psi_2\rangle + \dots. \tag{7.7}$$

The first order correction to the ground state is given by [156]

$$|\psi_1\rangle = \sum_{k \neq 0, l \neq 0} \frac{\langle kl|L|00\rangle}{\gamma_{00} - \gamma_{kl}}|kl\rangle, \tag{7.8}$$

where $\gamma_{ij} = \langle ij|C|ij\rangle$. As the total state is normalized, $|\psi_1\rangle$ is orthogonal to $|00\rangle$.

Note that from the assumption that $|\psi(\lambda)\rangle$ is a product state, it follows that $|\psi_1\rangle$ must also be orthogonal to all $|kl\rangle$, where $k, l > 0$. For qubits, this only concerns the case $k = l = 1$, but we formulate the argument directly for arbitrary dimensions. This orthogonality can be seen as follows: Assume that $0 < f := \langle kl|\psi_1\rangle$ for $k, l > 0$, and consider the state $|\varphi\rangle = (|00\rangle + |kl\rangle)/\sqrt{2}$. The state $|\varphi\rangle$ is effectively an entangled Bell state and it is known that for every product state $|a, b\rangle$, the overlap obeys $|\langle a, b|\varphi\rangle|^2 \leq 1/2$ [26]. For $\lambda = 0$, we have that $|\langle \psi(0)|\varphi\rangle|^2 = 1/2$ and in addition

$$\frac{\partial}{\partial \lambda}|\langle \psi(\lambda)|\varphi\rangle|\big|_{\lambda=0} = |\langle \psi_1|\psi\rangle| = f > 0, \tag{7.9}$$

so for small λ the overlap obeys $|\langle \psi(\lambda)|\varphi\rangle|^2 > 1/2$. Consequently $|\psi(\lambda)\rangle$ is entangled and we arrive at a contradiction.

Having established that $|kl\rangle$ for $k, l > 0$ is orthogonal to the first order expansion vector $|\psi_1\rangle$ we can conclude from Eq. (7.8) that

$$\langle 11|L|00\rangle = \langle 00|L|11\rangle = 0. \tag{7.10}$$

Since $L = L_A \otimes L_B$, it follows that either L_A or L_B must be diagonal in the computational basis. This is the contradiction to the statement that $[C_x, L_x] \neq 0$ for $x \in \{A, B\}$.

Degenerate ground state: Now we consider the case when C is degenerate, in which case both the ground (lowest eigenvalue) state and the most excited (highest eigenvalue) state must have two-fold degeneracy. This is because if only the ground state would be degenerate, the operator $-C$ could be used instead and the first case of the proof would apply.

Writing $C_A = \text{diag}(c_1, c_2)$ and $C_B = \text{diag}(c_3, c_4)$, the eigenvalues of C are given by $c_1 c_3$, $c_1 c_4$, $c_2 c_3$, $c_2 c_4$. Since we have the assumption that neither C_A commutes with L_A, nor C_B commutes with L_B, neither C_A nor C_B can be proportional to the identity. Thus, $c_1 c_3 \neq c_1 c_4$, $c_1 c_3 \neq c_2 c_3$, $c_1 c_4 \neq c_2 c_4$ and $c_2 c_3 \neq c_2 c_4$. The degeneracy can therefore only occur due to $c_1 c_3 = c_2 c_4$ and $c_1 c_4 = c_2 c_3$. It follows that without loss of generality we can fix the degenerate ground subspace to be spanned by the two product vectors $|00\rangle$ and $|11\rangle$. Note that in this two-dimensional subspace, $|00\rangle$ and $|11\rangle$ are the only product vectors.

The operator C is disturbed by the operator L and we want to characterize this using degenerate perturbation theory [156]. We define the projector $P = |00\rangle\langle 00| + |11\rangle\langle 11|$ and, according to perturbation theory, we need to diagonalize the operator PLP.

The ground state $|\chi\rangle$ of this operator is then the zeroth order of perturbation theory,meaning that in the limit $\lambda \searrow 0$, the state $|\chi\rangle$ approximates the ground state of the perturbed system arbitrarily well.

The vectors $|00\rangle$ and $|11\rangle$ cannot be eigenstates of PLP, as otherwise $\langle 11|L|00\rangle = \langle 00|L|11\rangle = 0$ again. So, $|\chi\rangle$ must be entangled, but then there are no product states in its vicinity and for small λ the operator $C + \lambda L$ must have an entangled ground state. $\qquad\square$

7.5 Systems of higher dimensions

While it was possible to give necessary and sufficient criteria for the usefulness of C and L in the case of two qubits, the situation changes for higher dimensional systems. In the case of a qubit-qutrit system, however, a similar statement is true if we assume that C or L has a non-degenerate ground state and most excited state:

Theorem 7.2. *In a qubit-qutrit system, the product observables $C = C_A \otimes C_B$ and $L = L_A \otimes L_B$, where the ground state and the most excited state of C are non-degenerate, can be used for entanglement detection, if and only if $[C_A, L_A] \neq 0$ and $[C_B, L_B] \neq 0$.*

Proof. We assume again that C is diagonal in the computational basis and that the ground state is given by $|00\rangle$. Using the same methods as in the proof of Theorem 7.1, one can show that the first order correction to the ground state, $|\psi_1\rangle$, must be orthogonal to $|00\rangle$ and to all $|kl\rangle$, with $k,l > 0$, i.e. to $|11\rangle$ and $|12\rangle$. Similar orthogonality constraints hold for the corrections to the most excited state. Thus, the operator L must have the following structure:

$$
L = \begin{pmatrix}
\cdot & \cdot & \cdot & \cdot & 0 & 0 \\
\cdot & \cdot & \cdot & \cdot & \cdot & 0 \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
0 & \cdot & \cdot & \cdot & \cdot & \cdot \\
0 & 0 & \cdot & \cdot & \cdot & \cdot
\end{pmatrix}. \tag{7.11}
$$

Due to the product structure of L, this means that L_A (or L_B) must be diagonal in the computational basis, too. This implies that it commutes with C_A (or C_B), leading to a contradiction. $\qquad\square$

The question remains whether a similar condition holds in higher dimensions as well. One direction of the statement is still true, i.e., if $[C_A, L_A] = 0$ or $[C_B, L_B] = 0$, entanglement detection is not possible, as the first part of the proof of Theorem 7.1 is valid in any dimension. In contrast, the converse direction does not hold, as one can find counterexamples of non-commuting C and L that have separable ground and excited states in any linear combination. These examples can be found already for the case of qubit-ququart, as well as qutrit-qutrit systems. The construction of these counterexamples can be found in Ref. [157].

7.6 Connection to joint measurability

An interesting consequence of Theorem 7.1 is that while entanglement detection is not possible with subsystem-wise commuting product observables, it is possible with jointly measurable observables. As an example, we consider the two POVMs

$$\{E_1^{(1)} = (\mathbb{1} + X/\sqrt{2})/2, \quad E_2^{(1)} = (\mathbb{1} - X/\sqrt{2})/2\}, \tag{7.12}$$

$$\{E_1^{(2)} = (\mathbb{1} + Z/\sqrt{2})/2, \quad E_2^{(2)} = (\mathbb{1} - Z/\sqrt{2})/2\}. \tag{7.13}$$

These two POVMs are noisy versions of Pauli X and Z measurements, and jointly measurable [158]. If we choose $C_A = C_B = E_1^{(1)}$ and $L_A = L_B = E_1^{(2)}$, then $[C_A, L_A] \neq 0 \neq [C_B, L_B]$, thus, entanglement detection is possible. Indeed, knowledge of $\langle C \rangle$ and $\langle L \rangle$ allows to recover $\langle X \otimes X \rangle$ and $\langle Z \otimes Z \rangle$. As we have discussed in the beginning of Section 7.2, this knowledge suffices for entanglement detection.

7.7 Conclusions

In this section, we analyzed the question in which cases knowing the expectation values of two product observables allows for entanglement detection. As product observables are usually easier to implement in experiments, and the number of two observables is the minimal number required to detect entanglement, this scenario is of great relevance.

We investigated the case of two-qubit and qubit-qutrit systems in great detail and gave necessary and sufficient criteria for general two-qubit observables and non-degenerate qubit-qutrit observables, i.e., they are able to detect entanglement whenever the individual commutators do not vanish. Finally, we showed that in contrast, there are jointly measurable observables that are able to detect entanglement.

Interestingly, while non-commutativity is a necessary criterion in all dimensions, it is only sufficient in the two cases mentioned above. This is in close resemblance to the PPT criterion for entanglement detection, which is necessary and sufficient only in these dimensions as well. This clearly deserves further investigation, as it might reveal a hidden mathematical connection between the two scenarios.

Furthermore, it would be beneficial to characterize the properties of higher-dimensional systems as well and find necessary or sufficient criteria there. However, this scenario is much more involved and is also numerically harder to treat due to the exponentially growing number of degrees of freedom. Finally, a generalization to more than two product observables might be fruitful. For example, it might be possible to find three observables where each pair of observables is useless, but joint knowledge of the expectation values of all three of them allows for entanglement detection.

8 Certifying quantum memories

Prerequisites

8.1 Introduction

In this final chapter of the thesis, we focus our attention on the problems of physical implementations of quantum computers. In contemporary implementations of these devices, error rates limit the performance, which is why contemporary devices are limited to approximately 50 qubits and restricted sets of quantum gates [159].

The errors are mainly due to two limitations: First, quantum gates are not implemented perfectly and do not behave correctly in all cases. Second, quantum states need to be stored intact for a certain amount of time to enable lengthy calculations, which requires deployment of quantum memories. The time from preparation until a stored quantum state degrades so significantly that it becomes useless for the computational task is called decoherence time [160]. The implementation of adequately working quantum memories can be the main obstacle in the construction of quantum computers. Therefore, it comes as no surprise that a sufficiently large decoherence time is one of DiVincenzo's criteria for the construction of useful quantum computers [161].

Quantum memories are not only important for quantum computers, but also for numerous experiments and protocols. For instance, implementing network protocols like quantum key distribution for spatially separated parties requires the ability to share quantum states over large distances. A promising proposal for this task makes use of quantum repeaters [162–164]. These are intermediate stations that, in the easiest implementation, share entangled Bell states with each other. The pairs are then used to teleport a quantum state from Alice to Bob at a later time, utilizing a quantum

teleportation scheme between the repeaters repeatedly. The functioning of this concept relies heavily on the intermediate parties being able to store the shared Bell pairs over long time intervals, making quantum memories an inevitable building block of repeater based networks.

Additionally, quantum memories could be of great advantage for single-photon sources, which are important quantum optical building blocks [165–168]. These photon sources usually use parametric down-conversion to create entangled photon pairs. If one of the photons is eventually detected, it is certain that a second photon was created, which can then be processed further. However, the creation is a stochastic process. For many applications, however, it is desirable to have access to photons at precise, deterministic times. Thus, quantum memories could be used to store the second photon, and the detection of the first photon acts as a herald that the quantum memory actually received a photon to store, from where it can be retrieved at the desired time.

All of these applications are reasons for the ongoing development of suitable quantum memory devices [169–175].

In this chapter, we study the performance of quantum memories from a theoretical point of view. We focus on quantum memories that are part of quantum computers, which give us the ability to perform arbitrary unitary pre- and post-processing. We consider the question of how to evaluate the quality of such devices. To that end, we survey existing quality measures, from which we extract a list of abstract criteria that such a quality quantifier should obey.

Most of the existing measures are based on entanglement. While some tasks indeed require a certain amount of entanglement, others require sufficient coherence in some preferred basis instead, for instance the phase discrimination task introduced in Section 2.8.2. Consequently, we define a family of three new quality measures based on how well the coherence is preserved by the memory. Finally, we show that the introduced measures fulfill the abstract criteria introduced before.

We begin with a brief overview of the main sources of errors in quantum memory devices.

8.2 Sources of errors in quantum memories

There are two fundamentally different types of errors that can occur during the storage of quantum states, especially if single photons are the carrier of information. The

memory can fail to emit a state at all, or the emitted state could differ too much from the input state.

The first kind of error is connected to the so-called efficiency of a device. It is defined as the probability that the memory emits an information carrier at all. Current implementations have efficiencies ranging from 5% for quantum dot-based devices, to nearly 100% in collective atomic gas-based devices [162].

Here, we are more concerned with the second kind of error, namely faulty output states, as the characterization of these errors is less straight-forward, but important for all applications, whereas a memory with small efficiency might still be useful in certain scenarios.

One important class of errors of the second kind are unitary rotations. For example, a trivial quantum memory for photons could consist of a long fiber coil that delays the propagation of the photon. Such fibers induce rotations to the polarization of the photon, which is described by a unitary rotation of the quantum state. If the fiber can be characterized sufficiently, this unitary is known and constant for each run. Similar effects can happen in ion-based memories, where background magnetic fields induce unitary rotations of states. However, we are mainly interested in memories embedded into a quantum computer, where such unitary errors could be easily corrected.

8.3   Existing quantum memory quality measures

Apart from the efficiency, the most commonly used performance measure for quantum memories is the fidelity. It is defined as the overlap between the incoming and the outgoing state. Thus, a unit fidelity indicates that the state was re-emitted unchanged, whereas vanishing fidelity means that an orthogonal state was reproduced instead.

The fidelities of contemporary quantum memories range from 0.7 in atomic gas-based memories to 0.94 for quantum dot devices [162]. For memories with low efficiencies, sometimes a conditional fidelity is used instead, where only runs with re-emitted quantum states are considered, where values of up to 0.97 are obtained for rare-earth doped crystal-based memories [162].

Depending on the specific application, the fidelity can be an insufficient choice for a performance measure. As mentioned before, in some cases fixed unitary rotations are correctable or do not matter at all, for example for certain Bell measurements [176]. As an alternative, it has been proposed to use the purity of the output as a performance measure in these cases instead [162]. However, this approach has other drawbacks: A

memory device that outputs a fixed pure state on demand will reach unit purity, even though the output is completely uncorrelated with the input.

Another approach is based on the capability of a memory to preserve entanglement, and some schemes have been developed to reduce the number of measurements in bipartite optical systems [177, 178]. Furthermore, in the case of untrusted measurement devices, quantum steering has been proposed as an alternative measure. In both cases, memories which do not conserve entanglement can be distinguished [179]. More recently, also a resource theory of quantum memories was developed [180]. Here, the free memories in a resource theoretic sense are those destroying the entanglement, and arbitrary classical pre- and post-processing is allowed in a quantum game assessing the performance of the memory.

Finally, it is possible to perform a full process tomography of the quantum memory, revealing its mathematical representation as a quantum channel [181, 182]. From this, all properties of the memory can be calculated. Process tomography, however, requires many well-characterized measurements as well as good state preparation capabilities and is therefore technically challenging and time-consuming.

8.4 Criteria for quality measures

Good quantum memories preserve as many of the non-classical properties as possible, as these are essential for the performance of quantum algorithms. A perfect quantum memory is given by the identity channel, its implementation, however, is difficult in practice.

In contrast, bad memories correspond to measure-and-prepare (M&P) schemes as introduced in Definition (2.10). These schemes can be simulated using classical memories only, by storing the classical measurement result and preparing a corresponding state at a later time.

We take these two observations and use them as a guiding principle for our requirements on measures for the quality of a memory. On the one hand, such measures should assign maximal values to the identity channel as well as mere unitary rotations, as these can be corrected for later on and therefore preserve the state. On the other hand, there should be a nontrivial upper bound for measure-and-prepare devices. Thus, a value exceeding this bound certifies genuine quantum memory.

This definition can be stated formally as follows:

Definition 8.1. A function $\mathcal{M} \mapsto Q(\mathcal{M}) \in [0,1]$ for channels $\mathcal{M}$ is called *memory quality measure*, if the following holds:

M1: $Q(\mathcal{M}) = 1$ if $\mathcal{M}(\rho) = V\rho V^\dagger$ for some unitary V,

M2: There is a constant $c \in [0,1)$ such that $Q(\mathcal{M}) \leq c$ if $\mathcal{M}$ is a M&P channel.

We call a memory quality measure *sharp*, if it additionally fulfills

M1': $Q(\mathcal{M}) = 1$ if and only if $\mathcal{M}(\rho) = V\rho V^\dagger$ for some unitary V.

While condition M1 requires that unitary channels including the identity channel have maximal quality, the stricter condition M1' requires that this is true only for unitary channels. Interestingly, M1' implies M2 already if the measure is continuous on the set of quantum channels, because the subset of measure-and-prepare channels is compact [7], implying that each M&P channel has finite distance to the set of unitary channels.

8.5 A coherence based quality measure

Given that most existing measures are either not fulfilling the above-given properties, or require enormous resources to be evaluated, we now want to define and characterize a measure that is relatively easy to evaluate, as well as being a memory quality measure in the sense defined above.

We base this measure on the ability of a quantum memory to preserve the coherence of quantum states. Coherence has experienced growing interest recently, partly because of theoretical advances in the field of resource theories, which led to a list of defining properties for coherence measures [54]. Consequently, many coherence measures have been found, and some of them have been introduced in Section 2.8 already.

For this section, there are several suitable choices of a coherence measure C. As we are concerned with coherences w.r.t. different bases and different dimensions, we adopt the following two conventions.

First of all, we label the D-dimensional basis w.r.t. which the coherence is measured by $\{|b_j\rangle\}_{j=1}^{D}$. This basis is conveniently represented by a unitary matrix U such that $|b_j\rangle = U|j\rangle$, where $|j\rangle$ denotes the j-th basis state from the canonical basis. We append the corresponding basis as a parameter to the measure C, i.e., we write $C_U(\rho)$ when referring to the coherence of the quantum state ρ w.r.t. the basis parameterized by U.

Second of all, we assert that the coherence measure is normalized to range from 0 (for incoherent states) to 1 (for maximally coherent states) in all dimensions.

The results obtained in this chapter are valid for all such measures as long as they are continuous, convex, and the only states maximizing it being

$$|\Psi_U^{\vec{\alpha}}\rangle := \frac{1}{\sqrt{D}} \sum_{j=0}^{D-1} e^{i\alpha_j} |b_j\rangle = UZ_{\vec{\alpha}}|+\rangle, \tag{8.1}$$

where $\vec{\alpha}$ is a D-dimensional phase vector and $Z_{\vec{\alpha}} = \sum_{j=1}^{D} e^{i\alpha_j}|j\rangle\langle j|$ is a phase gate with phases $\vec{\alpha}$. The state $|+\rangle$ is defined as

$$|+\rangle = \frac{1}{\sqrt{D}} \sum_j |j\rangle. \tag{8.2}$$

This last assumption is rather natural, as many popular coherence measures fulfill it. Among these are also the two measures introduced in Section 2.8, namely the robustness of coherence and the l_1-norm of coherence [55, 183]. Furthermore, these states are also maximally coherent in the sense of resource theories [54, 55].

As a concrete example of a coherence measure adapted to varying basis and normalization fulfilling all the properties required here, we extend the definition of the robustness of coherence from Eq. (2.62). The normalized, basis dependent robustness of coherence reads

$$C_{R,U}(\rho) := \frac{1}{D-1} \min_{\tau \in \mathcal{D}, s \geq 0} \left\{ s \left| \frac{\rho + s\tau}{1+s} \in \mathcal{I}_U \right. \right\}, \tag{8.3}$$

where $\mathcal{D}$ denotes the set of D-dimensional quantum states and $\mathcal{I}_U$ denotes the set of incoherent, i.e., diagonal states w.r.t the basis defined by U.

In the following, we will define a memory quality measure based on coherence. As such, the values it assigns to quantum memories should reflect its usefulness for coherence based tasks. Therefore, it should identify the most classical basis, that is, the basis in which all maximally coherent states are mapped to states of smallest coherence. This coherence then defines the quality.

Mathematically, we state this as follows:

Definition 8.2. Given a quantum channel $\mathcal{M}$, the quality Q_0 is defined as

$$Q_0(\mathcal{M}) := \min_U \max_{\vec{\alpha}} C_U[\mathcal{M}(|\Psi_U^{\vec{\alpha}}\rangle)]. \tag{8.4}$$

$$Q_0(\mathcal{M}) = \min_U \quad \max_{\vec{\alpha}} \quad |+\rangle - \boxed{Z_{\vec{\alpha}}} - \boxed{U} - \boxed{\mathcal{M}} - \boxed{U^\dagger} - \langle C$$

$$Q_-(\mathcal{M}) = \min_{U,U'} \max_{\vec{\alpha}} \quad |+\rangle - \boxed{Z_{\vec{\alpha}}} - \boxed{U} - \boxed{\mathcal{M}} - \boxed{U'^\dagger} - \langle C$$

$$Q_+(\mathcal{M}) = \min_U \quad \max_{|\psi\rangle} \quad |\psi\rangle - \boxed{\mathcal{M}} - \boxed{U^\dagger} - \langle C$$

FIGURE 8.1: The three measures Q_0, Q_- and Q_+ from Defs. 8.2 - 8.4, represented as quantum circuits. The measures are obtained by optimization over the input states and measuring the coherence of the output in certain bases which are optimized over as well.

Here, the maximization is over all maximally coherent states given by Eq. (8.1). Note that we write $\mathcal{M}(|\Psi_U^{\vec{\alpha}}\rangle)$ instead of $\mathcal{M}(|\Psi_U^{\vec{\alpha}}\rangle\langle\Psi_U^{\vec{\alpha}}|)$ to shorten the notation. The definition of Q_0 is visualized as a quantum circuit in Fig. 8.1.

If the robustness of coherence is used as the coherence measure, the value of Q_0 has an operational interpretation in the context of the phase discrimination task introduced in Section 2.8.2. There, the improvement of using quantum probe states over naive guessing is quantified by their coherence. Thus, Q_0 yields the minimal achievable advantage when storing proper probe states in the memory prior to such a discrimination task in an arbitrary basis.

Note that Q_0 is not the only possible performance measure based on coherence. In fact, it will be useful to define two similar measures that act as lower and upper bound on Q_0, respectively. First, it is possible to minimize over the basis of the maximally coherent states independently of the basis in which the coherence of the output is measured:

Definition 8.3. Given a quantum channel $\mathcal{M}$, the quality Q_- is defined as

$$Q_-(\mathcal{M}) := \min_{U,U'} \max_{\vec{\alpha}} C_{U'}[\mathcal{M}(|\Psi_U^{\vec{\alpha}}\rangle)]. \tag{8.5}$$

Clearly, $Q_-(\mathcal{M}) \leq Q_0(\mathcal{M})$.

Second, instead of maximizing over maximally coherent states, we can instead maximize over all states:

Definition 8.4. Given a quantum channel $\mathcal{M}$, the quality Q_+ is defined as

$$Q_+(\mathcal{M}) := \min_U \max_\rho C_U[\mathcal{M}(\rho)]$$
$$= \min_U \max_{|\psi\rangle} C_U[\mathcal{M}(|\psi\rangle)]. \tag{8.6}$$

Note that maximization over all states is equivalent to maximization over pure states due to the convexity of the coherence measure. Due to the additional freedom in the maximization, we have $Q_0(\mathcal{M}) \leq Q_+(\mathcal{M})$. The definitions of $Q_\pm$ are displayed as quantum circuits in Fig. 8.1 as well.

Finally, we remark that in parallel to the creation of this work, a similar approach has been developed by different authors, which also assesses the quality of memory devices based on coherence [184]. Their approach is based on the average preserved coherence.

8.6 Properties of the measures

Due to the optimization over the unitary basis, the three qualities are invariant under unitary pre- and post-processing. This means that for all channels $\mathcal{M}$ and unitary rotations $\mathcal{V}(\rho) = V\rho V^\dagger$ for some unitary matrix V, for Q_0 it holds that

$$Q_0(\mathcal{M}) = Q_0(\mathcal{V} \circ \mathcal{M} \circ \mathcal{V}^{-1}), \tag{8.7}$$

while for $Q_\pm$ it holds that

$$Q_\pm(\mathcal{M}) = Q_\pm(\mathcal{V} \circ \mathcal{M}) = Q_\pm(\mathcal{M} \circ \mathcal{V}). \tag{8.8}$$

Additionally, the quality measure Q_+ satisfies a useful pre-processing property:

Lemma 8.5. *The quality measure Q_+ cannot be increased by pre-processing of the input, i.e., $Q_+(\mathcal{M} \circ \mathcal{N}) \leq Q_+(\mathcal{M})$ for all quantum channels $\mathcal{M}$ and $\mathcal{N}$.*

Proof. By definition,

$$Q_+(\mathcal{M} \circ \mathcal{N}) = \min_U \max_\rho C_U(\mathcal{M}(\mathcal{N}(\rho)))$$
$$\leq \min_U \max_\rho C_U(\mathcal{M}(\rho)) = Q_+(\mathcal{M}), \tag{8.9}$$

which proves the lemma. □

Furthermore, the measures are continuous maps.

Lemma 8.6. *The quantities $Q_\pm$ and Q_0 are continuous.*

Proof. Let $\mathcal{M}$ be a quantum channel with the corresponding Choi state $\eta_{\mathcal{M}}$ given by Eq. (2.52),

$$\eta_{\mathcal{M}} = \mathbb{1} \otimes \mathcal{M}(|\phi^+\rangle), \tag{8.10}$$

with $|\phi^+\rangle$ being the maximally entangled state $\frac{1}{\sqrt{D}} \sum_i |ii\rangle$. Using the Choi state, the inner part of the expressions for Q_- and Q_0 can be written as

$$
\begin{aligned}
&C_{U'}(\mathcal{M}(|\Psi_U^{\vec{\alpha}}\rangle)) \\
=&C_{U'}(D \, \mathrm{Tr}_A[(|\Psi_U^{\vec{\alpha}}\rangle\langle\Psi_U^{\vec{\alpha}}|^{\mathrm{T}} \otimes \mathbb{1})\eta_{\mathcal{M}}]),
\end{aligned} \tag{8.11}
$$

which is continuous in α, U, U' and $\eta_{\mathcal{M}}$. Repeatedly applying the maximum theorem [185], and using the fact that the robustness of coherence is continuous [186], shows that Q_- and Q_0 are continuous in $\eta_{\mathcal{M}}$.

If a sequence of channels $\{\mathcal{M}_i\}_i$ converges to a channel $\mathcal{M}$ with regard to the diamond norm, then the sequence $\{\eta_{\mathcal{M}_i}\}_i$ must converge to $\eta_{\mathcal{M}}$ [187, 188]. This implies that the function above is also continuous in $\mathcal{M}$. For Q_+, a similar argument holds. $\qquad\square$

We still have to show that Q_0 and $Q_\pm$ are sharp memory quality measures in the sense of Definition 8.1. We begin with property M1.

Lemma 8.7. *The measures $Q_\pm$ and Q_0 fulfill property M1, i.e. $Q(\mathcal{V}) = 1$ for all unitary channels $\mathcal{V}$.*

Proof. As $Q_-(\mathcal{M}) \leq Q_0(\mathcal{M}) \leq Q_+(\mathcal{M})$, it suffices to show the property for Q_-. Furthermore, as Q_- is invariant under unitary rotations, it suffices to consider only the identity channel id. Recall that

$$Q_-(\mathrm{id}) = \min_{U,U'} \max_{\vec{\alpha}} C_{U'}(UZ_{\vec{\alpha}}|+\rangle) = 1, \tag{8.12}$$

where $Z_{\vec{\alpha}}$ is a diagonal matrix with phases $e^{i\alpha_j}$ as entries, is equivalent to the statement that for all bases U and U', there exists a maximally coherent state in U that is also maximally coherent in U'. This can be stated as follows: for all U there exist vectors $\vec{\alpha}$ and $\vec{\beta}$, such that

$$Z_{\vec{\beta}}^\dagger U Z_{\vec{\alpha}}|+\rangle = |+\rangle, \tag{8.13}$$

which is equivalent to the statement that the sets of maximally coherent states with regard to two different bases always have a non-empty intersection. This interesting geometrical question has been investigated and answered affirmatively recently; it was

shown that any unitary operator U can be decomposed as [189]

$$U = Z_1 X Z_2, \tag{8.14}$$

where Z_1 and Z_2 are diagonal unitaries with the upper left entry equal to 1 and X is a unitary matrix where the elements in each row and each column sum to 1. Inserting this decomposition into Eq. (8.13) shows that choosing $\vec{\alpha}$ and $\vec{\beta}$ such that $Z_{\vec{\alpha}} = Z_1^{\dagger}$ and $Z_{\vec{\beta}} = Z_2$ yield the desired equality, as $|+\rangle$ is an eigenstate of X. $\qquad\square$

Second, we show that also M1′ holds by showing the converse statement.

Theorem 8.8. $Q_{\pm}$ and Q_0 fulfill property M1′, i.e., if $Q(\mathcal{M}) = 1$, then $\mathcal{M}$ is a unitary channel.

Proof. To prove the theorem, it is sufficient to consider $Q_+(\mathcal{M}) = 1$, as $Q_-(\mathcal{M}) \leq Q_0(\mathcal{M}) \leq Q_+(\mathcal{M}) \leq 1$. If $Q_+(\mathcal{M}) = 1$, then for all unitaries U it holds that

$$\max_{|\psi\rangle} C_U[\mathcal{M}(|\psi\rangle)] = 1. \tag{8.15}$$

This implies that for all U, there exists a state $|\Phi\rangle$ and a maximally coherent state $|\Psi\rangle$ with regard to U such that

$$\mathcal{M}(|\Phi\rangle) = |\Psi\rangle. \tag{8.16}$$

To prove the statement, we show the following three facts:

(i) If $Q_+(\mathcal{M}) = 1$, then we can find a basis $\{|\Phi_i\rangle\}$ that is mapped to a basis $\{|\Psi_i\rangle\}$ by $\mathcal{M}$.

(ii) In the range of $\mathcal{M}$, there exist vectors $\{|\Psi_{1j}\rangle = \sum_{i=1}^D \beta_i^{(j)}|\Psi_i\rangle\}_{j=2}^D$ with the property $\beta_1^{(j)} \neq 0 \neq \beta_j^{(j)}$ for all j.

(iii) From the existence of the $|\Psi_i\rangle$ and $|\Psi_{1j}\rangle$, it follows that $\mathcal{M}$ is unitary.

For the first fact, in order to find state $|\Psi_1\rangle$, we simply choose a random basis and obtain a pure (maximally coherent) state in the range of $\mathcal{M}$ due to the property $Q_+(\mathcal{M}) = 1$. For the second state $|\Psi_2\rangle$, we choose a basis with $|\Psi_1\rangle$ as a basis state. The corresponding maximally coherent state has an overlap of $|\langle\Psi_1|\Psi_2\rangle| = \frac{1}{\sqrt{D}}$ and is therefore linearly independent. All other states $|\Psi_i\rangle$ can be found step by step: Let us assume that we have already found the linearly independent states $|\Psi_1\rangle, \dots, |\Psi_m\rangle$. We construct an orthonormal set of states spanning the same subspace and extend it

to an orthonormal basis. The corresponding maximally coherent state has nonvanishing overlap with the space orthogonal to $\text{span}\{|\Psi_1\rangle, \ldots, |\Psi_m\rangle\}$ and is therefore also linearly independent.

With this procedure, we obtain the nonorthonormal basis $\{|\Psi_i\rangle\}$. The corresponding preimages also form a basis, as, from the Kraus decomposition (see also below) it follows that the dimension of their span must be equal to D as well.

For the second fact, we have to show the existence of the vectors $\{|\Psi_{1j}\rangle\}$ with the properties mentioned above. It suffices to show the existence of $|\Psi_{12}\rangle$; the proof for the other $|\Psi_{1j}\rangle$ is analogous.

Given the basis $\{|\Psi_i\rangle\}$, we consider the normalized dual basis $\{|\gamma_i\rangle\}$ with the property $\langle\gamma_i|\Psi_j\rangle = c_i\delta_{ij}$ for some $c_i > 0$ [190]. In this basis, $\beta_i^{(j)} = c_i^{-1}\langle\gamma_i|\Psi_{1j}\rangle$ holds. Now we search for a vector $|\Psi_{12}\rangle$ in the range of $\mathcal{M}$ with the properties $\langle\gamma_1|\Psi_{12}\rangle \neq 0 \neq \langle\gamma_2|\Psi_{12}\rangle$, as from these conditions the presence of the desired coefficients $\beta_1^{(2)}$ and $\beta_2^{(2)}$ follows.

To this end, consider the orthonormal basis $|b_1\rangle = |\gamma_1\rangle$, $|b_2\rangle \propto |\gamma_2\rangle - \langle\gamma_1|\gamma_2\rangle|\gamma_1\rangle$ and the other $|b_i\rangle$ arbitrary. The maximally coherent state $|\Psi\rangle$ in the range of $\mathcal{M}$ in this basis can be written as $|\Psi\rangle = \frac{1}{\sqrt{D}}\sum_{k=1}^{D} e^{i\phi_k}|b_k\rangle$. The overlaps are given by

$$\langle\gamma_1|\Psi\rangle \propto e^{i\phi_1} \neq 0,$$
$$\langle\gamma_2|\Psi\rangle \propto \langle\gamma_2|b_1\rangle e^{i\phi_1} + \langle\gamma_2|b_2\rangle e^{i\phi_2}. \tag{8.17}$$

If $|\langle\gamma_2|b_1\rangle| \neq |\langle\gamma_2|b_2\rangle|$, $|\Psi_{12}\rangle = |\Psi\rangle$ satisfies the desired properties.

Otherwise, we instead choose the basis given by $|b_1'\rangle = \sqrt{\frac{2}{3}}|b_1\rangle + \sqrt{\frac{1}{3}}e^{i\theta}|b_2\rangle$ and $|b_2'\rangle = \sqrt{\frac{1}{3}}|b_1\rangle - \sqrt{\frac{2}{3}}e^{i\theta}|b_2\rangle$ and the other $|b_i'\rangle$ arbitrary. Now, the maximally coherent state $|\Psi'\rangle = \frac{1}{\sqrt{D}}\sum_{k=1}^{d} e^{i\phi_k'}|b_k'\rangle$, with respect to the basis $\{|b_i'\rangle\}$, in the range of $\mathcal{M}$ has the overlaps

$$\langle\gamma_1|\Psi'\rangle \propto \sqrt{\frac{2}{3}}e^{i\phi_1'} + \sqrt{\frac{1}{3}}e^{i\phi_2'} \neq 0, \tag{8.18}$$

$$\langle\gamma_2|\Psi'\rangle \propto (\sqrt{\frac{2}{3}}e^{i\phi_1'} + \sqrt{\frac{1}{3}}e^{i\phi_2'})\langle\gamma_2|b_1\rangle$$
$$+ (\sqrt{\frac{1}{3}}e^{i\phi_1'} - \sqrt{\frac{2}{3}}e^{i\phi_2'})e^{i\theta}\langle\gamma_2|b_2\rangle. \tag{8.19}$$

As in this case $|\langle\gamma_2|b_1\rangle| = |\langle\gamma_2|b_2\rangle|$, we can choose θ such that $\langle\gamma_2|b_1\rangle = e^{i\theta}\langle\gamma_2|b_2\rangle \neq 0$. Then the right-hand side of Eq. (8.19) is proportional to $(\sqrt{2} + 1)e^{i\phi_1'} + (1 - \sqrt{2})e^{i\phi_2'}$, which cannot vanish. Thus, in this case we choose $|\Psi_{12}\rangle = |\Psi'\rangle$.

Finally, concerning the third fact, as $\mathcal{M}$ is a quantum channel, it admits a Kraus representation, i.e., $\mathcal{M}(\rho) = \sum_{l=1}^{r} K_l \rho K_l^\dagger$ with $\sum_l K_l^\dagger K_l = \mathbb{1}$. Using the fact that the $|\Phi_i\rangle$ are mapped to pure states, we have for all $l = 1, \ldots, r$ that

$$K_l |\Phi_i\rangle = \mu_{li} |\Psi_i\rangle \tag{8.20}$$

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

$$K_l |\Phi_{1j}\rangle = \kappa_{lj} |\Psi_{1j}\rangle \tag{8.21}$$

for some $|\Phi_{1j}\rangle = \sum_{k=1}^{D} \alpha_k^{(j)} |\Phi_k\rangle$ and $j = 2, \ldots, D$.

Decomposing the right-hand side of Eq. (8.21) in terms of the basis $\{|\Psi_i\rangle\}$ and using linearity on the left-hand side, we have

$$\sum_{k=1}^{D} \mu_{lk} \alpha_k^{(j)} |\Psi_k\rangle = \kappa_{lj} \sum_{k=1}^{D} \beta_k^{(j)} |\Psi_k\rangle \tag{8.22}$$

for all l. Thus, for all l, j and k,

$$\mu_{lk} \alpha_k^{(j)} = \kappa_{lj} \beta_k^{(j)}. \tag{8.23}$$

For a fixed j, consider the two equations for $k = 1$ and $k = j$, where the corresponding $\beta_k^{(j)}$ do not vanish by assumption. If $\alpha_1^{(j)}$ or $\alpha_j^{(j)}$ were 0, $\kappa_{lj} = 0$ for all l would follow. This would imply that $\mathcal{M}(|\Phi_{1j}\rangle) = 0$, which cannot be true if $\mathcal{M}$ is a channel.

Otherwise, if κ_{lj} was 0 for one l, then this would imply that $\mu_{l1} = \mu_{lj} = 0$ for this l. However, $\mu_{l1} = 0$ implies that $\kappa_{lj'} = 0$ for all j', which in turn implies that $\mu_{lj'} = 0$ for all j'. Thus, K_l would map a whole basis to 0 and, therefore, vanishes and can be neglected from the decomposition of the channel.

Thus, we have that $\kappa_{lj} \neq 0$ and, from that, $\mu_{l1} \neq 0 \neq \mu_{lj}$. Then, the ratio

$$\frac{\mu_{l1}}{\mu_{lj}} = \frac{\beta_1^{(j)} \alpha_j^{(j)}}{\beta_j^{(j)} \alpha_1^{(j)}} \tag{8.24}$$

is independent of l. As this holds for all j, it follows from Eq. (8.20) that the K_l must be proportional to each other, i.e., $K_l \propto K_{l'}$. Using now that $\mathcal{M}$ is trace preserving, i.e. $\sum_l K_l^\dagger K_l = \mathbb{1}$, leads to $K_l^\dagger K_l \propto \mathbb{1}$. Thus, all Kraus operators have to be proportional to the same unitary V, and hence, $\mathcal{M}(\rho) = V \rho V^\dagger$. $\qquad \square$

It follows immediately from the proof above that, to completely characterize a unitary channel, it is sufficient to prepare a basis that is mapped to another basis by that channel and another pure state in the image which has nonvanishing coefficients in

the latter basis. If one can find such states, the channel is guaranteed to be unitary and is uniquely determined by those states up to a global phase. Since pure states can be characterized with few measurements [99, 191], the same can also be done with unitary quantum channels $\mathcal{M}$. Such a characterization has also been constructively obtained in [192].

Finally, as the continuity of $Q_\pm$ and Q_0 together with property M1' implies property M2, it follows that:

Corollary 8.9. *The quantities $Q_\pm$ and Q_0 are sharp memory quality measures.*

In the case of single-qubit channels, it is possible to find tight upper bounds for M&P channels for Q_0 and Q_+ of $\frac{1}{\sqrt{2}}$ and of $\frac{1}{\sqrt{5}}$ for Q_-. For the derivation of these bounds, see Ref. [186].

It should be noted that the measures introduced here are not faithful in the sense that any non-M&P channel can be detected. This is not possible with any efficiently computable single measure, because such a measure would solve the separability problem, which is NP-hard [193].

As a very simple example, we consider the depolarizing channel Δ_p of a single D-dimensional particle, given by [27]

$$\Delta_p(\rho) = p\rho + \frac{1-p}{D}\mathbb{1}. \tag{8.25}$$

Physically, this corresponds to a memory that outputs with probability p the correct state, but with probability $1 - p$ the output is completely random.

As the coherence measure, we use the normalized l_1-norm of coherence from Section 2.8.2. This measure is sensitive to the off-diagonal entries of the quantum state only. Thus, mixing it with the maximally mixed state yields only a factor, i.e.,

$$C_{l_1}[\Delta_p(\rho)] = C_{l_1}[p\rho + \frac{1-p}{D}\mathbb{1}] = pC_{l_1}(\rho). \tag{8.26}$$

This allows us to calculate $Q_\pm$ analytically:

$$Q_+(\Delta_p) = \min_U \max_\rho C_U[\Delta_p(\rho)] \tag{8.27}$$

$$= p \min_U \max_\rho C_U[\rho] \tag{8.28}$$

$$= p, \tag{8.29}$$

where the last equality is due to the fact that the second line corresponds to p times the quality of the identity channel, which is equal to unity by property M1.

Analogously, $Q_-(\Delta_p) = p$ and therefore $Q_0(\Delta_p) = p$ as well. This is a sensible value for the quality, as p corresponds directly to the probability that the channel works as expected.

8.7 Experimental estimation

The question remains of how the quality measures can be estimated in experiments. For single-qubit systems and memories close to a unitary channel, few measurements suffice to obtain good estimates [186].

For higher-dimensional channels, the estimation is more involved. In the following, we discuss how experimental data from higher-dimensional quantum memories $\mathcal{M}$ could be used to estimate the memory performance measure $Q_0(\mathcal{M})$. Since we know that $Q_0(\mathcal{M}) = 1$ iff $\mathcal{M}$ is unitary, we write $\mathcal{M} = \mathcal{V} + \mathcal{K}$, where $\mathcal{V}$ is some unitary channel and $\mathcal{K}(\rho) = \mathcal{M}(\rho) - \mathcal{V}(\rho)$ for all states ρ. From Lemma 8.7, it follows that with respect to any basis U with basis vectors $|b_i\rangle$, there always exist two maximally coherent states $|\phi\rangle$ and $|\psi\rangle$ such that $\mathcal{V}(|\phi\rangle) = |\psi\rangle$. Thus, for $\rho = \mathcal{M}(|\phi\rangle) = |\psi\rangle\langle\psi| + \mathcal{K}(|\phi\rangle\langle\phi|)$ we have that

$$
\begin{aligned}
C_U(\rho) &\geq -\frac{1}{D-1}\operatorname{Tr}(W\rho) \\
&= \frac{1}{D-1}\left(D\langle\psi|\rho|\psi\rangle - 1\right) \\
&= \frac{1}{D-1}\left(D + D\langle\psi|\mathcal{K}(|\phi\rangle\langle\phi|)|\psi\rangle - 1\right),
\end{aligned} \tag{8.30}
$$

where we have used the notion of coherence witnesses introduced in Ref. [56] with $W = \mathbb{1} - D|\psi\rangle\langle\psi|$, which gives a lower bound to the robustness of coherence. Let $\lambda = \min_\sigma \lambda_{\min}[\mathcal{K}(\sigma)]$, i.e., λ is the smallest eigenvalue of $\mathcal{K}(\sigma)$ for any state σ. Then,

$$
\begin{aligned}
Q_0(\mathcal{M}) &= \min_U \max_{\vec{\alpha}} C_U[\mathcal{M}(|\Psi_U^{\vec{\alpha}}\rangle)] \\
&\geq \frac{D(1+\lambda) - 1}{D-1}.
\end{aligned} \tag{8.31}
$$

To determine λ, we resort to the Choi matrix $\eta_\mathcal{K}$ of $\mathcal{K}$. Hence,

$$
\begin{aligned}
\lambda &= D\min_{\sigma,|s\rangle}\langle s|\operatorname{Tr}_A[(\sigma^T \otimes \mathbb{1})\eta_\mathcal{K}]|s\rangle \\
&= D\min_{|a\rangle|s\rangle}\langle a|\langle s|\eta_\mathcal{K}|a\rangle|s\rangle,
\end{aligned} \tag{8.32}
$$

which can be estimated using experimental data. For instance, let $\eta_{\mathcal{M}}$ and $|\phi_{\mathcal{V}}\rangle\langle\phi_{\mathcal{V}}|$ be the Choi matrix of the channels $\mathcal{M}$ and $\mathcal{V}$, respectively. $\mathcal{V}$ might be guessed heuristically from the obtained data, determining $|\phi_{\mathcal{V}}\rangle\langle\phi_{\mathcal{V}}|$. The experimental data will impose linear constraints on $\eta_{\mathcal{M}}$ and, hence, also on $\eta_{\mathcal{K}}$. Using a see-saw optimization, it is possible to optimize $\lambda = D\min_{\sigma,\rho}\mathrm{Tr}\big[(\sigma\otimes\rho)\eta_{\mathcal{K}}\big]$ over states σ and ρ with alternating semidefinite programs [59].

8.8 Conclusions

In this chapter, we had a close look at quantum memory devices as important building blocks for future quantum computers. As many tasks in a quantum computer rely on long decoherence times, the development and characterization of the memories become increasingly important. We highlighted the different kinds of errors that memories are prone to; loss of the quantum state (inefficiency) and erroneous output. Consequently, we discussed how the severity of the last kind of error can be assessed, and formulated criteria for bona fide quality measures.

As these criteria are not met by many currently used quality measures and given the fact that some quantum computation tasks require certain values of coherence in order to yield quantum advantage, we then defined three related measures based on the minimal coherence left in any basis and showed that they meet the criteria introduced before.

An important feature of quality measures is the existence of an upper bound on measure-and-prepare schemes, for which no quantum data needs to be stored. While we showed that our three measures fulfill these criteria, we did not yield a specific numerical value for this bound. This should be remedied in future work.

Finally, we gave a recipe on how the measures can be evaluated from experimental data.

Additionally, the methods introduced here could be generalized to other aspects of quantum computing and quantum information. For example, the results could be applied directly to the case of quantum teleportation schemes. Furthermore, they could be used to characterize the entangling power of two-qubit gates, whose ability to generate entanglement can be linked to increasing two-level coherences [194, 195].

Concluding remarks

This thesis was mainly concerned with deepening the understanding of capabilities and limitations of correlations in quantum states, and up to this point the word "correlation" appeared 142 times, or roughly once per page. However, there is a big difference between knowing the name of something and knowing something. Nevertheless, there is hope that the findings in this thesis help to illuminate the meaning behind the bare word.

To recapitulate, we began with the investigation of the marginal problem, i.e., whether correlations between a limited number of particles in a multi-particle state suffice to fix the joint state uniquely. We found that in the case of four-qudit states, the two-body marginals of certain particle pairs almost always suffice for this task. We generalized this statement to multipartite states of more than four parties by showing that certain correlations between all but two of them achieve the same determination of the global state.

We then generalized the marginal problem to the question of which correlations can fix a global state. Here, in the restricted case of multi-qubit states, we found that there is a deep connection between correlations among an even number and correlations among an odd number of the particles. In pure states of an odd number of parties, we found that the collection of odd correlations fixes the even correlations, whereas, in states of an even number of parties, the even correlations fix the odd ones. We highlighted the implications of this finding on the structure of ground states of Hamiltonians and entanglement detection.

We then considered sector lengths as quantifiers for the amount of correlation between a certain number of particles and evaluated their expressiveness for the properties of quantum states. We found that there are many monogamy-like restrictions on the sector lengths and that they are useful for the task of entanglement detection. Furthermore, we completely characterized admissible values of tuples of sector lengths in the case of two- and three-qubit states. Interestingly, the set of admissible tuples forms a convex polytope in these cases, a fact with no apparent reason that is worth

being investigated in more detail in the future. For one of the constraints describing this polytope for three-qubits, we found a connection to the strong subadditivity of linear entropies.

As sector lengths are local unitary invariants of degree two, we consequently explored how the additional knowledge of higher-degree invariants can help for the task of entanglement detection. We found that certain invariants of degree four connected to the distribution of measurement results are indeed helpful and allow for the formulation of more refined entanglement criteria. While we gave an analytical criterion in the case of two-qubit states, we formulated a conjecture based on numerical studies for states of three qubits.

We then turned our focus to questions of how entanglement can be detected with limited resources by considering scenarios where only the expectation values of two product observables are known. We found a necessary and sufficient criterion for two-qubit observables in order to be able to detect entanglement and similar results for a subset of qubit-qutrit observables.

In the last chapter, we developed criteria for measures aiming at assessing the performance of quantum memories. These devices are important building blocks for quantum computers and quantum communication devices, and their ability to store quantum states faithfully is essential for many applications in quantum computation and secure communication. Finally, we defined three quality measures which are based on coherence and fulfil the criteria, and showed how bounds on these measures can be found from experimental data.

Naturally, there are many unsolved problems and starting points for further research, which we highlighted in the conclusions of the corresponding chapters. We hope that not only the results, but also the tools developed in this thesis are helpful for future attempts to fill the gap between the word correlation and its true meaning.

Acknowledgments

I am indebted to many people who, in one way or the other, made the creation of this thesis possible.

First of all, I am grateful to my supervisor, Prof. Otfried Gühne, for giving me the opportunity to do my PhD in Siegen and for his guidance. When we met for the first time (while defusing a bomb), I did not even know where Siegen is located, and this was not the only lack of knowledge he eliminated.

I would like to thank everyone in the group for the wonderful atmosphere, the willingness to answer every stupid question at any time of the day and the inspiring discussions, especially during our lunch break activities.[1] I owe special thanks to my office mates Mariami Gachechiladze, Felix Huber, Tristan Kraft and Timo Simnacher for an endless amount of focused, disciplined and concentrated joint workdays. Timo, thank you for carrying my washing machine around and everything else! Mari, გმადლობთ, რომ დავითის ნათლია ხართ! I am obliged to the best secretary in the world, Daniela Lehmann. Without your glee and organizational assistance I would have descended into chaos about three years ago.

I am truly grateful to Jens Siewert for his hospitality and the great time in Bilbao. Furthermore, I am grateful to the countless number of great people from the community I met on the conferences and who gave me invaluable scientific input.

I acknowledge various support from the House of Young Talents Siegen and their scholarship program.

A thousand thanks go to my proof-readers Mariami, Felix, Tristan, Timo and Robert, without whom ~~tihs wrok wolud be totlaly unraedbale~~.

I am thankful to (and for) my wonderful wife and her incredible support and patience with me and our marvelous son, who helped a lot writing down this text by ~~slamming~~ typing on the keyboard. Last but not least, I would like to thank my family for the support and assistance and grandson/nephew-sitting.

---

[1] No kittens were harmed during the creation of this thesis.

List of publications

(A) Nikolai Wyderka, Felix Huber and Otfried Gühne
Almost all four-particle pure states are determined by their two-body marginals
Phys. Rev. A **96**, 010102 (2017)

(B) Nikolai Wyderka, Felix Huber and Otfried Gühne
Constraints on correlations in multiqubit systems
Phys. Rev. A **97**, 060101 (2018)

(C) Mariami Gachechiladze, Nikolai Wyderka and Otfried Gühne
The structure of ultrafine entanglement witnesses
J. Phys. A: Math. Theor. **51**, 365307 (2018)

(D) Andreas Ketterer, Nikolai Wyderka and Otfried Gühne
Characterizing multipartite entanglement with moments of random correlations
Phys. Rev. Lett. **122**, 120505 (2019)

(E) Timo Simnacher, Nikolai Wyderka, Cornelia Spee, Xiao-Dong Yu and Otfried Gühne
Certifying quantum memories with coherence
Phys. Rev. A **99**, 062319 (2019)

(F) Timo Simnacher, Nikolai Wyderka, René Schwonnek and Otfried Gühne
Entanglement detection with scrambled data
Phys. Rev. A **99**, 062339 (2019)

(G) Nikolai Wyderka and Otfried Gühne
Characterizing quantum states via sector lengths
arXiv:1905.06928

List of Figures and Tables

List of Figures

List of Tables

A A Sudoku-like game to prove sector length inequalities

In Section 5.3.1, we obtained an upper bound on the bipartite correlation length A_2 in multi-qubit states of $n \geq 3$ parties of $A_2 \leq \binom{n}{2}$. Here, we give an alternative, graphical proof for this fact for $n \geq 6$ that makes use of anticommuting sets and solving a Sudoku-like game.

As noted in the proof of Proposition 5.3, it is possible to distribute the Pauli operators of weight two acting on the pairs of parties $(1,2)$, $(1,3)$ and $(1,4)$ into three sets,

$$M_1 = \{XX\mathbb{1}\mathbb{1}, XY\mathbb{1}\mathbb{1}, XZ\mathbb{1}\mathbb{1}, \ Y\mathbb{1}X\mathbb{1}, Y\mathbb{1}Y\mathbb{1}, Y\mathbb{1}Z\mathbb{1}, \ Z\mathbb{1}\mathbb{1}X, Z\mathbb{1}\mathbb{1}Y, Z\mathbb{1}\mathbb{1}Z\}, \quad (\text{A.1})$$

$$M_2 = \{YX\mathbb{1}\mathbb{1}, YY\mathbb{1}\mathbb{1}, YZ\mathbb{1}\mathbb{1}, \ Z\mathbb{1}X\mathbb{1}, Z\mathbb{1}Y\mathbb{1}, Z\mathbb{1}Z\mathbb{1}, \ X\mathbb{1}\mathbb{1}X, X\mathbb{1}\mathbb{1}Y, X\mathbb{1}\mathbb{1}Z\}, \quad (\text{A.2})$$

$$M_3 = \{Z X\mathbb{1}\mathbb{1}, Z Y\mathbb{1}\mathbb{1}, Z Z\mathbb{1}\mathbb{1}, \ X\mathbb{1}X\mathbb{1}, X\mathbb{1}Y\mathbb{1}, X\mathbb{1}Z\mathbb{1}, \ Y\mathbb{1}\mathbb{1}X, Y\mathbb{1}\mathbb{1}Y, Y\mathbb{1}\mathbb{1}Z\}, \quad (\text{A.3})$$

such that in each set all operators pairwise anticommute. Together with the fact that for such an anticommuting set, the sum of squares of expectation values is bounded by one, this implies that $A_2^{(12)} + A_2^{(13)} + A_2^{(14)} \leq 3$.

We now want to adopt this method to prove the symmetrized bound of

$$A_2 = \sum_{i<j} A_2^{(ij)} \leq \binom{n}{2}. \tag{A.4}$$

The strategy is as follows: For n-partite states, we try to distribute the Pauli operators of weight two into sets like those in Eqs. (A.1) - (A.3) by grouping all $\binom{n}{2}$ pairs of parties into sets of three, having one party in common. If such a distribution can be found, then for each of the $\binom{n}{2}/3$ sets we obtain an upper bound of 3, yielding the desired bound.

We make the argument more apparent by considering the explicit example of $n = 6$. There, the 15 pairs of parties, $(1,2), (1,3), \ldots, (5,6)$ can be distributed into the

FIGURE A.1: Proving $A_2 \leq \binom{n}{2}$ for $n = 6$ by filling the grid according to the rules given in the text (from left to right, top to bottom): The entries for pairs $(1,2)$, $(1,3)$ and $(2,3)$, as well as $(4,5)$, $(4,6)$ and $(5,6)$ are fixed. Choosing then to fill $(3,4)$ with a horizontal bar fixes the remaining cells and yielding a solution to distribute the pairs into sets of three with one common pair.

following five sets:

$$\{(1,2),(1,3),(1,4)\}, \quad \{(2,3),(2,4),(2,6)\}, \quad \{(3,4),(3,5),(3,6)\},$$
$$\{(1,5),(2,5),(4,5)\}, \quad \{(1,6),(4,6),(5,6)\}. \tag{A.5}$$

The pairs in each set have one party in common, making it possible to distribute the corresponding Pauli operators into three anticommuting sets each and therefore proving the bound $A_2 \leq \binom{6}{2}$.

The question remains how such a distribution of pairs can be found. One strategy is to represent all pairs of parties as entries of an upper right triangular matrix. Each entry has now to be filled with either a horizontal ($|$) or a vertical ($—$) bar, according to the following rules:

- The number of horizontal bars in each row must be a multiple of three;

- The number of vertical bars in each column must be a multiple of three.
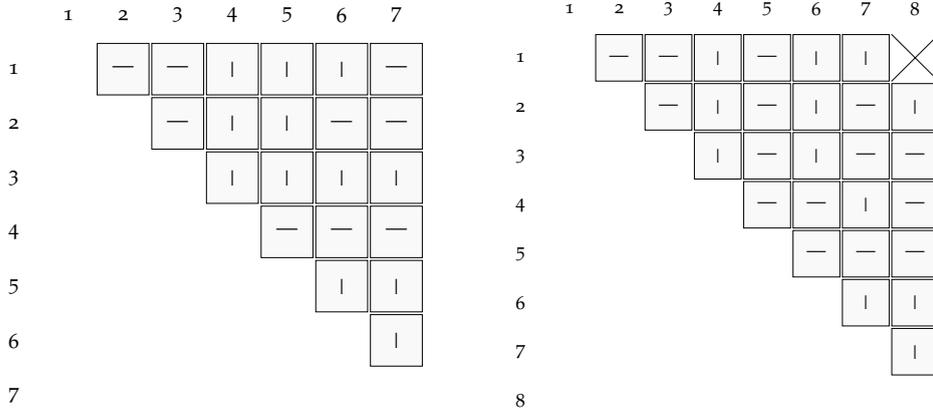
FIGURE A.2: Solutions to the game for $n = 7$ and $n = 8$. For $n = 8$, a trick has to be used, as the number of cells is not a multiple of three. Instead, a solution is found for the remaining 27 cells, after one of the boxes is struck out.

If such an assignment can be found, then the sets of pairs can be read off easily: Choose always three entries with horizontal bars in each row and put the corresponding pairs into one set, and do the same with sets of three vertical bars in each column.

As an example, consider again the case of $n = 6$. We display the upper triangular matrix in Fig. A.1. Indeed, many of the entries are fixed already. As there is not enough space to put at least three vertical bars into the first and second column, the entries corresponding to pairs $(1, 2)$, $(1, 3)$ and $(2, 3)$ must be filled with horizontal bars, and for similar reasons, $(4, 5)$, $(4, 6)$ and $(5, 6)$ have to be filled vertically. The entry for $(3, 4)$ can be filled arbitrarily for symmetry reasons, which fixes the rest of the entries to fulfill the constraints. If we choose to fill $(3, 4)$ with a horizontal bar, we obtain exactly the solution in Eq. (A.5).

The same strategy can be used to prove the bound for seven-qubit states, and a solution is displayed in Fig. A.2. For $n = 8$, however, the number of pairs, $\binom{8}{2} = 28$ is not a multiple of three, thus, there is no solution according to the rules. However, we can use the following trick: We strike out one of the cells corresponding to a fixed pair (i, j), and find a solution for the remaining 27 cells. This solution yields the upper bound

$$A_2 - A_2^{(ij)} \leq \binom{n}{2} - 1. \tag{A.6}$$

Having established this bound, we note that it holds for any choice of (i, j), as there are no distinguished particles. Thus, we can symmetrize Eq. (A.6) by summing over all $\binom{n}{2}$ choices for (i, j), yielding

$$\left[\binom{n}{2} - 1 \right] A_2 \leq \binom{n}{2} \left[\binom{n}{2} - 1 \right]. \tag{A.7}$$

Dividing both sides by $\left[\binom{n}{2} - 1\right]$, we obtain the bound $A_2 \leq \binom{n}{2}$ for $n = 8$, provided we find a solution for the 27 cell version. We show such a solution in Fig. A.2 as well.

Finally, we note that with this strategy solutions can be found inductively for all $n \geq 6$. However, as we have given an alternative proof already in the main text, we abstain from printing more of these solutions here.

B Sector length inequalities from projectors onto symmetric and antisymmetric subspaces

In this appendix, we introduce an alternative representation of sector length inequalities. As noted in Section 5.4.3, finding bounds on linear combinations of sector lengths is equivalent to solving a quadratic program to find $\min_\rho \text{Tr}[(\rho^{(A)} \otimes \rho^{(B)})\eta]$ with $\eta = \sum_k c_k \sum_{\Xi_k} \Xi_k^{(A)} \otimes \Xi_k^{(B)}$. Due to the special symmetric form, it is possible to express η in terms of local flip operators $F = \frac{1}{2}\sum_{j=0,x,y,z} \sigma_j \otimes \sigma_j$, which in turn can be written in their eigenbasis with the eigenvectors given by the projectors $\Pi_- = |\Psi^-\rangle\langle\Psi^-|$ and $\Pi_+ = |\Psi^+\rangle\langle\Psi^+| + |\Phi^-\rangle\langle\Phi^-| + |\Phi^+\rangle\langle\Phi^+|$ onto the antisymmetric and symmetric subspace, respectively. Here, $|\Psi^\pm\rangle$ and $|\Phi^\pm\rangle$ denote the usual Bell states. In this representation, the linear combination of sector lengths can be expressed as

$$\eta = \sum_{i_1\ldots i_n=\pm} \tilde{c}_{i_1\ldots i_n}\Pi_{i_1\ldots i_n} \tag{B.1}$$

with $\Pi_{i_1\ldots i_n} = \Pi_{i_1}^{(A_1,B_1)} \otimes \ldots \otimes \Pi_{i_n}^{(A_n,B_n)}$. The prefactors $\tilde{c}$ are connect to the prefactors c. This representation was used before to find entanglement witnesses and monotones [196–198]. In these references, the authors restrict themselves to $\tilde{c}_{i_1\ldots i_n} \geq 0$ to ensure positivity. As we have seen in Appendix B, this approach is too restrictive, as positivity under trace with symmetric product states is not equivalent to positivity of the matrix η. Nevertheless, it is interesting to note that the relevant inequalities in the case of three qubits have a particular form in this representation. The matrix η that yields the symmetric strong subadditivity is obtained by choosing $\tilde{c}_{---} = -3, \tilde{c}_{--+} = \tilde{c}_{-+-} = \tilde{c}_{+--} = 1$ and all other prefactors vanishing. The constraint $A_2 \leq 3$, however, can be expressed by choosing $\tilde{c}_{---} = -3, \tilde{c}_{-++} = \tilde{c}_{+-+} = \tilde{c}_{++-} = 1$. Usual state inversion is represented by $\tilde{c}_{---} = 1$. Therefore, it seems that the relevant inequalities correspond to some sort of extremal points in the set of coefficients $\tilde{c}$ that yield matrices that are positive under trace with positive product operators.

Bibliography

Introduction: Quote from The Big Bang Theory, Series 3, Episode 10.

[1] C. Pickover, *Archimedes to Hawking: laws of science and the great minds behind them* (Oxford University Press, 2008).

[2] A. Einstein, "Über einen die Erzeugung und Verwandlung des Lichtes betreffenden heuristischen Gesichtspunkt," Ann. Phys. (Berl.) **322**, 132 (1905).

[3] Planck Collaboration, P. A. Ade, N. Aghanim, M. Arnaud, M. Ashdown, J. Aumont, C. Baccigalupi, A. Banday, R. Barreiro, J. Bartlett, N. Bartolo, *et al.*, "Planck 2015 results - XIII. Cosmological parameters," Astron. Astrophys. **594**, A13 (2016).

[4] M. Planck, "Ueber das Gesetz der Energieverteilung im Normalspectrum," Ann. Phys. (Berl.) **309**, 553 (1901).

[5] D. A. Edwards, "The mathematical foundations of quantum mechanics," Synthese **42**, 1 (1979).

[6] W. Heisenberg, "Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik," Z. Phys. **43**, 172 (1927).

[7] I. Bengtsson and K. Życzkowski, *Geometry of quantum states: an introduction to quantum entanglement* (Cambridge University Press, 2017).

[8] H. Aschauer, J. Calsamiglia, M. Hein, and H. J. Briegel, "Local invariants for multi-partite entangled states allowing for a simple entanglement criterion," Quant. Inf. Comp. **4**, 383 (2004).

[9] K. Löwner, "Über monotone Matrixfunktionen," Mathematische Zeitschrift **38**, 177 (1934).

[10] K. Falconer, *Fractal geometry: mathematical foundations and applications* (John Wiley & Sons, 2004).

[11] S. Karuvade, P. D. Johnson, F. Ticozzi, and L. Viola, "Uniquely determined pure quantum states need not be unique ground states of quasi-local Hamiltonians," Phys. Rev. A **99**, 062104 (2019).

[12] J. Chen, H. Dawkins, Z. Ji, N. Johnston, D. Kribs, F. Shultz, and B. Zeng, "Uniqueness of quantum states compatible with given measurement results," Phys. Rev. A **88**, 012109 (2013).

[13] T. Xin, D. Lu, J. Klassen, N. Yu, Z. Ji, J. Chen, X. Ma, G. Long, B. Zeng, and R. Laflamme, "Quantum state tomography via reduced density matrices," Phys. Rev. Lett. **118**, 020401 (2017).

[14] A. Klyachko, "Quantum marginal problem and representations of the symmetric group," arXiv preprint quant-ph/0409113 (2004).

[15] A. Klyachko, "Quantum marginal problem and N-representability," J. Phys. Conf. Ser. **36**, 72 (2006).

[16] Y.-K. Liu, M. Christandl, and F. Verstraete, "Quantum computational complexity of the N-representability problem: QMA complete," Phys. Rev. Lett. **98**, 110503 (2007).

[17] A. D. Bookatz, "QMA-complete problems," Quant. Inf. Comp. **14**, 361 (2014).

[18] A. J. Coleman, "Structure of fermion density matrices," Rev. Mod. Phys. **35**, 668 (1963).

[19] D. A. Mazziotti, "Pure-n-representability conditions of two-fermion reduced density matrices," Phys. Rev. A **94**, 032516 (2016).

[20] A. Sawicki, M. Walter, and M. Kus, "When is a pure state of three qubits determined by its single-particle reduced density matrices?" J. Phys. A: Math. Theor. **46**, 055304 (2013).

[21] C. Schilling, C. L. Benavides-Riveros, and P. Vrana, "Reconstructing quantum states from single-party information," Phys. Rev. A **96**, 052312 (2017).

[22] N. Linden, S. Popescu, and W. Wootters, "Almost every pure state of three qubits is completely determined by its two-particle reduced density matrices," Phys. Rev. Lett. **89**, 207901 (2002).

[23] L. Diósi, "Three-party pure quantum states are determined by two two-party reduced states," Phys. Rev. A **70**, 010302 (2004).

[24] N. Linden and W. Wootters, "The parts determine the whole in a generic pure quantum state," Phys. Rev. Lett. **89**, 277906 (2002).

[25] N. S. Jones and N. Linden, "Parts of quantum states," Phys. Rev. A **71**, 012324 (2005).

[26] O. Gühne and G. Tóth, "Entanglement detection," Phys. Rep. **474**, 1 (2009).

[27] M. A. Nielsen and I. Chuang, *Quantum computation and quantum information* (Cambridge University Press, 2002).

[28] L. Gurvits, "Classical deterministic complexity of Edmonds' Problem and quantum entanglement," in *Proceedings of the thirty-fifth annual ACM symposium on Theory of computing* (ACM, 2003) p. 10.

[29] F. Mintert, A. R. Carvalho, M. Kuś, and A. Buchleitner, "Measures and dynamics of entangled states," Phys. Rep. **415**, 207 (2005).

[30] A. Uhlmann, "Concurrence and foliations induced by some 1-qubit channels," Int. J. Theor. Phys. **42**, 983 (2003).

[31] S. Hill and W. K. Wootters, "Entanglement of a pair of quantum bits," Phys. Rev. Lett. **78**, 5022 (1997).

[32] W. K. Wootters, "Entanglement of formation of an arbitrary state of two qubits," Phys. Rev. Lett. **80**, 2245 (1998).

[33] W. Hall, "Multipartite reduction criteria for separability," Phys. Rev. A **72**, 022311 (2005).

[34] V. Coffman, J. Kundu, and W. K. Wootters, "Distributed entanglement," Phys. Rev. A **61**, 052306 (2000).

[35] T. J. Osborne and F. Verstraete, "General monogamy inequality for bipartite qubit entanglement," Phys. Rev. Lett. **96**, 220503 (2006).

[36] T. Hiroshima, G. Adesso, and F. Illuminati, "Monogamy inequality for distributed Gaussian entanglement," Phys. Rev. Lett. **98**, 050503 (2007).

[37] J. San Kim, A. Das, and B. C. Sanders, "Entanglement monogamy of multipartite higher-dimensional quantum systems using convex-roof extended negativity," Phys. Rev. A **79**, 012329 (2009).

[38] Y.-K. Bai, Y.-F. Xu, and Z. Wang, "General monogamy relation for the entanglement of formation in multiqubit systems," Phys. Rev. Lett. **113**, 100503 (2014).

[39] C. Eltschka and J. Siewert, "Monogamy equalities for qubit entanglement from Lorentz invariance," Phys. Rev. Lett. **114**, 140402 (2015).

[40] W. Song, Y.-K. Bai, M. Yang, M. Yang, and Z.-L. Cao, "General monogamy relation of multiqubit systems in terms of squared Rényi-α entanglement," Phys. Rev. A **93**, 022306 (2016).

[41] Y. Luo, T. Tian, L.-H. Shao, and Y. Li, "General monogamy of Tsallis q-entropy entanglement in multiqubit systems," Phys. Rev. A **93**, 062340 (2016).

[42] A. Streltsov, G. Adesso, M. Piani, and D. Bruß, "Are general quantum correlations monogamous?" Phys. Rev. Lett. **109**, 050503 (2012).

[43] A. K. Ekert, "Quantum cryptography based on Bell's theorem," Phys. Rev. Lett. **67**, 661 (1991).

[44] M. Horodecki, P. Horodecki, and R. Horodecki, "Separability of mixed states: necessary and sufficient conditions," Phys. Lett. A **223**, 1 (1996).

[45] M. Horodecki, P. W. Shor, and M. B. Ruskai, "Entanglement breaking channels," Rev. Math. Phys. **15**, 629 (2003).

[46] M. M. Wolf, "Quantum channels & operations, guided tour," Lecture notes, Technische Universität München, `https://www-m5.ma.tum.de/foswiki/pub/M5/Allgemeines/MichaelWolf/QChannelLecture.pdf` (2012).

[47] K. Kraus, "General state changes in quantum theory," Annals of Physics **64**, 311 (1971).

[48] J. de Pillis, "Linear transformations which preserve hermitian and positive semidefinite operators," Pac. J. Math. **23**, 129 (1967).

[49] A. Jamiołkowski, "Linear transformations which preserve trace and positive semidefiniteness of operators," Rep. Math. Phys. **3**, 275 (1972).

[50] M.-D. Choi, "Completely positive linear maps on complex matrices," Linear Algebra Its Appl. **10**, 285 (1975).

[51] F. Huber, "Quantum states and their marginals: from multipartite entanglement to quantum error-correcting codes," PhD thesis, Universität Siegen (2017).

[52] F. Huber and N. Wyderka, "Table of AME states," `http://www.tp.nt.uni-siegen.de/+fhuber/ame.html` (2019).

[53] A. Streltsov, G. Adesso, and M. B. Plenio, "Colloquium: Quantum coherence as a resource," Rev. Mod. Phys. **89**, 041003 (2017).

[54] T. Baumgratz, M. Cramer, and M. B. Plenio, "Quantifying coherence," Phys. Rev. Lett. **113**, 140401 (2014).

[55] Y. Peng, Y. Jiang, and H. Fan, "Maximally coherent states and coherence-preserving operations," Phys. Rev. A **93**, 032326 (2016).

[56] C. Napoli, T. R. Bromley, M. Cianciaruso, M. Piani, N. Johnston, and G. Adesso, "Robustness of coherence: an operational and observable measure of quantum coherence," Phys. Rev. Lett. **116**, 150502 (2016).

[57] F. Alizadeh, "Combinatorial optimization with interior point methods and semi-definite matrices," PhD thesis, University of Minnesota (1991).

[58] A. Nemirovskii and Y. Nesterov, *Interior point polynomial algorithms in convex programming* (Society for Industrial and Applied Mathematics, 1994).

[59] S. Boyd and L. Vandenberghe, *Convex optimization* (Cambridge university press, 2004).

[60] R. M. Freund, "Introduction to semidefinite programming," Lecture notes, Massachusetts Institute of Technology, `https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-251j-introduction-to-mathematical-programming-fall-2009/readings/MIT6_251JF09_SDP.pdf` (2009).

[61] L. Vandenberghe and S. Boyd, "Semidefinite programming," SIAM Rev. **38**, 49 (1996).

[62] M. Slater, "Lagrange multipliers revisited," in *Traces and Emergence of Nonlinear Programming* (Springer, 2014) p. 293.

[63] R. F. Werner, "An application of Bell's inequalities to a quantum state extension problem," Lett. Math. Phys. **17**, 359 (1989).

[64] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, "Distinguishing separable and entangled states," Phys. Rev. Lett. **88**, 187904 (2002).

[65] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, "Complete family of separability criteria," Phys. Rev. A **69**, 022308 (2004).

[66] M. Born and V. Fock, "Beweis des Adiabatensatzes," Z. Phys. **51**, 165 (1928).

[67] T. Kato, "On the adiabatic theorem of quantum mechanics," J. Phys. Soc. Jpn. **5**, 435 (1950).

[68] D. L. Zhou, "Irreducible multiparty correlations can be created by local operations," Phys. Rev. A **80**, 022113 (2009).

[69] F. Huber and O. Gühne, "Characterizing ground and thermal states of few-body Hamiltonians," Phys. Rev. Lett. **117**, 010403 (2016).

[70] G. Tóth, C. Knapp, O. Gühne, and H. J. Briegel, "Spin squeezing and entanglement," Phys. Rev. A **79**, 042334 (2009).

[71] L. E. Würflinger, J.-D. Bancal, A. Acín, N. Gisin, and T. Vértesi, "Nonlocal multipartite correlations from local marginal probabilities," Phys. Rev. A **86**, 032117 (2012).

[72] M. Walter, B. Doran, D. Gross, and M. Christandl, "Entanglement polytopes: Multiparticle entanglement from single-particle information," Science **340**, 1205 (2013).

[73] N. Miklin, T. Moroder, and O. Gühne, "Multiparticle entanglement as an emergent phenomenon," Phys. Rev. A **93**, 020104 (2016).

[74] S. Straszewicz, "Über exponierte Punkte abgeschlossener Punktmengen," Fundam. Math. **24**, 139 (1935).

[75] A. J. Scott and C. M. Caves, "Entangling power of the quantum Baker's map," J. Phys. A: Math. Gen. **36**, 9553 (2003).

[76] S. Lloyd and H. Pagels, "Complexity as thermodynamic depth," Ann. Phys. (N.Y.) **188**, 186 (1988).

[77] H. Carteret, A. Higuchi, and A. Sudbery, "Multipartite generalization of the Schmidt decomposition," J. Math. Phys. **41**, 7932 (2000).

[78] V. Bužek, M. Hillery, and R. Werner, "Optimal manipulations with qubits: Universal-not gate," Phys. Rev. A **60**, R2626 (1999).

[79] A. Wong and N. Christensen, "Potential multiparticle entanglement measure," Phys. Rev. A **63**, 044301 (2001).

[80] S. S. Bullock, G. K. Brennen, and D. P. O'Leary, "Time reversal and n-qubit canonical decompositions," J. Math. Phys. **46**, 062104 (2005).

[81] A. Osterloh and J. Siewert, "Constructing N-qubit entanglement monotones from antilinear operators," Phys. Rev. A **72**, 012337 (2005).

[82] P. Butterley, A. Sudbery, and J. Szulc, "Compatibility of subsystem states," Found. Phys. **36**, 83 (2006).

[83] S. Designolle, O. Giraud, and J. Martin, "Genuinely entangled symmetric states with no N-partite correlations," Phys. Rev. A **96**, 032322 (2017).

[84] F. Huber and S. Severini, "Some Ulam's reconstruction problems for quantum states," J. Phys. A: Math. Theor. **51**, 435301 (2018).

[85] H. A. Kramers, "Théorie générale de la rotation paramagnétique dans les cristaux," Proc. Acad. Amst **33**, 959 (1930).

[86] E. Ising, "Beitrag zur Theorie des Ferromagnetismus," Z. Phys. **31**, 253 (1925).

[87] J. Spałek and A. Oleś, "Ferromagnetism in narrow s-band with inclusion of intersite correlations," Physica B+C **86**, 375 (1977).

[88] K. Chao, J. Spałek, and A. Oleś, "Kinetic exchange interaction in a narrow S-band," J. Phys. C: Solid State Phys. **10**, L271 (1977).

[89] K. Chao, J. Spałek, and A. Oleś, "Canonical perturbation expansion of the Hubbard model," Phys. Rev. B **18**, 3453 (1978).

[90] F. Huber, O. Gühne, and J. Siewert, "Absolutely maximally entangled states of seven qubits do not exist," Phys. Rev. Lett. **118**, 200502 (2017).

[91] A. Uhlmann, "Fidelity and concurrence of conjugated states," Phys. Rev. A **62**, 032307 (2000).

[92] M. Cheneau, P. Barmettler, D. Poletti, M. Endres, P. Schauß, T. Fukuhara, C. Gross, I. Bloch, C. Kollath, and S. Kuhr, "Light-cone-like spreading of correlations in a quantum many-body system," Nature **481**, 484 (2012).

[93] P. Jurcevic, B. P. Lanyon, P. Hauke, C. Hempel, P. Zoller, R. Blatt, and C. F. Roos, "Quasiparticle engineering and entanglement propagation in a quantum many-body system," Nature **511**, 202 (2014).

[94] J. K. Pachos and E. Rico, "Effective three-body interactions in triangular optical lattices," Phys. Rev. A **70**, 053620 (2004).

[95] H. Büchler, A. Micheli, and P. Zoller, "Three-body interactions with cold polar molecules," Nat. Phys. **3**, 726 (2007).

[96] C. Schmid, N. Kiesel, W. Wieczorek, H. Weinfurter, F. Mintert, and A. Buchleitner, "Experimental direct observation of mixed state entanglement," Phys. Rev. Lett. **101**, 260505 (2008).

[97] S. van Enk, "Direct measurements of entanglement and permutation symmetry," Phys. Rev. Lett. **102**, 190503 (2009).

[98] C. Zhang, S. Yu, Q. Chen, H. Yuan, and C. Oh, "Evaluation of entanglement measures by a single observable," Phys. Rev. A **94**, 042325 (2016).

[99] D. Goyeneche, G. Cañas, S. Etcheverry, E. Gómez, G. Xavier, G. Lima, and A. Delgado, "Five measurement bases determine pure quantum states on any dimension," Phys. Rev. Lett. **115**, 090401 (2015).

[100] P. Horodecki, "Separability criterion and inseparable mixed states with positive partial transposition," Phys. Lett. A **232**, 333 (1997).

[101] C. Eltschka and J. Siewert, "Distribution of entanglement and correlations in all finite dimensions," Quantum **2**, 64 (2018).

[102] P. Rungta, V. Bužek, C. M. Caves, M. Hillery, and G. J. Milburn, "Universal state inversion and concurrence in arbitrary dimensions," Phys. Rev. A **64**, 042315 (2001).

[103] R. M. Gingrich, "Properties of entanglement monotones for three-qubit pure states," Phys. Rev. A **65**, 052302 (2002).

[104] T. Brydges, A. Elben, P. Jurcevic, B. Vermersch, C. Maier, B. P. Lanyon, P. Zoller, R. Blatt, and C. F. Roos, "Probing Rényi entanglement entropy via randomized measurements," Science **364**, 260 (2019).

[105] C. Klöckl and M. Huber, "Characterizing multipartite entanglement without shared reference frames," Phys. Rev. A **91**, 042339 (2015).

[106] D. Gottesman, "Stabilizer codes and quantum error correction," PhD thesis, California Institute of Technology (1997).

[107] D. Petz and D. Virosztek, "Some inequalities for quantum Tsallis entropy related to the strong subadditivity," Math. Inequal. Appl. **18**, 555 (2015).

[108] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes* (Elsevier, 1977).

[109] M. Markiewicz, W. Laskowski, T. Paterek, and M. Żukowski, "Detecting genuine multipartite entanglement of pure states with bipartite correlations," Phys. Rev. A **87**, 034301 (2013).

[110] P. Kurzyński, T. Paterek, R. Ramanathan, W. Laskowski, and D. Kaszlikowski, "Correlation complementarity yields Bell monogamy relations," Phys. Rev. Lett. **106**, 180402 (2011).

[111] G. Tóth, C. Knapp, O. Gühne, and H. J. Briegel, "Spin squeezing and entanglement," Phys. Rev. A **79**, 042334 (2009).

[112] S. Wehner and A. Winter, "Higher entropic uncertainty relations for anti-commuting observables," J. Math. Phys. **49**, 062105 (2008).

[113] A. Higuchi, A. Sudbery, and J. Szulc, "One-qubit reduced states of a pure many-qubit state: polygon inequalities," Phys. Rev. Lett. **90**, 107902 (2003).

[114] B. Kraus, "Entanglement properties of quantum states and quantum operations," PhD thesis, University of Innsbruck (2003).

[115] A. Osterloh and J. Siewert, "Entanglement monotones and maximally entangled states in multipartite qubit systems," Int. J. Quantum Inf. **04**, 531 (2006).

[116] E. M. Rains, "Polynomial invariants of quantum codes," IEEE Trans. Inf. Theory **46**, 54–59 (2000).

[117] C. Eltschka, F. Huber, O. Gühne, and J. Siewert, "Exponentially many entanglement and correlation constraints for multipartite quantum states," Phys. Rev. A **98**, 052317 (2018).

[118] A. R. Calderbank, E. M. Rains, P. Shor, and N. J. Sloane, "Quantum error correction via codes over gf (4)," IEEE Trans. Inf. Theory **44**, 1369 (1998).

[119] E. M. Rains, "Quantum shadow enumerators," IEEE Trans. Inf. Theory **45**, 2361 (1999).

[120] M. C. Tran, B. Dakić, W. Laskowski, and T. Paterek, "Correlations between outcomes of random measurements," Phys. Rev. A **94**, 042302 (2016).

[121] C. Eltschka and J. Siewert, "Maximum N-body correlations do not in general imply genuine multipartite entanglement," arXiv preprint 1908.04220 (2019).

[122] D. Kaszlikowski, A. Sen, U. Sen, V. Vedral, A. Winter, *et al.*, "Quantum correlation without classical correlations," Phys. Rev. Lett. **101**, 070502 (2008).

[123] W. Laskowski, M. Markiewicz, T. Paterek, and M. Wieśniak, "Incompatible local hidden-variable models of quantum correlations," Phys. Rev. A **86**, 032105 (2012).

[124] M. C. Tran, M. Zuppardo, A. de Rosier, L. Knips, W. Laskowski, T. Paterek, and H. Weinfurter, "Genuine N-partite entanglement without N-partite correlation functions," Phys. Rev. A **95**, 062331 (2017).

[125] W. Kłobus, W. Laskowski, T. Paterek, M. Wieśniak, and H. Weinfurter, "Higher dimensional entanglement without correlations," Eur. Phys. J. D **73**, 29 (2019).

[126] G. Gour, S. Bandyopadhyay, and B. C. Sanders, "Dual monogamy inequality for entanglement," J. Math. Phys. **48**, 012108 (2007).

[127] A. Peres, "Separability criterion for density matrices," Phys. Rev. Lett. **77**, 1413 (1996).

[128] H.-P. Breuer, "Optimal entanglement criterion for mixed quantum states," Phys. Rev. Lett. **97**, 080501 (2006).

[129] W. Hall, "A new criterion for indecomposability of positive maps," J. Phys. A: Math. Gen. **39**, 14119 (2006).

[130] J. S. Bell, "On the Einstein Podolsky Rosen paradox," Physics Physique Fizika **1**, 195 (1964).

[131] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, "Bell nonlocality," Rev. Mod. Phys. **86**, 419 (2014).

[132] L. Aolita and S. Walborn, "Quantum communication without alignment using multiple-qubit single-photon states," Phys. Rev. Lett. **98**, 100501 (2007).

[133] V. D'ambrosio, E. Nagali, S. P. Walborn, L. Aolita, S. Slussarenko, L. Marrucci, and F. Sciarrino, "Complete experimental toolbox for alignment-free quantum communication," Nat. Commun. **3**, 961 (2012).

[134] J. I. de Vicente, "Separability criteria based on the Bloch representation of density matrices," Quant. Inf. Comp. **7**, 624 (2007).

[135] J. I. de Vicente, "Further results on entanglement detection and quantification from the correlation matrix criterion," J. Phys. A: Math. Theor. **41**, 065309 (2008).

[136] J. I. de Vicente and M. Huber, "Multipartite entanglement detection from correlation tensors," Phys. Rev. A **84**, 062306 (2011).

[137] P. Badziag, Č. Brukner, W. Laskowski, T. Paterek, and M. Żukowski, "Experimentally friendly geometrical criteria for entanglement," Phys. Rev. Lett. **100**, 140403 (2008).

[138] T. Lawson, A. Pappa, B. Bourdoncle, I. Kerenidis, D. Markham, and E. Diamanti, "Reliable experimental quantification of bipartite entanglement without reference frames," Phys. Rev. A **90**, 042336 (2014).

[139] S. D. Bartlett, T. Rudolph, and R. W. Spekkens, "Reference frames, superselection rules, and quantum information," Rev. Mod. Phys. **79**, 555 (2007).

[140] R. F. Werner, "Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model," Phys. Rev. A **40**, 4277 (1989).

[141] P. D. Seymour and T. Zaslavsky, "Averaging sets: a generalization of mean values and spherical designs," Adv. Math. **52**, 213 (1984).

[142] R. H. Hardin and N. J. Sloane, "McLaren's improved snub cube and other new spherical designs in three dimensions," Discrete Comput. Geom. **15**, 429 (1996).

[143] R. Horodecki and M. Horodecki, "Information-theoretic aspects of inseparability of mixed states," Phys. Rev. A **54**, 1838 (1996).

[144] C. G. Broyden, "The convergence of a class of double-rank minimization algorithms: 2. The new algorithm," IMA J. Appl. Math. **6**, 222 (1970).

[145] R. Fletcher, "A new approach to variable metric algorithms," Comput. J. **13**, 317 (1970).

[146] D. Goldfarb, "A family of variable-metric methods derived by variational means," Math. Comput. **24**, 23 (1970).

[147] D. F. Shanno, "Conditioning of quasi-Newton methods for function minimization," Math. Comput. **24**, 647 (1970).

[148] A. Ketterer, N. Wyderka, and O. Gühne, "Characterizing multipartite entanglement with moments of random correlations," Phys. Rev. Lett. **122**, 120505 (2019).

[149] G. Tóth, C. Knapp, O. Gühne, and H. J. Briegel, "Optimal spin squeezing inequalities detect bound entanglement in spin models," Phys. Rev. Lett. **99**, 250405 (2007).

[150] D. J. Wineland, J. J. Bollinger, W. M. Itano, and D. J. Heinzen, "Squeezed atomic states and projection noise in spectroscopy," Phys. Rev. A **50**, 67 (1994).

[151] A. Sørensen and K. Mølmer, "Spin-spin interaction and spin squeezing in an optical lattice," Phys. Rev. Lett. **83**, 2274 (1999).

[152] A. Sørensen, L.-M. Duan, J. I. Cirac, and P. Zoller, "Many-particle entanglement with Bose–Einstein condensates," Nature **409**, 63 (2001).

[153] R. Raussendorf and H. J. Briegel, "A one-way quantum computer," Phys. Rev. Lett. **86**, 5188 (2001).

[154] R. Raussendorf, D. E. Browne, and H. J. Briegel, "Measurement-based quantum computation on cluster states," Phys. Rev. A **68**, 022312 (2003).

[155] M. Van den Nest, W. Dür, A. Miyake, and H. Briegel, "Fundamentals of universality in one-way quantum computation," New J. Phys. **9**, 204 (2007).

[156] M. Stingl, "Quantentheorie," Lecture notes, Universität Münster, `http://www. uni-muenster.de/Physik.TP/archive/Lehre/Skripten/Stingl/qmskript.ps` (1997).

[157] M. Gachechiladze, N. Wyderka, and O. Gühne, "The structure of ultrafine entanglement witnesses," J. Phys. A: Math. Theor. **51**, 365307 (2018).

[158] T. Heinosaari and M. Ziman, *The mathematical language of quantum theory: from uncertainty to entanglement* (Cambridge University Press, 2011).

[159] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. Brandao, D. A. Buell, *et al.*, "Quantum supremacy using a programmable superconducting processor," Nature **574**, 505 (2019).

[160] K. Hornberger, "Introduction to decoherence theory," in *Entanglement and decoherence* (Springer, 2009) p. 221.

[161] D. P. DiVincenzo, "The physical implementation of quantum computation," Fortschritte der Phys. **48**, 771 (2000).

[162] C. Simon, M. Afzelius, J. Appel, A. B. de La Giroday, S. Dewhurst, N. Gisin, C. Hu, F. Jelezko, S. Kröll, J. Müller, *et al.*, "Quantum memories," Eur. Phys. J. D **58**, 1 (2010).

[163] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, "Quantum repeaters: the role of imperfect local operations in quantum communication," Phys. Rev. Lett. **81**, 5932 (1998).

[164] L.-M. Duan, M. Lukin, J. I. Cirac, and P. Zoller, "Long-distance quantum communication with atomic ensembles and linear optics," Nature **414**, 413 (2001).

[165] E. Knill, R. Laflamme, and G. J. Milburn, "A scheme for efficient quantum computation with linear optics," Nature **409**, 46 (2001).

[166] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. J. Milburn, "Linear optical quantum computing with photonic qubits," Rev. Mod. Phys. **79**, 135 (2007).

[167] N. Sangouard, C. Simon, J. Minář, H. Zbinden, H. De Riedmatten, and N. Gisin, "Long-distance entanglement distribution with single-photon sources," Phys. Rev. A **76**, 050301 (2007).

[168] N. Sangouard, C. Simon, H. De Riedmatten, and N. Gisin, "Quantum repeaters based on atomic ensembles and linear optics," Rev. Mod. Phys. **83**, 33 (2011).

[169] B. Julsgaard, J. Sherson, J. I. Cirac, J. Fiurášek, and E. S. Polzik, "Experimental demonstration of quantum memory for light," Nature **432**, 482 (2004).

[170] K. S. Choi, H. Deng, J. Laurat, and H. J. Kimble, "Mapping photonic entanglement into and out of a quantum memory," Nature **452**, 67 (2008).

[171] R. Zhao, Y. Dudin, S. Jenkins, C. Campbell, D. Matsukevich, T. Kennedy, and A. Kuzmich, "Long-lived quantum memory," Nat. Phys. **5**, 100 (2009).

[172] M. P. Hedges, J. J. Longdell, Y. Li, and M. J. Sellars, "Efficient quantum memory for light," Nature **465**, 1052 (2010).

[173] K. Jensen, W. Wasilewski, H. Krauter, T. Fernholz, B. M. Nielsen, M. Owari, M. B. Plenio, A. Serafini, M. Wolf, and E. Polzik, "Quantum memory for entangled continuous-variable states," Nat. Phys. **7**, 13 (2011).

[174] Y. Pu, N. Jiang, W. Chang, H. Yang, C. Li, and L. Duan, "Experimental realization of a multiplexed quantum memory with 225 individually accessible memory cells," Nat. Commun. **8**, 15359 (2017).

[175] W. Zhang, D.-S. Ding, Y.-B. Sheng, L. Zhou, B.-S. Shi, and G.-C. Guo, "Quantum secure direct communication with quantum memory," Phys. Rev. Lett. **118**, 220501 (2017).

[176] S. L. Braunstein and A. Mann, "Measurement of the Bell operator and quantum teleportation," Phys. Rev. A **51**, R1727 (1995).

[177] H. Häseler and N. Lütkenhaus, "Probing the quantumness of channels with mixed states," Phys. Rev. A **80**, 042304 (2009).

[178] H. Häseler, T. Moroder, and N. Lütkenhaus, "Testing quantum devices: Practical entanglement verification in bipartite optical systems," Phys. Rev. A **77**, 032303 (2008).

[179] M. F. Pusey, "Verifying the quantumness of a channel with an untrusted device," JOSA B **32**, A56 (2015).

[180] D. Rosset, F. Buscemi, and Y.-C. Liang, "Resource theory of quantum memories and their faithful verification with minimal assumptions," Phys. Rev. X **8**, 021033 (2018).

[181] I. L. Chuang and M. A. Nielsen, "Prescription for experimental determination of the dynamics of a quantum black box," J. Mod. Opt. **44**, 2455 (1997).

[182] M. Mohseni, A. Rezakhani, and D. Lidar, "Quantum-process tomography: Resource analysis of different strategies," Phys. Rev. A **77**, 032322 (2008).

[183] M. Piani, M. Cianciaruso, T. R. Bromley, C. Napoli, N. Johnston, and G. Adesso, "Robustness of asymmetry and coherence of quantum states," Phys. Rev. A **93**, 042107 (2016).

[184] F. Shahbeigi and S. J. Akhtarshenas, "Quantumness of quantum channels," Phys. Rev. A **98**, 042313 (2018).

[185] C. Berge, *Topological Spaces: including a treatment of multi-valued functions, vector spaces, and convexity* (Courier Corporation, 1997).

[186] T. Simnacher, N. Wyderka, C. Spee, X.-D. Yu, and O. Gühne, "Certifying quantum memories with coherence," Phys. Rev. A **99**, 062319 (2019).

[187] A. Y. Kitaev, "Quantum computations: Algorithms and error correction," Uspekhi Mat. Nauk **52**, 53 (1997).

[188] J. Watrous, *The theory of quantum information* (Cambridge University Press, 2018).

[189] M. Idel and M. M. Wolf, "Sinkhorn normal form for unitary matrices," Linear Algebra Its Appl. **471**, 76 (2015).

[190] M. R. Spiegel, *Schaum's outline of theory and problems of vector analysis and an introduction to tensor analysis* (McGraw-Hill, 1959).

[191] C. Carmeli, T. Heinosaari, M. Kech, J. Schultz, and A. Toigo, "Stable pure state quantum tomography from five orthonormal bases," EPL **115**, 30001 (2016).

[192] C. H. Baldwin, A. Kalev, and I. H. Deutsch, "Quantum process tomography of unitary and near-unitary maps," Phys. Rev. A **90**, 012110 (2014).

[193] S. Gharibian, "Strong NP-hardness of the quantum separability problem," Quant. Inf. Comp. **10**, 343 (2010).

[194] M. Ringbauer, T. R. Bromley, M. Cianciaruso, L. Lami, W. S. Lau, G. Adesso, A. G. White, A. Fedrizzi, and M. Piani, "Certification and quantification of multilevel quantum coherence," Phys. Rev. X **8**, 041007 (2018).

[195] T. Kraft and M. Piani, "Genuine correlated coherence," J. Phys. A: Math. Theor. **51**, 414013 (2018).

[196] F. Mintert, M. Kuś, and A. Buchleitner, "Concurrence of mixed multipartite quantum states," Phys. Rev. Lett. **95**, 260502 (2005).

[197] F. Mintert and A. Buchleitner, "Observable entanglement measure for mixed quantum states," Phys. Rev. Lett. **98**, 140505 (2007).

[198] R. Demkowicz-Dobrzański, A. Buchleitner, M. Kuś, and F. Mintert, "Evaluable multipartite entanglement measures: Multipartite concurrences as entanglement monotones," Phys. Rev. A **74**, 052303 (2006).